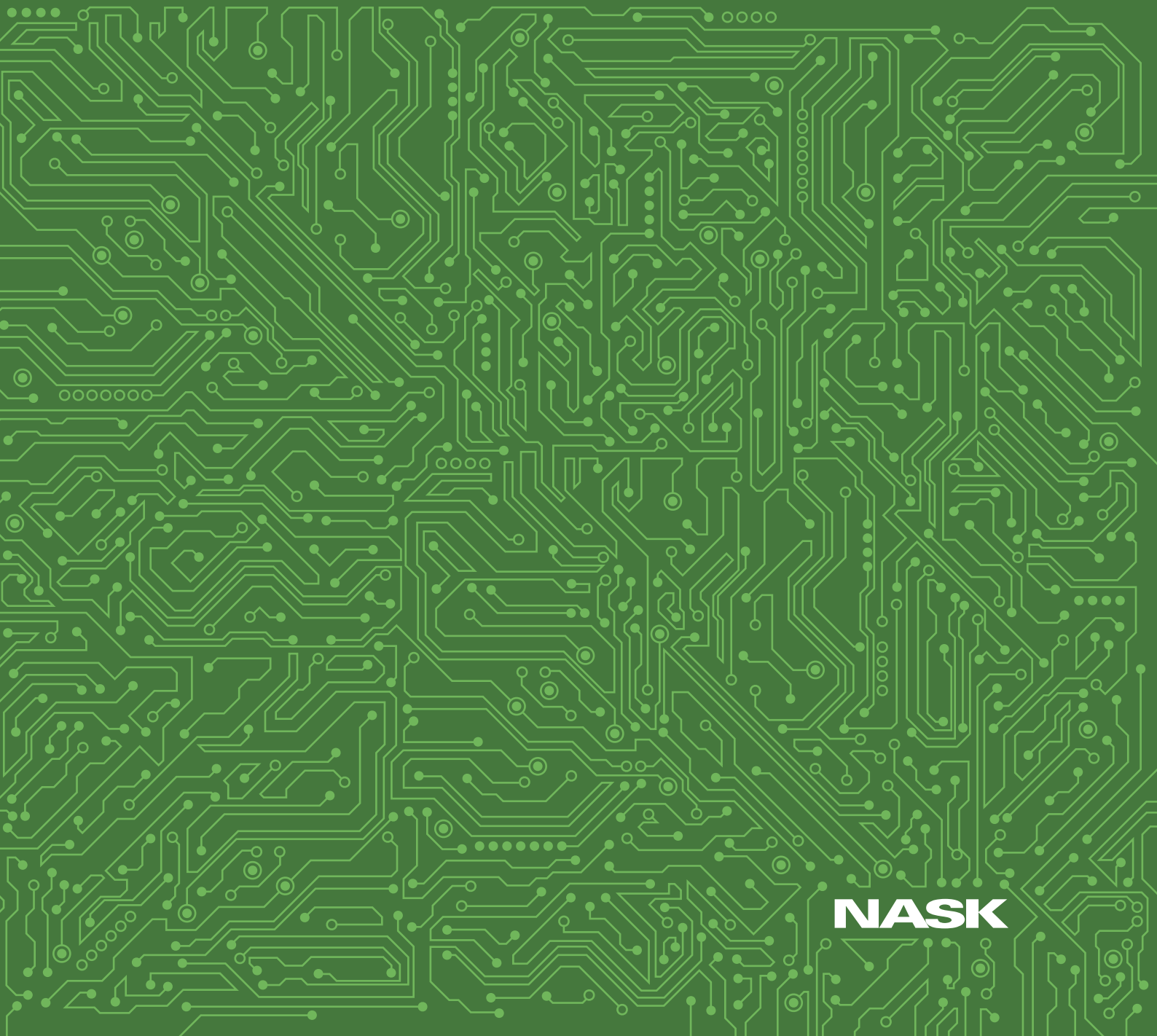
CERT POLSKA

RAPORT 2014

CERT.PL >_



NASK

CERT Polska Raport 2014

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:
Anna Nykiel

ISSN 2084-9079

CERT POLSKA

RAPORT 2014

CERT.PL

NASK

Spis treści

Wstęp

Zespół CERT Polska, funkcjonujący w Naukowej i Akademickiej Sieci Komputerowej, już od 19 lat monitoruje zagrożenia pojawiające się w polskich sieciach oraz aktywnie reaguje, by jak najefektywniej im przeciwdziałać.

W przedstawianym Państwu raporcie omawiamy najważniejsze trendy i zagadnienia związane z problematyką cyberbezpieczeństwa w Polsce w 2014 roku. Prezentujemy aktualne zagrożenia, kierunki ich rozwoju, informujemy o podejmowanych przez CERT Polska działaniach.

Raport składa się z kilku części. W pierwszej przedstawiamy swoiste podsumowanie całości – najważniejsze wnioski powstałe na podstawie obserwacji stanu bezpieczeństwa polskich sieci w 2014 r. Prezentujemy również najgroźniejsze metody, z jakich korzystali cyberprzestępcy. Analizujemy konkretne przypadki: ataki APT wymierzone w polskie podmioty, czy też złośliwe oprogramowanie, z którym zetknąć się mogli polscy użytkownicy bankowości internetowej. Spośród dziesięciu najczęściej spotykanych w Polsce zagrożeń opartych o złośliwe oprogramowanie aż cztery to trojany bankowe: ZeuS, ZeuS GameOver, Bankpatch, Banatrix. Autorstwo ostatniego z nich przypisuje się Polakom, dlatego zdecydowaliśmy się w raporcie przyjrzeć bliżej temu zjawisku.

W dalszej części przedstawiamy działania zespołu CERT Polska, podejmowane w 2014 r., prowadzone przez nas projekty, opracowane raporty, czy organizowane konferencje i szkolenia. W ubiegłym roku po raz kolejny zorganizowaliśmy w Polsce Europejski Miesiąc Bezpieczeństwa Cybernetycznego – akcję, której celem jest zarówno popularyzacja wiedzy o zagrożeniach, jak i promowanie bezpiecznego korzystania z nowych technologii wśród szerokiej grupy użytkowników sieci.

Ostatnim, bardzo ważnym elementem raportu są statystyki. Prowadzone przez CERT Polska analizy przypadków naruszeń bezpieczeństwa opierają się przede wszystkim o dane otrzymane ze stworzonej i prowadzonej przez Zespół platformy n6. Ich źródłem jest ponad 50 kanałów dystrybucyjnych dostarczających informacje o incydentach. Zdarzenia te wykrywane są w wyniku działań systemów ponad 30 różnych podmiotów z całego świata. Zebrane w ten sposób dane wraz z informacjami z naszych własnych źródeł umożliwiły zespołowi unikalną analizę stanu polskich sieci w 2014 r.

Zapraszamy Państwa do lektury naszego raportu. Zachęcamy do współpracy i uczestnictwa w podejmowanych przez nas projektach i inicjatywach. Bezpieczeństwo w sieci zależy od nas wszystkich – żaden podmiot działając samodzielnie nie sprawi, że sieć w Polsce będzie wolna od zagrożeń.

Ważne obserwacje

- Z danych, które posiadamy możemy wywnioskować, że średnio w ciągu każdych 24h w Polsce jest zainfekowanych 280 tysięcy komputerów.
- Zaobserwowaliśmy wzrost nadużyć domen typu DNT krótko żyjących adresów kupowanych „na próbę".
- Polskie podmioty były atakowane w ramach kampanii APT, takich jak Pawn Storm, Black Energy, Energetic Bear, ale Polska nie była głównym celem ataków.
- Wzrost działalności ukierunkowanej na użytkowników bankowości internetowej to najważniejszy i najbardziej niepokojący trend w 2014 roku. Wysokość wykradzionch kwot niejednokrotnie wynosiła kilkaset tysięcy złotych.
- W 2014 roku najbardziej popularnymi trojanami bankowymi w Polsce były ISFB, Tinba, Kronos, VMZeuS.
- Największymi botnetami w polskich sieciach są Conficker, ZeroAccess oraz ZeuS (i pochodne), ale tylko ZeroAccess oraz ZeuS zwiększyły procentowy udział wśród zainfekowanych komputerów. Znacznemu zmniejszeniu uległ botnet Virut.
- Wzrosła liczba ataków na klientów korporacyjnych i administrację samorządową.
- Zaobserwowaliśmy 7 scenariuszy ataków socjotechnicznych wykorzystywanych w kampaniach złośliwego oprogramowania.
- Widzimy coraz więcej ataków pochodzących z Polski, czasami nawet wykorzystujących autorskie złośliwe oprogramowanie: VBKlip czy Banatrix.
- Najpopularniejszą metodą infekowania polskich użytkowników Internetu są zainfekowane załączniki.
- Luki w protokołach lub aplikacjach stały się obiektem zainteresowań międzynarodowych mediów, co obserwować można było na przykładach podatności Heartbleed, Shellshock czy Poodle. Niestety wciąż jest widoczny brak komunikacji i zrozumienia między ekspertami, dziennikarzami i czytelnikami.
- Mimo dosyć poważnych i groźnych w potencjalnych skutkach luk Heartbleed czy Shellshock nie zaobserwowaliśmy ataków poważnie wpływających na działanie największych i najważniejszych usług w Internecie, ale ataki z wykorzystaniem tych luk wciąż trwają i prawdopodobnie długo jeszcze będziemy je obserwować.

- Tradycyjny phishing dotyczy coraz bardziej zróżnicowanych serwisów oprócz banków i usług finansowych, popularnymi celami stają się też np. serwisy gier online oraz administracja skarbowa.

- Choć ataki DDoS są utrapieniem większych dostawców treści, jak i branży ecommerce lub witryn i serwisów administracji publicznej, to jednak przeciętny internauta nie ponosi zazwyczaj wyjątkowych strat z tego tytułu. W 2014 warte uwagi były ataki wymierzone w witrynę Prezydenta RP i w witryny Giełdy Papierów Wartościowych, które miały znaczenie propagandowe i nie wyrządziły znaczących szkód użytkownikom Internetu.

- W 2014 roku miały miejsce wycieki danych, z których największy związany był z atakiem na Giełdę Papierów Wartościowych. Pozostałe były mniej znaczące.

- Złośliwe oprogramowanie na Androida jest obecne w Polsce, ale nie jest znaczącym problemem.

- Liczba otwartych serwerów DNS zmalała w porównaniu do 2013 r.roku. W dużej mierze do poprawy sytuacji przyczynił się Orange Polska.

- Najwięcej złośliwych adresów URL w domenie .pl było hostowanych w systemie autonomicznym należącym do Interia.pl sp. z o.o.

- Wśród błędnie skonfigurowanej infrastruktury dominuje protokół SSDP.

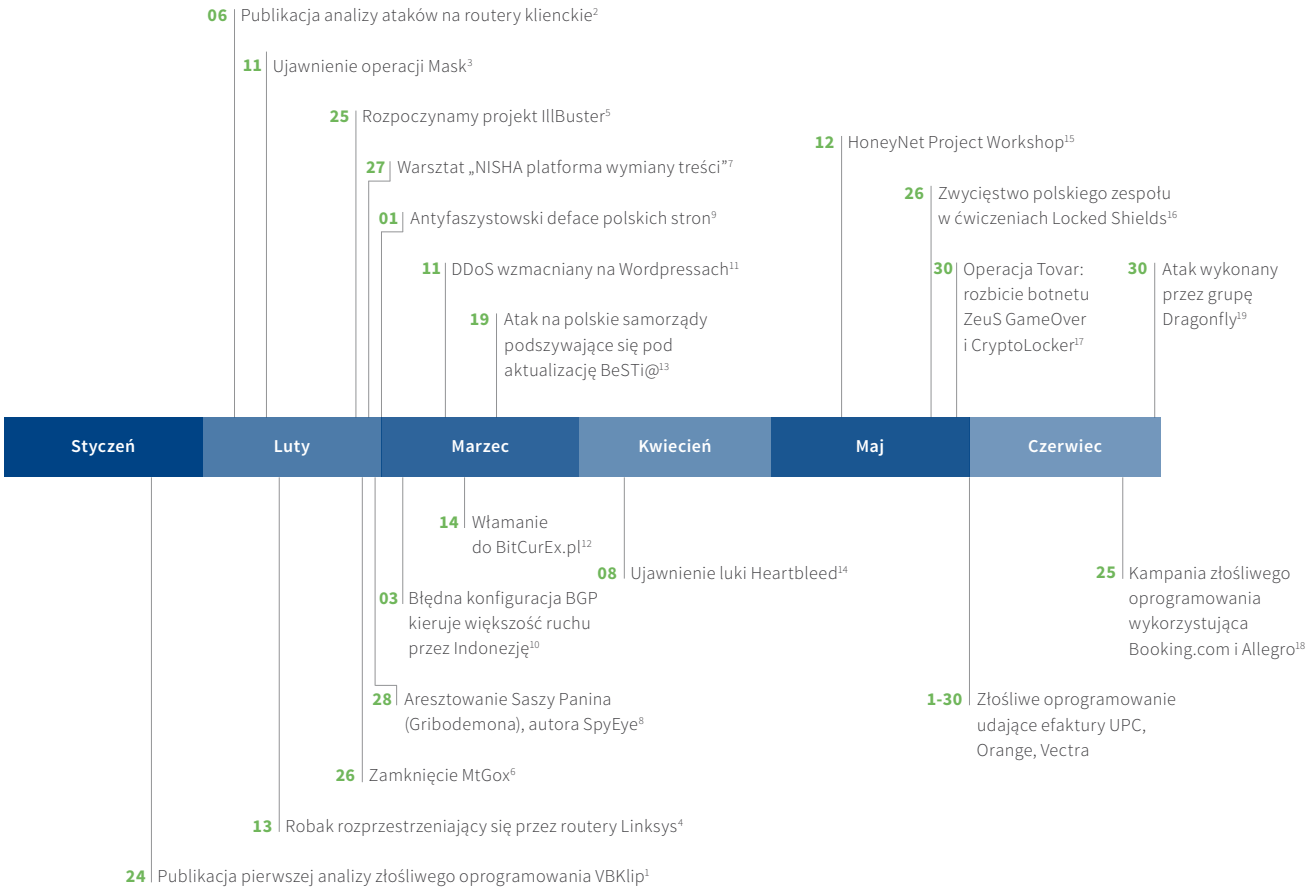
- Najczęstszymi domenami najwyższego poziomu, w których hostowano złośliwe URLe są: .com, .org i .ru.

- Udział procentowy złośliwych domen wśród wszystkich zarejestrowanych domen.pl jest zbliżony u wszystkich partnerów NASK.

- Statystyki dotyczące serwerów C&C nie zmieniły się znacząco w stosunku do poprzedniego roku. Dużą nowością jest pojawienie się Urugwaju na liście krajów, w których jest najwięcej serwerów C&C. Co więcej, wszystkie z tych serwerów znajdują się w jednym systemie autonomicznym.

- Spadek liczby skanowań. Dominujący port 23/TCP.

Kalendarium 2014



[1] http://www.cert.pl/news/7955

[2] http://www.cert.pl/news/8019

[3] http://niebezpiecznik.pl/post/operacja-maska-7-lat-w-ukryciu-prawie-400-ofiar-z-31-krajow-kolejny-rzadowy-malware/

[4] http://zaufanatrzeciastrona.pl/post/internetowy-robak-infekuje-nieza-bezpieczone-rutery-linksysa/

[5] http://www.cert.pl/news/8171

[6] http://zaufanatrzeciastrona.pl/post/tajemnicze-wlamanie-do-mtgox-czyli-jak-wartosc-bitcoinow-spadla-do-zera/

[7] http://nisha.cert.pl/node/224

[8] http://krebsonsecurity.com/2014/01/feds-to-charge-alleged-spyeye-trojan-author/

[9] http://niebezpiecznik.pl/post/ukranscy-anonimowi-podmienili-kilkanascie-polskich-stron-www/

[10] http://zaufanatrzeciastrona.pl/post/czemu-indonezyjski-operator-probowal-wczoraj-przejac-wieksza-czesc-internetu/

[11] http://niebezpiecznik.pl/post/trwaja-ataki-ddos-wykorzystujace-wordpressa-sprawdz-czy-twoj-blog-zostal-uzyty-w-ataku/

[12] http://niebezpiecznik.pl/post/bitcurex-polska-gielda-btc-zhackowana/

[13] http://zaufanatrzeciastrona.pl/post/ukierunkowany-atak-na-pracownikow-polskich-samorzadow/

[14] http://niebezpiecznik.pl/post/krytyczna-dziura-w-openssl-ponad-65-serwerow-w-internecie-podatnych-na-podsluch-i-to-od-2-lat/

[15] http://www.cert.pl/news/8196

[16] http://www.cert.pl/news/8647

[17] http://blog.shadowserver.org/2014/06/08/gameover-zeus-cryptolocker/

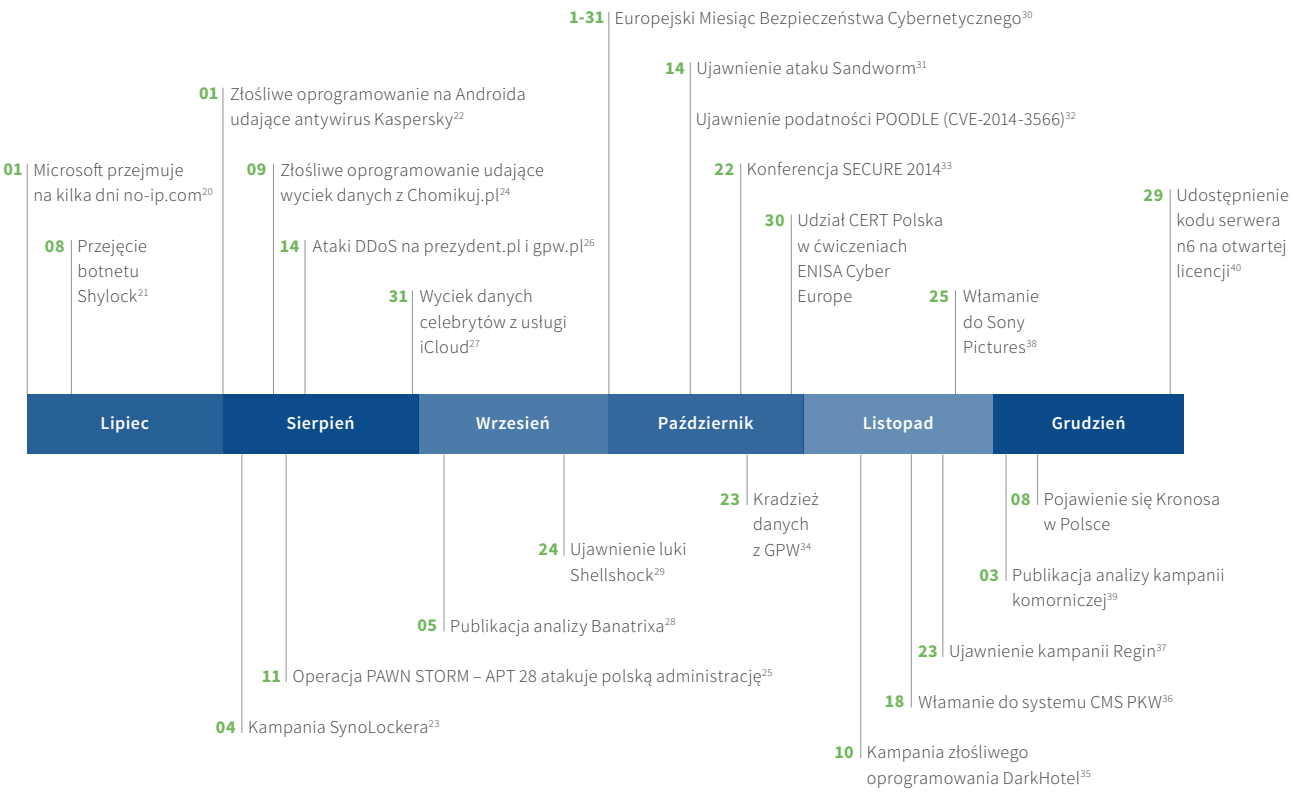
[18] http://www.cert.pl/news/8706, http://www.cert.pl/news/8798

[19] http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

[20] http://niebezpiecznik.pl/post/nie-dziala-ci-domena-od-no-ip-com-microsoft-ja-przejal/

[21] https://www.europol.europa.eu/content/global-action-targeting-shylock-malware

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



[22] http://niebezpiecznik.pl/post/wreszcie-ktos-zrobil-calkiem-dobry-fake-mail-czyli-twoj-bank-i-kaspersky/

[23] http://niebezpiecznik.pl/post/jesli-masz-nas-a-marki-synology-lepiej-zrob-kopie-bezpieczenstwa-czyli-synolocker-w-akcji/

[24] http://zaufanatrzeciastrona.pl/post/falszywy-wyciek-prawdziwych-danych-uzytkownikow-chomikuj-pl/

[25] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf

[26] http://niebezpiecznik.pl/post/cyber-berkut-atakuje-polskie-serwisy-internetowe-prezydent-plpadl-gwp-tez/

[27] http://en.wikipedia.org/wiki/2014_celebrity_photo_hack

[28] http://www.cert.pl/news/8999

[29] http://www.cert.pl/news/9083

[30] http://bezpiecznymiesiac.pl/

[31] http://niebezpiecznik.pl/post/4-nowe-i-krytyczne-dziury-w-windows-jedna-uzyta-przez-rosjan-atakujacych-polskie-firmy/

[32] https://www.openssl.org/~bodo/ssl-poodle.pdf

[33] http://secure.edu.pl

[34] http://niebezpiecznik.pl/post/gielda-papierow-wartosciowych-zhackowana/

[35] http://securelist.com/blog/research/66779/the-darkhotel-apt/

[36] http://niebezpiecznik.pl/post/wlamanie-na-serwery-panstwowej-komisji-wyborczej-wykradziono-hashe-hasel-i-klucze-urzednikow/

[37] http://niebezpiecznik.pl/post/zhackowal-komputery-komisji-europejskiej-nadajniki-sieci-gsm-oraz-komputer-prezydenta/

[38] http://niebezpiecznik.pl/post/sony-totalnie-zhackowane-wykradziono-olbrzymia-ilosc-danych-i-zablokowano-komputery-pracownikom-ponoc-takze-tym-w-polsce-siedziby-zamkniete-pracownicy-zwolnieni-do-domow/

[39] http://www.cert.pl/news/9484

[40] http://www.cert.pl/news/9635

Złośliwe oprogramowanie a sprawa polska

Rok 2014 stał pod znakiem incydentów o dużym znaczeniu biznesowym i politycznym: wycieków danych z kart kredytowych amerykańskiego sklepu Target, upadku giełdy bitcoinowej MtGox i politycznie motywowanych ataków Syryjskiej Armii Elektronicznej. Ujawniono też kilka bardziej zaawansowanych kampanii złośliwego oprogramowania, takich jak APT28, Regin, Careto, Sandworm czy Uroburos.

