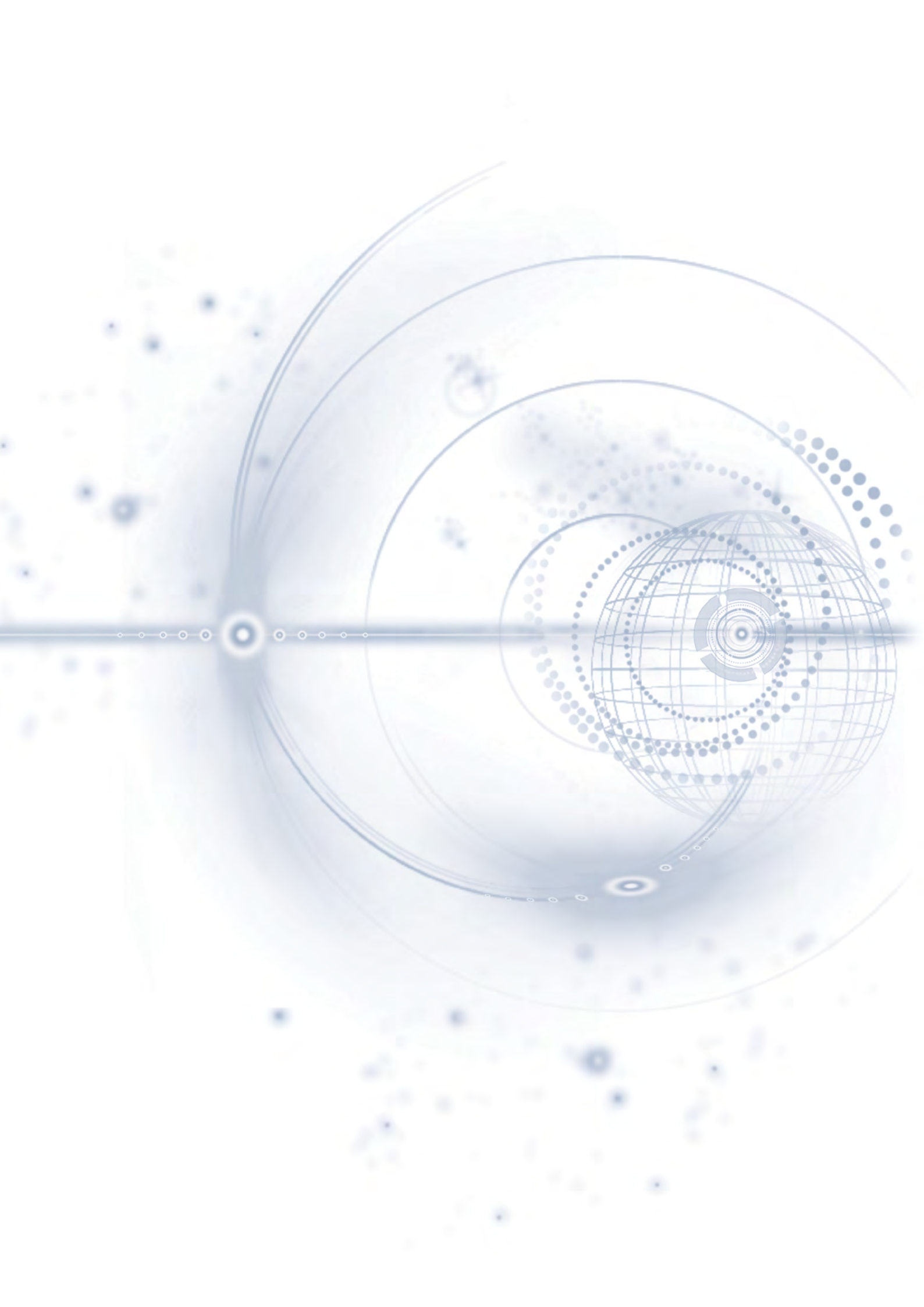
Zespół CERT Polska działa w ramach Naukowej i Akademickiej Sieci Komputerowej

Raport CERT Polska

Zawiera raport z systemu ARAKIS

Analiza incydentów naruszających bezpieczeństwo teleinformatyczne w roku 2011

CERT POLSKA NASK



Spis treści

1.1 Jak czytać ten dokument?

Niniejszy raport przedstawia wybrane statystyki z danych zebranych przez zespół CERT Polska w 2011 r. wraz z omówieniem i wnioskami. Dokument jest zorganizowany w podobny sposób do naszego raportu za 2010 rok. Dzięki temu możemy w tegorocznym raporcie porównać obserwacje z tymi, których dokonaliśmy w roku ubiegłym.

Ważną część raportu (rozdział 4) stanowią informacje na temat zagrożeń w polskich sieciach, przekazywane zespołowi CERT Polska przez różne podmioty związane z monitorowaniem i reagowaniem na zagrożenia, a także z wybranych systemów CERT Polska. Ponieważ uwzględniają one prawie wszystkich polskich operatorów, dają bardzo szeroki obraz tego, co naprawdę dzieje się w polskich zasobach internetowych.

Rozdziały 5 i 6 skupiają się na działalności operacyjnej CERT Polska. Dane w nich przedstawione pochodzą z systemu obsługi incydentów. Obejmują one zdarzenia, przy których była interwencja CERT Polska. Używana przy obsłudze incydentów klasyfikacja umożliwia porównania trendów w kolejnych latach w rozdziale 7.

W rozdziale 8 zostały omówione w szczegółach najważniejsze zjawiska, które pojawiły się bądź uaktywniły w sferze bezpieczeństwa w 2011 roku i w których analizę zaangażowany był zespół CERT Polska.

W Rozdziale 9 omawiamy najważniejsze wydarzenia związane z rozwojem naszego zespołu.

1.2 Najważniejsze obserwacje podsumowujące raport

- W drugiej połowie 2011 r. rozpoczęliśmy korzystanie z wielu nowych źródeł wiedzy o incydentach, co wpłynęło na znaczący wzrost liczby zgłoszeń automatycznych.

- W lutym pojawił się nowy wariant Zeusa atakujący polskich użytkowników. Był on wyjątkowy, ponieważ poza komputerami atakował również telefony komórkowe. Atakujący mógł czytać i modyfikować informacje - np. zawierające kody autoryzacji transakcji. Był to drugi w pełni udokumentowany tego typu przypadek na świecie.

- W kwietniu miał miejsce atak ukierunkowany na użytkowników Internetu. W masowo rozsyłanym mailu znajdowała się fałszywa faktura. Po jej otwarciu instalował się trojan SpyEye i następowało przejęcie kontroli nad komputerem. Od tego momentu były wykradane wszystkie poufne informacje wprowadzane przez użytkownika na stronach internetowych (w tym w systemach bankowości elektronicznej).

- Od końca kwietnia do czerwca 2011 r. doszło do wielu wycieków danych klientów usług elektronicznych. Najpoważniejsze dotyczyły firmy Sony. Z baz danych należących do niej usług PSN i SEN włamywacze wydostali dane łącznie 100 mln kont użytkowników, a prawdopodobnie także około 10 mln kart kredytowych. Dane użytkowników wyciekły także m.in. z Nintendo, Codemasters, pornograficznego serwisu pron.com oraz Citibanku (200 tys. kont). Część ataków przypisywana jest grupom Anonymous oraz LulzSec.

- W maju doszło do wycieku kodu trojana Zeus w wersji 2.0.8.9. Choć ułatwiło to zwalczanie tego złośliwego oprogramowania dzięki zwiększonym możliwościom analizy, pojawiły się jednocześnie doniesienia o nowych rodzajach malware'u, bazujących na wspomnianym kodzie.

- Jesienią pojawiła się nowa wersja Zeusa, wykorzystująca do propagacji i komunikacji z kontrolerem stworzoną przez siebie sieć peer-to-peer oraz generowanie nazw domen (mechanizm podobny jak w dobrze znanym Conficke-rze).

- W 2011 roku zaobserwowaliśmy aż 5,5 mln botów (prawie 10 mln zgłoszeń) u polskich operatorów. Najwięcej, prawie 2,5 mln, znajdowało się w sieciach TP.

- Podobnie jak w 2010 roku, Conficker był najczęściej występującym botem w polskich sieciach. Otrzymaliśmy aż 2,1 mln automatycznych zgłoszeń.

- Serwisy oferujące darmowe aliasy są coraz częściej wykorzystywane przez przestępców:
  - aż w 84% phishing był umieszczony w domenie .pl z ich użyciem,
  - 25% złośliwego oprogramowania obserwowanego w sandbox-ach i łączącego się do polskich sieci, wykorzystywało darmowe subdomeny.

- Polskie bezpłatne subdomeny, takie jak .osa.pl czy .bij.pl, zyskują na popularności wśród internetowych oszustów, którzy rejestrują je na potrzeby phishingu.

- Wśród incydentów obsłużonych nieautomatycznie przez CERT Polska, ponad połowę stanowił Phishing umieszczony w polskich sieciach. Zanotowaliśmy wzrost aż o 1/3 w stosunku do 2010 roku. Należy podkreślić, że większość przypadków dotyczyła zagranicznych podmiotów finansowych i nie stanowiła zagrożenia dla polskiego użytkownika.

- Najczęściej skanowanym portem w polskich sieciach był 445/TCP związany z podatnościami w windowsowej usłudze związanej z SMB. Jednakże liczba adresów IP skanujących ten port zmalała w stosunku do roku 2010 o ok. 29%. Skanowania na pozostałych portach w rankingu znacząco wzrosły w porównaniu do poprzedniego roku.

- Lista najbardziej zainfekowanych sieci w Polsce odzwierciedla w większości wielkość operatorów pod względem liczby użytkowników. Ugruntowana wydaje się pozycja operatorów mobilnych.

- Najwięcej serwerów C&C o charakterze IRC-owym w Polsce znajdowało się w hostowniach należących do podmiotów międzynarodowych (LEASEWEB, OVH), ale mających też sieci przypisane Polsce.

- Najwięcej zgłoszeń dotyczących złośliwych stron WWW dotyczyło domen takich jak strefa.pl, friko.pl, interia.pl, republika.pl, czyli oferujących darmową rejestrację stron.

- Stosunkowo niewiele mamy zgłoszeń ataków DDoS. Nie oznacza to oczywiście, że nie ma takich ataków − wynika to raczej z niechęci do zgłaszania, i trudności wykrycia takiej aktywności przez stronę trzecią (stąd niewiele zgłoszeń automatycznych).

- Wśród polskich operatorów internetowych brakuje woli do blokowania portu 25 TCP dla końcowych użytkowników, choć skuteczność takich działań została wykazana przez Telekomunikację Polską.

- Coraz więcej spamu pochodzi z sieci operatorów mobilnych. Dotyczy ich już niemal co piąte zgłoszenie.

- W Polsce znajduje się ponad 160 tysięcy źle skonfigurowanych serwerów DNS, które mogą być wykorzystywane w atakach DDoS. Problem dotyczy w zasadzie wszystkich operatorów.

2. Informacje o zespole CERT Polska

Zespół CERT Polska działa w strukturach **NASK** (Naukowej i Akademickiej Sieci Komputerowej) - instytutu badawczego prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne. CERT Polska to pierwszy powstały w Polsce zespół reagowania na incydenty (z ang. Computer Emergency Response Team). Aktywnie operując od 1996 roku w środowisku zespołów reagujących, stał się rozpoznawalnym i doświadczonym podmiotem w dziedzinie bezpieczeństwa komputerowego.

Od początku istnienia rdzeniem działalności zespołu jest obsługa incydentów bezpieczeństwa i współpraca z podobnymi jednostkami na całym świecie, zarówno w działalności operacyjnej, jak i badawczo-wdrożeniowej. Od 1998 roku CERT Polska jest członkiem międzynarodowego forum zrzeszającego zespoły reagujące - **FIRST**[1], a od roku 2000 należy do grupy roboczej europejskich zespołów reagujących - **TERENA TF-CSIRT**[2] i działającej przy niej organizacji **Trusted Introducer**[3]. W 2005 roku z inicjatywy CERT Polska powstało forum polskich zespołów abuse - **Abuse FORUM**, natomiast w 2010 r. CERT Polska dołączył do **Anti-Phishing Working Group**[4], stowarzyszenia gromadzącego firmy i instytucje aktywnie walczące z przestępczością w sieci.

Do głównych zadań zespołu CERT Polska należy:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci;
- aktywne reagowanie w przypadku wystąpienia bezpośrednich zagrożeń dla użytkowników;
- współpraca z innymi zespołami CERT w Polsce i na świecie;
- udział w krajowych i międzynarodowych projektach związanych z tematyką bezpieczeństwa teleinformatycznego;
- działalność badawcza z zakresu metod wykrywania incydentów bezpieczeństwa, analizy złośliwego oprogramowania, 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 w serwisie http://www.cert.pl/ oraz w serwisach społecznościowych Facebook i Twitter;
  - organizacja cyklicznej konferencji SECURE;
- niezależne analizy i testy rozwiązań z dziedziny bezpieczeństwa teleinformatycznego.

[1] *http://www.first.org/*

[2] *http://www.terena.org/activities/tf-csirt/*

[3] *http://www.trusted-introducer.org/*

[4] *http://www.antiphishing.org/*

3. Wprowadzenie

Od kliku lat obserwujemy istotną dla profilu działalności CERT Polska zmianę w rodzaju otrzymywanych przez nasz zespół zgłoszeń. Coraz mniej z nich wymaga bezpośredniej reakcji wewnątrz naszego zespołu, a przede wszystkim takie zgłoszenia były dotychczas przez nas rejestrowane, obsługiwane i wykazywane w statystykach. Otrzymujemy natomiast bardzo duże ilości danych dotyczących polskich sieci, pochodzące głównie ze zautomatyzowanych źródeł tworzonych przez podmioty zajmujące się bezpieczeństwem w Internecie. Dane takie, choć nieobsługiwane przez nas bezpośrednio, są przekazywane właściwym operatorom w ramach posiadanej przez nas sieci kontaktów. CERT Polska pełni więc w tym przypadku rolę koordynatora. Jest to rozwiązanie wygodne zarówno dla dostawców danych, którzy nie muszą samodzielnie poszukiwać kontaktów do poszczególnych zespołów reagujących u polskich dostawców, jak i dla operatorów internetowych, którzy mogą z jednego miejsca otrzymywać dotyczące ich informacje pochodzące z wielu źródeł.

Biorąc pod uwagę ogrom informacji przekazywanych do CERT Polska w ramach koordynacji, podjęliśmy wysiłek ustandaryzowania ich i wykorzystania w niniejszym raporcie celem pełniejszego zobrazowania tego, co faktycznie dzieje się w polskich zasobach w Internecie. Formuła jest zbliżona do naszego rocznego raportu za rok 2010. Pozwala to na dokonywanie porównań i wychwytywanie trendów w atakach. Warto jednak podkreślić, że w 2011 roku coraz więcej automatycznych źródeł zewnętrznych dostarczało nam informacje, co utrudnia porównania z danymi z ubiegłych lat. Staraliśmy się uwzględnić ten trend w analizach, stosując porównania tylko na źródłach danych, które raportują nam incydenty dotyczące zarówno Polski, jak i całego świata. Poza zgłoszeniami koordynowanymi, opisujemy również zgłoszenia wymagające szczególnego, bezpośredniego zaangażowania naszego zespołu w obsługę. Ponadto w raporcie opisujemy, naszym zdaniem najciekawsze zjawiska związane z bezpieczeństwem w Polsce - takie, w których analizę byliśmy bezpośrednio zaangażowani. Zawieramy również opis najważniejszych pozostałych obszarów aktywności zespołu CERT Polska w 2011 roku.

4. Statystyka zgłoszeń koordynowanych przez CERT Polska

W tej części raportu opisujemy wyniki analiz informacji dotyczących incydentów bezpieczeństwa, które zostały zebrane automatycznie.

4.1 Ilość informacji we wszystkich kategoriach

W roku 2011 r. otrzymaliśmy 21 210 508 zgłoszeń pochodzących z systemów automatycznych. Przeważająca większość dotyczyła botów, skanowania i spamu. Rozkład pozostałych kategorii, które wyróżniliśmy w raporcie, przedstawia poniższy wykres (zwracamy uwagę na skalę logarytmiczną!).

Dane pochodzą z wielu źródeł o bardzo zróżnicowanym charakterze. Dlatego sposoby ich zbierania oraz prezentacji znacznie różnią się między sobą.