W Polsce dominowały incydenty związane z przestępstwami finansowymi – ataki oprogramowania z rodzin ZeuS (w różnych wariantach), VBKlip i Banatrix. Zaobserwowaliśmy także kampanię instalującą proste oprogramowanie szpiegowskie Ardamax Keylogger.

Nowym zjawiskiem w 2014 r. były incydenty powiązane z kampanią APT, nazwaną przez firmę Trend Micro „Pawn Storm". Operatorzy tej kampanii – grupa APT28 – prowadzili w sierpniu 2014 r. celowane ataki phishingowe na polską administrację publiczną, a w lipcu udało im się zamieścić na stronach bip.gov.pl i ośrodka badawczego OBRUM exploit kity instalujące robaka Sednit. We wrześniu ofiarą podobnego ataku była strona irgit.pl – Izby Rozliczeniowej Giełd Towarowych. Polskie przedsiębiorstwa zostały zaatakowane w wyniku kampanii Black Energy i Energetic Bear, a kilku Polaków podróżujących po Dalekim Wschodzie narażonych było na efekty kampanii DarkHotel.

Po raz pierwszy w historii Polska znalazła się w obszarze zainteresowania operatorów ataków motywowanych politycznie i wywiadowczo. Miały miejsce również incydenty przeprowadzone na tle czysto politycznym – 14 sierpnia „Cyber-Berkut" przeprowadził atak DDoS na stronę prezydent.pl i gpw.pl, ta sama grupa podmieniła kilka polskich stron WWW, a 11 listopada w ramach #OpRemember Anonymous wykonała atak DDoS na Komisję Nadzoru Finansowego.

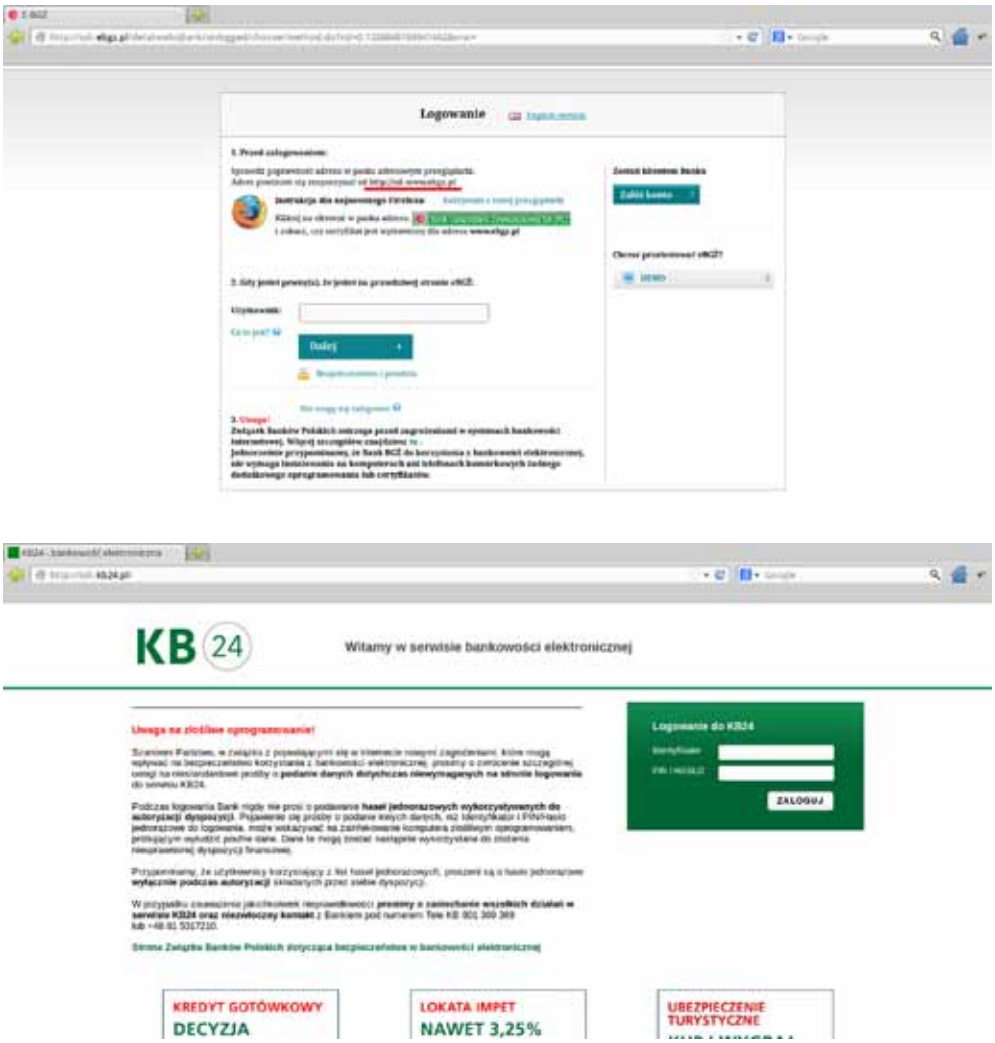
Pomimo tych zdarzeń można jednak stwierdzić, że Polska nie znajduje się w obszarze zainteresowań znaczących operatorów kampanii APT i należy się z tego stanu cieszyć oraz mieć nadzieję, że sytuacja będzie podobna i w następnych latach.

Największe zagrożenia w .pl

Rok 2014 obfitował w wiele niebezpiecznych zdarzeń, które stwarzały niemało zagrożeń dla użytkowników. Każde zagrożenie warto analizować, a następnie stopniować w zależności od strat, jakie mogą być jego wynikiem. I choć ataki DDoS są uciążliwe dla większych dostawców treści, branży e-commerce i witryn i serwisów administracji publicznej, to jednak przeciętny internauta nie ponosi zazwyczaj wyjątkowych strat z tego tytułu. Inaczej jest w przypadku złośliwego oprogramowania, którego celem jest przyniesienie jak największego zysku przestępcom. Realizowane jest to na dwa sposoby. Zainfekowany komputer można wykorzystać do dalszych ataków (DDoS, wysłanie spamu, klikanie w reklamy, hostowanie złośliwych treści, wykorzystanie jako proxy itp.) lub czerpać z niego zyski bezpośrednio (ransomware, kradzież danych, kradzieże z internetowych kont bankowych itp.). Oba scenariusze niestety nie omijają Polski. W 2014 r. zauważyliśmy wiele przypadków potwierdzających tę tezę i choć obie metody infekcji są groźne i niepożądane, zdecydowaliśmy się opisać bardziej szczegółowo wariant, w którym to użytkownik zainfekowanej stacji ponosi straty.

Ataki na użytkowników – złośliwe serwery DNS

W 2014 r. na uwagę zasługują dwa sposoby infekcji użytkownika. W pierwszej połowie roku obserwowaliśmy masowe włamania do domowych routerów, których podatności były szeroko nagłaśniane. Po kompromitacji urządzenia, przestępcy najczęściej zmieniali konfigurację serwerów DNS i przekierowywali zapytania do własnych, złośliwych resolverów. W ten sposób byli w stanie wyświetlić użytkownikowi fałszywe strony (przykładowo podszycie się pod wyszukiwarkę, jakiej używa internauta) i np. wstrzyknąć mu złośliwe oprogramowanie pod przykrywką aktualizacji wtyczki lub powszechnie używanego oprogramowania. Podszywali się również pod stronę banku, w którym ofiara ma swój rachunek. Wówczas, bazując na nieuwadze użytkownika (brak protokołu SSL przy nawiązywaniu połączenia), przestępca mógł poznać dane uwierzytelniające oraz spróbować wejść w interakcję z nieświadomym użytkownikiem.



Rysunek 1. Fałszywe ekrany logowania.

Ataki na użytkowników – kampanie złośliwego oprogramowania

W 2014 r. obserwowaliśmy rozsyłanie spamu ze złośliwym oprogramowaniem podszywającego się m. in. pod znane polskie i międzynarodowe firmy, takie jak: Allegro.pl, Orange, Play, TMobile, mBank, DHL, Netia, UPC, Poczta Polska, UPS, Booking.com czy Vodafone. Zdarzały się również wiadomości e-mail o zakupie poprzez opcję „Kup Teraz" laptopa, wraz z podanym numerem aukcji, bardzo przypominającej powiadomienia wysyłane przez serwis Allegro.pl.

Elementem wspólnym tych akcji był załącznik zawierający złośliwe oprogramowanie lub odnośnik do złośliwego oprogramowania.

Rysunek 2. Wiadomość podszywająca się pod informację o zakupie.

Kampanie zazwyczaj były dobrze przygotowane – powiadomienia wyglądały podobnie do tych, jakie rzeczywiście były wysyłane przez firmy lub mogłyby tak wyglądać (część firm, których tożsamości wykorzystano, nigdy nie wysyłała faktur w wiadomościach email). Większość firm starała się bardzo szybko reagować, informując klientów o phishingu oraz zmieniając wygląd i sposób komunikacji z konsumentami. Do takich praktyk zaliczamy np. zaprzestanie wysyłania faktur w wiadomościach e-mail, a jedynie umieszczanie informacji, gdzie taka faktura się znajduje (na przykład w panelu klienta) lub wysyłanie powiadomień z domeny reprezentującej markę (a nie korzystanie z adresów agencji marketigowej). Na plus możemy zaliczyć poprawne używanie mechanizmu SPF[1] przez większość firm, na minus – wciąż niewystarczające wsparcie tego mechanizmu przez serwery odbierające pocztę. O ile w poprzednich latach rynek trojanów bankowych w Polsce zdominowany był przez kolejne wersje ZeuSa, SpyEye'a a później Citadela (z zaznaczeniem obecności ZeuSa P2P/GameOver do końcówki grudnia 2012), tak w zeszłym roku zaobserwowaliśmy bardzo wyraźną zmianę. Obecnie przestępcy nie przywiązują się zbytnio do jednego rodzaju złośliwego oprogramowania i wykorzystują całą ich gamę. W zeszłym roku obserwowaliśmy działania przestępców stosujących złośliwe oprogramowania: VmZeus, KINS, Tinba, IFSB/Gozi2, Kronos, SmokeLoader (jako dropper). Natomiast w wyniku naszych badań mogliśmy stwierdzić, że wciąż istniał element wspólny kampanii w postaci wykorzystanych ATS-ów (ang. *Automatic Transfer Script* – szerzej opisane w Raporcie Rocznym CERT Polska 2013). Co więcej, również ATS-y były wykorzystywane przy serwowaniu webinjectów przy okazji DNS-ów.

[1] Sender Policy Framework http://www.openspf.org/

Heartbleed – CVE-2014-0160

7 kwietnia 2014 r. świat obiegła informacja o nowoodkrytej luce w popularnej bibliotece OpenSSL. Podatność znajdowała się od dwóch lat w wersjach 1.0.1a-f biblioteki i umożliwiała odczytanie fragmentu pamięci procesu, który korzysta z tej biblioteki. Biblioteki OpenSSL korzystają zarówno aplikacje serwerowe (np. WWW, poczta), jak i powszechnie używane aplikacje klienckie (chociaż najpopularniejsze przeglądarki nie używają tej biblioteki). Podatność została uznana za wyjątkowo niebezpieczną również z uwagi na prosty sposób jej wykorzystania, bez pozostawiania jakichkolwiek śladów na zaatakowanej stacji. Odkrycia luk dokonali niezależnie od siebie Neel Mehta z Google Security Team oraz fińska firma Codenomicon[2].

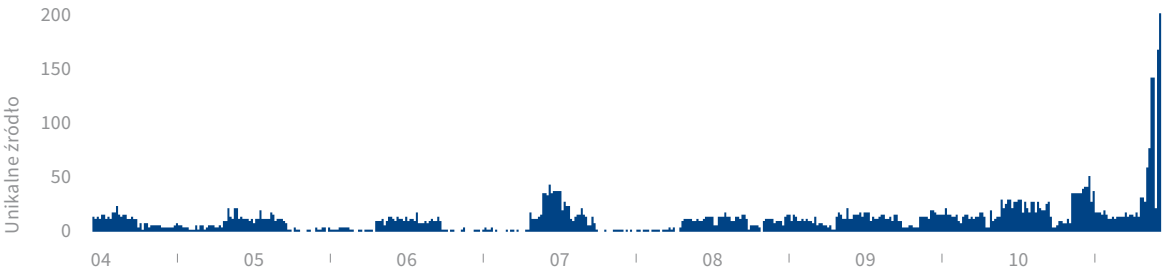
[2] http://www.smh.com.au/it-pro/security-it/heartbleed-disclosure-timeline-who-knew-what-and-when-20140415-zqurk.html

W jakim stopniu polskie serwisy były zagrożone?

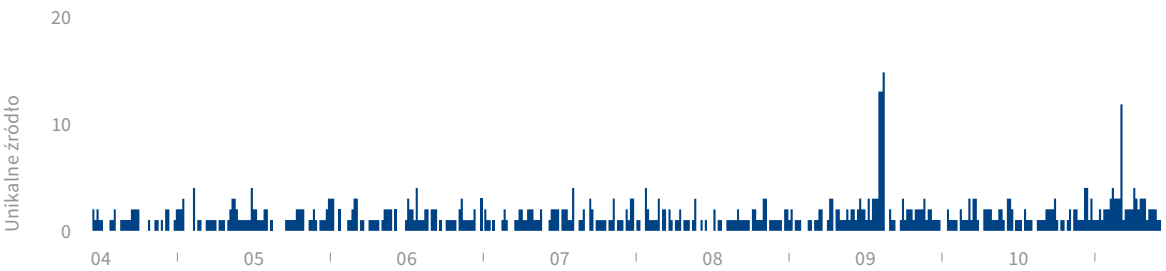
Ze skanowania portu 443/TCP (domyślny port, na którym działa HTTPS) w polskiej przestrzeni adresów IP wynikało, że:

- na 15 737 adresach wykryliśmy podatną usługę, co stanowi 1,8% wszystkich adresów IPv4, na których był otwarty port 443,
- na 675 478 adresach wykryliśmy działającą, ale niepodatną usługę, co stanowi 76,8% adresów z otwartym portem 443.

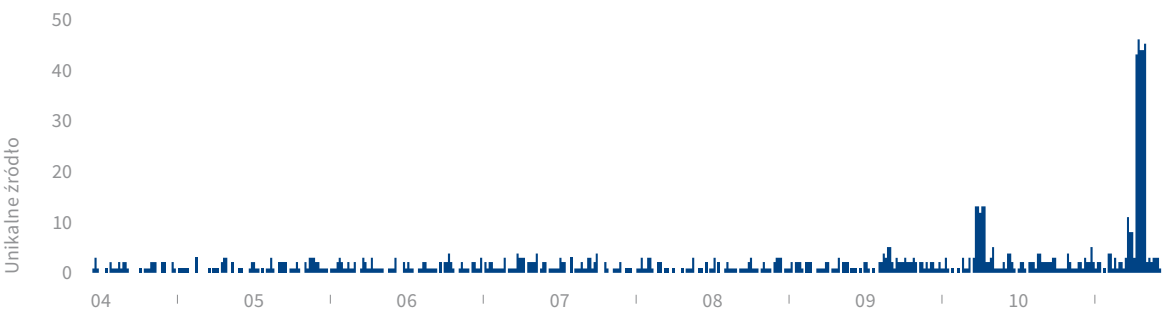
Pozostałe adresy albo nie odpowiadały, albo zgłaszały błąd połączenia. Najczęściej podatność wykrywana była w nazwach domen zakończonych na .edu.pl. Z 13 490 najpopularniejszych (według serwisu alexa.com) adresów w domenie .pl 765 (5.7%) było podatnych, w tym kilkanaście adresów dużych sklepów internetowych. W systemie ARAKIS również zaobserwowaliśmy wzrost aktywności na portach TCP, które są najczęściej związane z SSL: 443 (HTTPS), 465 (SMTPS), 993 (IMAP), 995 (POP3).



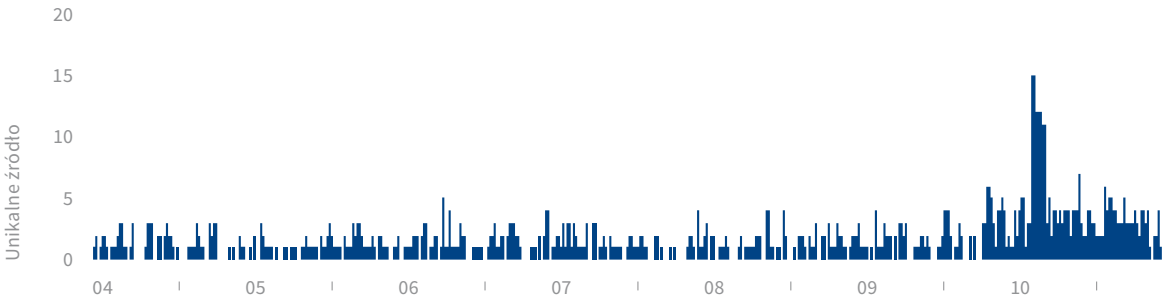
Rysunek 3. Docelowy port 443/TCP. Od 04.04.2014 10:10:06 do 11.04.2014 10:10:06.



Rysunek 4. Docelowy port 465/TCP. Od 04.04.2014 10:06:43 do 11.04.2014 10:16:43.

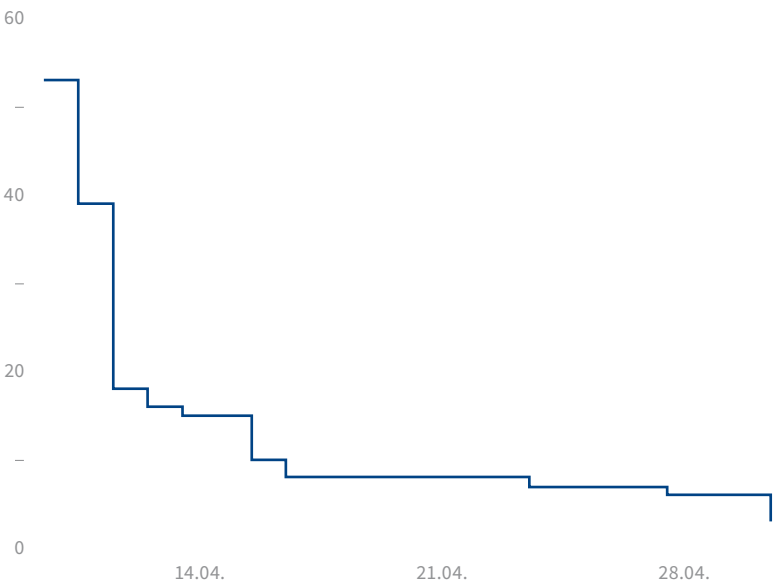


Rysunek 5. Docelowy port 993/TCP. Od 04.04.2014 10:10:56 do 11.04.2014 10:10:56.



Rysunek 6. Docelowy port 995/TCP. Od 04.04.2014 10:11:23 do 11.04.2014 10:11:23.

Monitorowaliśmy także tempo łatania luki w serwisach WWW administracji publicznej i wojska (gov.pl i mil.pl). Dwie doby po publicznym ujawnieniu podatności 57 z 698 aktywnych serwisów (8,1%) używało podatnej wersji biblioteki. Liczba ta szybko spadała i na koniec 10 kwietnia (trzeci dzień od publikacji) pozostało tylko 18 podatnych serwisów (2,6%). Spadek liczby podatnych serwisów ilustruje rysunek 7.



Rysunek 7. Spadek liczby podatnych serwisów.

Następstwa luki

CVE-2014-0160 zasługuje na uwagę również z innych względów. Jest to pierwsza luka, której upublicznienie spotkało się z wyjątkowym zainteresowaniem mediów. Podatność doczekała się własnego loga oraz domeny[3]. Przy okazji wywowała szeroką dyskusję o odpowiedzialnym ujawniu podatności.

[3] http://heartbleed.com/

Shellshock[4]

We wrześniu ogłoszono istnienie kolejnej groźnej luki, odkrytej przez Stéphane'a Chazelasa. Podatność ta dotyczyła powłoki bash i pozwalała na zdalne wykonanie kodu przy pewnych założeniach, np. przez moduł CGI do serwera Apache, serwer OpenSSH (z wykorzystaniem opcji „ForceCommand") i wiele innych programów wykorzystujących ten sam mechanizm przetwarzania zmiennych środowiskowych. Pierwszy oficjalny patch nie usuwał całkowicie podatności. Wkrótce zostały opublikowane kolejne, bardzo podobne podatności, m.in. przez Michała Zalewskiego. Ostatecznie 1 października ogłosił on, że załatane zostały wszystkie znane luki. Jednak podatność ta jest nadal wykorzystywana, np. przez złośliwe oprogramowanie w celu rozprzestrzeniania się[5, 6, 7].

W 2014 r. zapoczątkowany został trend, polegający na przedstawianiu podatności w sposób medialno-marketingowy (nadawanie nazw, tworzenie logo, powstawanie dedykowanych serwisów poświęconych jednej luce, itp.). Dzięki temu informacja na temat danego zagrożenia może dotrzeć do szerokiego grona odbiorców. Przy komunikacji skierowanej do zwykłego użytkownika łatwo niestety o nieporozumienia, błędy i niezamierzone przekłamania wynikające nie ze złej woli, a braku zrozumienia trudnej, wysokospecjalistycznej tematyki.[8,9] Stwierdzenia takie jak: „Eksperci ds. bezpieczeństwa internetowego nadal próbują załatać dziurę pozostawioną przez wirus Heartbleed czyli błąd w protokole OpenSSL." wynikają zapewne z trudności w komunikacji między ekspertami, dziennikarzami i odbiorcami tekstu.[10]

[4] CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187

[5] http://blog.malwaremustdie.org/2014/09/mmd-0028-2014-fuzzy-reversing-new-china.html

[6] http://blog.malwaremustdie.org/2014/10/mmd-0029-2015-warning-of-mayhem.html

[7] http://blog.malwaremustdie.org/2015/01/mmd-0030-2015-new-elf-malware-on.html

[8] http://tvn24bis.pl/wiadomosci-gospodarcze,71/wirus-grozniejszy-niz-heartbleed-shellshock-moze-zaatakowac-500-milionow-urzadzen,472263.html

[9] http://tvn24bis.pl/wiadomosci-gospodarcze,71/pierwsze-aresztowanie-zwiazane-z-heartbleed-to-19-letni-kanadyjski-haker,419382.html

[10] http://tvn24bis.pl/wiadomosci-gospodarcze,71/czeka-nas-powtorka-z-heartbleed-wykryto-nowa-luke-w-kodzie,437143.html, dostęp: 25 luty 2015

Analizy przypadków

APT w Polsce

APT (z ang. *Advanced Persistent Threat*) jest akronomimem stworzonym przez Siły Powietrzne Stanów Zjednoczonych w celu prowadzenia rozmów na temat ataków z firmami z sektora cywilnego nie ujawniając zbytnich szczegółów na temat atakującego. Był on używany także do określenia ataków na urządzenia elektroniczne i sieci komputerowe. Atak APT charakteryzują trzy główne cechy[11]:

- atakujący jest zaznajomiony i opanował zaawansowane metody ataku na komputery i sieci komputerowe oraz posiada umiejętność tworzenia własnego kodu wykorzystującego luki w zabezpieczeniach (Advanced),
- atakujący ma jasno określone i sprecyzowane cele – wykonuje z góry ustalone rozkazy i zadania (Persistent),
- atakujący jest zorganizowany, zmotywowany i posiada odpowiednie środki finansowe (Threat).

Używanie akronimu APT stało się w ciągu ubiegłych lat bardzo modne, przez co powyższa definicja powoli traci na znaczeniu. Coraz częściej APT staje się tożsame z jednym z następujących, bardzo subiektywnych, przypadków:

- „zaawansowane" złośliwe oprogramowanie,
- złośliwe oprogramowanie atakujące „ważne" instytucje,
- złośliwe oprogramowanie atakujące wybrane, nawet niekiedy niezbyt jasno określone, cele (dawniej taki atak nazywano „atakiem ukierunkowanym").

Uzyskane w wyniku APT dane mogą być w najprostszym przypadku sprzedane dając przestępcom korzyści finansowe, lub w przypadku, gdy APT jest wykorzystywane przez obcy wywiad bądź na jego zlecenie – dając przewagę ekonomiczną lub technologiczną. Z każdym rokiem pojawia się coraz więcej informacji o wykrytym zaawansowanym złośliwym oprogramowaniu oraz celach jego użycia.

Poniżej prezentujemy krótkie podsumowanie ataków nazywanych przez niektórych „APT" (w dowolnym z powyższych znaczeń), których ofiarami padli użytkownicy polskich sieci.

[11] SANS Technology Institute, *Assessing Outbound Traffic to Uncover Advanced Persistent Threat*, http://www.sans.edu/student-files/ projects/JWP-Binde-McRee-OConnor.pdf, dostęp: 27.02.2015

Grupa SandWorm oraz malware BlackEnergy

W październiku 2014 r. została upubliczniona informacja o działaniach grupy przestępczej o nazwie SandWorm, pochodzącej rzekomo z Rosji. Głównymi celami jej ataków były placówki rządowe oraz NATO, instytucje akademickie, z sektora energetycznego, telekomunikacyjnego oraz obronnego. Osoba, która stawała się celem ataku w danej instytucji była zawsze bardzo precyzyjnie dobierana, np. otrzymywała fałszywe emaile z informacjami o konferencjach, w których ma zamiar uczestniczyć. Badacze z firmy iSIGHT Partners upublicznili wyniki analizy[12], z których wynika, że głównym celem operacji przeprowadzanej przez grupę SandWorm było wykradanie poufnych danych. Ataki spearphishing, przeprowadzane przez tę grupę, polegały na dostarczaniu do precyzjnie wybranych odbiorców specjalnie spreparowanych plików pakietu Microsoft Office, np. prezentacji PowerPoint lub dokumentów Word. Pliki te zawierały exploit na podatność CVE-2014-4114[13] lub CVE-2013-3906[14] pozwalający na zdalne wykonanie kodu. Otwarcie takiego pliku skutkowało pobraniem i instalacją złośliwego oprogramowania o nazwie BlackEnergy, które umożliwiało atakującym przejęcie kontroli nad komputerem ofiary.

Najwięcej ofiar ataków ulokowanych było w Polsce i na Ukrainie, a według informacji udostępnionych przez firmę iSIGHT Partners, głównym celem w Polsce ataku był sektor energetyczny. Na podstawie danych uzyskanych od badaczy z ESET udało się zidentyfikować 28 unikalnych adresów IP w Polsce oraz 43 unikalne adresy na Ukrainie, które zostały zarażone botem BlackEnergy.

[12] iSIGHT discovers zero-dayvulnerability CVE-2014-4114 used in Russian cyber-espionage campaign, http://www.isightpartners.com/2014/10/cve-2014-4114/, dostęp: 27.02.2015

[13] Vulnerability Summary for CVE-2014-4114, https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4114, dostęp: 27.02.2015

[14] Vulnerability Summary for CVE-2013-3906, https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-3906, dostęp: 27.02.2015

Grupa APT28, operacja Pawn Storm oraz malware SEDNIT

Jednym z głośniejszych wydarzeń w środowisku bezpieczeństwa komputerowego był raport opublikowany przez analityków z firmy FireEye,[15] dotyczący grupy przestępczej określonej jako APT28. Według informacji zawartych w raporcie, działania operacyjne tej grupy mogły być wspierane przez rosyjski rząd i miały na celu pozyskiwanie strategicznych dla niego informacji. Twórcy złośliwego oprogramowania, które było dystrybuowane przez tę grupę, także najprawdopodobniej pochodzili z Rosji, na co wskazują przeprowadzone przez FireEye analizy jego kodu.

Procedura zdobywania dostępu do komputera ofiary była wielostopniowa i rozpoczynała się od ataku typu spearphishing. Najpierw wysyłany był email, który zawierał złośliwy załącznik w postaci dokumentu stworzonego w pakiecie Microsoft Office. Po jego otwarciu następowało uruchomienie złośliwego kodu poprzez wykorzystanie jednej z kilku podatności, np. zawartej w kontrolce ActiveX (CVE-2012-0158[16]) wchodzącej w skład kontrolek pakietu MS Office. Następnie za pomocą modułu droppera nazwanego „Sourface" pobierany i instalowany był backdoor Eviltoss, którego zadaniem była kradzież danych i zbieranie informacji o komputerze ofiary. Ogół złośliwego oprogramowania używanego przez grupę APT28 został określony nazwą Sednit i zawierał w swoim zestawie wiele dodatkowych wyspecjalizowanych modułów umożliwiających m.in.: dostęp zapisanych danych uwierzytelniających, dysków i urządzeń sieciowych, wykonywania zmian w rejestrze systemu Windows, uruchamiania nowych procesów oraz logowanie tego, co użytkownik wpisuje na klawiaturze. Celem ataków grupy APT28 były instytucje stojące na straży bezpieczeństwa (np. NATO), a także placówki rządowe w Gruzji (np. Ministerstwo Obrony) oraz Europie Wschodniej, m.in. na Węgrzech oraz w Polsce.

Podobne ataki miały miejsce między lipcem a wrześniem 2014 r. Przypisuje się je działaniom w ramach operacji Pawn Storm, opisanej w raporcie Trend Micro[17]. Odpowiedzialna za nie grupa przestępcza doprowadziła do udanego ataku na[18] kilka rządowych stron internetowych, a także strony Izby Rozliczeniowej Giełd Towarowych. W sierpniu natomiast rozsyłane przez nią były złośliwe pliki .mht (tzw. archiwum HTML), które, podobnie jak w przypadku działań grupy APT28, wykorzystywały lukę w kontrolce ActiveX oznaczoną CVE-2012-0158. Celem ataków przeprowadzanych w Polsce byli pracownicy kilku instytucji rządowych. Podobnie jak w przypadku działań grupy APT28 ataki rozpoczynały się od rozsyłania spersonalizowanych wiadomości email (spearphishing) do osób zajmujących wysokie stanowiska.

[15] APT28: A Window into Russia's Cyber Espionage Operations?: https://www.fireeye.com/content/dam/legacy/resources/pdfs/apt28.pdf, dostęp 02.03.2015

[16] Vulnerability Summary for CVE-2012-0158, https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0158, dostęp 02.03.2015

[17] Raport Trend Micro o operacji Pawn Storm: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf, dostęp 02.03.2015

[18] Operation Pawn Storm: The Red in SEDNIT: http://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-the-red-insednit/, dostęp 02.03.2015

Grupa Dragonfly/Energetic Bear

Na przełomie czerwca i lipca 2014 r. opublikowano raporty firm Symantec[19] i Kaspersky[20] na temat działalności grupy przestępczej Dragonfly, zwanej też Energetic Bear. Grupa ta działała co najmniej od 2011 r. i początkowo jej działania były skierowane przeciwko przedsiębiorstwom z branży obronnej i lotniczej ze Stanów Zjednoczonych oraz Kanady. W 2013 r. obiektem zainteresowań przestępców stały się firmy z branży energetycznej, operatorzy rurociągów naftowych i systemów przesyłowych energii elektrycznej oraz elektrownie zlokalizowane w Stanach Zjednoczonych i Europie.

Grupa Dragonfly używała trzech różnych metod prowadzących do zainfekowania komputera ofiary. Pierwszą z nich była wysyłka dobrze przygotowanych maili spearphishingowych z adresów w domenie gmail.com z załączonym dokumentem PDF wykorzystującym lukę w Adobe Flash (CVE-2011-0611). W czerwcu 2013 r. Dragonfly zaczął kompromitować strony internetowe związane z branżą energetyczną wstrzykując do ich kodu iframe'y, przekierowujące potencjalne ofiary do stron hostujących exploit kit LightsOut lub jego nowszą wersję, nazywaną Hello. W przypadku tej metody zainfekowania ofiary, exploit kit dostarcza backdoor Oldrea (nazywany też Havex lub Energetic Bear RAT) lub trojan Karagany.

Trzecią i zarazem najbardziej zaawansowaną metodą infekcji stosowaną przez Dragonfly było użycie pakietów oprogramowania ICS dostępnego na stronach producentów tego typu rozwiązań. Pakiety z oprogramowaniem zostały zarażone koniem trojańskim, a następnie ponownie umieszczone na tych stronach, co spowodowało mylne wrażenie, że są bezpieczne. Według raportu firmy Symantec, skompromitowane oprogramowanie ICS było dostępne do pobrania przez około 10 dni w kwietniu 2014 r. Z zainfekowanej maszyny przestępcy byli w stanie przesyłać wykradzione dane, wgrywać i uruchamiać własne pliki, a także przechwytywać hasła i robić zdjęcia ekranów.

Na podstawie danych pozyskanych z systemu n6 zidentyfikowaliśmy 350 unikalnych adresów IP w Polsce zainfekowanych Energetic Bear.

[19] Dragonfly: Cyberespionage Attacks Against Energy Suppliers http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf, dostęp: 27.02.2015

[20] Energetic Bear Crouching Yeti http://securelist.com/files/2014/07/EB-YetiJuly2014-Public.pdf, dostęp: 27.02.2015

Grupa Darkhotel

W listopadzie 2014 r. opublikowano raport dotyczący działalności grupy przestępczej Darkhotel (inna nazwa Tapaoux). Według analityków z firmy Kaspersky przestępcy od 2007 r. infekowali sieci komputerowe luksusowych hoteli w Japonii, w których zatrzymywali się pracownicy kadry kierowniczej i R&D firm z branży elektronicznej, farmaceutycznej i motoryzacyjnej. Skompromitowane hotelowe sieci WiFi wymagały od potencjalnych ofiar podania nazwiska oraz numeru pokoju, przez co przestępcy precyzyjnie wybierali swoje ofiary. Infekcja odbywała się poprzez zainstalowanie sugerowanych potencjalnej ofierze aktualizacji popularnych pakietów oprogramowania uprzednio zarażonych koniem trojańskim. Oprogramowanie instalujące zainfekowane „aktualizacje" nie wzbudzało podejrzeń ze względu na podpisanie go za pomocą skompromitowanego przez przestępców urzędu certyfikacji. W sumie grupa Darkhotel była w posiadaniu kluczy prywatnych co najmniej 10 urzędów certyfikacji, przy czym posługiwały się one słabym, bo zaledwie 512-bitowym kluczem. Zarażone oprogramowanie instalowało na komputerze ofiary backdoory, umożliwiające pobranie z przeglądarek internetowych danych dostępowych do kont pocztowych i serwisów społecznościowych. Co ciekawe, pierwsze połączenie zainfekowanego komputera do serwera C&C następowało zazwyczaj po ok. 180 dniach od infekcji, a zmiana strony kodowej systemu operacyjnego na język koreański powodowała samoczynne usunięcie złośliwego oprogramowania. Grupa Darkhotel posługiwała się narzędziami: Tapaoux, Pioneer, Karba i Nemim. Na podstawie danych z systemu n6 ustaliliśmy 36 zainfekowanych unikalnych adresów IP pochodzących z Polski, w tym 16 z nich należy do sieci mobilnych.

Błędnie skonfigurowane serwery i usługi w Polsce

W 2013 r. rozpoczęliśmy dystrybucję danych dotyczących błędnie skonfigurowanych serwerów DNS i NTP wykorzystywanych do odbitych ataków DDoS. Rok 2014 pokazał kreatywność atakujących, którzy atakami DDoS z wykorzystaniem protokołów sprzed ponad 30 lat, takich jak CHARGEN (Character Generator Protocol, RFC864) i QOTD (Quote Of The Day, RFC865) przypomnieli o ich istnieniu. Odbite ataki DDoS były wykonywane także, podobnie jak w latach ubiegłych, w oparciu o protokoły DNS (Domain Name System) i NTP (Network Time Protocol) oraz z wykorzystaniem protokołu SSDP (Simple Service Discovery Protocol), SNMP (Simple Network Management Protocol) i NetBIOS (Network Basic Input/Output System). Ofiarą ataku DDoS bazującego na protokołach NTP i SSDP była między innymi Korea Północna w grudniu 2014 r[21].

Wspólną cechą wymienionych protokołów jest stworzenie ich w oparciu o podatny na spoofing protokół UDP. Ataki odbite (ang. *reflected*) wykorzystują możliwość wysłania pakietu IP z podmienionym adresem źródłowym. Po dotarciu do serwera docelowego odpowiedź zostanie wysłana pod zadeklarowany fałszywy adres, a nie do rzeczywistego nadawcy pakietu. Ograniczeniem ataków z podmienionym adresem źródłowym jest brak możliwości nawiązania pełnej sesji protokołu TCP, co jednak nie dotyczy bezpołączeniowego protokołu UDP.

[21] http://www.arbornetworks.com/asert/2014/12/north-korea-goes-offline/, dostęp: 03 marca 2015.

Skąd się biorą podatne serwery i usługi?

DNS jest jednym z kluczowych protokołów stosowanych w internecie. Dostarcza on mechanizmy pozwalające na przypisywanie nazw domenowych (np. www.cert.pl) do adresów IP serwerów, na których dana usługa jest uruchomiona (np. 162.159.246.20) Zwalnia to użytkowników Internetu z konieczności pamiętania adresów serwisów w formie numerycznej.

NTP to powszechnie wykorzystywana usługa, której zadaniem jest synchronizacja zegarów z wzorcowymi źródłami czasu.

SNMP jest protokołem służącym do zarządzania urządzeniami sieciowymi (np. rutery, przełączniki) poprzez sieci IP. Obecnie SNMP jest wspierany przez większość urządzeń sieciowych.

SSDP jest protokołem stworzonym przez firmy Microsoft i HewlettPackard służącym do wykrywania urządzeń UPnP (Universal Plug-and-Play).

Netbios to pochodzący z lat osiemdziesiątych protokół umożliwiający aplikacjom opartym na API NetBIOS komunikację w sieciach TCP/IP.

QOTD wysyłający w jednym pakiecie UDP cytat dnia (Quote Of The Day) i **CHARGEN** (The Character Generator Protocol) odpowiadający 72 znakami ASCII są protokołami powstałymi ponad 30 lat temu, służącymi do testowania łączności sieciowej. Serwer usługi CHARGEN był niegdyś często zaimplementowany w drukarkach sieciowych.

Wzmocniony atak odbity wykorzystuje fakt, że niektóre usługi sieciowe generują odpowiedź znacznie większą w stosunku do zapytania. Przykładowo, wysłanie 20-30 bajtów do podatnego serwera DNS może spowodować odesłanie nawet 20-krotnie większej odpowiedzi, ale wysłanie pakietu UDP z 1 bajtową treścią do serwera usługi CHARGEN generuje odpowiedź 74 bajtową, a w przypadku QOTD odpowiedź często przekracza ponad 100 bajtów. Rekordzistą pod względem wzmocnienia definiowanego jako stosunek długości treści pakietu UDP otrzymanego przez ofiarę do długości treści pakietu UDP wysłanego przez atakującego jest protokół NTP generujący odpowiedź kilkaset razy większą od otrzymanego zapytania.
Generowanie dużej odpowiedzi jest naturalnym zachowaniem w przypadku takich protokołów jak CHARGEN i QOTD, podczas gdy duża odpowiedź z serwera NTP, zawierająca np. listę jego ostatnich klientów świadczy o złej konfiguracji serwera. Wystawianie „na świat" protokołów SSDP i SNMP związane jest prawdopodobnie z domyślną konfiguracją niektórych routerów.

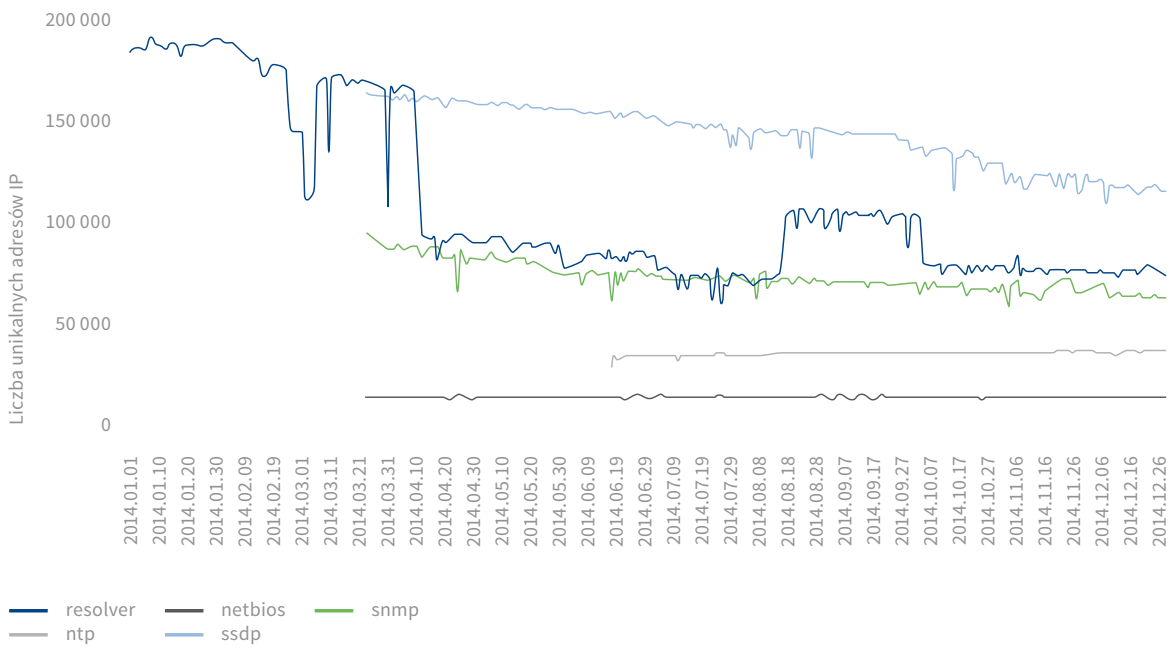
Podatne serwery i usługi w ciągu roku w Polsce

W 2014 r. do CERT Polska zaczęły napływać informacje o adresach IP zlokalizowanych w Polsce z błędnie skonfigurowanymi usługami: CHARGEN, Netbios, NTP, SNMP, SSDP, QOTD.

Poz.	Usługa	Liczba unikalnych adresów IP w ciągu roku	Średnia liczba adresów IP widziana dziennie
1	SSDP	2 562 309	144 189
2	SNMP	2 325 483	67 176
3	DNS	2 226 699	101 020
4	NTP	278 484	33 112
5	Netbios	186 101	13 070
6	QOTD	21 993	442
7	CharGen	18 997	839

Tabela 1. Najczęściej występujące błędnie skonfigurowane serwery i usługi w Polsce.

W tabeli 1 przedstawiliśmy dane dotyczące najczęściej występujących usług wykorzystywanych do ataków DDoS. Na podstawie liczby zaobserwowanych unikalnych adresów IP zlokalizowanych w Polsce można wnioskować, że największym problemem jest protokół SSDP. Niewiele mniej unikalnych adresów udostępniało podatne usługi SNMP i DNS. Najmniej popularne protokoły QOTD i CHARGEN zostały zaobserwowane na ponad stukrotnie mniejszej liczbie adresów w porównaniu do liderów zestawienia.



Rysunek 8. Liczba unikalnych adresów IP z podatnymi usługami i protokołami (dns, ntp, netbios, ssdp, snmp) w 2014 roku. [dane: 150.csv].