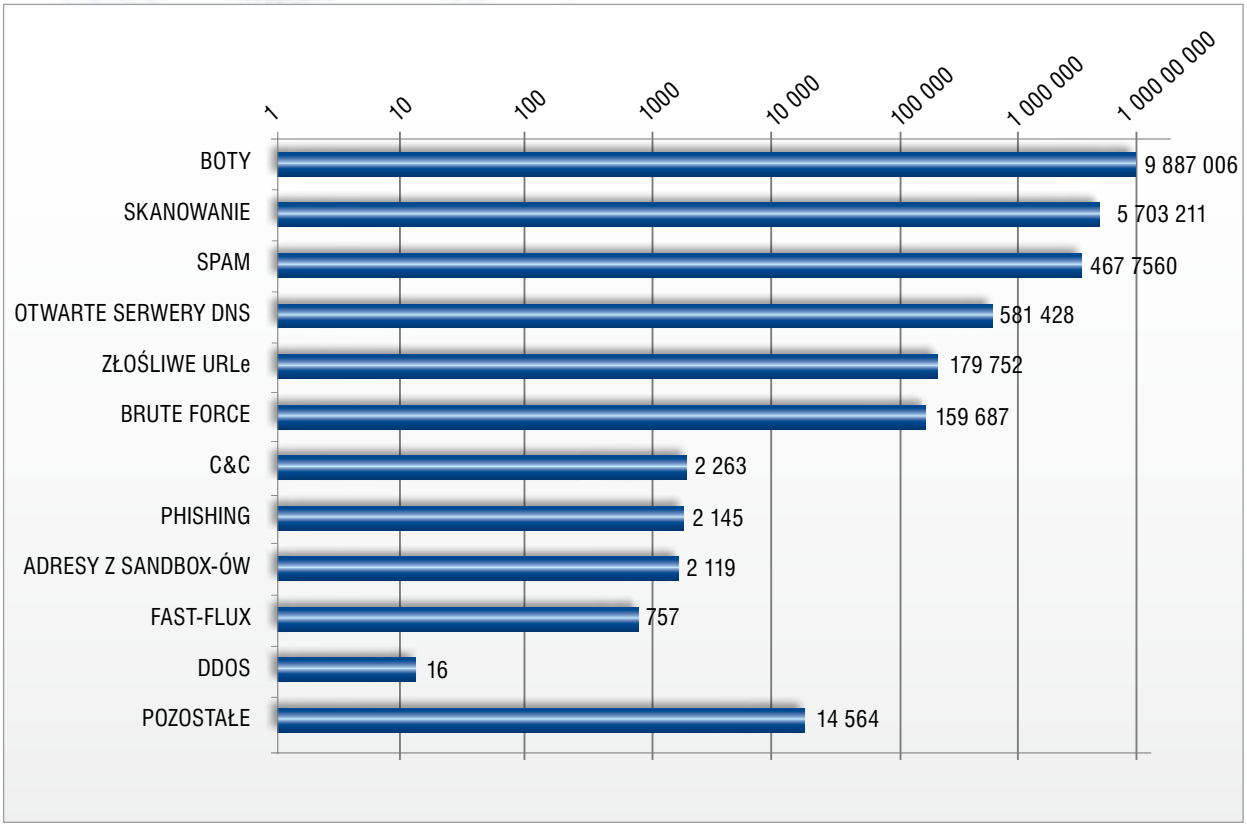


Tabela 4.1. Liczba zgłoszeń automatycznych w poszczególnych kategoriach

W stosunku do ubiegłego roku rozszerzyliśmy kategorie zgłoszeń z 10 na 12 grup. Wyróżnione kategorie to: boty, skanowanie, spam, złośliwe adresy URL, ataki brute force (nowa kategoria), otwarte serwery DNS (nowa kategoria), serwery C&C, przypadki phishingu, dane z sandbox-ów, Fast-flux, DDoS i pozostałe.

Porównując powyższe dane z danymi z 2010 roku (a także z naszym raportem półrocznym za 2011) można zaobserwować duży wzrost liczby zgłoszeń. Wynika to przede wszystkim z faktu, że dodaliśmy wiele nowych źródeł informacji w drugim półroczu 2011 r. W niektórych przypadkach, jak np. C&C, w wykresie powyżej prezentujemy zgłoszenia, a nie jak w roku ubiegłym unikalne adresy, stąd znacznie większa liczba zgłoszeń. Fakt dodawania nowych źródeł utrudnia porównanie z latami ubiegłymi, ale umożliwia lepsze zorientowanie się w poziomie zainfekowania i wykorzystywania do ataków sieci w Polsce.

W kolejnych podrozdziałach szczegółowo analizujemy wszystkie wyżej wymienione typy zgłoszeń.

4. Statystyka zgłoszeń koordynowanych przez CERT Polska

4.2 Phishing

W 2011 roku otrzymaliśmy 266 300 informacji o tradycyjnym phishingu. Informacje te dotyczyły 222 214 różnych adresów URL w 139 770 domenach na 40 091 unikalnych adresach IP. Rozkład liczby zgłoszeń phishingu według krajów, w których był umieszczony, widoczny jest w tabeli 4.2.1.

Pozycja	Kraj	Liczba zgłoszeń	% udział w zgłoszeniach
1	US	135 405	50,8%
2	HK	17 963	6,7%
3	DE	12 680	4,8%
4	CA	11 943	4,5%
5	GB	9 822	3,7%
6	CZ	8 706	3,3%
7	FR	6 492	2,4%
8	BR	6 240	2,3%
9	RU	5 580	2,1%
10	CH	5 358	2,0%
17	PL	2 120	0,8%

Tabela 4.2.1. Rozkład liczby zgłoszeń phishingu według krajów

W porównaniu z ubiegłym rokiem zwiększył się udział Stanów Zjednoczonych, które samodzielnie odpowiedzialne są za ponad połowę utrzymywanych stron z phishingiem. Jest to zapewne spowodowane bardzo korzystnym stosunkiem ceny do jakości usług hostingowych, z których przestępcy chętnie korzystają, jeśli jest to bardziej opłacalne niż włamywanie się na istniejące strony. Trzeba tu zauważyć, że administratorzy takich usług są w trudnej pozycji, ponieważ nie jest możliwe monitorowanie wszystkich treści, które klienci umieszczają na serwerach. Tymczasem już bardzo krótki czas aktywności strony phishingowej (od wysłania odnośników do niej w spamie aż do jej wykrycia, zgłoszenia i usunięcia) w zupełności wystarczy, aby przestępca uzyskał zwrot kosztów poniesionych na jej legalne utrzymanie.

Co ciekawe, na drugim miejscu według liczby zgłoszeń znalazł się Hong Kong (17 963; 6,7%), a na szóstym - Czechy (8 706; 3,3%). W obu przypadkach strony przypisane były do stosunkowo niewielkiej liczby adresów IP. W Czechach 4 772 różne adresy URL znajdowały się pod 275 adresami IP (średnio 17,35 na jednym), a w Hong Kongu 17 640 URL przypadało na 705 IP (średnio 25,02 na jeden). W istocie w obu przypadkach znacząca większość stron znajdowała się na kilku serwerach hostingowych, pod różnymi adresami, w większości w bezpłatnych domenach np. .co,. co lub .tk. Na marginesie, obie te domeny zostały w 2011 roku usunięte przez Google z wyników wyszukiwarki. Jest to dobitny przykład na to, że pozwalanie na bezpłatną rejestrację domeny bez weryfikacji abonenta nie jest najlepszym pomysłem. Niestety, tego rodzaju przypadków nie brak także na polskim podwórku. Od kilku lat narasta problem serwisów oferujących bezpłatne subdomeny do samodzielnego zarządzania, z nazwami generowanymi wedle uznania. Domeny takie jak .osa.pl czy .bij.pl używane były przez przestępców z całego świata do rejestracji adresów takich jak 1tem.taebao.cem.d2wmj1o.osa.pl i wykorzystywania ich do phishingu. Łącznie aż 5 980 (4,3%) domen hostujących phishing znajdowało się w .pl. Aż 5 033 z nich to bezpłatne subdomeny! W przypadku pozostałych domen doszło najprawdopodobniej do włamania na istniejące strony. W tabeli 4.2.2. znajduje się lista domen, z których usług najchętniej korzystali przestępcy.

osa.pl	4 031
bij.pl	576
bee.pl	154
345.pl	118
122.pl	65
orge.pl	56
inn.pl	30

Tabela 4.2.2. Lista domen najczęściej wykorzystywanych do phishingu

4. Statystyka zgłoszeń koordynowanych przez CERT Polska

Aby zmniejszyć zainteresowanie swoimi usługami wśród przestępców, firmy oferujące bezpłatne aliasy powinny zadbać o to, aby klient był rozliczalny (była przeprowadzana weryfikacja jego tożsamości np. z użyciem karty kredytowej) oraz o to, aby niedopuszczalne było wykorzystywanie nazw serwisów, które często padają ofiarami phishingu, w szczególności banków.

darmowe poddomeny.pl	528
inne darmowe poddomeny	29
inne rejestracje	69
włamania	208

Tabela 4.2.3. Rozkład metod wykorzystywanych do phishingu w sieciach polskich operatorów

Jeśli chodzi o phishing umieszczony w polskich sieciach (niezależnie od domeny, w której znajdował się dany URL), otrzymaliśmy 2 120 takich zgłoszeń, dotyczących 1 464 adresów URL w 812 domenach na 505 adresach IP. Rozkład strategii użytych przy phishingu w sieciach polskich operatorów pokazuje tabela 4.2.3.

Kolejna tabela zawiera informacje o dziesięciu operatorach, których najczęściej dotyczyły zgłoszenia. Dominacja operatorów hostingowych nie powinna być zaskoczeniem, ponieważ najczęściej właśnie tam przestępcy wykupują usługi bądź szukają ofiar włamania. Stosunek liczby zgłoszeń do unikalnych adresów IP, których dotyczyły, można odnosić do czasu i skuteczności reagowania danego operatora - im mniejszy, tym szybciej dany adres był usuwany.

	ASN	Nazwa	Zgłoszenia	IP	Zgłoszenia/IP	URL
1	15 967	NetArt	514	167	3,08	352
2	12 824	HOME.PL	359	60	5,98	269
3	49 102	CONECTED	186	1	186,00	104
4	5 617	TP	162	40	4,05	91
5	43 470	LiveNet-PL	75	6	12,50	42
6	29 522	KEI	70	24	2,92	60
7	29 314	VECTRA	65	4	16,25	36
8	6 714	GTS	46	8	5,75	34
9	43 333	CIS NEPHAX	40	10	4,00	25
10	15 694	ATM	40	4	10,00	19

Tabela 4.2.4. Zestawienie operatorów, których najczęściej dotyczyły zgłoszenia

4.3 Strony związane ze złośliwym oprogramowaniem

Ta kategoria obejmuje zgłoszenia ze źródeł automatycznych dotyczące przypadków utrzymywania w sieciach polskich operatorów plików związanych ze złośliwym oprogramowaniem. Zaliczamy tu przede wszystkim:

- kod służący przełamaniu zabezpieczeń przeglądarki lub jednego z jej rozszerzeń,
- plik wykonywalny (w tym pobierany w wyniku działania powyższego kodu),
- pliki konfiguracyjne służące do sterowania uruchomionym w systemie złośliwym oprogramowaniem.

4. Statystyka zgłoszeń koordynowanych przez CERT Polska

Ze względu na fakt, że w drugiej połowie 2011 roku zaczęliśmy korzystać z wielu nowych źródeł informacji, statystyki uległy zmianie. Otrzymaliśmy znacznie więcej zgłoszeń, liczonych jako unikalne kombinacje dnia zgłoszenia IPiURL. Nie zawsze ze wszystkich źródeł otrzymujemy informacje o zagrożeniach znajdujących się na serwerach w innych krajach niż Polska. Tak więc, nie zawsze jesteśmy w stanie porównać sytuację Polski względem świata - porównania robimy tylko na bazie źródeł, które dostarczają nam dane zarówno dla Polski, jak i reszty świata. Do analiz sytuacji wewnątrz polskich sieci wykorzystujemy natomiast wszystkie źródła, jakie posiadamy.

Pozycja	Kraj	Procentowy udział w zgłoszeniach
1	US	41,10%
2	CN	15,42%
3	KR	9,62%
4	RU	5,48%
5	DE	4,12%
6	CA	3,03%
7	FR	2,78%
8	UA	2,37%
9	BR	2,17%
10	EU	1,77%
11	GB	1,50%
12	PL	1,43%
13	IT	1,33%
14	CZ	1,12%
15	NL	1,11%
16	JP	0,65%
17	TR	0,65%
18	SE	0,59%
19	HU	0,48%
20	RO	0,35%
	POZOSTAŁE	2,94%

Tabela 4.3.1. Liczba przypadków złośliwego oprogramowania na stronach WWW według lokalizacji geograficznej (kraje)

Statystyki dla świata nie uległy znaczącym zmianom względem 2010 roku. Na pierwszym miejscu nadal znajdują się Stany Zjednoczone, których dotyczy 41,10% zgłoszeń. Na drugim miejscu są Chiny - 15,42%. Polska, podobnie jak w roku ubiegłym jest na 12 miejscu, z podobnym procentem zgłoszeń - 1,43%.

Podobnie jak w roku ubiegłym, porównując między sobą poszczególne kraje, w których utrzymywane były pliki związane ze złośliwym oprogramowaniem, warto zwrócić uwagę na wysoką pozycję (poza Chinami) Rosji i Ukrainy. Zestawiając poniższą tabelę z podobną tabelą dla phishingu widać, że pozycje tych krajów (w szczególności Chin) są istotnie wyższe w kategorii związanej ze złośliwym oprogramowaniem. Tak jak w poprzednim roku uważamy, że możliwą interpretacją jest to, że pliki ze złośliwym oprogramowaniem w tych krajach nie pojawiają się wyłącznie w wyniku ślepych ataków hakerskich (wtedy rozkład powinien być podobny jak dla phishingu), ale że kraje te wybierane są celowo. Z jednej strony wielu chińskich i rosyjskich dostawców usług hostingowych ma opinię „bulletproof hosting" ze względu na trudności w uzyskaniu od nich wsparcia w usunięciu szkodliwych zasobów. Z drugiej strony dość częste są spekulacje, że internetowi przestępcy działają w Chinach, Rosji czy na Ukrainie za cichym przyzwoleniem wpływowych środowisk. Oczywiście, obie teorie nie wykluczają się i nie są jedynymi możliwymi wytłumaczeniami nadzwyczaj wysokiej pozycji tych trzech krajów w tabeli.

Łącznie dla Polski (domena .pl i/lub hostowane w Polsce) otrzymaliśmy w 2011 roku 272 546 zgłoszeń, w tym 3 000 unikalnych IP, 38 472 adresów URL oraz 6 999 domen. Z tych zgłoszeń, 179 752 raportowanych przypadków było hostowanych w Polsce i rozkładało się na 2 576 IP, 27 991 adresów URL oraz 5 637 domen. Wśród zgłoszeń o złośliwych adresach URL z domeny .pl hostowanych poza Polską dominowały Niemcy i Francja. Tylko 3 z 424 adresów IP poza krajem znajdowały się Chinach - udostępniały one złośliwe pliki wykonywalne.

4. Statystyka zgłoszeń koordynowanych przez CERT Polska

W zestawieniach największej liczby zgłoszeń, unikalnych IP, adresów URL oraz domen dominowali najwięksi dostawcy usług hostingowych: Home.pl, Netart oraz Krakowskie E-Centrum Informatyczne Jump. Obserwacje te są zbliżone do tych dokonanych w 2010 roku, ale inne niż te z pierwszego półrocza 2011 - co być może wynika z faktu uzyskania dostępu do wielu nowych źródeł informacji. Czasami jednak w czołówce znajdowali się także dostawcy usług internetowych - np. w kategorii najwięcej unikalnych złośliwych IP dominowała Netia. Relatywnie nisko znajdowała się za to TP. Warto zwrócić uwagę na brak obecności w czołówce operatorów sieci mobilnych.

W tabeli 4.3.5 zilustrowano domeny pod kątem największej liczby zgłoszonych unikalnych złośliwych adresów URL. Pierwszy wniosek to fakt braku domen darmowych wykorzystywanych w phishingu np. bee.pl/osa.pl, widywanych również w danych z sandbox-ów. Są za to wykorzystywane inne domeny, które są rozdawane darmowo (patrz tabela 4.3.6). Najczęściej złośliwe oprogramowanie było dystrybuowane zarówno z chińskiej domeny p-upfile.co.cc jak i mypromofile.info. Złośliwe oprogramowanie z tych domen przyjmowało postać pliku SetupXXX.exe, gdzie XXX to cyfry odwzorowujące jego kolejne wersje. Rozpoznawane było przez oprogramowanie antywirusowe jako trojan bankowy typu Zeus, ale w zależności od wersji, również jako oprogramowanie udające program antywirusowy (tzw. rogue antivirus). Wydaje się, że domeny zostały zarejestrowane specjalnie w tym celu (tak jak dwie ostatnie z tabeli 4.3.5). Inaczej wygląda sprawa kolejnych sześciu (poz. 3 do poz. 7) domen z tabeli, do których się włamano, a następnie hostowano malware różnego typu.

	Liczba zgłoszeń	Procentowy udział	System autonomiczny	Operator
1	30 330	16,87%	12 824	HOME.PL
2	19 336	10,76%	29 522	KEI
3	14 960	8,32%	15 967	NETART
4	13 341	7,42%	16 138	INTERIA
5	10 853	6,04%	12 741	NETIA

Tabela 4.3.2. Liczba przypadków zgłoszeń złośliwego oprogramowania na polskich stronach WWW według systemów autonomicznych

	Liczba unikalnych IP	Procentowy udział	System autonomiczny	Operator
1	607	23,56%	12 741	NETIA
2	499	19,37%	12 824	HOME.PL
3	231	8,97%	15 967	NETART
4	163	6,33%	5 617	TP
5	96	3,73%	29 522	KEI

Tabela 4.3.3. Liczba przypadków zgłoszeń złośliwego oprogramowania na polskich stronach WWW pod kątem unikalnych IP znajdujących się u polskich operatorów

	Liczba unikalnych URL	Procentowy udział	System autonomiczny	Operator
1	4 622	16,51%	12 824	HOME.PL
2	3 832	13,69%	16 138	INTERIA
3	2 093	7,48%	29 522	KEI
4	2 012	7,19%	15 967	NETART
5	1 230	4,39%	12 741	NETIA

Tabela 4.3.4. Liczba przypadków zgłoszeń złośliwego oprogramowania na polskich stronach WWW pod kątem unikalnych URL

Pozycja	Liczba unikalnych złośliwych adresów	Nazwa domeny
1	1 984	p-upfile.co.cc
2	1 040	mypromofile.info
3	926	kamp.nazwa.pl
4	558	esflores.kei.pl
5	493	noclegi-i.pl
6	375	dementia.waw.pl
7	367	www.sp2osiek.pl
8	336	www.teatr-pismo.pl
9	314	acletan.strefa.pl
10	295	canrilric.strefa.pl

Tabela 4.3.5. Ranking domen hostujących złośliwe oprogramowanie pod kątem unikalnych adresów URL

4. Statystyka zgłoszeń koordynowanych przez CERT Polska

Liczba unikalnych IP	Nazwa domeny
2 402	strefa.pl
1 770	com.pl
1 124	friko.pl
1 081	interia.pl
1 064	republika.pl
1 041	nazwa.pl
815	w8w.pl
700	yoyo.pl
676	waw.pl
576	kei.pl
493	noclegi-i.pl

Tabela 4.3.6. Ranking domen drugiego poziomu, na których hostowano złośliwe oprogramowanie pod kątem unikalnych złośliwych URL

Niestety, nie dysponujemy dokładnymi statystykami dotyczącymi rozkładu charakteru złośliwego oprogramowania na stronach. Naszym zdaniem wiodącą formą infekcji użytkownika końcowego są mechanizmy inżynierii społecznej: użytkownik sam instaluje sobie złośliwe oprogramowanie poprzez ściągnięcie i uruchomienie pliku wykonywalnego. Warto jednak zwrócić uwagę, że w drugiej popularnej i znacznie groźniejszej kategorii ataków - drive-by download (atak, w którym cały proces infekcji odbywa się w pełni automatycznie przez lukę w przeglądarce lub jej wtyczce w sposób niezauważalny dla użytkownika) - istotnym zjawiskiem w 2011 roku były ataki na przeglądarki wykorzystujące Javę. Dlatego zalecamy odinstalowanie Javy na swoim komputerze, jeżeli nie jest niezbędna do wykonywania codziennych czynności.