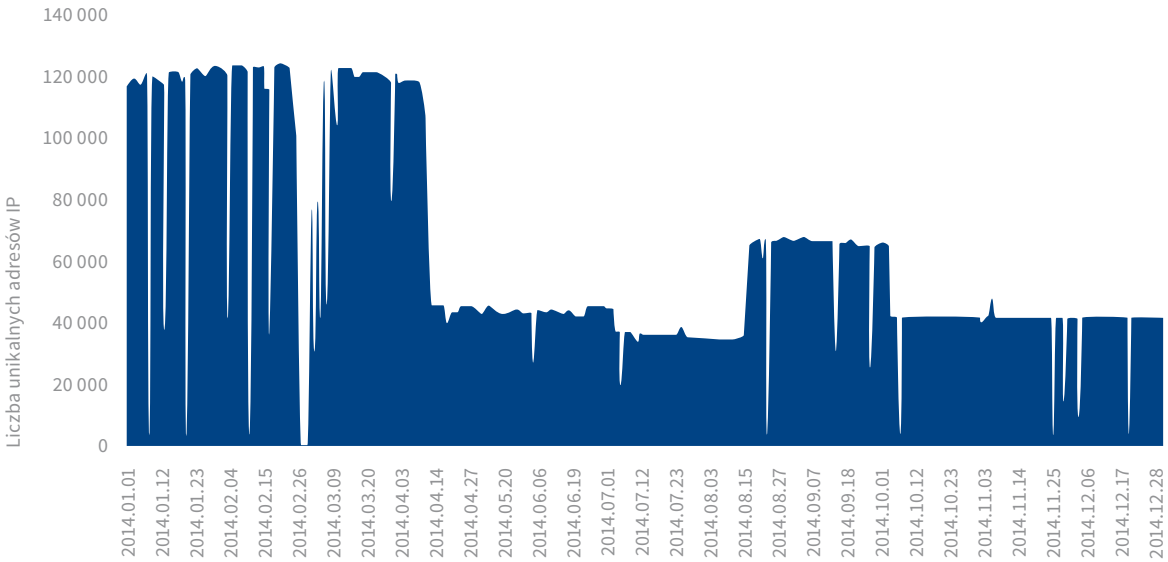
Na rysunku 8 przedstawiono dzienną liczbę unikalnych adresów IP, dla których uzyskaliśmy informacje o błędnie skonfigurowanych usługach. Większość danych zaczęliśmy otrzymywać na przełomie pierwszego i drugiego kwartału 2014 r.

Największy w ciągu roku spadek liczby podatnych serwerów zauważyliśmy w przypadku usługi DNS. Pod koniec 2014 r. otrzymywaliśmy każdego dnia informacje o ok. 75 000 adresów IP, podczas gdy na początku roku liczba ta była ponad dwukrotnie większa. Na spadek liczby otwartych serwerów DNS mogły mieć wpływ różnego rodzaju medialne doniesienia o kolejnych atakach DDoS przeprowadzonych z użyciem serwerów DNS, zorganizowane programy uświadamiające, takie jak „Open Resolver Scanning Project”[22] prowadzony przez Fundację Shadowserver, a przede wszystkim działania podjęte przez Orange Polska. Mniejszy spadek odnotowaliśmy w przypadku protokołów SSDP i SNMP. Liczba podatnych serwerów usług NTP i Netbios nie uległa zmniejszeniu, co jest niepokojące w kontekście częstych ataków DDoS z wykorzystaniem protokołu NTP. Dla protokołów CHARGEN i QOTD nastąpił wzrost liczby zaobserwowanych adresów, ale i tak stanowią one znikomą część pozostałych podatnych serwerów.

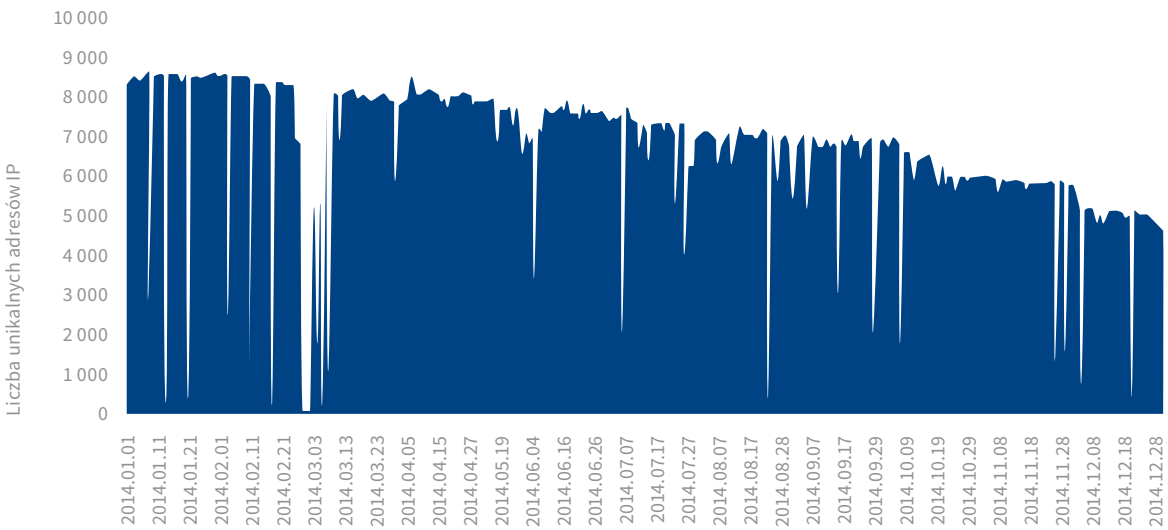
[22] https://dnsscan.shadowserver.org/. Dostęp: 03.03.2015

Otwarte serwery DNS w polskich systemach autonomicznych

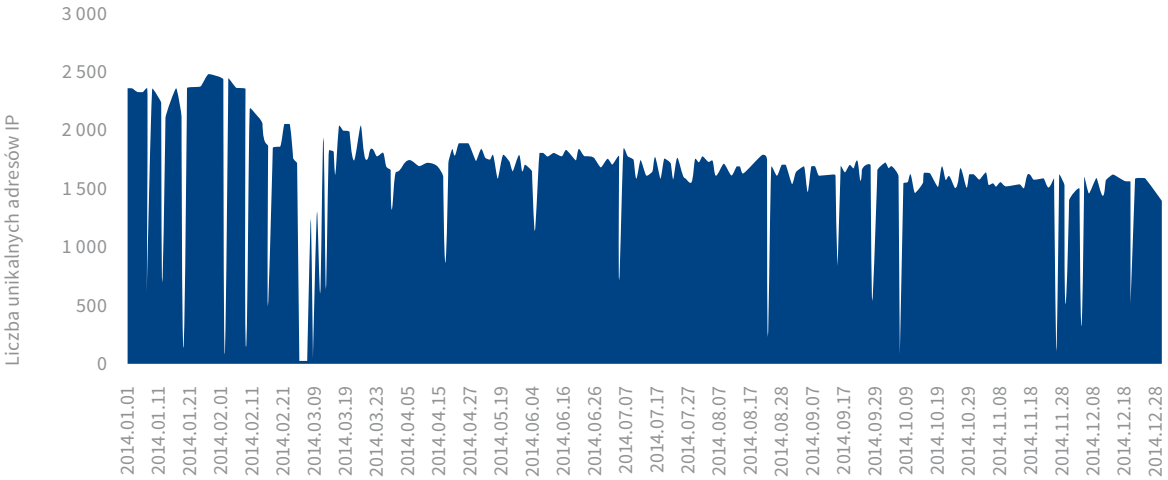
Na rysunkach 9-14 przedstawiamy dzienny rozkład liczby unikalnych adresów IP w tych polskich systemach autonomicznych, w których zaobserwowaliśmy ich najwięcej w ciągu roku. Analizując wykresy można łatwo zauważyć, że nie wszyscy dostawcy podejmują skuteczne działania prowadzące do zmniejszania liczby podatnych serwerów. W przypadku protokołu DNS, największy spadek odnotowaliśmy w Orange, gdzie na początku kwietnia 2014 r. gwałtownie (o $^2/_3$) spadła liczba otwartych serwerów DNS. W wyniku analizy danych pochodzących z systemu n6, wyciągnęliśmy wniosek, że spadek ten jest efektem działań podjętych przez Orange w przypadku usługi dostępu do Internetu DSL przeznaczonej dla firm. Zmniejszenie liczby podatnych serwerów DNS jest też widoczne w Netii, GTS i UPC. W przypadku Multimedia Polska i Vectra liczba otwartych serwerów DNS utrzymywała się na w miarę stałym poziomie, a w T-Mobile Polska minimalnie wzrosła w ciągu roku.



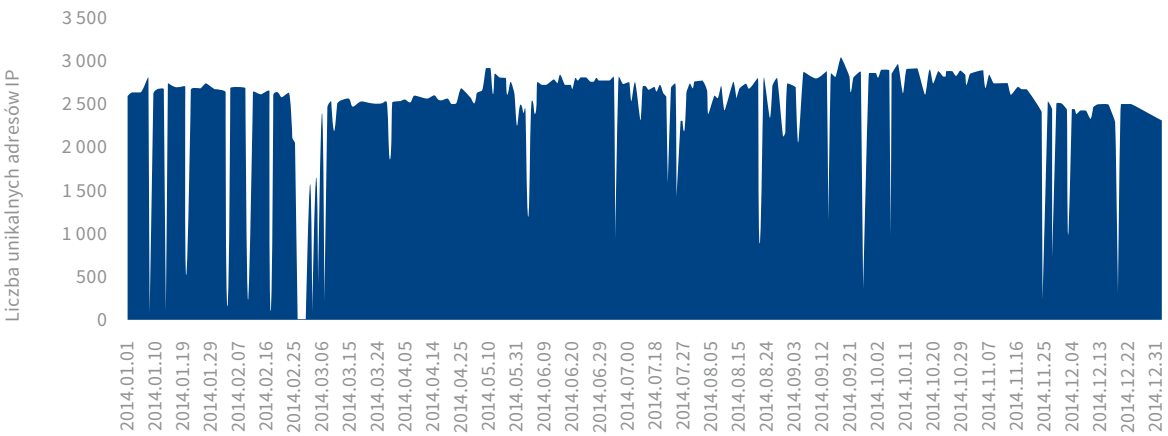
Rysunek 9. AS5617 – Orange.



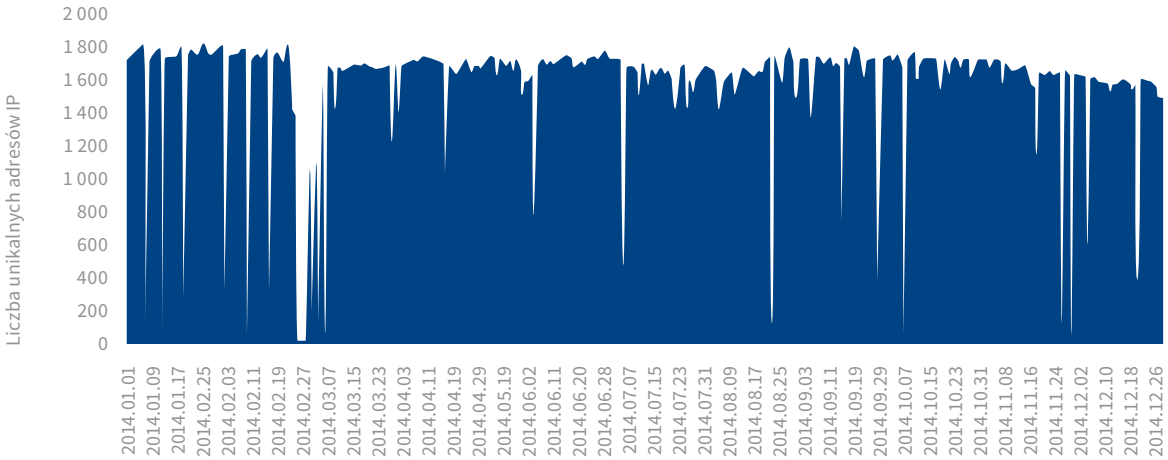
Rysunek 10. AS12741 – Netia.



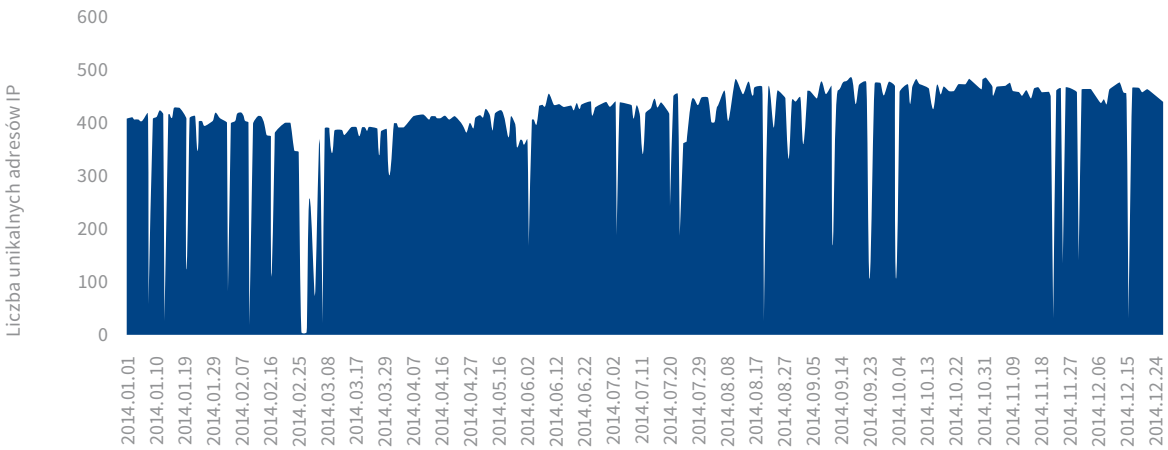
Rysunek 11. AS6714 – GTS.



Rysunek 12. AS21021 – Multimedia.



Rysunek 13. AS29314 – Vectra.



Rysunek 14. AS12912 – T-Mobile.

Urządzenia z uruchomioną usługą SNMP

Jak wykazały nasze analizy, większość urządzeń z uruchomioną usługą SNMP to modele domowych routerów. Nie powinno być to zaskoczeniem, ponieważ sam protokół SNMP został stworzony w celu zarządzania urządzeniami sieciowymi po protokole IP. Poza tym, część dostępnych na rynku modeli routerów domowych posiada w domyślnej konfiguracji aktywowanego agenta protokołu SNMP, co w połączeniu z niezbyt wysoką świadomością przeciętnych użytkowników routerów stwarza potencjalne źródło ataku DDoS.

W 2014 roku otrzymaliśmy 17 398 675 zgłoszeń dotyczących 2 325 483 unikalnych adresów IP, wśród których były 110 409 unikalne odpowiedzi na komunikaty *sysName* i *sysDescr.* W tabeli 2 przedstawiamy 10 najpopularniejszych odpowiedzi zwracanych przez podatne urządzenia.

Poz.	Unikalnych IP	Odpowiedź SNMP	Producent
1	1 540 995	TD-W8901G	TP-LINK
2	1 172 505	System Description	–
3	667 374	ADSL Modem	–
4	502 459	Wireless ADSL Gateway	Netgear
5	243 576	AirLive WT-2000A	AirLive
6	177 942	TD-8961ND	TP-LINK
7	76 564	TD-8840T 2.0	TP-LINK
8	70 151	Residental ADSL Gateway	Thomson
9	69 595	802.11n Wireless ADSL 2/2+ Router	Planet
10	58 341	RTL867x System Description	–

Tabela 2. Najczęściej spotykane odpowiedzi SNMP.

Najwięcej zgłoszeń związanych było z routerami firmy TP-LINK, popularnej wśród polskich użytkowników, przy czym w większości zgłoszenia dotyczyły starszych modeli. Przypuszczamy, że w nowszych typach urządzeń problem domyślnie aktywnego agenta SNMP został wyeliminowany. Co ciekawe, wśród odpowiedzi SNMP pojawiły się także te, pochodzące z drukarek sieciowych.

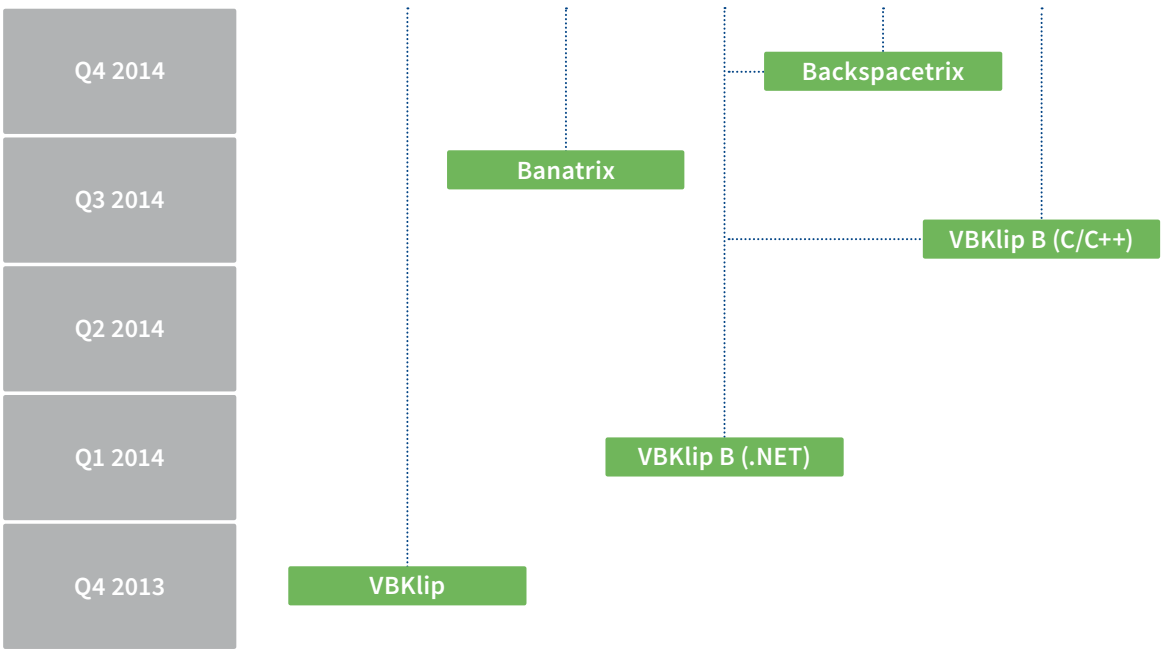
Dobrą prognozą na przyszłość jest fakt, że obserwujemy spadkową tendencję liczby urządzeń z błędnie skonfigurowanym protokołem SNMP. Analizując dane pod kątem producentów w zdecydowanej większości także obserwujemy spadek. Jedynym producentem sprzętu, w przypadku którego zauważyliśmy wzrost liczby zgłoszeń jest Zhone.

Polskie złośliwe oprogramowanie

Od ostatniego kwartału 2013 r. oraz przez cały rok 2014 zauważyliśmy znaczny wzrost ataków złośliwego oprogramowania napisanego przez osoby swobodnie posługujące się językiem polskim. Jednym z pierwszych polskich złośliwych programów był VBKlip, zwany też Banapter bądź ClipBanker. Jego działanie polegało na prostym pomyśle. Za każdym razem, gdy w schowku systemu Windows znajdował się numer konta bankowego – 26 cyfr rozdzielonych spacjami bądź nie – zostawał on podmieniany na inny numer konta.

Często, aby np. zapłacić fakturę, kopiujemy numer rachunku bankowego do schowka, a następnie wklejamy go w serwisie bankowości elektronicznej. Zmiana tego numeru w międzyczasie może zostać niezauważona, jeśli nie porównamy jeszcze raz numeru rachunku, na który zamierzamy wykonać przelew z tym na fakturze.

Wokół tego prostego, ale skutecznego pomysłu zbudowane zostały również inne wersje złośliwego oprogramowania. Podzieliliśmy je wszystkie na różne rodziny tak, aby pokazać złożoność zjawiska. Poniższy diagram obrazuje powiązania pomiędzy poszczególnymi rodzinami złosliwego oprogramowania.



Rysunek 15. Rozwój polskiego złośliwego oprogramowania w poszczególnych kwartałach.

VBKlip

Malware napisany jest w całości w Visual Basic 6.0. Zarówno dropper (część odpowiedzialna za dostarczenie odpowiednich plików na komputer ofiary) jak i właściwe złośliwe oprogramowanie są napisane w tym języku. Całość składa się z kilku współpracujących ze sobą komponentów:

- Komponent odpowiedzialny za zbieranie i wysyłanie raportów. Raporty zawierają takie dane, jak:
  - nazwa banku ofiary – zebrana z paska tytułu przeglądarki internetowej,
  - nazwa przeglądarki internetowej,
  - czas lokalny,
  - wersja złośliwego oprogramowania,
  - identyfikator konta słupa, na które nastąpiła podmiana.
- Komponent odpowiedzialny za podmianę numeru konta.
- Komponent, którego rolą jest szyfrowanie komunikacji z serwerem C&C i pobranie nowego numeru konta do podmiany. Jest on też odpowiedzialny za to, żeby restartować pozostałe komponenty, jeśli któryś z nich przestanie działać.
- Keylogger, którego zadaniem jest logowanie oraz zapisywanie w sposób zaszyfrowany wszystkich naciśniętych klawiszy. Następnie przesyłane są one razem ze wcześniej wspomnianym raportem.

W ciągu kilku miesięcy zagrożenie ewoluowało i zmieniało się wielokrotnie. Funkcja keyloggera została dodana w nowszych wersjach. Podobnie zmieniała się treść raportów czasami była na przykład wzbogacana o spis procesów działających na maszynie.

Jednym z ciekawszych przypadków ataku jest sytuacja, kiedy pewna osoba starała się podać drugiej swój numer konta w celu dokonania przelewu. Jednak kopiując swój numer rachunku nie zauważyła, że został on podmieniony. W efekcie wysłany został numer rachunku słupa, na który druga osoba, nieświadomie i mimo niezainfekowanego komputera przelała pieniądze.

VBKlip.B

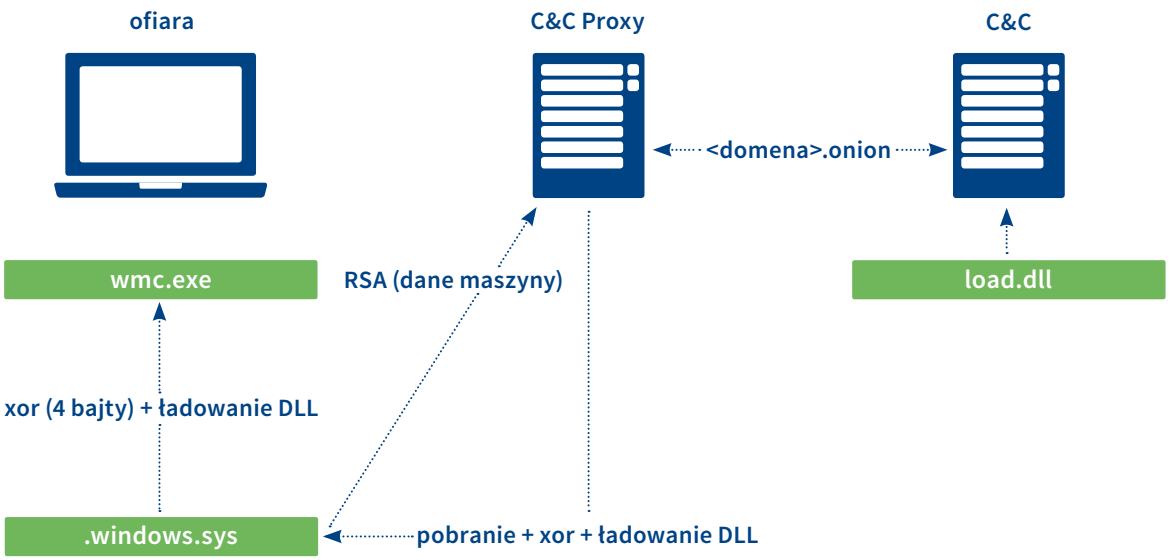
Powyższy pomysł stał się inspiracją dla innego autora złośliwego oprogramowania, który napisał własną wersję malware'u. Początkowo była ona pisana w środowisku .NET, a następnie w językach C oraz C++. Wszystkie te wersje nie komunikowały się z serwerem C&C, a jedynie miały zapisany na stałe numer konta. Cały kod to zaledwie kilka linijek, ale wiemy co najmniej o kilku przypadkach, kiedy z sukcesem udało się przestępcy ukraść środki z kont bankowych.