4.4 Z piaskownicy do polskich sieci, czyli adresy odwiedzane przez malware

Ta kategoria informacji jest rozszerzeniem kategorii boty i uwzględniamy w niej adresy, które odwiedzane były przez złośliwe oprogramowanie zainstalowane w laboratoriach wewnątrz sandbox-u, czyli w dużym skrócie, specjalnie przygotowanego środowiska, służącego do kontrolowanego uruchamiania różnego rodzaju podejrzanego oprogramowania. Zaobserwowaliśmy 2 119 unikalnych adresów WWW oraz FTP, do których łączyło się oprogramowanie uruchamiane w sandbox-ach.

Do adresów tych łączyło się w sumie 2 113 unikalnych plików. Ponad 31% z nich zostało rozpoznanych przez programy antywirusowe jako złośliwe oprogramowanie (na podstawie Cymru Malware Hash Registry - http://www.team-cymru.org/Services/MHR/).

Najczęściej obserwowaliśmy połączenia do serwera geoloc.daiguo.com. Wyodrębniliśmy 429 zapytań. Wszystkie były takie same, przy czym każde z nich zostało wygenerowane przez złośliwe oprogramowanie o innej sumie MD5. Są to zapytania mające na celu uzyskanie informacji o pochodzeniu geograficznym zainfekowanej maszyny.

Pozycja	URL lub adres IP	Liczba zapytań
1	geoloc.daiguo.com	429
2	www.bee.pl	424
3	212.33.79.77	275
4	pelcpawel.fm.interia.pl	167
5	www.bigseekpro.com	72
6	s1.footballteam.pl	61
7	mattfoll.eu.interia.pl	61
8	appmsg.gadu-gadu.pl	61
9	www.tibissa.com	58
10	213.108.56.140	58

Tabela 4.4.1. Adresy odwiedzane przez malware

Równie często (424 razy) notowaliśmy połączenia do serwera www.bee.pl. Jest to serwis oferujący darmowe aliasy często wykorzystywany przez autorów złośliwego oprogramowania do przekierowania ofiar do serwerów C&C. Podobnie jak w przypadku phishingu, zauważyliśmy dość duże zainteresowanie przestępców tego typu usługami. W sumie odnotowaliśmy aż 520 takich połączeń (tabela 4.4.2.). Poza bee.pl przestępcy wykorzystywali domeny osa.pl, 345.pl, bij.pl oraz orge.pl.

4. Statystyka zgłoszeń koordynowanych przez CERT Polska

275 razy notowaliśmy połączenia do serwera o adresie IP 212.33.79.77. Wszystkie były wygenerowane przez ten sam złośliwy plik. Jest to komunikacja zainfekowanych maszyn do centrum zarządzającego.

Bardzo ciekawa sytuacja dotyczy adresów w domenie interia.pl: pelcpawel.fm.interia.pl, radson_master.fm.interia.pl oraz mattfoll.eu.interia.pl. We wszystkich przypadkach winowajcą był koń trojański o nazwie Sality. Tak jak w poprzednim przypadku łączył się on do centrów zarządzających. Interesujący jest fakt, że wszystkie z nich znajdowały się w domenie Interii.

W przypadku appmsg.gadu-gadu.pl, tak jak w ubiegłym roku, mieliśmy do czynienia z połączeniami inicjującymi do sieci gadu-gadu.

Pozycja	Domena	Liczba zapytań
1	bee.pl	424
2	osa.pl	48
3	345.pl	32
4	bij.pl	8
5	orge.pl	8

Tabela 4.4.2. Połączenia do bezpłatnych subdomen

Co do pozostałych adresów, niestety nie udało się jednoznacznie ustalić, w jakim celu były one odwiedzane. Mogła to być zarówno działalność złośliwego oprogramowania, jak i ruch generowany przez zwykłe aplikacje sprawdzane przez użytkownika w sandbox-ie.

4.5 Spam z polskich sieci

W 2011 roku otrzymaliśmy 4 677 560 zgłoszeń spamu pochodzącego z polskich sieci. Należy podkreślić, że w ogromniej większości nie dotyczą one pojedynczych niechcianych przesyłek, lecz źródeł - najczęściej zainfekowanych lub źle skonfigurowanych maszyn, z których każda wysyłała nierzadko dziesiątki tysięcy listów. Liczba zgłoszeń jest mniejsza niż rok wcześniej, lecz trend w tym roku był nieznacznie wzrostowy, z chwilowym spadkiem w okresie wakacyjnym. Ponad połowa wszystkich zgłoszeń dotyczyła zaledwie trzech operatorów - Netii (31%), Telekomunikacji Polskiej (17%) oraz Multimedia Polska (10%). Dane analizowane przez nas dotyczą większości, lecz nie wszystkich polskich sieci, stąd nie należy ich przenosić na zależności ogólnopolskie. Zależności pomiędzy uwzględnionymi operatorami są jednak rzeczywiste. Dysproporcja między Telekomunikacją Polską i Netią jest łatwo dostrzegalna, w szczególności jeśli wziąć pod uwagę udział w rynku obu operatorów. Wynika ona z rozwiązań technicznych stosowanych od blisko dwóch lat w Telekomunikacji Polskiej, a przede wszystkim domyślnego blokowania portu 25 TCP dla użytkowników końcowych. Niestety, mimo znakomitej skuteczności takiego rozwiązania, nie zostało ono wprowadzone dotąd przez pozostałych dużych operatorów.

Dzieląc liczbę zgłoszeń przez liczbę unikalnych przypadków, których dotyczyły (1 253 528) otrzymujemy 3,73. Liczba ta, biorąc pod uwagę, że liczba zgłoszeń dla jednego przypadku jest silnie związana z czasem aktywności danego źródła, może być traktowana jako współczynnik uporczywości - przy identycznym sposobie obliczenia dla poszczególnych systemów autonomicznych będzie on tym większy, im dłużej źródła utrzymują się „przy życiu" w danej sieci. Niskie wartości mogą wynikać zarówno ze skuteczności operatora w szybkim radzeniu sobie z problemem, jak i z dynamicznego przyznawania adresów. W tym drugim przypadku zarażone maszyny są po prostu identyfikowane jako nowe źródła za każdym razem, gdy odnawiają dzierżawę. Należy więc je interpretować łącznie z liczbą zgłoszeń. Uporczywość dla dziesięciu sieci, których najczęściej dotyczyły zgłoszenia (łącznie 89,5%), wahała się od 1,23 do 23,51.

4. Statystyka zgłoszeń koordynowanych przez CERT Polska

Na uwagę zasługują także wysokie pozycje operatorów mobilnych. Wszyscy oni zmieścili się w pierwszej dziesiątce według bezwzględnej liczby zgłoszeń, łącznie odpowiadając za niemal co piąte zgłoszenie (19,5%). Biorąc pod uwagę unikalne adresy IP zgłoszone jako źródła spamu, niemal wszyscy operatorzy wyprzedzają nawet Telekomunikację Polską! Nieco niżej znajduje się jedynie T-Mobile. Statystyka ta jest niewątpliwie wynikiem sposobu przyznawania adresów w tych sieciach (krótka dzierżawa DHCP), jednak nie powinna być całkowicie lekceważona, ponieważ duże pokrycie przestrzeni adresowej adresami uznanymi za rozsyłające spam może decydować o umieszczaniu znacznych części sieci na czarnych listach. To nie pozostaje bez znaczenia dla użytkowników, którym nagle zostaje uniemożliwione wysyłanie poczty. Wydaje się, że operatorzy mobilni będą musieli zmierzyć się z problemem spamu z ich sieci w niedalekiej przyszłości. Tym bardziej, że usługi mobilnego dostępu do Internetu na pewno nie będą tracić na popularności, a w wielu miejscach już dziś są traktowane jako alternatywa dla stałego łącza.

	ASN	Nazwa operatora	Liczba zgłoszeń	Udział	Liczba unikalnych źródeł	Udział	Uporczywość
1	12741	NETIA	1 452 218	31,0%	391 405	31,2%	3,71
2	5617	TP	797 275	17,0%	107 477	8,6%	7,42
3	21021	MULTIMEDIA	468 932	10,0%	70 265	5,6%	6,67
4	43447	ORANGE	360 078	7,7%	194 319	15,5%	1,85
5	29314	VECTRA	353 998	7,6%	19 664	1,6%	18,00
6	8374	PLUS	265 747	5,7%	188 951	15,1%	1,41
7	39603	PLAY	182 600	3,9%	147 554	11,8%	1,24
8	20960	Telekomunikacja Kolejowa	128 293	2,7%	5 458	0,4%	23,51
9	12912	T-MOBILE	97 283	2,1%	79 278	6,3%	1,23
10	12476	ASTER	78 451	1,7%	3 348	0,3%	23,43

Tabela 4.5.1. Ranking operatorów według liczby zgłoszeń spamu

4.6 Skanowanie

Wszystkie zgłoszenia ujęte w poniższych statystykach były przekazane automatycznie. Ogółem otrzymaliśmy 5 703 211 zgłoszeń o skanowaniu, którym źródłem była Polska. W zestawieniu uwzględniono dane przysyłane przez naszych partnerów z ich systemów monitoringu oraz pochodzące z systemu ARAKIS.

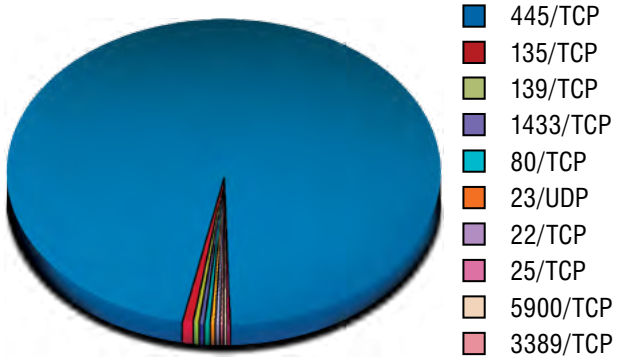
Najczęściej skanowane usługi

Statystyki w Tabeli 4.6.1 przedstawiają TOP 10 portów docelowych pod kątem unikalnych źródłowych adresów IP, których źródłem były adresy IP z Polski.

4. Statystyka zgłoszeń koordynowanych przez CERT Polska

Pozycja	Port docelowy	Liczba unikalnych IP	Zmiana w stosunku do 2010 r.	Prawdopodobny wiodący mechanizm ataków
1	445/TCP	205 243	-29,00%	Ataki typu buffer overflow na usługi Windows RPC
2	135/TCP	2 560	0,00%	Ataki na windowsową usługę DCE/RPC
3	139/TCP	2 062	95,00%	Ataki na usługę NetBIOS / współdzielenie plików i drukarek
4	1433/TCP	1 124	100,00%	Ataki na MS SQL
5	80/TCP	914	63,50%	Ataki na aplikacje webowe
6	23/TCP	440	40,00%	Ataki na usługę telnet
7	22/TCP	435	-1,00%	Ataki słownikowe na serwery SSH
8	25/TCP	434	62,00%	Prawdopodobne próby rozsyłania spamu
9	5900/TCP	401	29,00%	Ataki na VNC
10	3389/TCP	394	166,00%	Ataki słownikowe na RDP (zdalny pulpit) - w dużej mierze aktywność robaka Morto

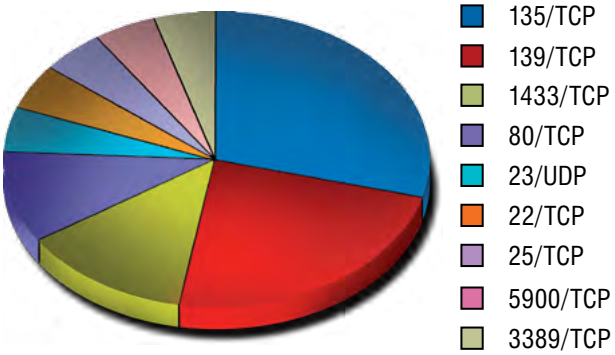
Tabela 4.6.1. TOP 10: porty docelowe pod kątem unikalnych źródłowych adresów IP, których źródłem były adresy z Polski



Wykres 4.6.2. TOP 10: unikalne źródłowe IP per port

Pierwsze miejsce w rankingu - podobnie jak w roku ubiegłym - zajmuje port 445/TCP. Większość najpoważniejszych, a więc najczęściej wykorzystywanych luk w systemach Windows znajduje się w usługach nasłuchających na tym porcie. Jednakże pomimo że nadal przewaga tego portu nad pozostałymi jest bardzo duża, to zmalała ona w stosunku do roku 2010. Ponadto zmniejszyła się o około 29% sumaryczna liczba unikalnych adresów IP, które skanowały ten port.

Na drugim miejscu znajduje się nieobecny w zeszłorocznym zestawieniu TOP 10 port 135/TCP, na którym domyślnie nasłuchuje usługa Windows DCE/RPC (Distributed Computing Environment / Remote Procedure Calls). Wielokrotnie wykrywano w niej wiele podatności, poprzez jedną z nich propaguje się znany i działający już od dawna robak Blaster. Jednakże w roku 2011 nie było nowych robaków wykorzystujących do propagacji port 135.



Wykres 4.6.3. TOP 10: unikalne źródła per port (bez 445/TCP)

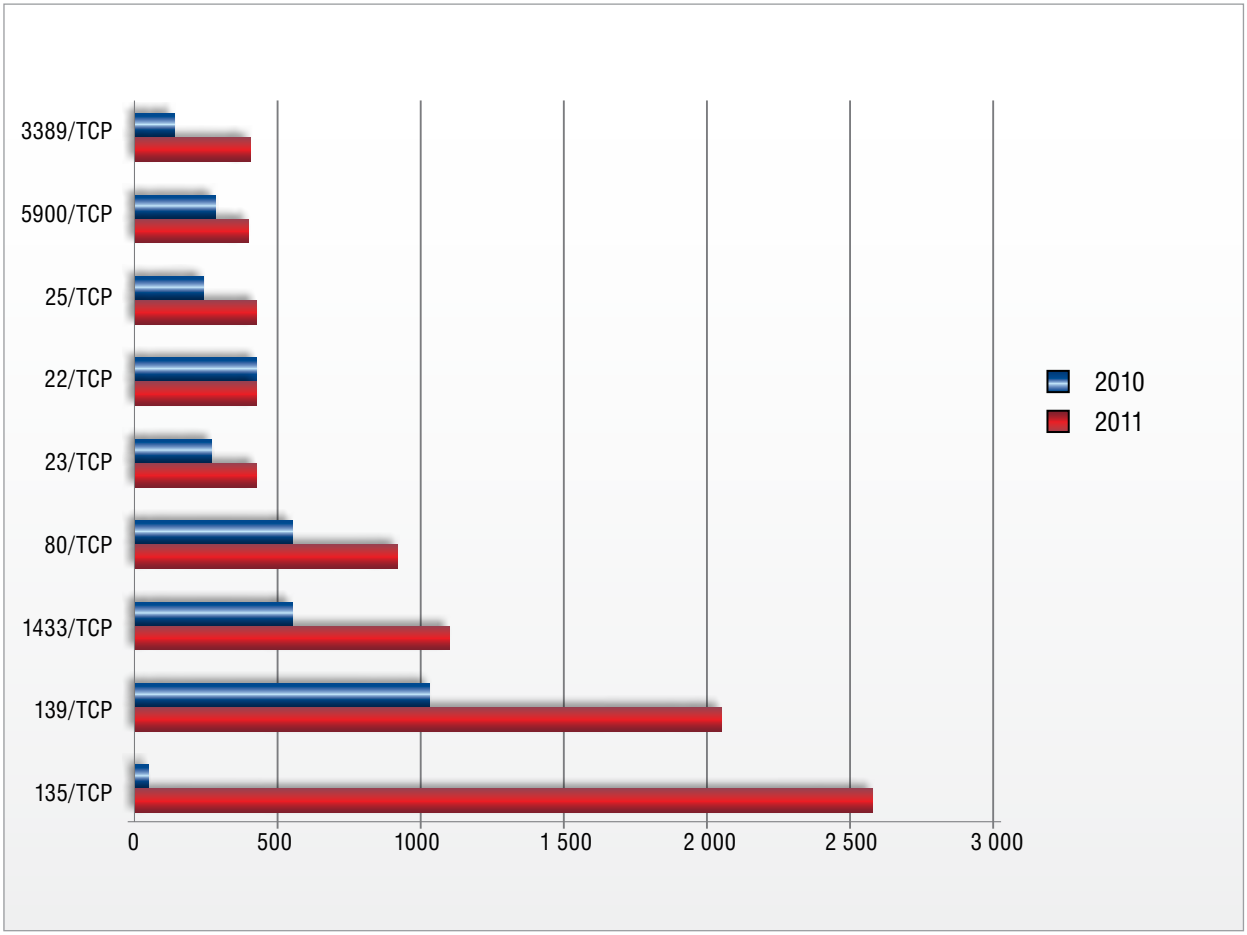
4. Statystyka zgłoszeń koordynowanych przez CERT Polska

W rankingu TOP 10 pojawiły się - oprócz wymienionego wyżej 135/TCP - także porty 25/TCP (usługa pocztowa SMTP) oraz 3389/TCP. Ten ostatni związany jest z usługą Windows Microsoft Terminal Server używającą protokołu RDP (wykorzystywany przez tzw. zdalny pulpit). Pojawienie się go w rankingu w większości przypadków spowodowane jest działającym w sieciach od sierpnia robakiem Morto, który masowo infekował systemy Windows i propagował się dalej. Co ciekawe, Morto nie wykorzystuje żadnej luki, a jedynie odgaduje hasła użytkowników. Jednocześnie - poza aktywnością robaka Morto - obserwowaliśmy wzrost skanowań na tym porcie niezwiązanych z robakiem.

W stosunku do roku ubiegłego wzrosło zainteresowanie prawie wszystkimi portami wymienionymi w rankingu, poza 445/TCP. Znaczący wzrost został zaobserwowany przede wszystkim na portach 1443/TCP (ok. +100%) - usługa Microsoft SQL Server, 139/TCP (ok. +95%) - usługa NetBIOS, 80/TCP (ok. 64%) - aplikacje webowe, oraz 23/TCP (ok. +40%) - usługa telnet.

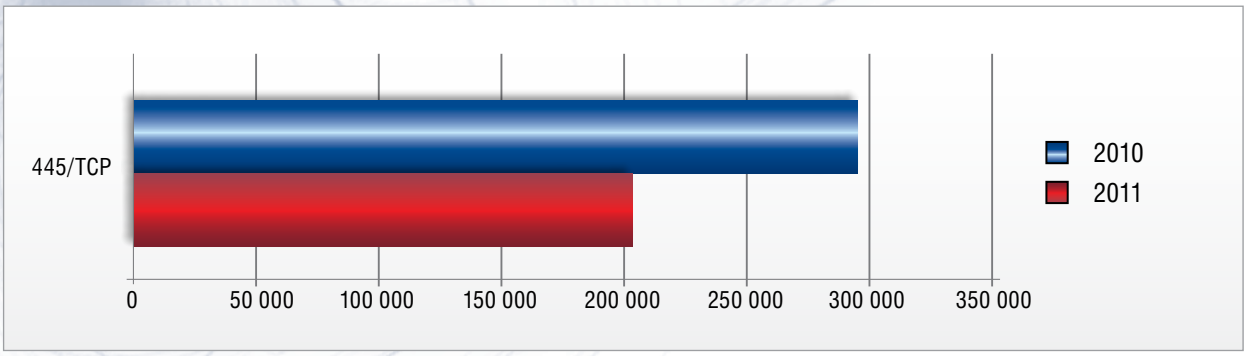
Podobnie jak w roku ubiegłym, interesujący jest fakt stosunkowo wysoko ulokowanych ataków na usługi natywne dla systemów Unix/Linux: telnet (port 23/TCP) oraz SSH (22/TCP). W przypadku SSH są to w przeważającej większości ataki słownikowe.

Ciekawym zjawiskiem jest brak obecności w pierwszej dziesiątce portu 5060/UDP związanego z atakami na usługę VoIP. Liczba unikalnych IP na tym porcie zmniejszyła się w stosunku do roku 2010 o ok. 66%.



Wykres 4.6.4. TOP 10: unikalne IP per port - porównanie z rokiem 2010

4. Statystyka zgłoszeń koordynowanych przez CERT Polska



Wykres 4.6.5. Unikalne IP per port 445/TCP - porównanie z rokiem 2010

Najbardziej zainfekowane sieci w Polsce

Tabela 4.6.6. przedstawia rozkład zainfekowanych unikalnych adresów IP należących do poszczególnych polskich operatorów.

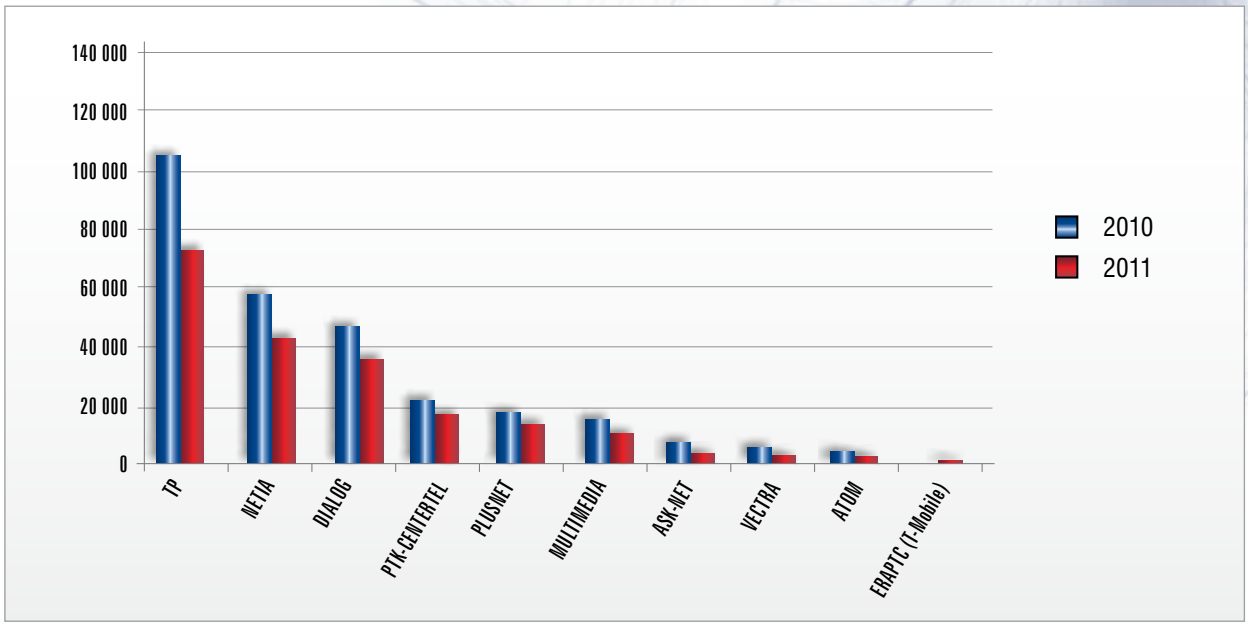
Kolejność numerów AS polskich operatorów jest niemal identyczna jak w roku ubiegłym - jest to jednocześnie odzwierciedlenie wielkości poszczególnych operatorów pod względem liczby użytkowników. Jedyna różnica to wypadnięcie z rankingu UPC (AS9141).

Liczba zainfekowanych komputerów wyraźnie spadła względem roku 2010 u wszystkich operatorów. Największym spadkiem może poszczycić się Vectra (spadek o 57%), ATOM (spadek o 46%), ASK (spadek o 44%) oraz górująca w rankingu TP (spadek o 41%).

Pozycja	Nazwa operatora	Numer ASN	Liczba unikalnych skanujących IP	Zmiana w stosunku do roku 2010
1	TP	AS5617	74 854	-41,00%
2	NETIA	AS12741	43 011	-24,00%
3	DIALOG	AS15857	34 684	-26,50%
4	ORANGE	AS43447	18 441	-25,00%
5	PLUS	AS8374	16 111	-12,40%
6	MULTIMEDIA	AS21021	11 762	-27,80%
7	ASK-NET	AS25388	2 739	-44,00%
8	VECTRA	AS29314	2 052	-57,50%
9	GTS	AS6714	1 749	-46,40%
10	T-MOBILE	AS12912	1 008	–

Tabela 4.6.6. Rozkład zainfekowanych IP w Polsce

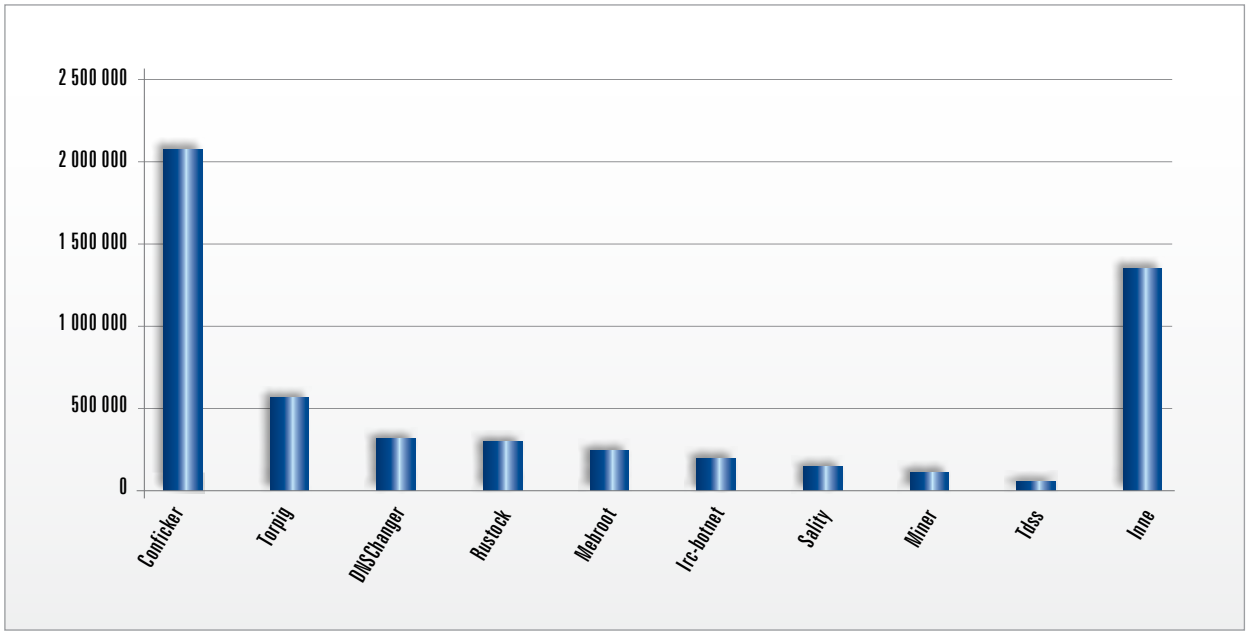
4. Statystyka zgłoszeń koordynowanych przez CERT Polska



Wykres 4.6.7. TOP 10 operatorów w Polsce pod kątem liczby unikalnych skanujących IP

4.7 Boty w polskich sieciach

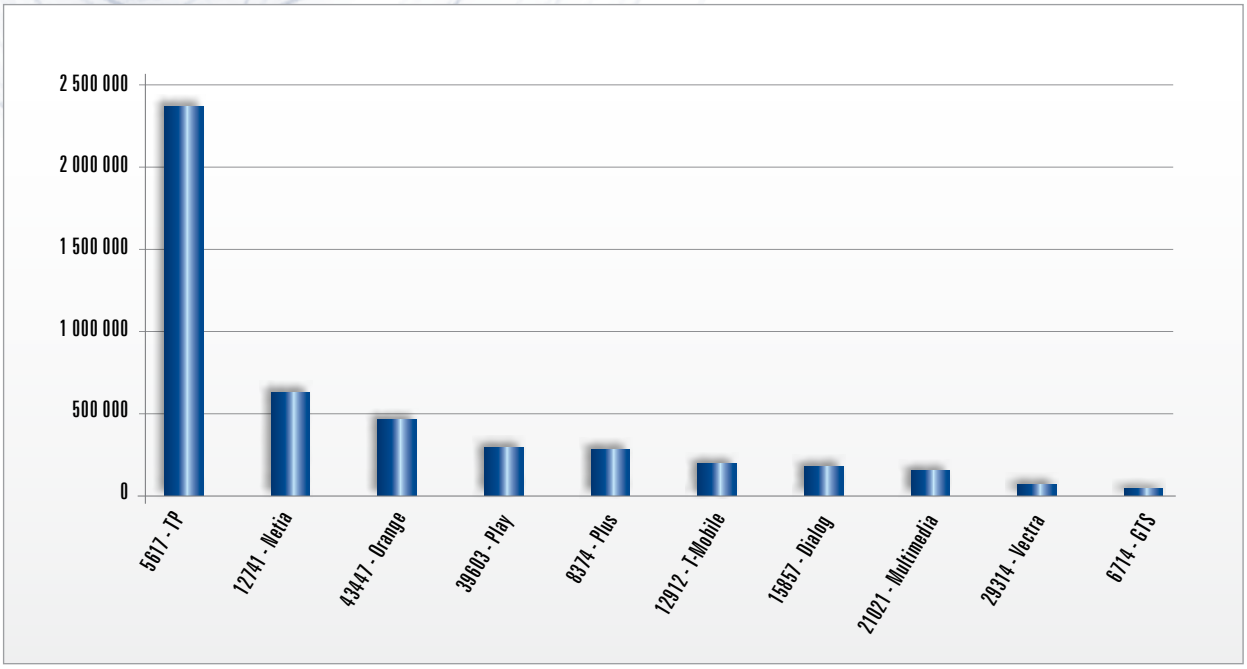
Kategoria ta uwzględnia komputery będące członkami botnetów i znajdujące się w polskich sieciach, a nieuwzględnione w innych kategoriach. Choć najpopularniejszym zastosowaniem botnetów jest rozsyłanie spamu, mogą one być wykorzystane do dowolnych innych zastosowań: wykradania danych wymagających dużego pasma (DDoS) lub dużej mocy obliczeniowej albo po prostu jako dodatkowa warstwa anonimizacji.



Wykres 4.7.1. Liczba botów według typów

4. Statystyka zgłoszeń koordynowanych przez CERT Polska

Najwięcej botów zauważyliśmy w AS 5617 należącym do TP. Była to liczba bliska 2,5 mln, prawie czterokrotnie przewyższająca liczbę botów w AS 12741 należącym do Netii (ok. 630 tys.). Nie ulega wątpliwości, że najwięcej botów znajduje się w sieciach operatorów, którzy dostarczają Internet odbiorcom indywidualnym. Są to duzi dostawcy, tacy jak TP czy Netia, dostawcy Internetu mobilnego - Orange, Play, Plus i T-Mobile oraz dostawcy Internetu w sieciach kablowych - Multimedia i Vectra. Prawie połowa wszystkich botów (ok. 45%) znajdowała się w sieci TP, zaś 12% w sieci Netii.



Wykres 4.7.2. Rozkład botów w poszczególnych AS-ach

4.8 Serwery Command & Control

W 2011 roku otrzymaliśmy 2 263 zgłoszeń (liczonych jako unikalne kombinacje dzień/IP) z systemów automatycznych dotyczących 59 unikalnych serwerów w Polsce wykorzystywanych w charakterze Command & Control do zarządzania botnetami.

Jest to więcej niż w ubiegłorocznym raporcie (za 2010 rok) i półrocznym (za 2011 rok) ze względu na fakt dodania nowych źródeł zewnętrznych.

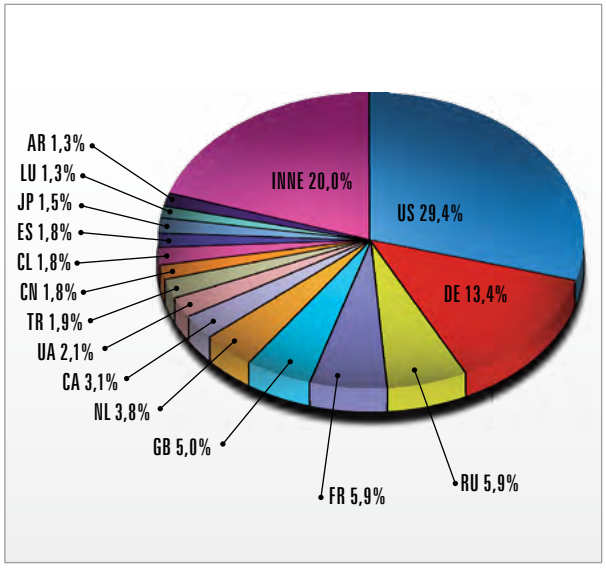
Pozycja	ASN	Operator	Liczba unikalnych C&C
1	16 276	OVH	22
2	16 265	LEASEWEB	9
3	5 617	TP	5
4	12 741	NETIA	5
5	28 753	LEASEWEB	2

Tabela 4.8.1. Liczba unikalnych serwerów C&C w Polsce pod kątem lokalizacji

4. Statystyka zgłoszeń koordynowanych przez CERT Polska

Podobnie jak w latach ubiegłych, większość zgłoszeń dotyczyła serwerów IRC (większość również na przypisanym tej usłudze standardowym porcie 6667/TCP). Zdecydowanym liderem został debiutujący w naszych raportach w tej kategorii francuski OVH, który podobnie jak holenderski LEASEWEB ma w RIPE sieci przypisane do Polski.

W skali światowej już tradycyjnie najwięcej kontrolerów C&C znajdowało się w USA - 29,4%. Razem z Niemcami Stany Zjednoczone hostują ich prawie 50%. Podobnie jak w zeszłym roku, w czołówce znajdują się państwa zachodnioeuropejskie, takie jak Francja, Wielka Brytania i Holandia. Wyżej niż w ubiegłorocznym raporcie znajduje się Rosja - na 3. miejscu. Z kolei Chiny znowu znajdują się relatywnie nisko - dopiero na 10 pozycji. Według danych nam dostępnych również Polska pod tym względem prezentuje się bardzo korzystnie, dopiero na 23 miejscu.