Banatrix

W ubiegłym roku najbardziej zaawansowanym zagrożeniem polskiego pochodzenia był z pewnością Banatrix. W sierpniu 2014 r. otrzymywaliśmy sygnały od użytkowników, którzy twierdzili, że pomimo przepisania numeru rachunku bankowego, wciąż zostawał on podmieniony. Po uzyskaniu próbki od jednego ze zgłaszających okazało się, że złośliwe oprogramowanie podmienia numer rachunku w pamięci procesu przeglądarki.

Banatrix przeszukuje listę procesów pod kątem obecności procesu jednej z czterech popularnych przeglądarek internetowych – Internet Explorer, Firefox, Opera lub Chrome. Jeśli taki proces zostanie odnaleziony, wówczas złośliwe oprogramowanie przeszukuje jego pamięć. W pamięci przeglądarki znajdują się między innymi dane, które sami wprowadziliśmy – na przykład numer konta do przelewu. Po znalezieniu takiego numeru zostaje on podmieniony na inny, pobrany z serwera zarządzającego złośliwego oprogramowania.

Jednak samo złośliwe oprogramowanie mogło przeprowadzić więcej szkodliwych działań. Możliwe było wykonanie dowolnego kodu na komputerze ofiary. Poniższy diagram ilustruje działanie Banatrixa na zainfekowanym komputerze.



Rysunek 16. Schemat działania złośliwego oprogramowania Banatrix.

Dropper rozpakowuje dwa pliki: jeden plik wykonywalny (wmc.exe / wms.exe) i drugi, będący zaszyfrowaną biblioteką DLL (.windows.sys / .sys). Zadaniem pierwszego pliku jest odszyfrowanie, wczytanie, a następnie zaszyfrowanie innym kluczem i zapisanie bibiblioteki DLL. Biblioteka następnie:

1. Łączy się do serwera C&C proxy, wysyłając podstawowe dane dotyczące maszyny (np. wersja systemu operacyjnego czy nazwa użytkownika) oraz adres w domenie .onion, z którym chce się połączyć.
2. Serwer C&C proxy łączy się do prawdziwego serwera C&C w sieci TOR (korzystając z *hidden service*) i przekazuje informacje.
3. C&C proxy przesyła dodatkowy, zaszyfrowany plik DLL, którego kod powinien zostać wykonany na maszynie ofiary.
4. Plik DLL zostaje wykonany na komputerze ofiary, ale nie jest zapisywany – znajduje się tylko w pamięci procesu.

Najnowsza wersja złośliwego oprogramowania używa również algorytmu generowania nazw domenowych (z ang. DGA). Algorytm ten jest używany, aby utrudnić analizę i sinkholing tego zagrożenia.

Backspacetrix

Odkrytym pod koniec roku 2014 zagrożeniem była kolejna podróbka autorstwa twórcy VBKlip.B. Tym razem postanowił on podrobić pomysł, który mieli autorzy Banatrixa. Bardzo proste rozwiązanie, napisane w środowisku .NET, które logowało wszystkie wciśnięte klawisze i jeśli było wpisanych 26 cyfr (nie licząc białych znaków), to symulowało odpowiednią liczbę wciśnięcie klawiszy shift i backspace, co skutkowało usunięciem wszystkich wpisanych znaków. Wówczas wpisywane jest 26 cyfr numeru konta słupa. Powodowało to efekt podobny do opisanego wcześniej, ale realizowane było w bardzo prosty sposób. Ponownie, nie było komunikacji sieciowej z serwerem C&C.

Działania CERT Polska

Ćwiczenia NATO „Locked Shields”

W 2014 r. polska drużyna, w której skład wchodziły również osoby z CERT Polska, wygrała ćwiczenia NATO pod kryptonimem „Locked Shields”. Ćwiczenia trwały przez pięć dni, od 20 do 24 maja i wzięło w nich udział 12 zespołów z 17 krajów. Każda z drużyn miała w swojej sieci 50 maszyn wirtualnych, które musiała obronić przed atakami Red Team. Wśród maszyn wirtualnych były kamery IP, zapory sieciowe pfSense, urządzenia VoIP czy też działające pod systemem Android. Ćwiczenie nie tylko testowało umiejętność obrony przed atakami sieciowymi, wykorzystującymi zarówno IPv4 jak i IPv6, ale też zdolność do wykrycia wcześniej skompromitowanych systemów w już istniejącej sieci. Oprócz CERT Polska, w skład drużyny wchodzili również pracownicy MIL-CERT, SKW, ABW, CERT-GOV oraz WAT. „Locked Shields” organizowane jest przez Centrum Doskonałości Współpracy Obronnej Cyberprzestrzeni NATO (NATO Cooperative Cyber Defence Centre of Excellence).

Platforma n6

Platforma n6 (Network Security Incident eXchange) to stworzony przez CERT Polska automatyczny system służący do zbierania, przetwarzania i dystrybucji informacji związanych z bezpieczeństwem komputerowym. Jego celem jest efektywne, niezawodne i szybkie dostarczenie dużych ilości informacji o zagrożeniach właściwym podmiotom: właścicielom, administratorom i operatorom sieci. Przy pomocy n6 przetwarzamy codziennie miliony zdarzeń z Polski i całego świata, a następnie przekazujemy je ponad dwustu odbiorcom. Więcej informacji o platformie dostępne jest na stronie: n6.cert.pl

W minionym roku uruchomiliśmy testowo kolejną wersję systemu, rozszerzoną o nowe funkcje. Dla użytkowników najistotniejszą zmianą jest jednolity interfejs programistyczny do wszystkich rodzajów danych, które udostępniamy w ramach platformy. Ułatwia to korzystanie z systemu, w szczególności integracja n6 z wewnętrznymi systemami bezpieczeństwa (np. IDS, SIEM) będzie znacznie prostsza w realizacji.

W grudniu udostępniliśmy istotną część kodu źródłowego nowej wersji n6 na otwartej licencji (GPL), aby zmniejszyć bariery techniczne związane z dzieleniem się danymi między organizacjami. Opublikowany komponent platformy to biblioteka języka Python – n6sdk – która pozwala na łatwe podłączenie się do źródła danych (np. baza danych SQL) i udostępnienie informacji uwierzytelnionym odbiorcom poprzez interfejs programistyczny REST zgodny z n6.

› Więcej informacji o n6sdk i repozytorium Git z kodem źródłowym znajduje się w serwisie GitHub: https://github.com/CERT-Polska/n6sdk

Projekt NECOMA

Kontynuujemy prace w ramach europejskojapońskiego projektu NECOMA (Nippon-European Cyberdefense-Oriented Multilayer threat Analysis). To projekt badawczy rozpoczęty w roku 2013, którego celem jest podniesienie poziomu bezpieczeństwa teleinformatycznego poprzez zwiększenie odporności na już istniejące oraz nowe zagrożenia.

Założenia NECOMA były opisane w poprzednim raporcie rocznym. W 2014 r. pracownicy naukowi NASK opublikowali szereg artykułów z wynikami badań prowadzonych w ramach projektu[23]. Rozwinęliśmy również platformę n6 na potrzeby wymiany danych pomiędzy organizacjami partnerskimi, czego efektem było wydanie n6 SDK (jak wspominamy powyżej).

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

[23] Publikacja dostępna na zasadzie otwartego dostępu: „Comparative study of supervised learning methods for malware analysis", http://www.itl.waw.pl/czasopisma/JTIT/2014/4/24.pdf

Biuletyn „OUCH!"

„Czym jest złośliwe oprogramowanie?", „Jak zabezpieczyć domową sieć?", „Co zrobić po włamaniu?" – to tylko niektóre z tematów poruszonych w biuletynie „OUCH!" w 2014r. „OUCH!" jest wydawanym co miesiąc darmowym biuletynem dla użytkowników komputerów zawierający zestaw porad dotyczących bezpieczeństwa. Każde wydanie składa się z krótkiego, w przystępny sposób przedstawionego wybranego zagadnienia wraz z listą wskazówek jak można chronić siebie, swoich najbliższych i swoją organizację. Biuletyn jest publikowany aż w 23 językach.

Dzięki współpracy CERT Polska i SANS Institute, polska wersja biuletynu ukazuje się od kwietnia 2011 r. Treść każdego biuletynu „OUCH!" jest tworzona i konsultowana przez zespół SANS „Securing The Human" uznanego dostawcę treści dotyczących bezpieczeństwa on-line. Autorami poszczególnych wydań są eksperci związani bezpośrednio z zagadnieniami bezpieczeństwa w IT, audytorzy, czy administratorzy. CERT Polska tworzy polską wersję biuletynu dostosowując do polskich realiów nie tylko język, ale także szczegóły omawianych zagadnień.

Biuletyn jest przeznaczony dla użytkowników nieposiadających szerokiej wiedzy o bezpieczeństwie komputerowym, a poszczególne problemy opisane są w sposób zrozumiały dla przeciętnego użytkownika. Zespół CERT Polska zachęca do rozpowszechniania magazynu „OUCH!" w firmach, placówkach oświatowych i domach, szczególnie wśród osób, które nie posiadają zaawansowanej wiedzy o bezpieczeństwie.

Im bardziej świadomi zagrożeń staną się użytkownicy, tym trudniej będzie skutecznie działać przestępcom.

› Wszystkie polskie wydania „OUCH!" można znaleźć pod adresem: http://www.cert.pl/ouch.

Projekt NISHA

W marcu 2014 r. zakończył się projekt NISHA (*Network for Information Sharing and Alerting*), którego celem była popularyzacja informacji związanych z bezpieczeństwem online oraz stworzenie pilotażowej sieci złożonej z czterech głównych portali informacyjnych, działających w każdej z instytucji biorących udział w projekcie. W skład konsorcjum realizującego projekt NISHA wchodził CERT Polska (NASK), narodowe zespoły CERT z Węgier i Portugalii oraz Instytut Bezpieczeństwa Informatycznego z niemieckiej Westfälischen Hochschule. Portale wymieniają między sobą informacje o bezpieczeństwie oraz udostępniają je lokalnie w swoich językach narodowych. Polski portal dostępny jest pod adresem http://nisha.cert.pl.

Każdy z partnerów, poza wzajemną wymianą danych, miał na celu dotarcie z informacjami zawartymi w sieci NISHA do użytkowników domowych oraz kadry pracowniczej sektora małych i średnich przedsiębiorstw. Skupienie się na tych grupach wynikało z faktu, że poprzez swoją liczebność odgrywają kluczową rolę w bezpieczeństwie Internetu, będąc jednocześnie łatwym celem ataków z powodu niewystarczającej znajomości zagadnień bezpieczeństwa.

W celu realizacji tego zadania każdy z partnerów zorganizował spotkania tematyczne, na których prezentowany był projekt NISHA oraz możliwości współpracy w ramach jego rozwijania. Spotkanie zorganizowane przez CERT Polska odbyło się 27 lutego 2014 w siedzibie NASK i zostało poświęcone zagadnieniom skutecznego przepływu informacji o bezpieczeństwie informatycznym, począwszy od twórców, aż do odbiorców końcowych.

NISHA: Prezentacja Łukasza Siewierskiego „Ekonomia podziemia”.

Podczas warsztatu omawiano sposób dotarcia z informacją na temat bezpieczeństwa komputerowego do przeciętnego odbiorcy. Niezwykle istotnym elementem w tym procesie są pośrednicy wymiany informacji czyli media, a także jednostki edukacyjne, firmy i organizacje, które jednocześnie również mogą być narażone na ataki. Warsztat skupił się na możliwościach, potrzebach i istniejących problemach we współpracy pomiędzy podmiotami tworzącymi eksperckie treści o bezpieczeństwie a pośrednikami mającymi na celu dotarcie do użytkownika końcowego.

Dzięki spotkaniu udało się zidentyfikować podstawowe problemy związane z dostarczaniem informacji o bieżących zagrożeniach. Głównym powodem braku zainteresowania takimi treściami wśród zwykłych użytkowników jest nieodpowiedni język przekazywanej informacji, który bardzo często jest zbyt techniczny i zawiera sformułowania, które są zrozumiałe wyłącznie dla samych ekspertów. Ponadto w dalszym ciągu nie istnieje jeden spójny zbiór podstawowej wiedzy i zagadnień związanych z bezpieczeństwem komputerowym. Posiadanie takiego repozytorium pomogłoby w dalszym tworzeniu materiałów edukacyjnych i napisanych zrozumiałym językiem artykułów opisujących aktualne zagrożenia.

W Polsce istnieje wiele podmiotów posiadających odpowiednie kwalifikacje i wiedzę, aby tworzyć wartościowe materiały edukacyjne o bezpieczeństwie teleinformatycznym. Jednak zazwyczaj dużą barierą jest trudność w dotarciu z nimi do użytkownika końcowego. Użytkownicy również rzadko odwiedzają specjalistyczne portale i nie starają się dokształcać we własnym zakresie. Istnieje ogromny potencjał płynący z zawiązania współpracy pomiędzy ekspertami dostarczającymi rzetelne, merytoryczne treści a podmiotami, które mogą przekazać techniczne informacje w przystępnej formie dużo szerszej grupie odbiorców niż specjalistyczna jednostka.

Projekt NISHA był współfinansowany przez Komisję Europejską w ramach programu „The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks" (CIPS).

Europejski Miesiąc Bezpieczeństwa Cybernetycznego

W październiku 2014 r. po raz trzeci w Europie oraz drugi raz w Polsce przeprowadzona została europejska kampania mająca na celu szerzenie wiedzy o bezpieczeństwie komputerowym pod nazwą Europejski Miesiąc Bezpieczeństwa Cybernetycznego. W ramach ECSM (European Cyber Security Month) Komisja Europejska oraz Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA) wspierały inicjatywy podejmowane w krajach UE skierowane do użytkowników cyberprzestrzeni. NASK oraz CERT Polska przyłączyły się do tej szczytnej inicjatywy poprzez utworzenie serwisu bezpiecznymiesiac.pl, gdzie prezentowano wydarzenia zainicjowane przez NASK w ramach tej kampanii.

Jednym z nich był quiz wiedzy „Bezpieczeństwo w Internecie". Skierowany do szerokiej grupy użytkowników Internetu miał na celu sprawdzenie podstawowej wiedzy związanej z bezpieczeństwem komputerowym i teleinformatycznym. Quiz jest w dalszym ciągu dostępny na stronie portalu NISHA (http://nisha.cert.pl/quiz). Pytania zawarte w quizie weryfikują znajomość zagadnień poruszanych na łamach polskiej wersji biuletynu „OUCH!", wydawanego co miesiąc przez Instytut SANS i CERT Polska. Poza weryfikacją posiadanej wiedzy, quiz ma także walory edukacyjne, gdyż każde z pytań jest skomentowane przez eksperta i odsyła do źródeł, które w przystępnej formie wprowadzają w tematykę pytania.

Kolejna inicjatywa była skierowana do studentów i polegała na rozwiązaniu zadania HackMe. Zadanie polegało na wydobyciu zaszyfrowanych plików z zapisu ruchu sieciowego w formacie PCAP. Stopień trudności nie okazał się zbyt wysoki, a odpowiedzi zostały przesłane jeszcze przed ostatecznym terminem zakończenia zadania. Za najszybsze poprawne rozwiązania przewidziane były nagrody książkowe dotyczące inżynierii wstecznej oprogramowania.

› Zadanie jest wciąż dostępne (wraz z rozwiązaniem) pod adresem: http://www.cert.pl/news/9120.

SECURE 2014

SECURE 2014 odbył się w dniach 22-23 października w Centrum Nauki Kopernik w Warszawie. W konferencji wzięło udział ponad 350 uczestników, którzy mieli możliwość wybierania spośród 39 prelekcji przygotowanych przez 47 prelegentów. Dzień przed konferencją odbyły się warsztaty SECURE Hands-on, prowadzone przez wykładowców z CERT Polska.

Wykład otwierający SECURE 2014 wygłosił znany specjalista ds. bezpieczeństwa z fińskiej firmy F-Secure Mikko Hypponen. Mikko nie po raz pierwszy był gościem SECURE. Tym razem pojawił się z prezentacją „The Arms Race" stanowiącą dobre wprowadzenie w tematy aktualnego krajobrazu zagrożeń. Niemniej interesujące prezentacje wygłosili także Stephen Brannon z firmy Verizon oraz Ilkka Sovanto z fińskiego zespołu rządowego NCSC-FI. Brannon omówił unikatowy raport na temat incydentów teleinformatycznych, stworzony przez Verizon wspólnie z dziesiątkami podmiotów z całego świata (w tym CERT Polska). Ilkka Sovanto opowiedział natomiast o procesie analizy i ujawniania podatności na przykładzie bardzo medialnego przypadku Heartbleed, w analizę którego mocno zaangażowany był osobiście. Wśród sesji równoległych nie zabrakło zarówno tematów mocno technicznych (np. Mateusz „j00ru" Jurczyk o ryzykach związanych z analizą złośliwego oprogramowania, Maciej Kotowicz mówił o złośliwych załącznikach do fałszywych faktur), jak i lżejszych (ciekawa analiza potknięć przestępców korzystających z TOR Adama Haertle).

Jedna z sesji poświęcona została tematom bezpieczeństwa w mało znanych lub mało zbadanych obszarach: bezzałogowych platform latających (prezentacja ekipy z LogicalTrust), sieci VLC (Grzegorz Blinowski z Politechniki Warszawskiej) i systemów wbudowanych (firmware.re).

Drugiego dnia w sesji plenarnej wystąpił m.in. znany z SECURE 2013 kontrowersyjny Bill Hagestad II, przyglądający się z bliska działalności chińskich i rosyjskich hakerów oraz Jart Armin (Cyberdefcon), który opowiedział o cyberprzestępczości mierzonej konkretnymi liczbami czy kwotami pieniędzy. Armin poruszył przy okazji temat rozpoczętego w 2014 r. projektu CyberROAD, w którym udział bierze CERT Polska (patrz s.37). W sesjach równoległych wystąpili m.in. Nikolay Koval z ukraińskiego rządowego zespołu CERT, Michał Sajdak (sekurak.pl) i Jurriaan Bremer (współautor Cuckoo Sandbox).

Drugi dzień konferencji zakończyło losowanie nagród w konkursach przygotowanych przez organizatorów i partnerów konferencji, w tym w konkursie CTF organizowanym przez zespół DragonSector.

› Prezentacje z konferencji dostępne są w postaci slajdów na stronie konferencji http://www.secure.edu.pl/historia/2014/program.php oraz nagrań wideo na kanale YouTube CERT Polska: http://goo.gl/y6kaSC

Raport dla ENISA

W minionym roku CERT Polska na zlecenie ENISA (Europejskiej Agencji Bezpieczeństwa Sieci i Informacji) przygotował raport „Actionable Information for Security Incident Response". Publikacja jest skierowana do członków zespołów reagujących na incydenty, jak i również do wszystkich, które zbierają, analizują i dzielą się informacjami dotyczącymi bezpieczeństwa komputerowego.

Tytułowa „actionable information" obejmuje szeroki zakres informacji dotyczących bezpieczeństwa, które mogą być podstawą podjęcia konkretnych działań zmierzających do ograniczenia lub eliminacji zagrożeń dla zasobów informatycznych. CERT Polska od wielu lat jest zaangażowany w wymianę tego rodzaju informacji, m.in. poprzez platformę n6 (patrz: s. 36), jednak w naszej opinii dotychczasowe publikacje nie opisały problemów związanych z tą tematyką w wyczerpującym stopniu. Stąd podstawowym celem przygotowanego raportu było całościowe przedstawienie procesu przetwarzania różnych rodzajów informacji przez zespoły reagujące na incydenty.

W raporcie zdefiniowaliśmy pojęcie „actionable information" w kontekście bezpieczeństwa komputerowego, zindentyfikowalismy jego kluczowe właściwości oraz zaproponowaliśmy uogólniony model przetwarzania danych przez zespoły reagowania na incydenty. Przestawiliśmy również trzy szczegółowe studia przypadków: zastosowanie wskaźników infekcji (indicators of compromise) w celu odparcia ukierunkowanego ataku, czy też monitorowanie botnetów, aby zwiększyć poziom świadomości sytuacyjnej oraz skuteczną wymianę danych na poziomie krajowym.

Do raportu dołączone jest praktyczne ćwiczenie, ilustrujące wykorzystanie narzędzi dostępnych na wolnych licencjach (open-source) do przetwarzania informacji i odparcia ataku. Drugi załącznik to zestawienie 53 technicznych standardów istotnych dla wymiany danych oraz 16 ogólnodostępnych systemów do przetwarzania i zarządzania informacjami związanymi z bezpieczeństwem.

› Dokumenty są dostępne do pobrania ze strony ENISA[24]:

- Actionable information for security incident response
- Standards and tools for exchange and processing of actionable information
- Ćwiczenie: Using indicators to enhance defence capabilities [PDF]

[24] ENISA: www.enisa.europa.eu

Rozpoczął się Projekt CyberROAD

CyberROAD jest projektem badawczym finansowanym przez Komisję Europejską w ramach programu FP7, którego celem jest określenie obecnych i przyszłych problemów w walce z cyberprzestępczością i cyberterroryzmem oraz wypracowanie planu badań nad tymi zagadnieniami. Pierwszym krokiem projektu jest uzyskanie obrazu obecnej sytuacji technologicznej, społecznej, gospodarczej, politycznej, i prawnej, która przyczynia się do rozwoju cyberprzestępczości i cyberterroryzmu. Następnie zebrane scenariusze opisujące powyższą sytuację zostaną przeanalizowanie w celu identyfikacji luk, przyszłych możliwych kierunków rozwoju oraz priorytetów badawczych. W ramach badań nad cyberprzestępczością podjęto decyzję skupienia się na Polsce jako przykładowym kraju, dla którego dokonana zostanie analiza porównawcza tego zjawiska z innymi krajami Europy i świata. Widocznym publicznie działaniem projektu było opublikowanie ankiety dotyczącej cyberprzestępczości. Projekt CyberROAD rozpoczął się w maju 2014 r. i ma potrwać 24 miesiące. Zrzesza 20 podmiotów z 11 państw. Polskę reprezentuje NASK w postaci zespołu CERT Polska.

› Więcej informacji można znaleźć na stronie projektu: http://www.cyberroad-project.eu/

Raport Verizon DBIR

W 2014 r. zespół CERT Polska wziął udział w projekcie amerykańskiego dostawcy usług internetowych Verizon – opracowania światowego *Data Breach Investigations Report*. Raport stanowi analizę danych i statystyk zebranych z 50 różnych organizacji na świecie dotyczących potwierdzonych incydentów bezpieczeństwa. W ubiegłym roku zebrano aż 63 tysiące incydentów, które dotyczyły 95 państw świata. 92% analizowanych incydentów udało się zredukować do 9 podstawowych scenariuszy ataków. Wśród najpoważniejszych scenariuszy, zwrócono uwagę na dynamiczny wzrost udanych ataków na terminale płatnicze (Point of Sale intrusions) z użyciem złośliwego oprogramowania, w dużym stopniu udanych ataków z wykorzystaniem aplikacji webowych, coraz więcej przypadków zakończonych sukcesem ataków cyberwywiadowczych oraz skimerów kart kredytowych. Zespół CERT Polska był autorem akapitu w raporcie poświęconemu trojanom bankowym i atakom finansowym w Polsce.

› Raport Verizon DBIR dostępny jest na stronie http://www.verizonenterprise.com/DBIR/2014/

Projekt ILLBuster

Celem rozpoczętego w 2014 r. projektu ILLBuster jest stworzenie systemu automatycznej analizy i wykrywania szkodliwych i nielegalnych stron internetowych. Detekcja ma odbywać się poprzez analizę ruchu DNS, a system powinien wykrywać strony zawierające złośliwy kod, pornografię dziecięcą, phishing i oferty sprzedaży podrobionych towarów. NASK jest liderem technicznej części projektu – ILLBuster wykorzystuje platformę n6 jako źródło danych, a skaner oparty jest na opracowanym przez nas oprogramowaniu Honey Spider Network 2.

Projekt finansowany jest przez Komisję Europejską w ramach programu grantowego ISEC HOME/2012/ISEC/AG/4000 „Zapobieganie i zwalczanie przestępczości", a realizuje go konsorcjum składające się z włoskich uczelni – Università de Cagliari i Università degli Studi di Milano-Bicocca, amerykańskiego University of Georgia, włoskich sił policyjnych – Guardia di Finanza i Polizia Postale, szwedzkiej firmy Netclean, włoskiej organizacji pozarządowej Tech and Law Center oraz CERT Polska.

› Więcej o projekcie: http://pralab.diee.unica.it/en/ILLBuster

The Honeynet Project Security Workshop w Warszawie

W dniach 12-14 maja 2014 r. odbyła się kolejna edycja konferencji The Honeynet Project Security Workshop. Znana na całym świecie konferencja już od wielu lat przyciąga ekspertów bezpieczeństwa komputerowego. Ubiegłoroczna edycja odbyła się w Warszawie i zgromadziła ponad 160 uczestników z całego świata. W jej przygotowa-

niu aktywny wkład mieli eksperci CERT Polska oraz Polskiej Kapituły The Honeynet Project, którzy pomogli skonstruować agendę, zadbać o promocję i pozyskanie sponsorów, a także sprawnie przeprowadzić całe wydarzenie. W agendzie konferencji znalazły się prelekcje poświęcone najnowszym trendom w rozwoju złośliwego oprogramowania oraz metodom walki z tego typu zagrożeniami, a także prezentacje narzędzi użytecznych w analizie danych oraz wykrywaniu ataków na infrastrukturę. Ostatni dzień konferencji poświęcony był warsztatom, na których uczestnicy mogli uzyskać wiedzę dotyczącą analizy wstecznej złośliwego oprogramowania w systemach Windows oraz Android, poznać najnowsze metody zabezpieczania infrastruktury zbudowanej na bazie wirtualizacji oraz dowiedzieć się, czym są botnety i jak można walczyć z tym zagrożeniem używając narzędzi dostarczanych przez członków Fundacji The Honeynet Project.

Wystąpienia publiczne

W roku 2014 członkowie zespołu CERT Polska przeprowadzili 5 warsztatów i 4 szkolenia, przedstawili 29 prezentacji i referatów na seminariach i konferencji, oraz wzięli udział w dyskusji panelowej.

CERT Polska przygotował dwie konferencję: międzynarodowe spotkanie SECURE 2014 oraz warsztat „NISHA – platforma wymiany treści". CERT Polska wsparł także organizację warsztatów Honeynet Project.

Poza konferencjami organizowanymi w kraju, przedstawiciele CERT Polska wystąpili między innymi na sympozjum FIRST w Zurichu, eCrime (Birmingham), konferencji FIRST w Bostonie oraz Botconfie (Nancy).

ARAKIS 2.0 – EWS nowej generacji

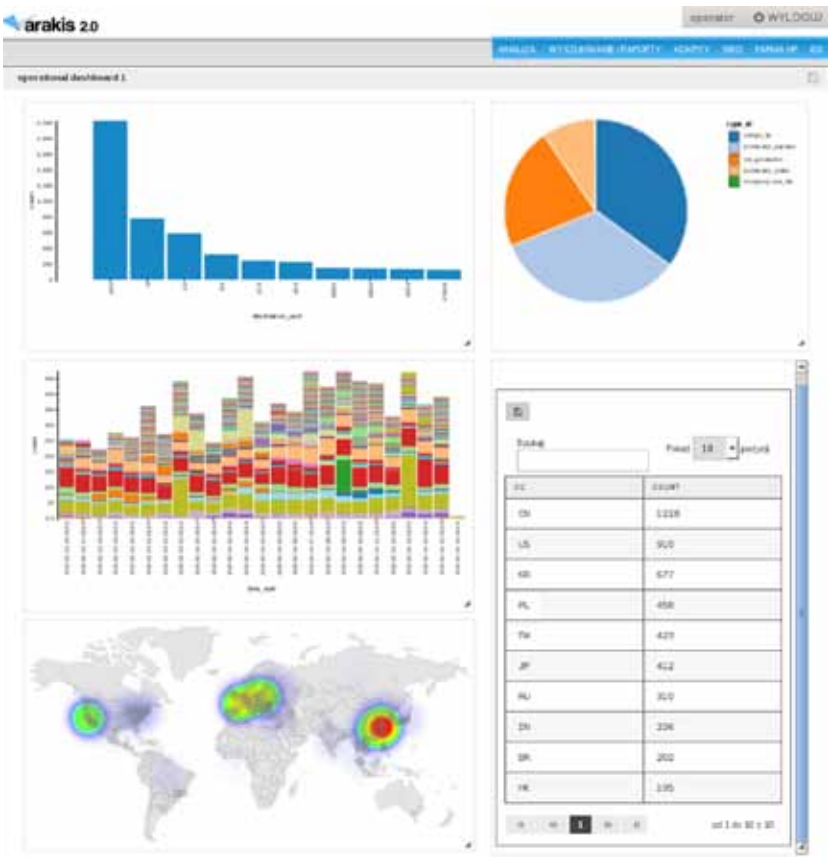
ARAKIS jest modularnym systemem wczesnego ostrzegania przed zagrożeniami sieciowymi (ang. *Early Warning System*). Głównym jego celem jest automatyczne znajdowanie wzorców ataków i zagrożeń poprzez heurystyczną analizę ruchu sieciowego.

Pierwsza wersja systemu powstała w 2007 r. W roku 2014, na bazie doświadczeń z systemem ARAKIS 1, zostało ukończone tworzenie wersji drugiej. Główny cel pozostał niezmieniony, lecz sposób jego realizacji uległ gruntownym modyfikacjom – system został zaprojektowany i napisany od nowa.

ARAKIS 2.0 korzysta z najnowszych algorytmów automatycznego wykrywania powtarzających się wzorców zagrożeń. Ruch jest zbierany przez rozproszone w sieciach sensory, oraz poddawany szeregom równoległych analiz w centralnym klastrze obliczeniowym. Główne źródło danych pozostało niezmienne – jest nim nieprodukcyjny ruch do honeypotów (systemów-pułapek), które jednak zostały wymienione na nowsze, bardziej interaktywne i odpowiadające aktualnym trendom w atakach (ataki na aplikacje internetowe, serwery ssh, systemy SCADA). Narzędzia honeypotowe zostały umiejscowione w chmurze (honeyfarm), dzięki czemu pułapki stały się mniej podatne na awarie, łatwiej je też aktualizować oraz rozbudowywać o kolejne narzędzia. Dodatkowo system został rozszerzony o opcjonalną możliwość analizy ruchu produkcyjnego wewnątrz sieci korporacyjnych, a także analizę logów z produkcyjnych serwerów WWW. Aby zapewnić maksimum prywatności i nie

ingerować w poufne dane przesyłane chronionymi sieciami, analiza wewnątrzkorporacyjnego ruchu opiera się jedynie na nagłówkach protokołów sieciowych do warstwy czwartej, bez analizy danych zawartych w treści. ARAKIS 2.0 jest zasilany wiedzą z platformy n6 oraz wskaźnikami infekcji (indicators of compromise) dostarczającymi przez analityków CERT Polska. Dzięki temu system posiada możliwie najbardziej aktualne informacje np. o serwerach C&C, złośliwych adresach IP, źródłach phishingu, itp., które wykorzystuje do wykrywania infekcji wewnątrz chronionych sieci.

Oprócz samych zaawansowanych analiz ważne jest również, by ich wyniki prezentować w sposób przyjazny użytkownikowi . Głównym odbiorcą nowej wersji systemu są eksperci z dziedziny bezpieczeństwa IT. Dlatego w ARAKIS 2.0 położony został szczególny nacisk na wszechstronność i dowolność w odpytywaniu i prezentowaniu pozyskanych informacji, korelacji wyników analiz, tworzenia statystyk i prezentacji wyników. Aby to osiągnąć stworzony został język zapytań AQL (ARAKIS Query Language), który pozwala wyświetlać dowolne dane przechowywane w systemie, posiada szereg funkcji statystycznych, a także umożliwia wyświetlanie wyników w postaci tabelarycznej, map lub jednego z ośmiu typów wykresów. Dzięki AQL można także tworzyć okresowe raporty o różnorodnym poziomie zaawansowania – od podstawowego podsumowania statystycznego do szczegółowego raportu z analizy śledczej.



Rysunek 17. Interfejs ARAKIS 2.0 AQL w akcji.

Realizacja projektu ARAKIS 2.0 trwała od lutego 2012 roku do marca 2014 w ramach umowy NASK z Ministerstwem Nauki i Szkolnictwa Wyższego. W projektowanie i tworzenie systemu były zaanagażowane osoby z Działu Rozwoju Oprogramowania NASK, CERT Polska, oraz z Pracowni Metod Bezpieczeństwa Sieci i Informacji z Pionu Naukowego NASK.

Statystyki

Botnety w Polsce

W sekcji opiszemy dane z wielkości botnetów w Polsce, które zostały przedstawione w poniższych tabelach. Dane o botnetach w polskich sieciach pochodzą z projektu n6. Z posiadanych danych możemy wywnioskować, że średnio w ciągu każdych 24 h w Polsce jest infekowanych 280 tysięcy komputerów. Rzeczywista liczba jest prawdopodobnie wyższa – szacujemy, że o kilkanaście procent.

Poz.	Procent zainfekowanych adresów IP	Maksymalna dzienna liczba unikalnych adresów IP	Numer AS	Nazwa Operatora
1	4,02%	27 354	12912	TMobile Polska
2	2,44%	15 607	39603	P4 (Play)
3	2,31%	13 693	21021	Multimedia Polska
4	2,09%	30 520	12741	Netia
5	1,71%	9 051	29314	Vectra
6	1,68%	92 340	5617	Orange Polska
7	1,54%	3 837	20960	TK Telekom
8	1,44%	19 099	8374	Plus
9	0,95%	14 544	6830	UPC Polska
10	0,78%	2 528	43939	Internetia

Tabela 1. Dane dotyczące infekcji u polskich operatorów.

W tabeli 1 przedstawiono udział zainfekowanych adresów IP polskich operatorów. Na pierwszych czterech miejscach znalazły się te same sieci, co w roku 2013, jednak przewaga T-Mobile znacznie się zmniejszyła. U wszystkich operatorów można zauważyć, że zwiększyła się dzienna liczba unikalnych adresów IP. Należy zwrócić uwagę, że u części operatorów głównie komórkowych adres IP zmienia się bardzo często (częściej, niż raz na dzień, tzw. „Internet mobilny"), przez co liczba dziennych zainfekowanych unikalnych adresów klientów może być zawyżona.

Poz.	Nazwa botnetu	Liczba adresów IP	Udział procentowy
1	Conficker	62 221	22,19%
2	ZeroAccess	32 460	11,57%
3	Zeus (w tym Citadel i pochodne)	25 311	9,03%
4	Sality	14 003	4,99%
5	Zeus GameOver	12 513	4,46%
6	Ircbot	10 768	3,84%
7	Bankpatch	6 086	2,17%
8	Banatrix	5 385	1,92%
9	Virut	4 014	1,43%
10	Kelihos	3 922	1,40%
	Pozostałe	103 750	37,00%

Tabela 2. Największe botnety w Polsce.

Największym botnetem w Polsce (tabela 2) nadal pozostaje Conficker, chociaż jego udział procentowy zmniejszył się o 4,6 punktu procentowego. Na drugim miejscu jest ZeroAccess, który w roku ubiegłym był na pozycji trzeciej. Jednakże jego udział procentowy niewiele się zmienił. Pierwszą trójkę zamyka ZeuS, w skład którego wliczaliśmy Citadel i pochodne. Jego udział procentowy zwiększył się o niecałe 2 punkty procentowe. Należy zanotować, że znacząco zmniejszył się udział procentowy botnetu Sality, który z drugiego miejsca i udziału ok. 14% w 2013 roku spadł na czwarte z udziałem zaledwie ok. 5% rynku w roku ubiegłym.

Conficker i Virut są botnetami, nad którymi przestępcy nie mają kontroli, nie są one zatem aktywne. Conficker jest sinkholowany od 2009r., natomiast Virut od 2013 r. (w sinkholowaniu tego drugiego znaczny udział ma CERT Polska). Ich obecność w tabeli 2 świadczy m.in. o tym, że większość zainfekowanych komputerów pozostaje zarażona złośliwym oprogramowaniem przez lata, nierzadko aż do końca eksploatacji stacji roboczej. Dodatkowo Conficker jest robakiem, który rozprzestrzenia się wykorzystując głównie luki w systemie operacyjnym użytkownika, ale także za pomocą dysków przenośnych. Virut to wirus, co oznacza, że dołącza swój kod do innych plików, przez co trudniej mu się rozprzestrzeniać od Cornfickera. Jednak wciąż zdarzają się przypadki nowych infekcji Virutem w wyniku uruchomienia jednego z zainfekowanych plików, które można ściągnąć z internetowych zasobów od lat.

Wśród dziesięciu największych botnetów w Polsce aż cztery są trojanami bankowymi.

Poz.	Nazwa Botnetu	Liczba adresów IP	Udział procentowy
1	Zeus	25 311	45,80%
2	Zeus Gameover	12 513	22,64%
3	Bankpatch	6 086	11,01%
4	Banatrix	5 385	9,74%
5	Gozi	2 752	4,98%
	Pozostałe	3 218	5,82%

Tabela 3. Dane dotyczące trojanów bankowych.

W tabeli 3 zostały podane botnety, które są zagrożeniem dla klientów bankowości elektronicznej. W większości trojanów bankowych wykorzystywany jest mechanizm modyfikacji strony internetowej na zainfekowanym komputerze, przez co przestępcy mają pełny dostęp do konta ofiary i mogą przelewać środki znajdujące się na nim. Innego sposobu używa Banatrix, zauważony przez CERT Polska w 2013 r., który podmienia numer konta bankowego w pamięci procesu przeglądarki.

Statystyka obsłużonych incydentów

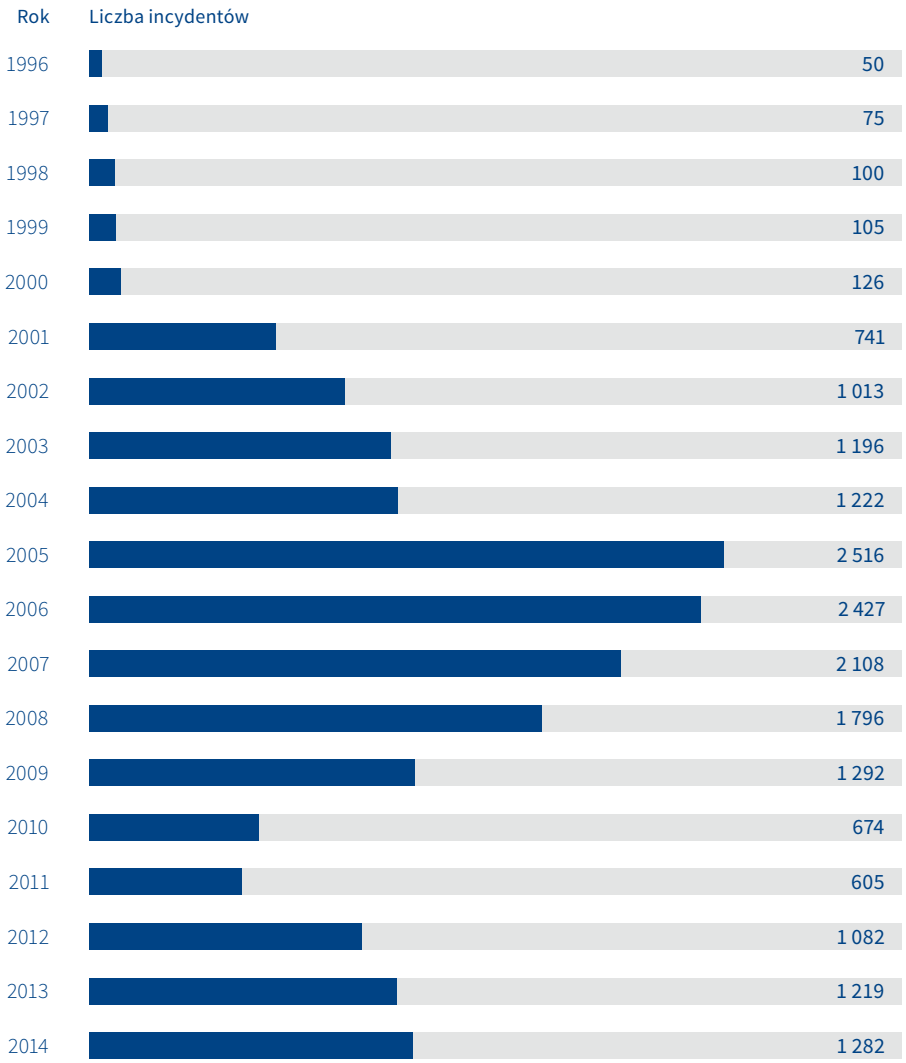
W tej części raportu prezentujemy opracowane przez CERT Polska statystyki otrzymanych przez zespół zgłoszeń, które zostały przez nas obsłużone w sposób nieautomatyczny. Dotyczą one zarówno zgłoszeń ze źródeł zewnętrznych, jak i z własnych wewnętrznych systemów.

W 2014 r. zespół CERT Polska obsłużył ręcznie 1 282 incydenty. Większość z nich dotyczyła oszustw komputerowych (47,28%) oraz obraźliwych i nielegalnych treści (28,86%).

Zgłaszającymi i poszkodowanym były głównie firmy komercyjne (odpowiednio 59,44% oraz 47,11%). Zgłaszający pochodził najczęściej z zagranicy (66,69%), zaś poszkodowany – z Polski (31,59%).

Rodzaj zgłoszenia	Liczba zgłoszeń	Udział procentowy
Obraźliwe i nielegalne treści	370	28,86
Spam	365	28,47
Dyskredytacja, obrażanie	0	0
Pornografia dziecięca, przemoc	2	0,16
Niesklasyfikowane	3	1
Złośliwe oprogramowanie	98	7,64
Wirus	0	0
Robak sieciowy	0	0
Koń trojański	8	0,62
Oprogramowanie szpiegowskie	0	0
Dialer	0	0
Niesklasyfikowane	90	7,02
Gromadzenie informacji	98	7,64
Skanowanie	13	1,01
Podsłuch	0	0
Inżynieria społeczna	0	0
Niesklasyfikowane	5	0,39
Próby włamań	36	2,81
Wykorzystanie znanych luk systemowych	4	0,31
Próby nieuprawnionego logowania	5	0,39
Wykorzystanie nieznanych luk systemowych	1	0,08
Niesklasyfikowane	26	2,03
Włamania	13	1,01
Włamanie na konto uprzywilejowane	1	0,08
Włamanie na konto zwykłe	7	0,55
Włamanie do aplikacji	0	0
Niesklasyfikowane	5	0,39
Dostępność zasobów	69	5,38
Atak blokujący serwis (DoS)	6	0,47
Rozproszony atak blokujący serwis (DDoS)	63	4,91
Sabotaż komputerowy	0	0
Niesklasyfikowane	0	0
Atak na bezpieczeństwo informacji	25	1,95
Nieuprawniony dostęp do informacji	8	0,62
Nieuprawniona zmiana informacji	0	0
Niesklasyfikowane	17	1,95
Oszustwa komputerowe	613	47,82
Nieuprawnione wykorzystanie zasobów	5	0,39
Naruszenie praw autorskich	0	0
Kradzież tożsamości, podszycie się	383	29,88
Niesklasyfikowane	225	17,55
Inne	40	3,12

Tabela 4. Incydenty obsłużone przez CERT Polska według typów.



Rysunek 18. Liczby incydentów obsłużonych ręcznie przez CERT Polska.

W 2014 r. odnotowaliśmy dość dużą liczbę incydentów związanych z phishingiem (29,88%). Należy podkreślić, że były to głównie incydenty dotyczące phishingu umieszczonego na polskich serwerach, bądź phishingu polskich instytucji, znajdującego się na serwerach zagranicznych.