Wykres 4.8.1. Kraje, w których najczęściej znajdowały się serwery C&C

4.9 Ataki DDoS

W roku 2011 otrzymaliśmy 16 automatycznych zgłoszeń zawierających informacje o atakach DDoS na serwery znajdujące się w polskich sieciach. Były to przypadki wydania rozkazu, zauważone na inwigilowanych serwerach C&C. Cztery ataki zostały wykonywane na serwery gier. Pozostałe według naszych analiz dotyczyły użytkowników indywidualnych. Jest to więcej niż w 2010 roku, w którym odnotowaliśmy 11 takich przypadków, jednak w dalszym ciągu niewiele w porównaniu do innych kategorii zgłoszeń. Niestety, nie wynika to z tego, że ataków takich rzeczywiście jest niewiele. Raczej jest to problem braku monitorowania w sposób automatyczny przez strony trzecie tego typu ataków.

4.10 Ataki brute-force

Otrzymaliśmy 159 687 zgłoszeń dotyczących ślepych prób logowania się do usług. Ataki takie, zwane „brute-force", służyły kiedyś do odgadywania haseł metodą prób i błędów. Dziś zazwyczaj związane są z próbami uzyskania dostępu poprzez użycie domyślnych haseł, błędów w konfiguracji lub podatności w implementacji funkcji logowania.

Wszystkie zgłoszenia dotyczyły prób logowania do usługi SSH. Ich liczba nie odpowiada jednak zdecydowanie skali problemu. Wszystkie próby pochodziły bowiem jedynie ze 127 unikalnych adresów IP. Daje to średnio 1 257 prób/adres, przy czym mediana rozkładu wynosi 11, a 85% adresów wygenerowało mniej niż 1000 prób. Dane te, zgodnie ze statystykami z rozdziału 4.6 pokazują, że ataki na serwisy takie jak SSH są dziś znacznie mniej popularne niż kilka lat temu. Z pewnością jest to w dużej mierze konsekwencją coraz większej skuteczności zabezpieczeń technicznych, a także polityk bezpieczeństwa - przynajmniej w zakresie dostępu zdalnego. Włamywacze, zupełnie racjonalnie, poszukują dziś łatwiejszych celów, wykorzystując choćby inżynierię społeczną czy aplikacje webowe, które z definicji muszą być udostępnione publicznie.

Większość wspomnianych prób miała miejsce od końca lutego do końca marca 2011 roku.

4. Statystyka zgłoszeń koordynowanych przez CERT Polska

4.11 Serwery Fast-flux

Fast-flux to technologia polegająca na rozproszeniu infrastruktury (w szczególności serwerów treści) na wielu maszynach - zazwyczaj będących częścią botnetu - w celu utrudnienia jej inwigilacji i usunięcia. Metoda ta jest często wykorzystywana m.in. przy phishingu, spamie (do utrzymywania stron, na które zwabiani są odbiorcy) czy dystrybucji pornografii. Fast-flux wykorzystuje domeny administrowane przez przestępców. Odpowiednie rekordy są często i cyklicznie zmieniane, w każdej chwili oferując kilka adresów IP dla danej nazwy domenowej. W 2011 r. otrzymaliśmy 757 zgłoszeń przypadków hostowania domen Fast-flux w adresach IP polskich sieci. Jak nietrudno się domyślić, wszystkie komputery wykorzystywane w procederze znajdowały się w sieciach dostarczających Internet użytkownikom końcowym, co widać w tabeli 4.11.1.

Liczba zgłoszeń	ASN	Operator
613	5 617	TP
82	12 741	Netia
42	29 314	Vectra
16	21 021	Multimedia
3	12 476	Aster
1	13 119	ACI

Tabela 4.11.1. Lokalizacja komputerów wykorzystywanych do sieci Fast-flux

Zgłoszenia dotyczyły 17 różnych domen, z których najbardziej aktywna korzystała z aż 336 polskich adresów. W przypadku większości domen wykorzystywana infrastruktura była znacznie mniejsza, najczęściej obejmując nie więcej niż 52 polskie adresy IP (15 domen).

Obserwowany czas wykorzystywania pojedynczej domeny w polskich sieciach (prawdopodobnie blisko związany z jej czasem życia) wynosił nie więcej niż 2 miesiące. Co ciekawe, nie zaobserwowaliśmy żadnego przypadku wykorzystywania jednego adresu dla więcej niż jednej domeny. Może to świadczyć o tym, że poszczególne botnety nie dzielą ze sobą infrastruktury i nie są wynajmowane konkurencji, przynajmniej do usług Fast-flux.

4.12 Otwarte serwery DNS

W tej kategorii znajdują się źle skonfigurowane serwery DNS, umożliwiające rekursywne odpytywanie z dowolnego miejsca w sieci. Takie ustawienie pozwala na wykorzystywanie ich w atakach DDoS przez zwiększenie wolumenu ruchu (*traffic amplification*) w wyniku zapytań DNS ze sfałszowanym adresem źródłowym.

W 2011 r. otrzymaliśmy aż 581 428 informacji o 160 682 unikalnych adresach IP, na których znajdowały się takie serwery. Wskazuje to na sporą skalę tego problemu w Polsce. Rozkład dziesięciu systemów autonomicznych, w których najczęściej umieszczone były otwarte serwery DNS, znajduje się w tabeli 4.12.1.

Liczba zgłoszeń	% udział w zgłoszeniach	ASN	Operator
63574	39,6%	5 617	TP
18667	11,6%	12 741	Netia
16941	10,5%	43 447	Orange
7023	4,4%	20 960	TKTELEKOM
6157	3,8%	6 714	GTS
4116	2,6%	50 994	E-SBL-AS e-SBL.net
3430	2,1%	21 021	MULTIMEDIA
2722	1,7%	29 314	VECTRA
1998	1,2%	29 665	SPEED-SOFT
1798	1,1%	13 000	LEON-AS

Tabela 4.12.1. Rozkład dziesięciu systemów autonomicznych, w których najczęściej umieszczone były otwarte serwery DNS

4.13 Pozostałe zgłoszenia

Pozostałe 14,5 tys. zgłoszeń dotyczyło rozmaitych rodzajów automatycznie wykrywanych zagrożeń, przede wszystkim nieprawidłowo skonfigurowanych urządzeń, takich jak serwery proxy czy routery.

5. Statystyka incydentów obsłużonych przez CERT Polska

Ta część raportu poświęcona jest incydentom zarejestrowanym w systemie obsługi zgłoszeń, a więc takim, które zostały obsłużone bezpośrednio przez zespół CERT Polska. W wielu aspektach są one uzupełnieniem obrazu zaprezentowanego w rozdziale 3, uwzględniają bowiem zjawiska wychodzące poza automatyczne systemy zbierania informacji - mniej masowe, lecz często poważne, wymagające interwencji człowieka.

5.1 Liczba przypadków naruszających bezpieczeństwo teleinformatyczne

W roku 2011 obsłużyliśmy 605 incydentów naruszajacych bezpieczeństwo teleinformatyczne. W następnych rozdziałach znajduje się ich szczegółowa klasyfikacja.

5.2 Typy odnotowanych incydentów

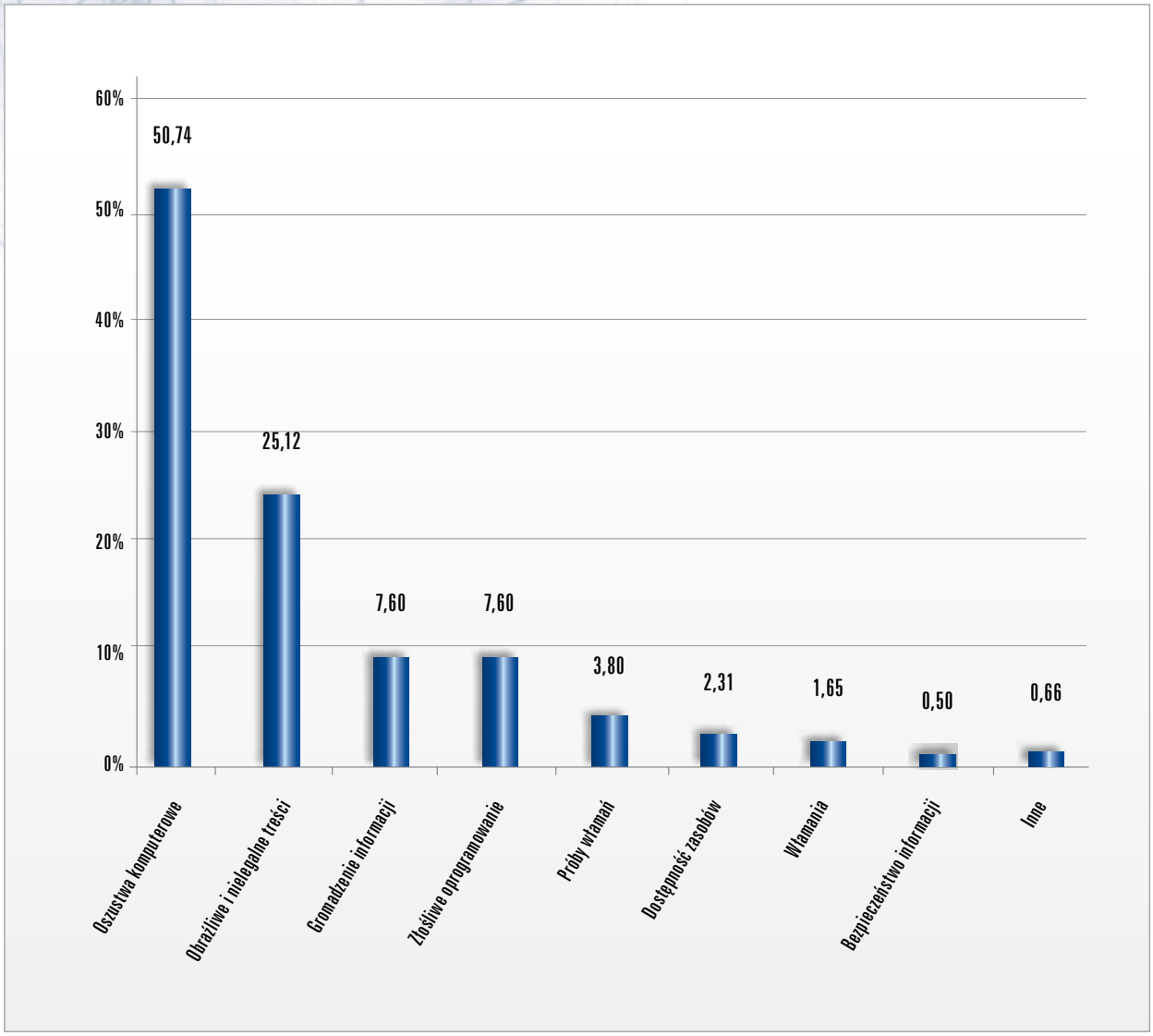
Typ/Podtyp incydentu	Liczba	Suma-typ	Procent-typ
Obraźliwe i nielegalne treści	2	152	25,12
Spam	144		
Dyskredytacja, obrażanie	3		
Pornografia dziecięca, przemoc[5]	3		
Złośliwe oprogramowanie	39	46	7,60
Wirus	2		
Robak sieciowy	0		
Koń trojański	5		
Oprogramowanie szpiegowskie	0		
Dialer	0		
Gromadzenie informacji	1	46	7,60
Skanowanie	42		
Podsłuch	0		
Inżynieria społeczna	3		
Próby włamań	7	23	3,80
Wykorzystanie znanych luk systemowych	11		
Próby nieuprawnionego logowania	5		
Wykorzystanie nieznanych luk systemowych	0		
Włamania	3	10	1,65
Włamanie na konto uprzywilejowane	4		
Włamanie na konto zwykłe	2		
Włamanie do aplikacji	1		
Atak na dostępność zasobów	0	14	2,31
Atak blokujący serwis (DoS)	3		
Rozproszony atak blokujący serwis (DDoS)	11		
Sabotaż komputerowy	0		
Atak na bezpieczeństwo informacji	0	3	0,50
Nieuprawniony dostęp do informacji	2		
Nieuprawniona zmiana informacji	1		
Oszustwa komputerowe	1	307	50,74
Nieuprawnione wykorzystanie zasobów	0		
Naruszenie praw autorskich	1		
Kradzież tożsamości, podszycie się (w tym phishing)	305		
Inne	4	4	0,66
SUMA	605	605	100

Tabela 5.2.1. Incydenty obsłużone przez CERT Polska według typów

[5] *Wszelkie zgłoszenia dotyczące nielegalnych treści w rozumieniu polskiego prawa kierowane są do zespołu Dyżurnet.pl, również działającego w ramach NASK (http://www.dyzurnet.pl/)*

5. Statystyka incydentów obsłużonych przez CERT Polska

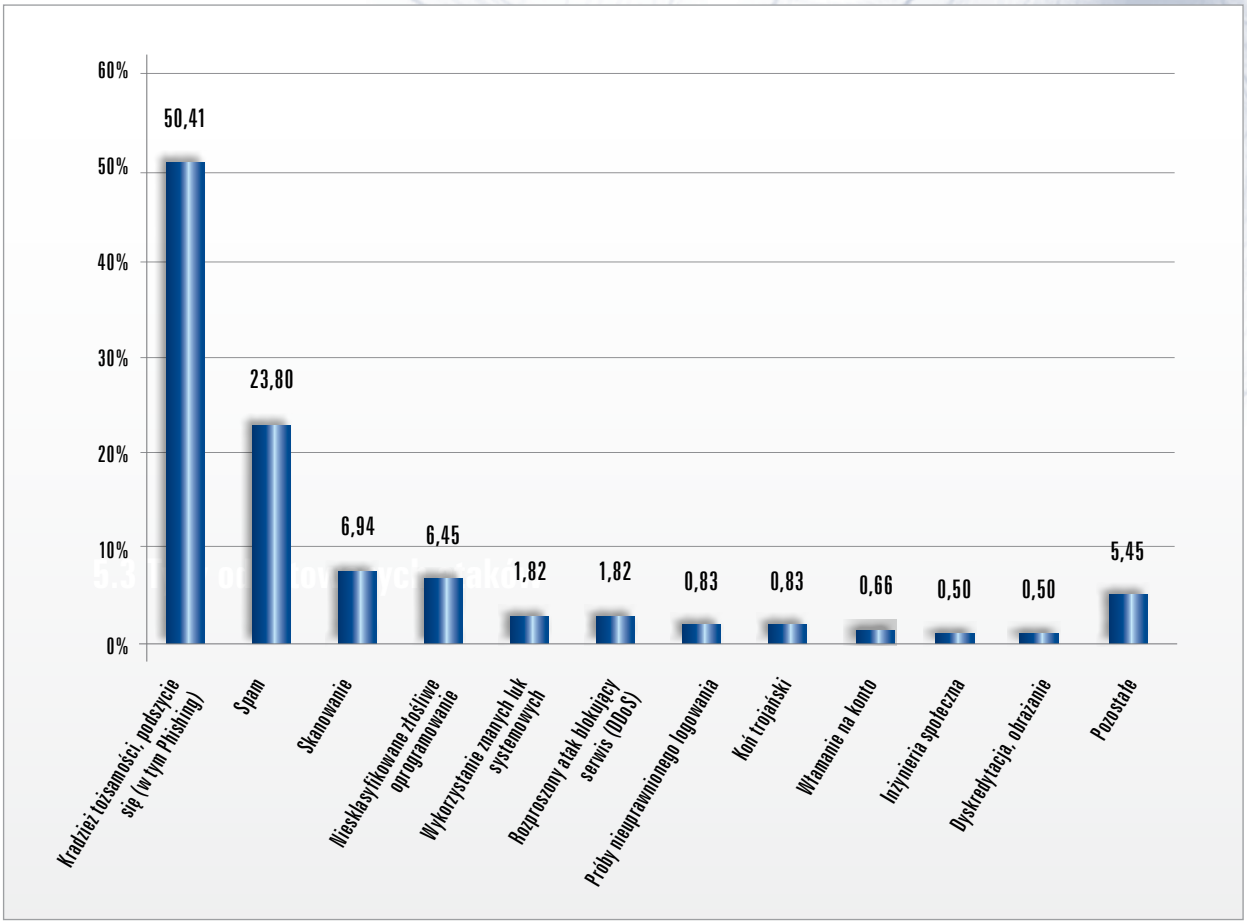
5.3 Typy odnotowanych ataków



Wykres 5.3.1. Rozkład procentowy typów incydentów

Tak jak w roku poprzednim najczęściej występującym typem incydentów były *Oszustwa komputerowe* (50,74%). Należy zaznaczyć, że w roku 2011 odnotowaliśmy ich o 1/3 więcej niż w roku 2010 (38,5%). W głównej mierze, wpływ miały tu zgłoszenia dotyczące *Kradzieży tożsamości*, podszycia się, szczególnie te dotyczące *Phishingu*. *Oszustwa komputerowe* stały się zdecydowanie dominującym typem incydentów. Na drugiej pozycji odnotowaliśmy *Obraźliwe i nielegalne treści*. Stanowiły one 25,12% zarejestrowanych przypadków. Najczęściej w tej kategorii mieliśmy do czynienia ze zgłoszeniami rozsyłanego spamu. Na trzeciej pozycji ex aequo zanotowaliśmy *Gromadzenie informacji* oraz *Złośliwe oprogramowanie* (po 7,6%). Obydwa typy mają mniejszy udział niż w roku poprzednim. *Złośliwe oprogramowanie* o 5,9%, zaś *Gromadzenie informacji* o 2,19%.

5. Statystyka incydentów obsłużonych przez CERT Polska



Wykres 5.3.2. Rozkład procentowy podtypów incydentów

W przypadku podtypów incydentów najczęściej występowała *Kradzież tożsamości, podszycie się* (50,41%). Oznacza to wzrost aż o 1/3 w stosunku do roku 2010. Praktycznie wszystkie zgłoszone incydenty dotyczyły *Phishingu* umieszczonego na polskich serwerach. Ofiarami były najczęściej instytucje finansowe z zagranicy. Odnotowaliśmy 29 przypadków dotyczących polskich podmiotów.

23,8% incydentów dotyczyło Spamu. Były to w większości zgłoszenia pochodzące ze Spam-Copa, dotyczące polskich komputerów, które wysyłały niezamówioną ofertę handlową. Na trzecim i czwartym miejscu odnotowaliśmy kolejno *Skanowania* (6,94%) oraz N*iesklasyfikowane złośliwe oprogramowanie* (6,45%). W porównaniu do roku 2010 na uwagę zasługuje dwukrotny spadek incydentów dotyczących *Niesklasyfikowanego złośliwego oprogramowania*.

5.4 Zgłaszający, poszkodowani, atakujący

Na potrzeby statystyk odnotowywane są trzy kategorie podmiotów związanych z incydentami: zgłaszający incydent, poszkodowany w incydencie i odpowiedzialny za przeprowadzenie ataku, czyli atakujący.

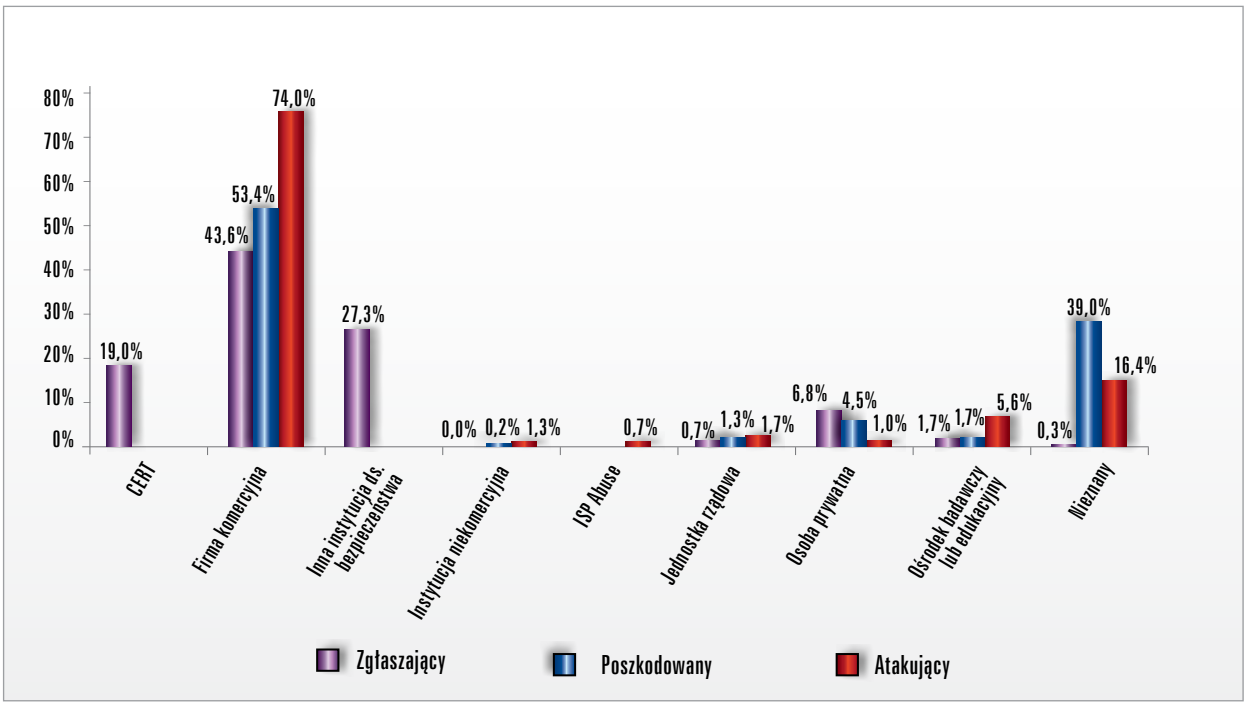
Dodatkowo kategorie te uwzględniane są w rozbiciu na podmiot krajowy i podmiot zagraniczny.

Tabela 5.4.1 przedstawia zbiorcze zestawienie danych dotyczących podmiotów incydentu.

5. Statystyka incydentów obsłużonych przez CERT Polska

Podmiot	Zgłaszający	%	Poszkodowany	%	Atakujący	%
Osoba prywatna	41	6,78	27	4,46	6	0,99
CERT[6]	115	19,01	0	0,00	0	0,00
ISP Abuse	4	0,66	0	0,00	0	0,00
Inna instytucja ds. bezpieczeństwa	165	27,27	0	0,00	0	0,00
Firma komercyjna	264	43,64	323	53,39	448	74,05
Ośrodek badawczy lub edukacyjny	10	1,65	10	1,65	34	5,62
Instytucja niekomercyjna	0	0,00	1	0,17	8	1,32
Jednostka rządowa	4	0,66	8	1,32	10	1,65
Nieznany	2	0,33	236	39,01	99	16,36
Kraj	126	20,83	80	13,22	520	85,95
Zagranica	478	79,01	299	49,42	13	2,15
Nieznany	1	0,17	226	37,36	72	11,9

Tabela 5.4.1. Rodzaje podmiotów ujętych w klasyfikacji incydentów



Wykres 5.4.2. Źródła zgłoszeń, atakujący i poszkodowani

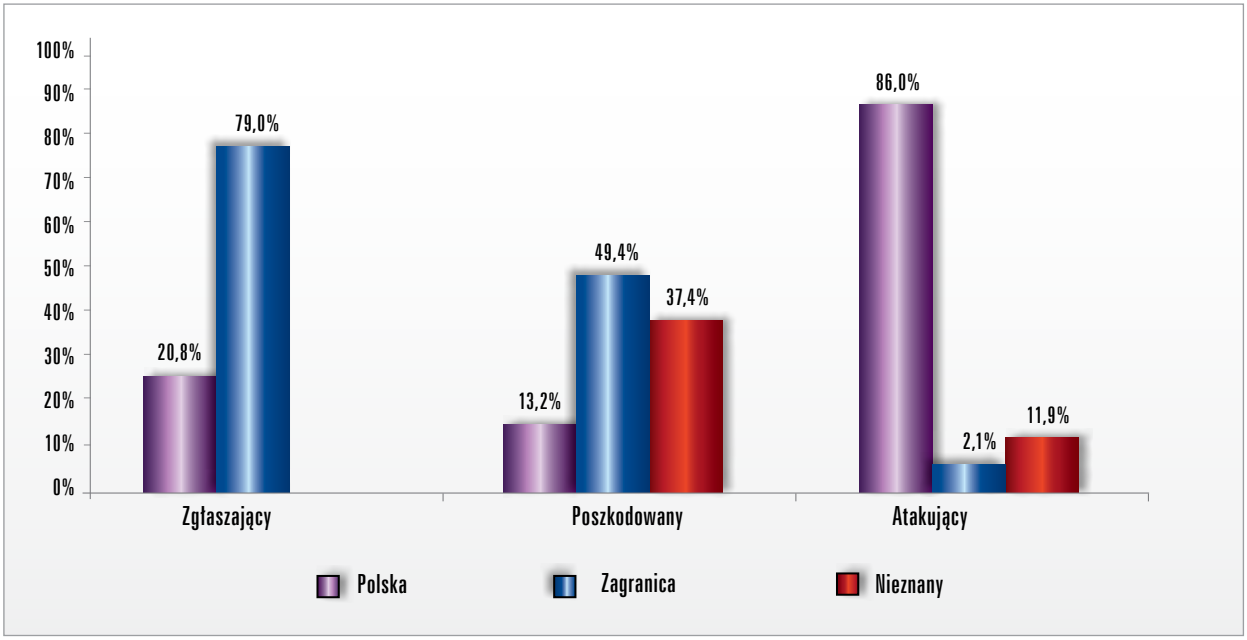
[6] *Zawiera zgłoszenia pochodzące z systemów automatycznych, w tym także z systemu ARAKIS*

5. Statystyka incydentów obsłużonych przez CERT Polska

W roku 2011 najczęściej otrzymywaliśmy zgłoszenia od *Firm komercyjnych* (43,6%). W większości dotyczyły one *Phishingu* i były przesyłane przez instytucje finansowe bądź też podmioty je reprezentujące. 27,3% incydentów było zgłoszonych przez inną *Instytucję ds. bezpieczeństwa*. Większość z nich pochodziła ze SpamCopa i dotyczyła rozsyłania spamu przez polskich użytkowników Internetu. 19% zgłoszeń otrzymaliśmy od innych zespołów CERT. Najczęściej dotyczyły one *Phishingu*.

W ponad połowie przypadków (53,4%) poszkodowanym podmiotem były *Firmy komercyjne*. Najczęściej padały one ofiarą *Phishingu*. W 39% *Poszkodowany* pozostawał *Nieznany*. Jest to wynik zgłoszeń, dotyczących głównie *Spamu* i *Skanowania*, które były przesyłane przez *Zgłaszającego* (np. SpamCopa) w imieniu osób trzecich.

Aż w 74% przypadków atakującym była *Firma komercyjna*. Jest to wynik, na który w dużej mierze mają wpływ lokalni dostawcy Internetu oraz firmy hostingowe. CERT Polska zazwyczaj nie posiada informacji o końcowym użytkowniku, znajdującym się za bramą lokalnego dostawcy oraz o właścicielu strony WWW umieszczonej w farmie hostingowej. Wówczas za atakującego przyjmuje się ostatni znany podmiot czyli *Firmę komercyjną*. Najczęściej hostowała ona *Phishing* oraz rozsyłała *Spam*. 16,4% *Atakujących* pozostało nieznanych. Tak jak w latach poprzednich ukrywał się on za serwerem Proxy, botnetem, TOR-em czy przejętą maszyną nieświadomej ofiary.



Wykres 5.4.3. Pochodzenie zgłaszającego, poszkodowanego i atakującego

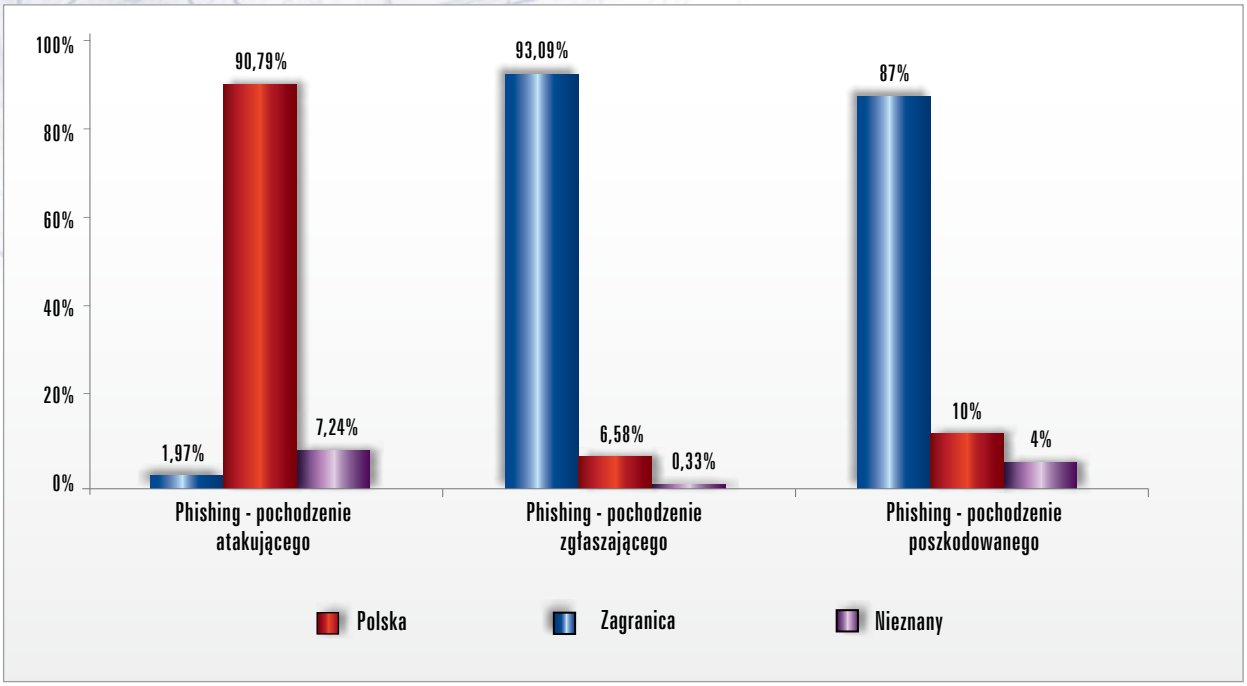
W 2011 roku zgłaszający aż w 79% pochodzili z zagranicy. Jest to wynik dużej ilości incydentów dotyczących *Phishingu* oraz *Spamu*, które były raportowane przez zagraniczne podmioty. Tylko w 1/5 przypadków *Zgłaszający* pochodził z Polski.

Prawie połowa poszkodowanych pochodziła z zagranicy. Większości z nich padła ofiarą *Phishingu*. Aż w 37,4% przypadków pochodzenia *Poszkodowanego* pozostało nieznane. Jest to wynik wspomnianych wcześniej zgłoszeń, składanych np. przez Spamcopa w imieniu osób trzecich. Tylko 13,2% *Poszkodowanych* pochodziło z Polski.

W przypadku *Atakujących* aż 86% pochodziło z Polski. Jest to naturalną konsekwencją obsługi zgłoszeń dotyczących domeny .pl. Tylko 11,9% *Atakujących* pochodziło z zagranicy. Głównie były to incydenty dotyczące hostowania *Phishingu*.

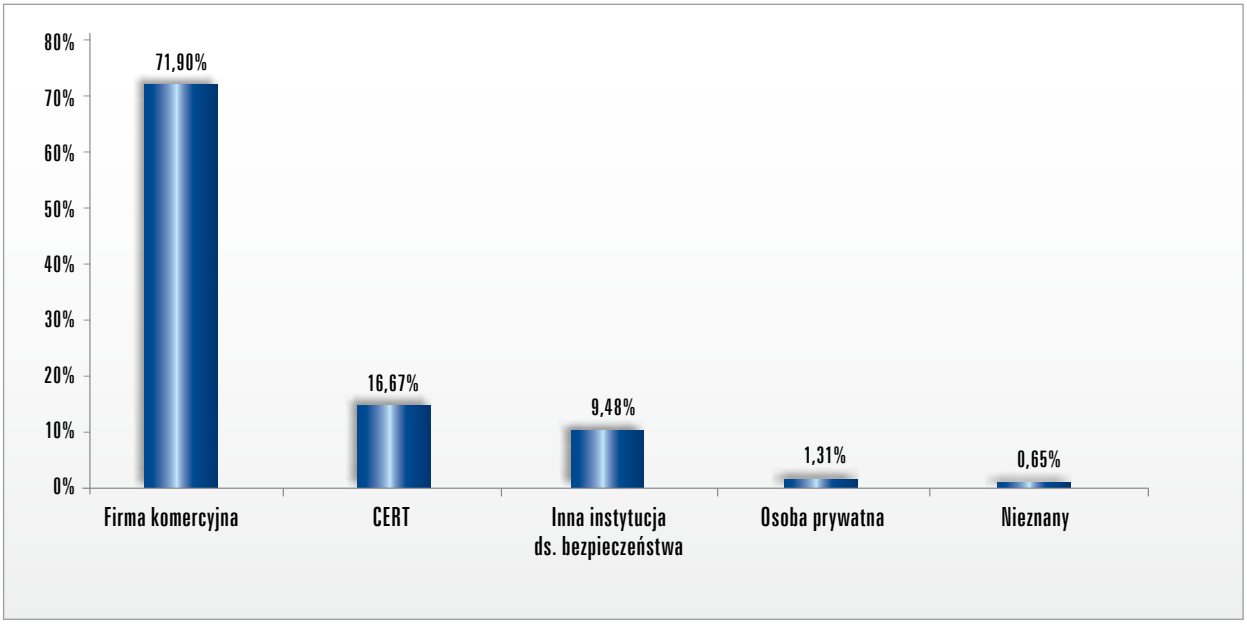
6. Statystyki dodatkowe, dotyczące zgłoszeń obsługiwanych ręcznie

6.1 Phishing w roku 2011



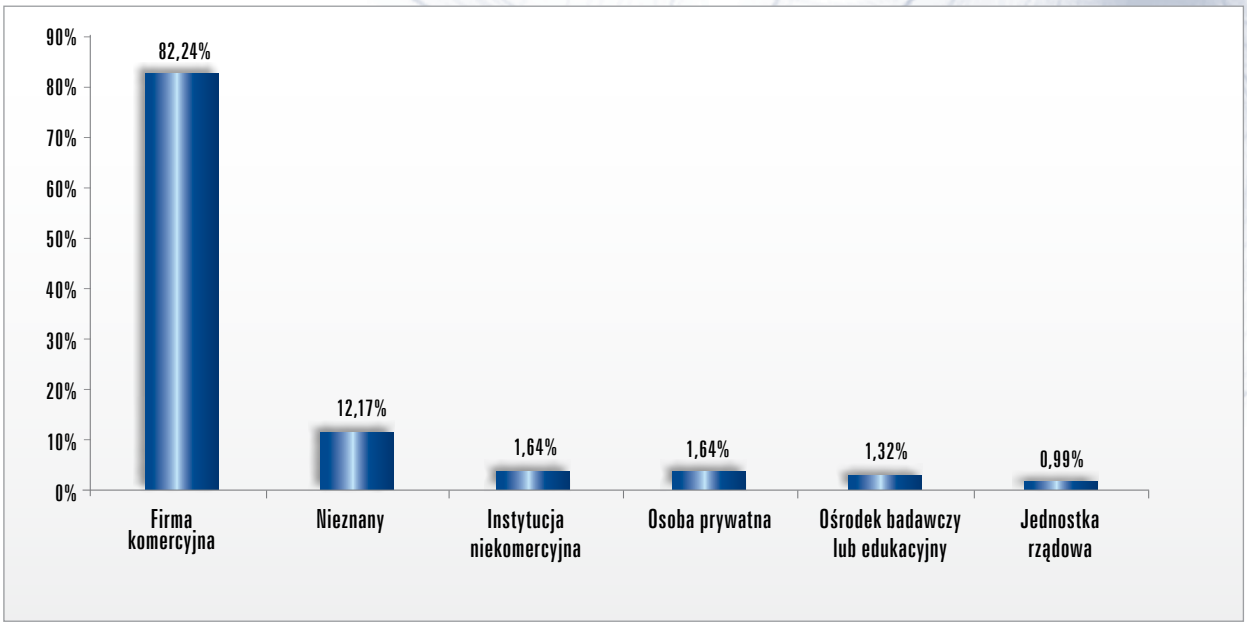
Wykres 6.1.1. Phishing - pochodzenie atakującego, zgłaszającego i poszkodowanego

Ponieważ docierają do nas głównie zgłoszenia dotyczące polskich sieci, to najczęściej odnotowywaliśmy *Phishing* umieszczony na polskich serwerach. Stanowił on 90,79% ogółu. Jeżeli chodzi o zgłaszających to pochodzili oni w większości z zagranicy (93,09%). Ofiarą najczęściej były również podmioty zagraniczne (87%). Tylko 10% incydentów dotyczyło polskich podmiotów.