Na przestrzeni całego roku odnotowaliśmy kilka poważnych kampanii atakujących polskich użytkowników bankowości elektronicznej. Najciekawsze były ataki, w których przestępcy w ramach jednej kampani spamowej dystrybuowali nawet do 20-tu różnych adresów URL, na których znajdował się ten sam phishing.

Tak jak w latach poprzednich, w ujęciu ogólnoświatowym skala zjawiska była znacznie większa, niż ta obserwowana przez CERT Polska.

Dość znacznie zmalał odsetek incydentów dotyczących złośliwego oprogramowania, z 26,26% w 2013 roku do 7,64% w roku 2014.

Tak jak to miało już miejsce w latach poprzednich, ewolucja złośliwego oprogramowania wymusiła na nas zmianę podejścia, jeżeli chodzi o tworzenie i klasyfikowanie incydentów. Większość z zanotowanych przez CERT Polska incydentów dotyczyła złośliwego oprogramowania atakującego polskiego użytkownika. Jako jeden incydent traktowano zazwyczaj całą kampanię, identyfikowaną po celu ataku (zazwyczaj określona grupa użytkowników bankowości elektronicznej) oraz umiejscowieniu serwerów C&C i ATS (automatyczny system transakcyjny). W ramach takiej kampanii zgrupowane może być od kilkunastu do kilkudziesięciu zgłoszeń dotyczących tego samego złośliwego oprogramowania.

Nowością w roku 2014 było pojawienie się dużej liczby niesklasyfikowanych oszustw komputerowych (17,55% ogółu). To incydenty, które są powiązane z kampaniami atakującymi użytkowników polskiej bankowości elektronicznej i dotyczą kont słupów wykorzystywanych przez przestępców. Cały proceder jest związany z różnymi rodzajami złośliwego oprogramowania, począwszy od VBKlipa, a kończąc na rzekomych fakturach, powiadomieniach czy dokumentach rozsyłanych w imieniu znanych firm.

Należy zdecydowanie podkreślić, że wzrost działalności ukierunkowanej na użytkowników bankowości internetowej jest według CERT Polska najważniejszym i najbardziej niepokojącym trendem w 2014 r. Zrealizowane zostały wszystkie znane nam do tej pory oraz zupełnie nowe scenariusze zmierzające do kradzieży środków, a wykradzione kwoty niejednokrotnie wynosiły kilkaset tysięcy złotych.

Serwery C&C

Dziennie otrzymywaliśmy średnio 147 zgłoszeń dotyczących nowych adresów IP i nazw domenowych używanych jako serwery C&C. Natomiast w ciągu całego roku otrzymaliśmy informacje o 8 304 unikalnych adresach IP oraz 7 647 unikalnych nazwach domenowych (z ang. FQDN – *Fully Qualified Domain Name*) używanych jako serwery zarządzające botnetami (C&C).

Z uwagi na charakter 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.

Adresy IP

Otrzymaliśmy zgłoszenia dotyczące adresów IP ze 104 krajów. Podobnie jak w poprzednich latach najwięcej złośliwych serwerów było umieszczonych w Stanach Zjednoczonych (prawie 29%). Ponad 70% spośród wszystkich serwerów C&C hostowane jest w 10 krajach, przedstawionych w tabeli 5.

Poz.	Kraj	Liczba IP	Udział
1	Stany Zjednoczone	2 397	28,7%
2	Ukraina	706	8,5%
3	Niemcy	629	7,6%
4	Rosja	603	7,3%
5	Holandia	319	3,8%
6	Francja	296	3,6%
7	Wielka Brytania	249	3,0%
8	Urugwaj	242	2,9%
9	Kanada	236	2,8%
10	Grecja	204	2,5%
...	...	...	...
16	Polska	76	0,9%

Tabela 5. Kraje, w których hostowanych jest najwięcej serwerów C&C.

Zaobserwowaliśmy 1 626 różnych systemów autonomicznych, w których umiejscowione były serwery C&C. Prawie 1/5 wszystkich złośliwych serwerów zlokalizowana było wśród 10 AS-ów.

Poz.	Numer AS	Nazwa AS	Liczba IP	Udział
1	16276	OVH Systems	332	4,0%
2	6057	Administracion Nacional de Telecomunicaciones	242	2,9%
3	3320	Deutsche Telekom AG	168	2,0%
4	24940	Hetzner Online AG	167	2,0%
5	6799	Ote SA (Hellenic Telecommunications Organisation)	160	1,9%
6	13335	CloudFlare, Inc.	137	1,6%
7	36351	SoftLayer Technologies Inc.	124	1,5%
8	26496	GoDaddy.com, LLC	102	1,2%
9	15895	„Kyivstar” PJSC	100	1,2%
10	47583	Hostinger International Limited	98	1,2%

Tabela 6. Systemy autonomiczne, w których hostowane jest najwięcej C&C.

W Polsce serwery C&C znajdowały się na 76 różnych adresach IP (16 miejsce na świecie z 0,9% udziałem) w 36 systemach autonomicznych. W tabeli 7 prezentujemy zestawienie 14 systemów autonomicznych, w jakich znajdowało się najwięcej serwerów zarządzających botnetami (68% wszystkich złośliwych serwerów w Polsce).

Poz.	Numer AS	Nazwa AS	Liczba IP	Udział
1	59491	Livenet Sp. z o.o.	10	13,2%
1	51290	HOSTEAM S.C.	10	13,2%
3	12824	home.pl sp.z.o.o. 5 6,6%	5	6,6%
3	198540	Przedsiebiorstwo Uslug Specjalistycznych ELAN mgr inz. Andrzej Niechcial	5	6,6%
5	15967	nazwa.pl S.A.	4	5,3%
6	49792	IONICPLAS	2	2,6%
6	15694	ATM S.A.	2	2,6%
6	43939	Internetia Sp.z o.o.	2	2,6%
6	12618	PLBYDMANCOM	2	2,6%
6	42154	„EuroNet” s.c. Jacek Majak, Aleksandra Kuc	2	2,6%
6	6714	GTS Poland Sp. z o.o.	2	2,6%
6	198414	BiznesHost.pl sp. z o.o.	2	2,6%
6	5617	Orange Polska Spolka Akcyjna	2	2,6%
6	197226	„SPRINT”	2	2,6%

Tabela 7. Systemy autonomiczne, w których hostowanych jest najwięcej serwerów C&C w Polsce.

Nazwy domenowe

Otrzymaliśmy również zgłoszenia o 7 647 pełnych nazwach domenowych (FQDN), które pełniły rolę serwerów zarządzających botnetami. Zostały one zarejestrowane w obrębie 137 domen pierwszego poziomu (Top Level Domain), prawie 30% w .com.

Poz.	TLD	Liczba domen	Udział
1	.com	2241	29,3%
2	.net	1 058	13,8%
3	.org	590	7,7%
4	.info	532	7,0%
5	.ru	357	4,7%
6	.de	249	3,3%
7	.biz	237	3,1%
8	.su	198	2,6%
9	.in	186	2,4%
10	.br	152	2,0%

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

Złośliwe strony

Otrzymaliśmy 21 231 896 zgłoszeń o unikalnych złośliwych adresach URL. Z tego 593 136 zgłoszeń dotyczyło unikalnych adresów URL w domenie .pl.

Opracowanie danych dotyczących domeny .pl

Dziennie otrzymywaliśmy informację średnio o 1 625 złośliwych adresach internetowych w domenie .pl.

Poz.	Unikalnych adresów URL	Nazwa domenowa
1	46 942	mattfoll.eu.interiowo.pl
2	12 832	premiumfilmy.pl
3	7 707	interiowo.pl
4	5 639	bialydom.pl
5	5 325	static.sd.softonic.pl
6	5 105	aanna74.eu.interiowo.pl
7	4 904	prywatneznajomosci.cba.pl
8	4 630	polityczni.pl
9	4 521	gim8.pl
10	4 053	meczyk.pl

Tabela 9. Pełne nazwy domenowe, na których było najwięcej unikalnych adresów URL.

W tabeli 9 znajdują się pełne nazwy domenowe, na których, według otrzymanych przez nas informacji, znajduje się najwięcej złośliwych adresów URL w domenie .pl.

Poz.	Liczba unikalnych adresów URL	Adres IP	Numer AS	Nazwa AS
1	57 393	217.74.66.183	AS16138	INTERIA.PL Sp z.o.o.
2	44 722	217.74.65.161	AS16138	INTERIA.PL Sp z.o.o.
3	21 799	217.74.65.163	AS16138	INTERIA.PL Sp z.o.o.
4	11 950	193.203.99.113	AS47303	Redefine Sp. z o.o.
5	8 973	46.41.144.24	AS12824	home.pl sp. z o.o.
6	8 737	193.203.99.114	AS47303	Redefine Sp. z o.o.
7	8 438	95.211.144.89	AS16265	LeaseWeb B.V.
8	7 378	217.74.65.162	AS16138	INTERIA.PL Sp z.o.o.
9	6 101	85.17.73.180	AS16265	LeaseWeb B.V.
10	5 569	37.59.49.187	AS16276	OVH SAS

Tabela 10. Adresy IP, na których znajduje się najwięcej złośliwych adresów URL.

W tabeli 10 znajdują się adresy IP, na których znalazło się najwięcej złośliwych adresów URL. Podobnie jak w 2013 r. w czołówce znalazł się hosting Interii. Natomiast w tabeli 3 zaprezentowane są systemy autonomiczne, w których było najwięcej złośliwych adresów URL. W czołówce jest nadal home.pl, OVH, Onet oraz Interia. W tabeli nr 2 nie ma adresu 148.81.111.99 należącego do puli adresów przeznaczonych do wykorzystania przez sinkhole'a stworzonego i utrzymywanego przez CERT Polska.

Poz.	Liczba unikalnych adresów URL	Numer AS	Nazwa AS
1	132 170	16138	INTERIA.PL Sp z.o.o.
2	89 178	12824	home.pl sp. z o.o.
3	31 244	16276	OVH SAS
4	27 061	47303	Redefine Sp. z o.o.
5	23 510	16265	LeaseWeb B.V.
6	23 497	15967	Netia SA
7	18 499	24940	Hetzner Online AG
8	9 694	29522	Krakowskie e-Centrum Informatyczne JUMP
9	8 869	12741	Netia SA
10	7 098	12990	Grupa Onet.pl S.A.

Tabela 11. Systemy autonomiczne, w których znajduje się najwięcej złośliwych adresów URL.

Podobnie w tabeli 11 na 10 miejscu znajdował się pierwotnie AS1887, należący do NASK. Został on z niej usunięty ze względu na dużą liczbę złośliwych adresów wynikającą ze znajdującego się w tym systemie autonomicznym sinkhole'a CERT Polska. W tabeli 4 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 analogicznego zestawienia w 2013 r.

Poz.	Liczba unikalnych adresów URL	Kraj
1	404 364	Polska
2	27 484	Niemcy
3	21 459	Holandia
4	19 242	Francja
5	7 169	Stany Zjednoczone
6	5 395	Hiszpania
7	1 683	Wielka Brytania
8	786	Kanada
9	353	Czechy
10	289	Rosja

Tabela 12. Kraje, w których hostowano najwięcej złośliwych adresów URL z domeny .pl.

Opracowanie danych globalnych

Dziennie otrzymywaliśmy średnio informację o 58 169 złośliwych adresach internetowych.

W tabeli 13 znajdują się pełne nazwy domenowe, na których, według otrzymanych przez nas informacji, znajduje się najwięcej złośliwych adresów URL.

Poz.	Unikalnych adresów URL	Nazwa domenowa
1	223 473	hao.ie768.com
2	172 607	download.goobzo.com
3	163 088	www.horizoncardservices.com
4	152 444	down.llrx.org
5	146 734	dde.de.drivefilesb.com
6	110 637	s1.upgrade.mkjogo.com
7	107 273	www.iblowjob.com
8	100 320	dc589.2shared.com
9	98 524	esd.nzs.com.br
10	86 000	kyle.mxp4037.com

Tabela 13. Pełne nazwy domenowe, na których było najwięcej unikalnych adresów URL.

Poz.	Unikalnych adresów URL	Adres IP	Numer AS	Nazwa AS	Kraj
1	294 226	222.186.60.12	23650	CHINANET jiangsu province backbone	Chiny
2	290 889	222.186.60.2	23650	CHINANET jiangsu province backbone	Chiny
3	237 944	222.186.60.44	23650	CHINANET jiangsu province backbone	Chiny
4	202 698	123.150.206.130	17638	ASN for TIANJIN Provincial Net of CT	Chiny
5	200 426	118.121.252.162	4134	Chinanet	Chiny
6	190 026	5.135.246.48	16276	OVH Systems	Francja
7	172 763	107.20.238.80	14618	Amazon.com, Inc.	Stany Zjednoczone
8	163 088	67.192.100.25	33070	Rackspace Hosting	Stany Zjednoczone
9	143 243	115.29.226.120	37963	Alibaba (China) Technology Co., Ltd.	Chiny
10	141 740	103.249.72.30	132827	GATEWAY-AS-AP GATEWAY INC,JP	Japonia

Tabela 14. Adresy IP, na których znajduje się najwięcej złośliwych adresów URL.

W tabeli 14 znajdują się adresy IP, na których znalazło się najwięcej złośliwych adresów URL. Wszystkie adresy z pierwszej piątki zlokalizowane są w Chinach. Natomiast w tabeli 15 zaprezentowane są systemy autonomiczne, w których było najwięcej złośliwych adresów URL. W czołówce znajdują się największe firmy hostingowe świata: Amazon i OVH. Na trzecim miejscu sklasyfikowany został chiński system autonomiczny China Telecom Backnobe.

Poz.	Liczba unikalnych adresów URL	Numer AS	Nazwa AS
1	1 504 917	AS16509	Amazon.com, Inc.
2	1 412 769	AS16276	OVH SAS
3	1 125 198	AS4134	China Telecom Backbone
4	1 022 558	AS23650	CHINANET jiangsu province backbone
5	876 696	AS14618	Amazon.com, Inc.
6	736 794	AS20940	Akamai International B.V.
7	580 083	AS37963	Hangzhou Alibaba Advertising Co..Ltd.
8	511 871	AS26496	GoDaddy.com, LLC
9	486 203	AS15169	Google Inc.
10	430 375	AS46606	Unified Layer

Tabela 15. Systemy autonomiczne, w których znajduje się najwięcej złośliwych adresów URL.

Poz.	Liczba unikalnych adresów URL	Kraj
1	8 493 123	Stany Zjednoczone
2	3 503 922	Chiny
3	1 332 016	Francja
4	1 023 746	Niemcy
5	747 611	Holandia
6	719 451	Europa
7	620 753	Rosja
8	528 220	Polska
9	417 986	Hong Kong
10	383 700	Wielka Brytania

Tabela 16. Kraje, w których hostowano najwięcej złośliwych adresów URL.

W tabeli 16 znajdują się kraje, w których hostowano najwięcej złośliwych adresów URL. Niechlubne czołowe miejsca zajmują państwa, w których zlokalizowane są największe hostownie, sklasyfikowane w tabeli 12. Zajmująca 6 miejsce w tabeli „Europa" dotyczy systemów autonomicznych, dla których nie można jednoznacznie ustalić kraju, ze względu np. na prowadzoną działalność w wielu krajach europejskich.

Poz.	Liczba unikalnych adresów URL	TLD
1	11 390 264	.com
2	1 763 566	.net
3	1 100 521	.org
4	1 011 063	.ru
5	593 136	.pl
6	570 705	.info
7	368 501	.br
8	361 077	.biz
9	324 013	.de
10	314 480	.cn

Tabela 17. Domeny najwyższego poziomu, w których hostowano najwięcej złośliwych adresów URL.

W tabeli 17 przedstawiamy 10 najpopularniejszych domen najwyższego poziomu, w których hostowano złośliwe URL-e. Na 5 miejscu znalazła się domena .pl, ale oczywiście wynika to z charakteru danych źródłowych, skupionych w większości na dostarczaniu informacji o domenie .pl lub stronach hostowanych w Polsce.

Phishing

W sekcji tej uwzględniamy wyłącznie statystyki dotyczące phishingu w tradycyjnym rozumieniu tego słowa, to jest podszywania się (przede wszystkim z wykorzystaniem poczty elektronicznej i stron WWW) pod znane marki celem wyłudzenia wrażliwych danych i/lub korzyści finansowych. Nie odnosimy się tu więc choćby do masowo obserwowanych w ubiegłym roku fałszywych faktur, których celem było nakłonienie użytkownika do otwarcia zainfekowanego załącznika. O zjawisku tym piszemy na s.12.

Statystyki dotyczą stron hostowanych w Polsce, a więc nie uwzględniają phishingów polskich instytucji, które hostowane były za granicą, na przykład kampanie kierowane w ubiegłym roku na klientów PKO BP czy mBanku, o których piszemy na s.12.

W 2014 r. obsłużyliśmy 85893 zgłoszenia phishingu w polskich sieciach, dotyczące 18 775 adresów URL w 4 862 domenach, na 1 989 adresach IP. a podstawie liczby domen i adresów IP można wnioskować o niewielkim ilościowym wzroście problemu względem roku 2013.

Ze względu na zmianę modelu otrzymywania zgłoszeń dotyczących m.in. phishingu – znaczna część z nich pobierana jest automatycznie z różnych źródeł z zadaną częstotliwością, a nie przesyłana przez stronę zewnętrzną – nie podajemy w statystykach „surowej" liczby zgłoszeń dla każdego systemu autonomicznego. Byłaby ona bowiem zdeterminowana przede wszystkim częstotliwością odpytywania zewnętrznych źródeł. Jako przybliżenie tej podawanej w ubiegłych latach wartości, podajemy liczbę „adresodni", czyli iloczyn liczby adresów IP hostujących phishing i liczby dni, przez które były aktywne.

Poz.	Numer AS	Nazwa AS	Liczba IP	Liczba URL	Adresodni
1	12824	home.pl sp. z o.o.	700	8 928	13906
2	15967	nazwa.pl S.A. (d.NetArt)	295	2 828	1891
3	59491	Livenet Sp. z o.o.	82	1 103	412
4	43333	CIS NEPHAX	61	386	985
5	29522	Krakowskie eCentrum Informatyczne JUMP	58	174	974
6	198414	BiznesHost.pl	50	235	358
7	16276	OVH	45	355	955
8	15694	ATM S.A.	45	136	619
9	41079	SuperHost.pl sp. z o.o.	38	740	1796
10	5617	Orange Polska S.A.	35	110	239

Tabela 18. Polskie systemy autonomiczne, w których znajdowało się najwięcej stron phishingowych.

Na liście sieci, w których najczęściej znajdował się phishing nie ma istotnych zmian – zdecydowanymi liderami pozostają największe polskie hostownie czyli home.pl oraz nazwa.pl (dawniej NetArt). Na dalszych pozycjach nastąpiły niewielkie przetasowania, lecz różnice w liczbie adresów IP, których dotyczył problem są nieznaczne.

Poz.	Cel	Liczba przypadków
1	PayPal	1456
2	Steam	111
3	AOL	48
4	Apple	43
5	Itau	42
6	eBay	36
7	Capitec Bank	36
8	Internal Revenue Service	20
9	Allegro	16
10	Bradesco	15
11	NatWest Bank	12
12	Visa	11
13	Poste Italiane	11
14	Cielo	10
15	Wells Fargo	9
	inne banki	50

Tabela 19. Cele ataków phishingowych.

Wiele nowości znalazło się za to wśród głównych „celów" phishingu hostowanego w Polsce. Choć dominującą marką pozostaje zdecydowanie PayPal, wysoko zadebiutował serwis Steam, a także wyraźniej zaznaczona została pozycja banków. W pierwszej dziesiątce pojawił się serwis Allegro (16 przypadków). Poza tabelą znalazła się inna polska marka – PKO BP (2 przypadki hostowane w Polsce). Co ciekawe, Google i Amazon także wypadły poza pierwszą piętnastkę, notując odpowiednio 8 i 6 przypadków. Ciekawym trendem jest też rosnące zainteresowanie serwisami administracji skarbowej – amerykański IRS zadebiutował na 8 miejscu z 20 przypadkami, natomiast poza pierwszą piętnastką znalazły się także urzędy: południowoafrykański i brytyjski (po 2 przypadki).

Błędnie skonfigurowane serwery i usługi w Polsce

W 2014 r. otrzymaliśmy zgłoszenia dotyczące 3 440 981 unikalnych adresów IP, na których znajdowały się błędnie skonfigurowane serwery i usługi w Polsce. Dla każdego protokołu wybraliśmy 10 systemów autonomicznych, w których zaobserwowaliśmy najwięcej unikalnych adresów IP związanych z podatnymi protokołami. W tabelach znajduje się także zestawienie liczby unikalnych adresów IP widzianych w ciągu roku w stosunku do liczby IP w danym systemie autonomicznym, oraz udział liczby unikalnych adresów IP pochodzących z danego systemu autonomicznego w sumie wszystkich otrzymanych zgłoszeń.

Chargen

Otrzymaliśmy 18 997 zgłoszeń o unikalnych adresach IP.

Poz.	Liczba unikalnych adresów URL	Numer AS	Nazwa AS	% sieci	Udział
1	12 727	5617	Orange Polska Spolka Akcyjna	0,23%	66,99%
2	1 536	12741	Netia SA	0,10%	8,09%
3	1 432	8374	Polkomtel Sp. z o.o.	0,11%	7,54%
4	1 045	12912	T-MOBILE POLSKA S.A.	0,15%	5,50%
5	653	29314	VECTRA S.A.	0,12%	3,44%
6	308	6830	Liberty Global Operations B.V.	0,01%	1,62%
7	72	39375	Telekomunikacja Podlasie Sp. z o.o.	0,26%	0,38%
8	62	8477	ZTS Echostar Studio Poznan Poland	0,09%	0,33%
9	41	30838	Jerzy Krempa „Telpol” PPMUE	0,16%	0,22%
9	41	41809	Enterpol	0,33%	0,22%

Tabela 20. Polskie systemy autonomiczne, w których znajdowało się najwięcej otwartych serwerów CharGen.

DNS

Otrzymaliśmy 2 226 699 zgłoszeń o unikalnych adresach IP. Na szczególną uwagę zasługuje system autonomiczny Spółdzielnia Telekomunikacyjna OST, w którym prawie 2/3 wszystkich adresów IP służyło jako otwarty serwer DNS.