Wykres 6.1.2. Phishing - zgłaszający

6. Statystyki dodatkowe, dotyczące zgłoszeń obsługiwanych ręcznie

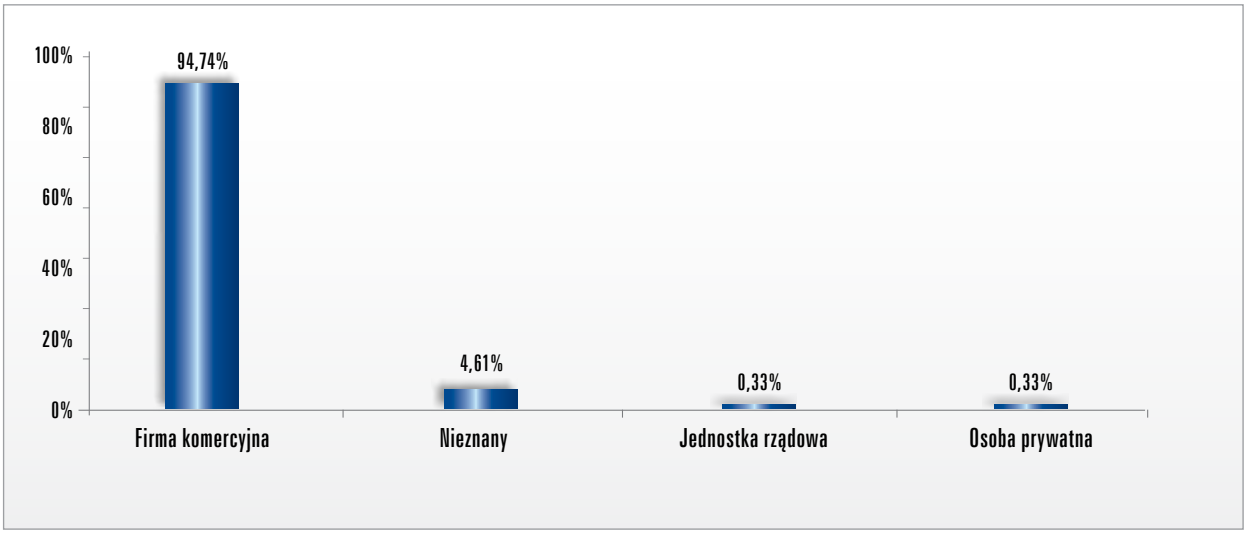


Wykres 6.1.3. Phishing - atakujący

Phishing był najczęściej zgłaszany przez *Firmę komercyjną* (71,9%). Były to głównie atakowane podmioty finansowe lub firmy je reprezentujące. 16,67% zgłoszeń pochodziło od zespołów typu CERT. 9,48% incydentów zgłosiły *Inne instytucje ds. bezpieczeństwa*.

W przypadku atakującego, najczęściej mieliśmy do czynienia z *Firmą komercyjną* (82,24%). Były to zazwyczaj przypadki *Phishingu* umieszczonego na serwerach firm świadczących usługi hostingowe. W ponad 12% przypadków nie udało nam się ustalić tożsamości atakującego. Były to zazwyczaj maszyny, które hostowały tylko i wyłącznie stronę podszywającą się pod daną instytucję, a wpisy w bazie ripe.net zawierały tylko dane ISP.

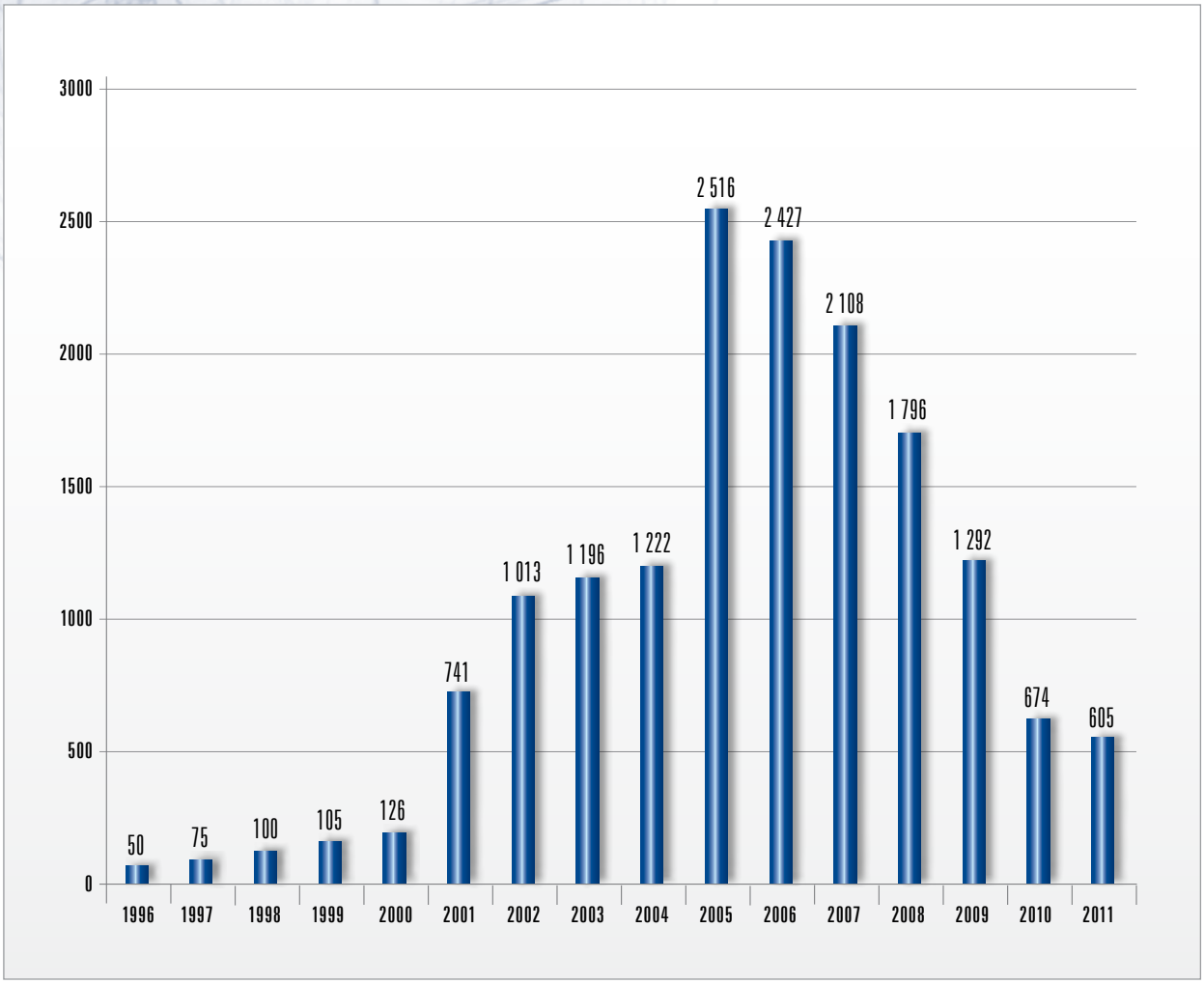
Aż 94,74% ofiar stanowiły *Firmy komercyjne*. Były to głównie zagraniczne podmioty finansowe. W 4,61% ofiara pozostała nieznana. Są to przypadki, gdzie w momencie obsługi zgłoszenia fałszywa strona została już zablokowana, a treść zgłoszenia oraz ciągi w adresie nie wskazywały na konkretny podmiot.



Wykres 6.1.4. Phishing - poszkodowani

7. Trendy w kolejnych latach

7.1 Liczba incydentów w latach 1996 – 2011



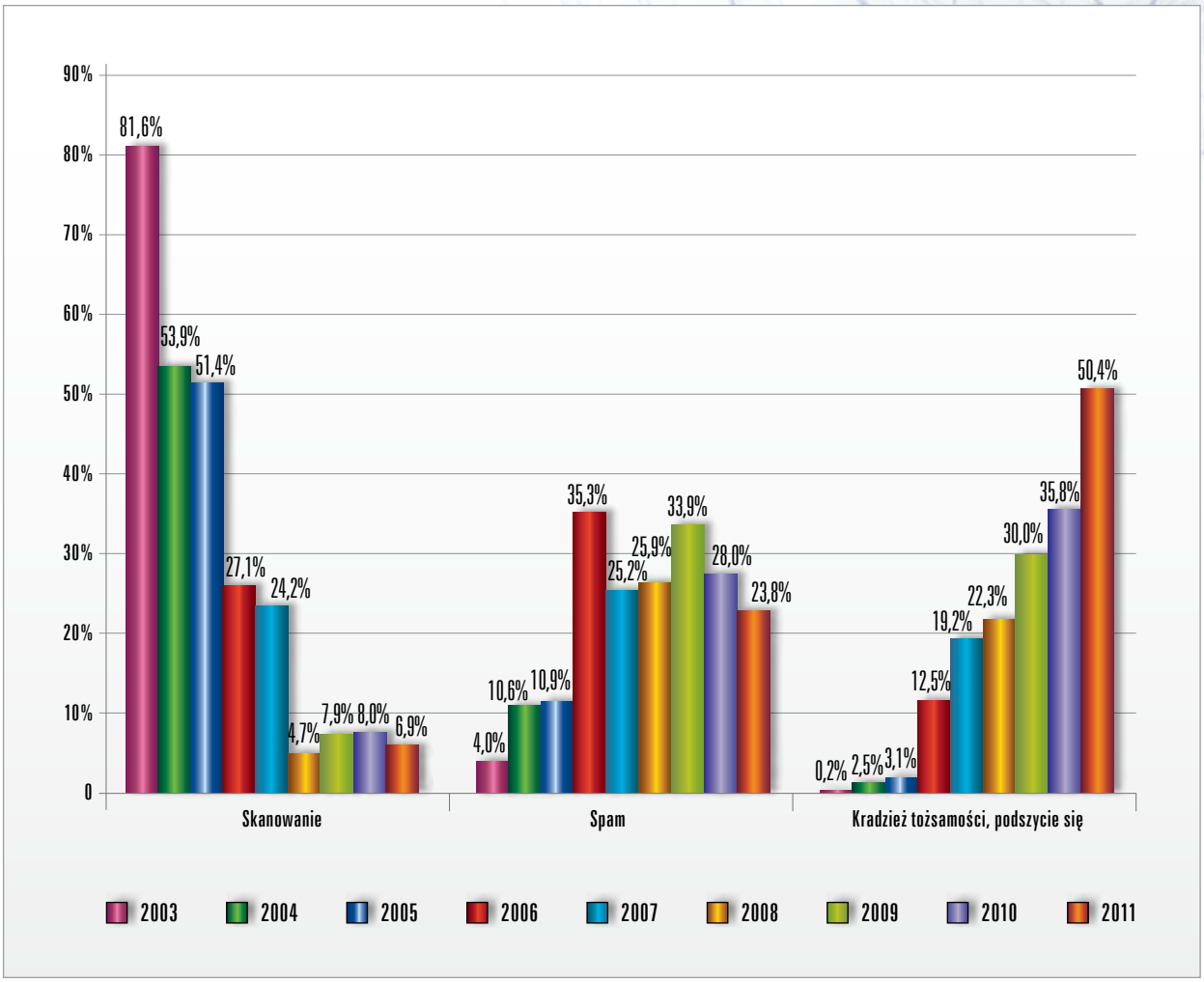
Wykres 7.1.1. Liczba incydentów w latach 1996 – 2010

Kolejny rok z rzędu zanotowaliśmy mniejszą liczbę incydentów. Od kliku lat zauważamy, że dociera do nas coraz mniej zgłoszeń dotyczących polskich ISP. Zgłoszenia trafiają bezpośrednio do właściciela sieci. Poziom obsługi incydentów przez dużych dostawców Internetu i treści oraz firmy hostingowe jest z roku na rok wyższy. W związku z tym zespół CERT Polska notuje coraz mniej próśb o pomoc w przypadku, gdy nie ma reakcji z ich strony.

Zgłoszenia trafiające do CERT Polska są za to coraz bardziej poważne i skomplikowane, jak np. te dotyczące *Phishingu* i *Złośliwego oprogramowania*, a proces ich obsługi znacznie się wydłużył. Obsługa spraw dotyczących kontrolerów odpowiedzialnych za ataki na użytkowników polskich banków potrafi zająć nawet kilka tygodni.

7.2 Rozkład procentowy podtypów incydentów w latach 2003 – 2011

Od roku 2003 statystyki są tworzone w oparciu o tę samą klasyfikację. Umożliwia to nam porównanie rozkładu procentowego incydentów na przestrzeni czasu (patrz wykres 7.2.1).



Wykres 7.2.1. Rozkład procentowy podtypów incydentów w latach 2003 – 2011

W roku 2011 nie nastąpiła znacząca zmiana trendów zaobserwowanych w poprzednich latach. *Skanowania* nadal są marginalne w porównaniu z latami 2003 – 2005. Od kilku lat utrzymują się na poziomie kilku procent. W przypadku *Spamu* od kilku lat nie notujemy dużych wzrostów czy spadków. Pomimo tego *Spam* stanowi niezmiennie znaczący odsetek incydentów.

Dodatkowo należy podkreślić, że skala zjawiska jest o wiele większa. CERT Polska odnotowuje tylko zgłoszone przypadki spamu rozsyłanego przez maszyny znajdujące się w obrębie domeny .pl. Nadal utrzymuje się wyraźny trend wzrostowy jeżeli chodzi o incydenty dotyczące *Kradzieży tożsamości, podszycia się*. Jest to w chwili obecnej najczęściej pojawiający się incydent. W porównaniu do 2010 roku, zanotowaliśmy wzrost w tej kategorii o 40%.

8. Najważniejsze zjawiska okiem CERT Polska

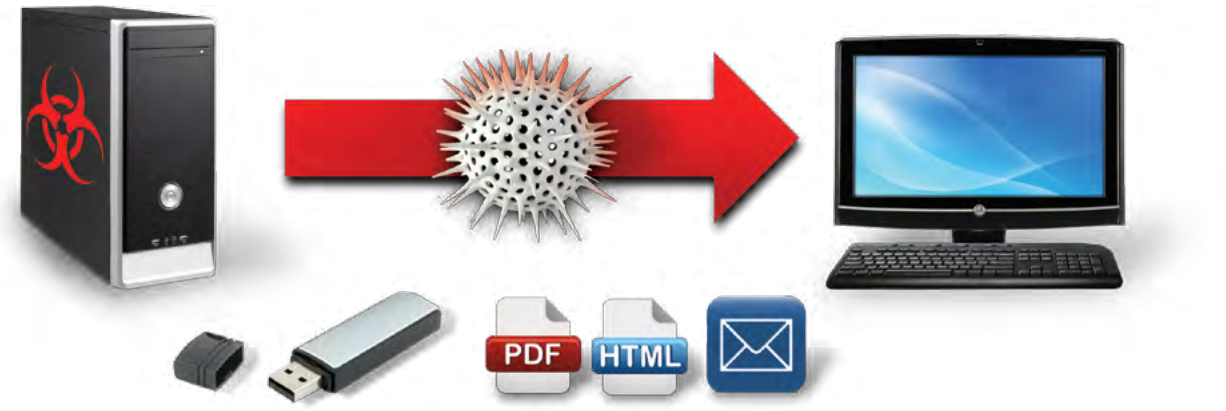
W tym rozdziale opisujemy najważniejsze zjawiska związane z bezpieczeństwem w sieci w 2011 roku, w których rozpracowanie byliśmy bezpośrednio zaangażowani.