Poz.	Liczba unikalnych adresów URL	Numer AS	Nazwa AS	% sieci	Udział
1	1 752 713	5617	Orange Polska Spolka Akcyjna	31,80%	77,32%
2	230 243	12741	Netia SA	15,73%	10,16%
3	77 559	21021	Multimedia Polska S.A.	13,08%	3,42%
4	25 139	12912	T-MOBILE POLSKA S.A.	3,70%	1,11%
5	18 256	29314	VECTRA S.A.	3,46%	0,81%
6	13 632	6714	GTS Poland Sp. z o.o.	3,77%	0,60%
7	10 659	6830	Liberty Global Operations B.V.	0,11%	0,47%
8	7 099	38987	Spółdzielnia Telekomunikacyjna OST	63,02%	0,31 %
9	6 770	20960	TK Telekom sp. z o.o.	2,72%	0,30%
10	5 324	13000	Leon sp. z o.o.	10,83%	0,23%

Tabela 21. Polskie systemy autonomiczne, w których znajdowało się najwięcej otwartych serwerów DNS.

Netbios

Otrzymaliśmy 186 101 zgłoszeń o unikalnych adresach IP. Decyzja Orange o blokowaniu w kierunku do klienta portu 137/UDP, na którym słucha protokół Netbios, przyczyniła się do spadku Orange w porównaniu z 2013 r. na 3 miejsce.

Poz.	Liczba unikalnych adresów URL	Numer AS	Nazwa AS	% sieci	Udział
1	69 492	12741	Netia SA	4,75%	37,34%
2	41 095	21021	Multimedia Polska S.A.	6,93%	22,08%
3	20 937	5617	Orange Polska Spolka Akcyjna	0,38%	11,25%
4	5 021	12912	T-MOBILE POLSKA S.A.	0,74%	2,70%
5	4 253	13110	INEA S.A.	2,61%	2,29%
6	2 631	5550	Technical University of Gdansk, Academic Computer Center TASK	4,01%	1,41%
7	2 215	8970	WROCMAN-EDU	3,38%	1,19%
8	2 071	6714	GTS Poland Sp. z o.o.	0,57%	1,11%
9	1 825	8374	Polkomtel Sp. z o.o.	0,14%	0,98%
10	1 719	198414	Biznes-Host.pl sp. z o.o.	20,35%	0,92%

Tabela 22. Polskie systemy autonomiczne, w których znajdowało się najwięcej otwartych serwerów Netbios.

NTP

Otrzymaliśmy 278 484 zgłoszeń o unikalnych adresach IP.

Poz.	Liczba unikalnych adresów URL	Numer AS	Nazwa AS	% sieci	Udział
1	219 430	5617	Orange Polska Spolka Akcyjna	3,98%	78,79%
2	21 143	12741	Netia SA	1,44%	7,59%
3	4 147	6714	GTS Poland Sp. z o.o.	1,15%	1,49%
4	3 158	21021	Multimedia Polska S.A.	0,53%	1,13%
5	1 932	12912	T-MOBILE POLSKA S.A.	0,28%	0,69%
6	1 656	13110	INEA S.A.	1,02%	0,59%
7	1 334	20804	Exatel S.A.	0,71%	0,48%
8	1 143	15997	ITSA	3,49%	0,41%
9	1 106	8374	Polkomtel Sp. z o.o	0,08%	0,40%
10	874	31229	E24 sp. z o.o.	3,45%	0,31%

Tabela 23. Polskie systemy autonomiczne, w których znajdowało się najwięcej otwartych serwerów NTP.

QOTD

Otrzymaliśmy 21 993 zgłoszeń o unikalnych adresach IP.

Poz.	Liczba unikalnych adresów URL	Numer AS	Nazwa AS	% sieci	Udział
1	14 193	5617	Orange Polska Spolka Akcyjna	0,26%	64,53%
2	2 296	12741	Netia SA	0,16%	10,44%
3	1 484	8374	Polkomtel Sp. z o.o.	0,11%	6,75%
4	1 126	29314	VECTRA S.A.	0,21%	5,12%
5	1 045	12912	T-MOBILE POLSKA S.A.	0,15%	4,75%
6	450	6830	Liberty Global Operations B.V.	0,01%	2,05%
7	119	41809	Enterpol	0,97%	0,54%
8	79	39375	Telekomunikacja Podlasie Sp. z o.o.	0,28%	0,36%
9	68	56575	TepsaNet Stanislaw Nowacki	3,32%	0,31%
10	55	13110	INEA S.A.	0,03%	0,25%

Tabela 24. Polskie systemy autonomiczne, w których znajdowało się najwięcej otwartych serwerów QOTD.

SNMP

Otrzymaliśmy 2 325 483 zgłoszeń o unikalnych adresach IP. Podobnie jak w przypadku statystyk otwartych serwerów DNS, 2/3 adresów IP systemu autonomicznego Spółdzielnia Telekomunikacyjna OST odpowiada na komunikację opartą o protokół SNMPv2.

Poz.	Liczba unikalnych adresów URL	Numer AS	Nazwa AS	% sieci	Udział
1	1 718 526	5617	Orange Polska Spolka Akcyjna	31,18%	73,90%
2	498 100	12741	Netia SA	34,03%	21,42%
3	33 046	12912	T-MOBILE POLSKA S.A.	4,86%	1,42%
4	23 401	6714	GTS Poland Sp. z o.o.	6,46%	1,01%
5	7 587	38987	Spółdzielnia Telekomunikacyjna OST	67,36%	0,33%
6	6 609	29007	Petrotel Sp. z o.o.	40,34%	0,28%
7	3 371	6830	Liberty Global Operations B.V.	0,04%	0,14%
8	3 352	20960	TK Telekom sp. z o.o.	1,35%	0,14%
9	2 826	29314	VECTRA S.A.	0,53%	0,12%
10	1 630	24709	MNI Telecom S.A. IP Backbone	3,64%	0,07%

Tabela 25. Polskie systemy autonomiczne, w których znajdowało się najwięcej otwartych serwerów SNMP.

SSDP

Otrzymaliśmy 2 562 309 zgłoszeń o unikalnych adresach IP. SSDP jest protokołem, o którym dostaliśmy najwięcej zgłoszeń w kategorii błędnie skonfigurowanych serwerów i usług. Systemem autonomicznym o największej liczbie adresów IP z uruchomioną usługą SSDP w stosunku do liczby wszystkich adresów IP w systemie autonomicznym jest Spółdzielnia Telekomunikacyjna OST. Wysokie miejsce zajął też system autonomiczny Petrotel Sp. z o.o.

Poz.	Liczba unikalnych adresów URL	Numer AS	Nazwa AS	% sieci	Udział
1	1 751 912	5617	Orange Polska Spolka Akcyjna	31,79%	68,37%
2	371 063	12741	Netia SA	25,35%	14,48%
3	195 854	21021	Multimedia Polska S.A.	33,02%	7,64%
4	68 820	29314	VECTRA S.A.	13,02%	2,69%
5	30 596	12912	T-MOBILE POLSKA S.A.	4,50%	1,19%
6	20 302	6830	Liberty Global Operations B.V.	0,21%	0,79%
7	16 060	6714	GTS Poland Sp. z o.o.	4,44%	0,63%
8	8 209	38987	Spółdzielnia Telekomunikacyjna OST	72,88%	0,32%
9	7 393	29007	Petrotel Sp. z o.o.	45,12%	0,29%
10	5 129	31304	Espol Sp. z o.o.	23,85%	0,20%

Tabela 26. Polskie systemy autonomiczne, w których znajdowało się najwięcej otwartych serwerów SSDP.

Skanowanie

Kategoria skanowanie opisuje przypadki wykrytych prób nieautoryzowanych połączeń. Mogą one świadczyć o infekcji komputera, z którego zostało zainicjowane połączenie, o tym, że nastąpiło włamanie i przejęcie kontroli nad komputerem lub być świadomym złośliwym działaniem użytkownika. Wszystkie zgłoszenia ujęte w poniższych statystykach były przekazane automatycznie. W zestawieniu ujęto dane przysyłane przez naszych partnerów oraz pochodzące z naszych własnych systemów monitoringu. Dane te trafiają do systemu n6 – platformy służącej do gromadzenia, przetwarzania i przekazywania informacji o zdarzeniach dotyczących bezpieczeństwa w sieci.

W roku 2014 otrzymaliśmy zgłoszenia dotyczące 876 970 unikalnych adresów IP (więcej o 45,5 tysiąca niż w roku 2013), z których odbywało się skanowanie usług sieciowych. Adresy te pochodziły z 217 krajów. Z samych polskich sieci zanotowaliśmy 107 141 unikalnych adresów IP.

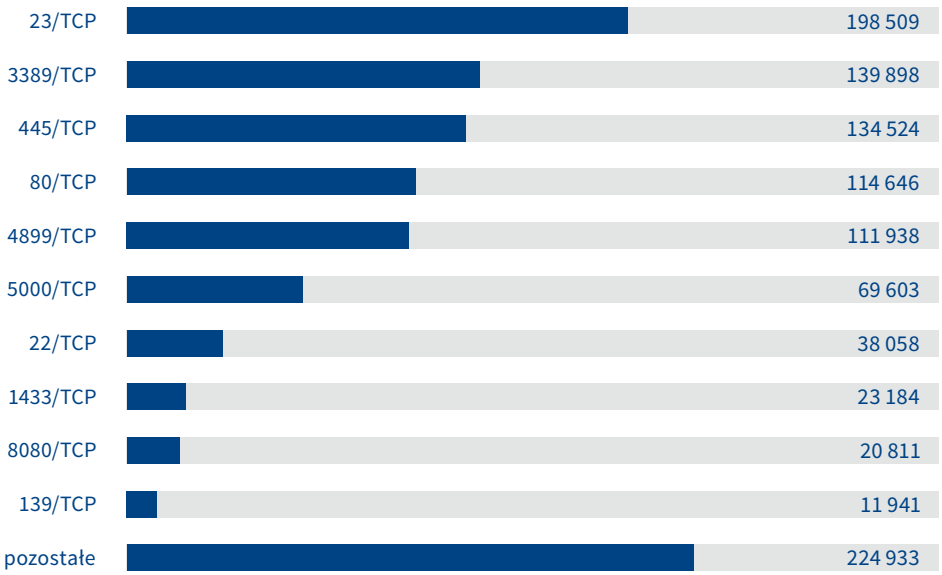
Ze względu na naturę otrzymywanych przez nas danych – niektóre pochodzą z naszych własnych źródeł (wówczas celem jest adres IP znajdujący się w Polsce), podczas gdy inne pochodzą z zewnętrznych źródeł (wówczas skanującym jest komputer z polskiej sieci), postanowiliśmy podzielić te statystyki na trzy części – skanowane usługi, gdzie nie ma znaczenia, jaki kraj jest źródłem ataku ani do jakiej sieci należy docelowy adres IP; skanowania dotyczące Polski; oraz skanowania dotyczące zagranicy.

Skanowane usługi

W minionym roku najczęściej skanowanym portem był 23/TCP, na którym stoi usługa telnet. Jest to duża zmiana w stosunku do roku ubiegłego – liczba unikalnych źródłowych adresów IP wzrosła z niespełna 65 tysięcy do prawie 200 tysięcy. Znaczny wzrost aktywności – choć bez zmiany pozycji w rankingu – zanotowano także na porcie 80/TCP (serwery WWW, głównie aplikacje internetowe), gdzie liczba unikalnych źródłowych adresów IP wzrosła o ponad 60% w stosunku do roku 2013. Największy spadek skanowań – prawie o połowę – nastąpił dla windowsowej usługi RPC (port 445/TCP), oraz – o ponad połowę – dla również windowsowej aplikacji bazodanowej MS SQL. W tabeli 27 i na rysunku 19 znajduje się 10 najczęściej skanowanych portów.

Poz.	Port docelowy	Liczba IP	Udział	Usługa
1	23/TCP	198 509	18,2 %	telnet
2	3389/TCP	139 898	12,9 %	RDP (zdalny pulpit)
3	445/TCP	134 524	12,4 %	Windows RPC
4	80/TCP	114 646	10,5 %	Serwery WWW i aplikacje internetowe
5	4899/TCP	111 938	10,3 %	Radmin
6	5000/TCP	69 603	6,4 %	Różne
7	22/TCP	38 058	3,5 %	SSH
8	1433/TCP	23 184	2,1 %	MS SQL
9	8080/TCP	20 811	1,9 %	Proxy i cache dla serwerów WWW
10	139/TCP	11 941	1,1 %	NetBIOS, współdzielenie plików i
	pozostałe	224 933	20,7 %	drukarek

Tabela 27. Najczęściej skanowane porty.



Rysunek 19. Najczęściej skanowane porty.

Reguły Snort

Reguły Snort są używane do identyfikacji ataków. W tabeli 28 zaprezentowano 10 najczęściej dopasowywanych reguł widzianych podczas skanowania przez system ARAKIS.

Poz.	Reguła Snort	Liczba IP	Udział	Port docelowy
1	RDP connection request	131 256	21,21 %	3389/TCP
2	MS Terminal server request	130 943	21,16 %	3389/TCP
3	Radmin Remote Control Session Setup Initiate	110 297	17,82 %	Głównie 4899/TCP
4	WEB-IIS view source via translate header	70 034	11,32 %	80/TCP
5	Potential SSH Scan	23 232	3,75 %	22/TCP
6	Suspicious inbound to MSSQL port 1433	23 032	3,72 %	1433/TCP
7	RDP disconnect request	16 097	2,60 %	3389/TCP
8	LibSSH Based SSH Connection – Often used as a BruteForce Tool	15 541	2,51 %	22/TCP
9	Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection	10 403	1,68 %	3389/TCP
10	Suspicious inbound to mySQL port 3306	6 317	1,02 %	3306/TCP
	pozostałe:	81 739	13,21 %	—

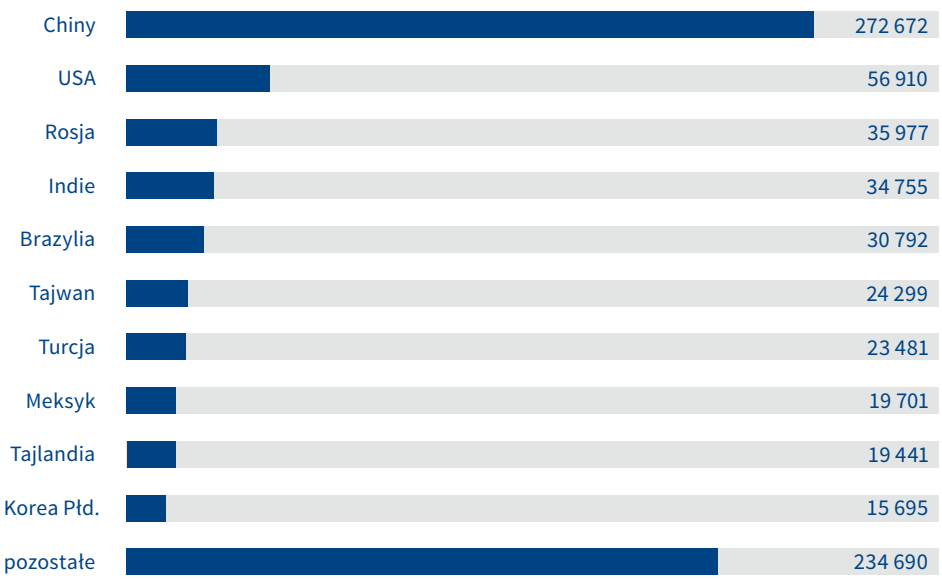
Tabela 28. Najczęstsze reguły Snort zebrane z systemu ARAKIS.

Zagraniczne sieci

Skanowania z zagranicznych adresów w ponad 1/3 pochodziły z Chin. Pozostałe kraje miały znacznie mniejszy udział w skanowaniach, lecz pierwsza trójka pozostaje bez zmian w stosunku do 2013 r. Dziesięć najbardziej aktywnych krajów zaprezentowanych jest w tabeli 29 oraz na rysunku 20.

Poz.	Kraj	Liczba IP	Udział
1	Chiny	272 672	35,5%
2	USA	56 910	7,4%
3	Rosja	35 977	4,7%
4	Indie	34 755	4,5%
5	Brazylia	30 792	4,0%
6	Tajwan	24 299	3,2%
7	Turcja	23 481	3,1%
8	Meksyk	19 701	2,6%
9	Tajlandia	19 441	2,5%
10	Korea Płd	15 695	2,0%
	pozostałe:	234 690	30,5%

Tabela 29. Kraje, z których pochodziło najwięcej skanowań (z wyłączeniem Polski).



Rysunek 20. Kraje, z których pochodziło najwięcej skanowań (z wyłączeniem Polski).

W tabeli 30 zaprezentowano systemy autonomiczne, z których pochodziło najwięcej skanowań. Pierwszy system autonomiczny – China Telecom Backbone – wystąpił ponad cztery razy częściej niż kolejny w zestawieniu, pochodzący również z Chin. W pierwszej dziesiątce znalazł się jeszcze trzeci dostawca z tego kraju. Ciekawostką jest fakt, że nie występuje żadna sieć autonomiczna z USA, a ten kraj był na drugim miejscu w rankingu krajów. Wynika to najprawdopodobniej z tego, że w USA istnieje bardzo dużo dostawców posiadających własne numery AS, które są stosunkowo małe. W Chinach ma miejsce odwrotne zjawisko, gdzie istnieją duże państwowe sieci.

Poz.	Numer AS	Nazwa AS	Kraj	Liczba IP	Udział
1	4134	China Telecom Backbone	Chiny	184 592	23,32%
2	4837	China Unicom Backbone	Chiny	43 534	5,50%
3	9121	Turk Telekomunikasyon Anonim Sirketi	Turcja	18 698	2,36%
4	3462	Data Communication Business Group	Tajwan	18 696	2,36%
5	8151	Uninet S.A. de C.V.	Meksyk	15 823	2,00%
6	9829	BSNL (Bharat Sanchar Nigam Ltd)	Indie	15 759	1,99%
7	18881	Global Village Telecom	Brazylia	7 952	1,00%
8	4766	Korea Telecom	Korea Płd.	7 082	0,89%
9	4812	Shanghai Telecom	Chiny	6 992	0,88%
10	17552	True Internet Co.,Ltd.	Tajlandia	6 716	0,85%
	pozostałe:			465 791	58,84%

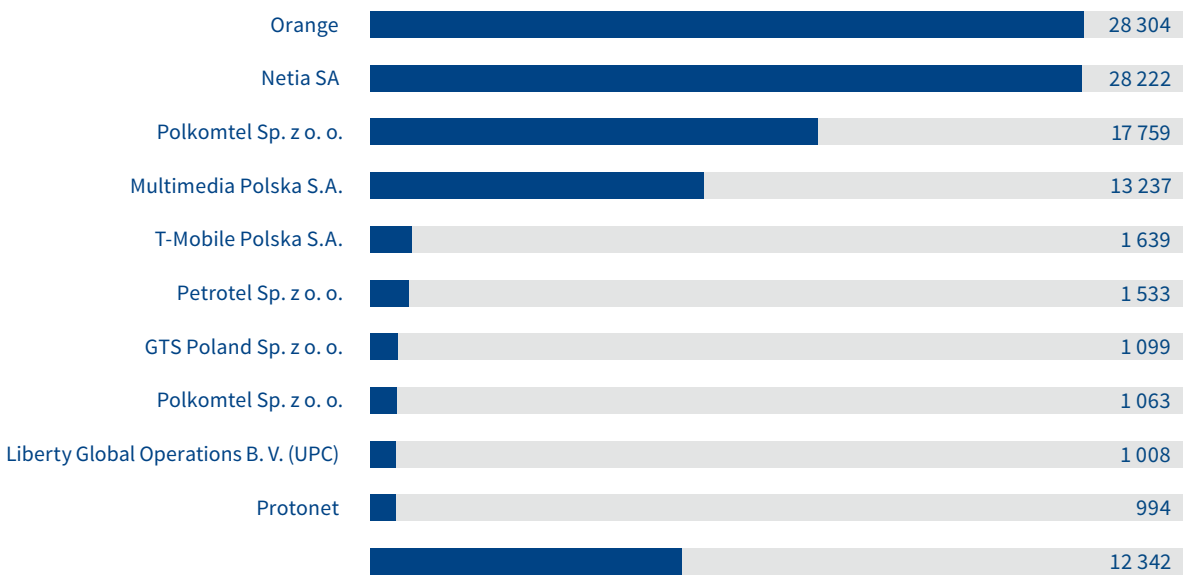
Tabela 30. Zagraniczne systemy autonomiczne, z których pochodziło najwięcej skanowań.

Polskie sieci

W ubiegłym roku nastąpiła zmiana na niechlubnej pozycji lidera, którego tytuł należał przez ostatnie lata do Netii. Najwięcej zgłaszanych do zespołu różnych adresów IP pochodziło z sieci Orange (ASN5617), natomiast Netia zajęła drugą pozycję. Należy jednak zwrócić uwagę, że różnica w liczbie adresów IP jest minimalna. Pełne zestawienie znajduje się w tabeli 31 oraz na rysunku 21.

Poz.	Nr AS	Nazwa AS	Liczba IP	Udział
1	5617	Orange	28 304	26,40%
2	12741	Netia SA	28 222	26,33%
3	8374	Polkomtel Sp. z o.o.	17 759	16,57%
4	21021	Multimedia Polska S.A.	13 237	12,35%
5	12912	T-mobile Polska SA	1 639	1,53%
6	29007	Petrotel Sp. z o.o.	1 533	1,43%
7	6714	GTS Poland Sp. z o.o.	1 099	1,03%
8	21243	Polkomtel Sp. z o.o.	1 063	0,99%
9	6830	Liberty Global Operations B.V. (UPC)	1 008	0,94%
10	49185	Protonet	994	0,93%
	pozostałe:		12 342	11,5 %

Tabela 31. Polskie systemy autonomiczne, z których pochodziło najwięcej skanowań.



Rysunek 21. Polskie systemy autonomiczne, z których pochodziło najwięcej skanowań.

Informacje o CERT Polska

Zespół CERT Polska działa w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej) – instytutu badawczego prowadzącego działalność naukowa, 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 tematyka 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.

KONTAKT

Zgłaszanie incydentów: cert@cert.pl

Zgłaszanie spamu: spam@cert.pl

Informacja: info@cert.pl

Klucz PGP: www.cert.pl/pub/0x553FEB09.asc

Strona WWW: www.cert.pl

Facebook: fb.com/CERT.Polska

RSS: www.cert.pl/rss

Twitter: @CERT_Polska, @CERT_Polska_en

NASK/CERT Polska

Ul. Wąwozowa 18, 02-796 Warszawa

Telefon: +48 22 38 08 274

Faks: +48 22 38 08 399