8.1 ZITMO - Zeus-in-the-Mobile

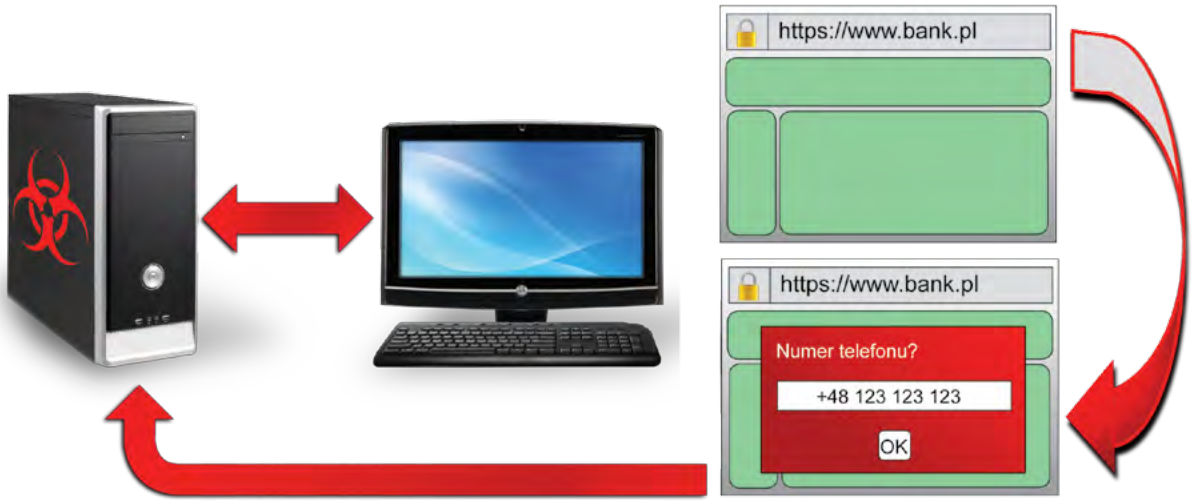
ZITMO, czyli Zeus In The Mobile to zagrożenie, które na początku 2011 roku pojawiło się w Polsce. Jest to nowa odmiana trojana ZeuS, która poza komputerem ofiary atakuje również jej telefon komórkowy. Atakujący może czytać oraz modyfikować informacje zawarte w SMS takie jak kody autoryzacji transakcji czy wiadomości potwierdzające wykonane operacje bankowe.

W jaki sposób infekowane były telefony komórkowe?

1. W wyniku instalacji złośliwego oprogramowania, atakujący zyskiwał kontrolę nad komputerem ofiary. Nie wiadomo jakie było pierwotne źródło infekcji − zakładamy, że mogło być ich wiele, np. specjalnie spreparowana strona WWW, plik .pdf, zainfekowany pendrive czy e-mail zawierający złośliwy załącznik.

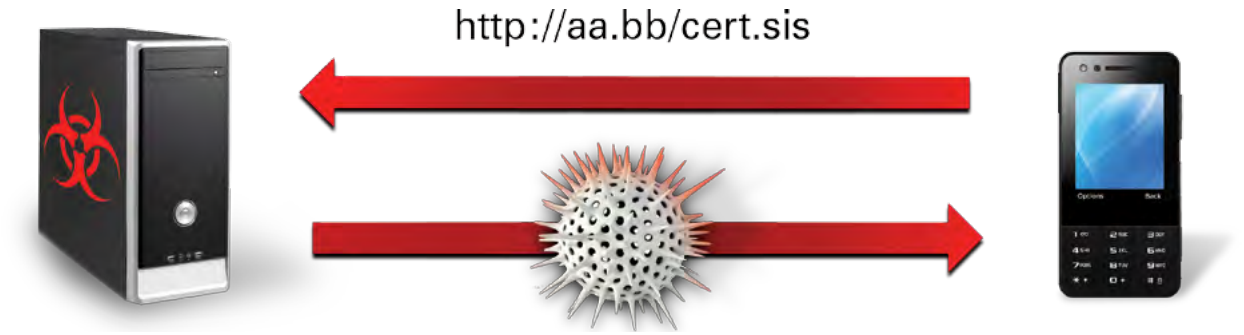


2. Po zainfekowaniu komputera złośliwe oprogramowanie podmieniało w locie (na komputerze ofiary) treść zaufanej strony. Po pomyślnym zalogowaniu do banku pojawiał się monit z prośbą o podanie numeru oraz wybranie z listy modelu telefonu.

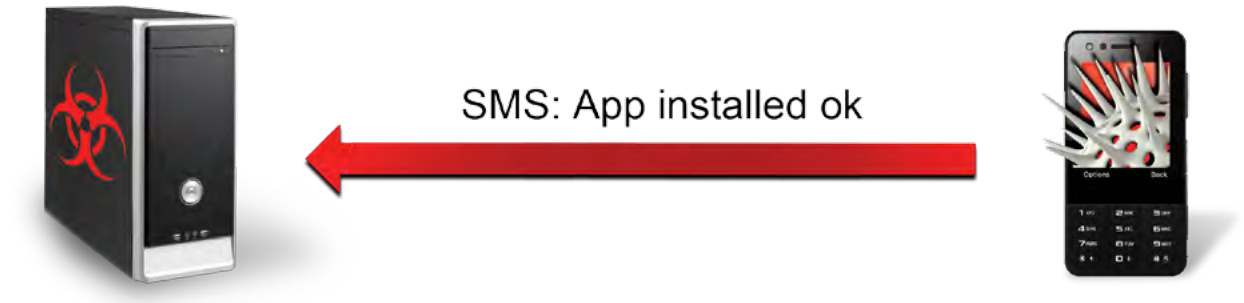


3. Po uzupełnieniu formularza dane przesyłane były do serwera zarządzającego. Atakujący po zdobyciu numeru wysyłał SMS z linkiem do złośliwego oprogramowania (przeznaczonego na konkretny model telefonu).

4. Nieświadomy zagrożenia użytkownik próbował otworzyć otrzymany link. W konsekwencji na telefonie instalowała się aplikacja (złośliwe oprogramowanie).



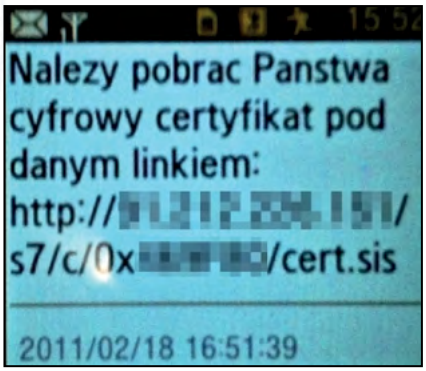
5. Zainfekowany telefon wysyłał atakującemu SMS z informacją o poprawnym zainstalowaniu złośliwego oprogramowania. Atakujący od tego momentu miał pełną kontrolę nad komputerem oraz telefonem ofiary.



8. Najważniejsze zjawiska okiem CERT Polska

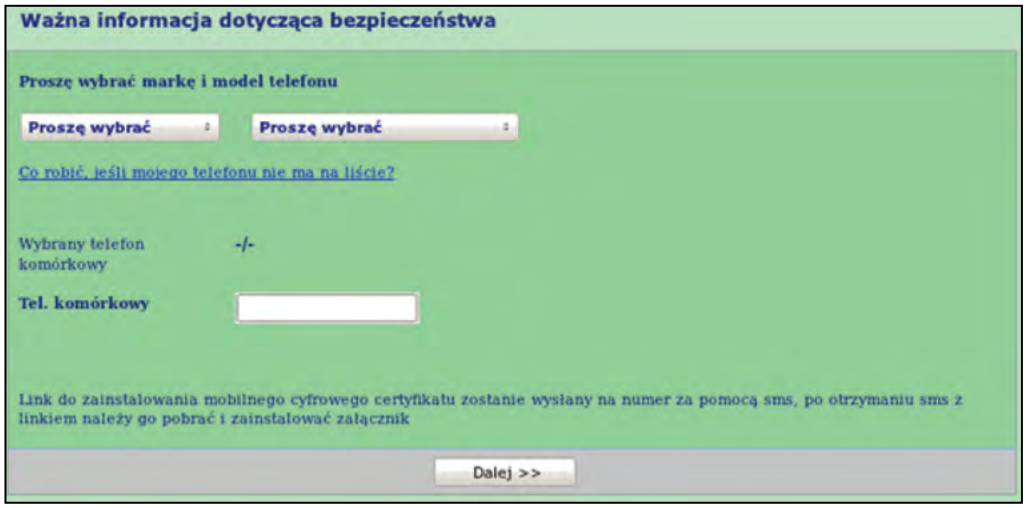
Kto mógł zostać ofiarą ZITMO?

Lista modeli telefonów, które mogły stać się celem ataku (na nich mogło zostać zainstalowane złośliwe oprogramowanie) znajduje się pod adresem http://www.cert.pl/wp-content/uploads/atakowanetel.html. Są to telefony pracujące pod kontrolą trzech systemów operacyjnych: BlackBerry, Symbian oraz Windows Mobile. Wysyłany do ofiary SMS zawierał informację o cyfrowym certyfikacie oraz link kończący się ciągiem znaków „cert.jad", „cert.sis" lub „cert.cab" (patrz zdjęcie po prawej).



Jak ustrzec się infekcji oraz zapobiec kradzieży danych (i środków pieniężnych)?

Należy być czujnym podczas logowania do banku. Ostrzegawcze światło powinno zapalić się, jeżeli zauważymy jakąś nową informację lub funkcjonalność o której bank nie informował wcześniej. Może być to pytanie o model, numer telefonu, czy też monit o podanie jednocześnie więcej niż jednego kodu jednorazowego (TAN). W takiej sytuacji zawsze najlepiej zgłosić taki incydent do biura obsługi banku.



Rysunek 8.1.1. Ekran proszący użytkownika o podanie numeru telefonu oraz wybranie marki i modelu

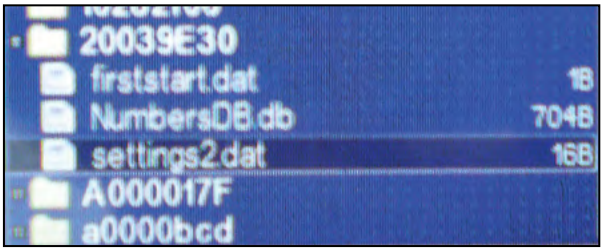
Więcej informacji o złośliwym oprogramowaniu

Po zainstalowaniu na telefonie, aplikacja (bez wiedzy właściciela) wysyła SMS o treści „App Installed OK" na zdefiniowany numer telefonu zarządcy. We wszystkich próbkach, którymi dysponował CERT Polska, występował ten sam numer telefonu. Zaczynał się on od cyfr 44778148**** i pochodził z Wielkiej Brytani. Poniżej zamieszczamy krótki opis działania oprogramowania na każdej z podatnych platform.

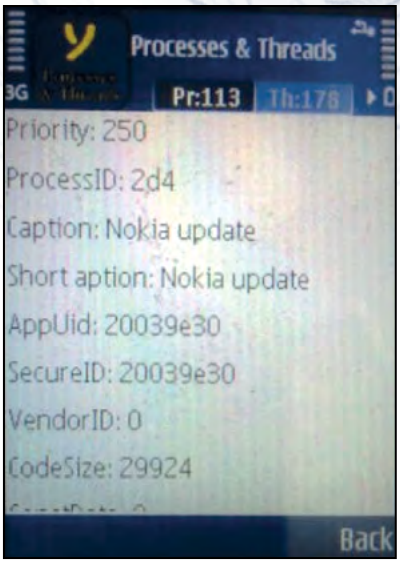
8.1.1 Symbian

Na telefony z systemem operacyjnym Symbian wysyłane były SMS zawierające link do pliku cert.sis. Po zainstalowaniu malware tworzył proces nazwany „Nokia update" (rysunek po prawej). W pamięci telefonu zapisywał pliki (rysunek poniżej):

```
C:\private\20039E30\firststart.dat
C:\private\20039E30\NumbersDB.db
C:\private\20039E30\settings2.dat
```



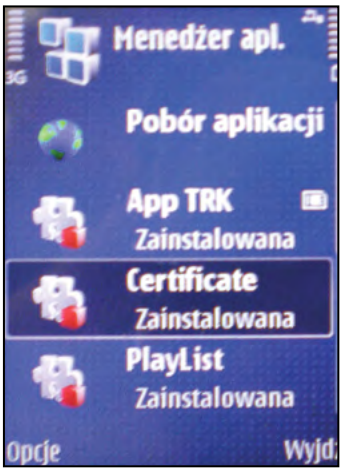
W nich przechowywane były informacje o ustawieniach oraz numerach, które mają być podsłuchiwane przez trojana.

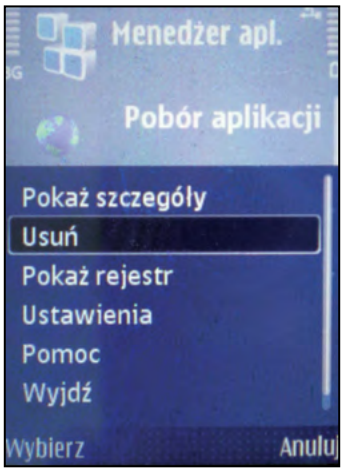


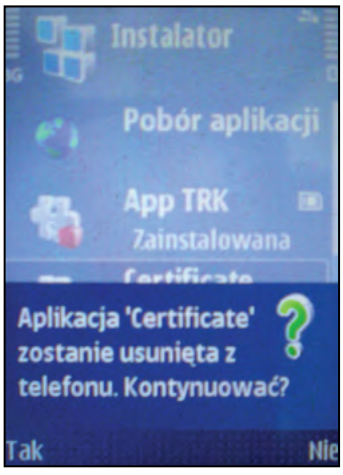
Deinstalacja

Aby odinstalować złośliwe oprogramowanie otwieramy menedżer aplikacji oraz odnajdujemy aplikację „Certificate". Następnie z menu kontekstowego wybieramy opcję usuń, a potem potwierdzamy zamiar usunięcia aplikacji.

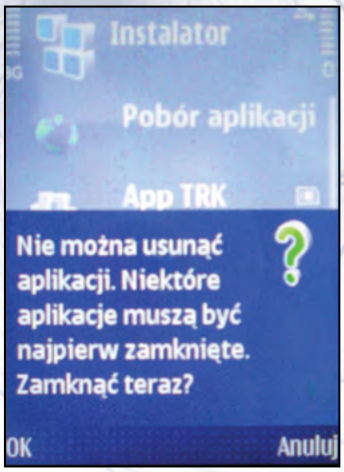
W przypadku pojawienia się ostrzeżenia o konieczności zamknięcia aplikacji odpowiadamy twierdząco (OK). Po rozpoczęciu procesu usuwania aplikacji powinno pojawić się okno proszące o podanie kodu lub hasła. Numer ten jest zakodowany wewnątrz złośliwego programu. Kod umożliwiający usunięcie malware (w przypadku infekcji z lutego 2011 r.) to: **45930**

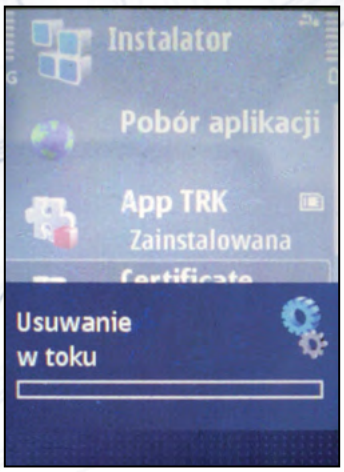


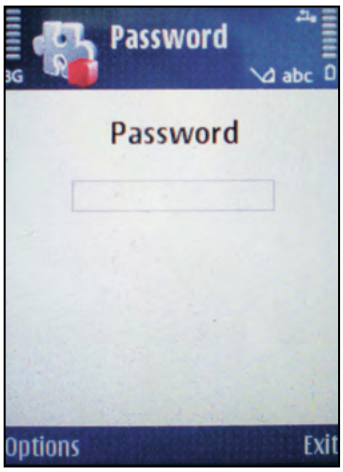




8. Najważniejsze zjawiska okiem CERT Polska

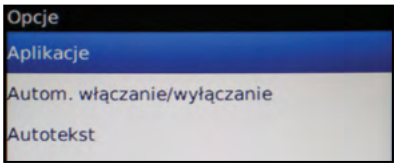


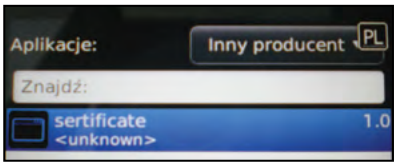


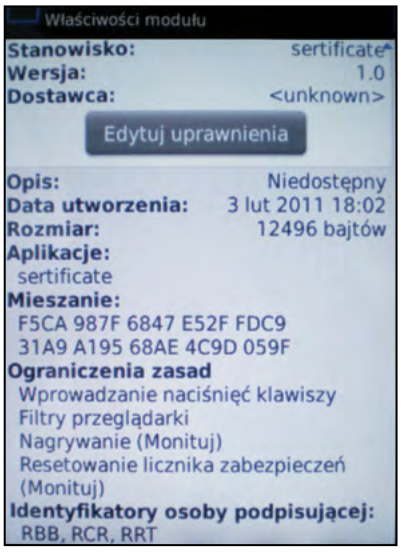


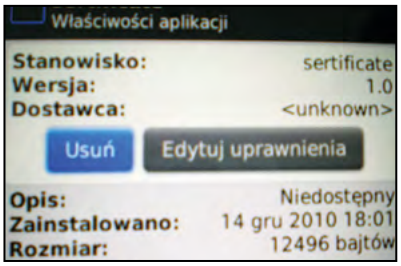
8.1.2 BlackBerry

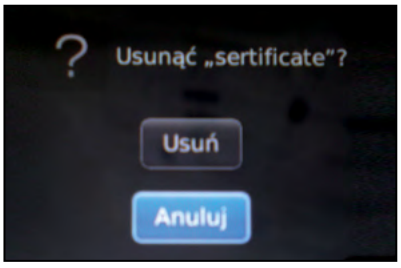
Paczka infekująca platformę blackberry rozsyłana była w pliku „cert.jad". Po jego uruchomieniu ściągany i instalowany był jeden z plików: „sertificate.jar" lub „sertificate.cod". Po zainstalowaniu aplikacja widoczna jest w menu „Opcje-> Aplikacje" pod nazwą „sertificate". Po kliknięciu w pozycję z aplikacją pojawia się okno umożliwiające przeglądanie szczegółowych informacji na jej temat. W tym samym oknie mamy również możliwość usunięcia niechcianego oprogramowania poprzez naciśnięcie przycisku „Usuń". Zostanie jedynie wyświetlony monit potwierdzający usunięcie. Po wykonaniu operacji odzyskujemy kontrolę nad naszym telefonem.





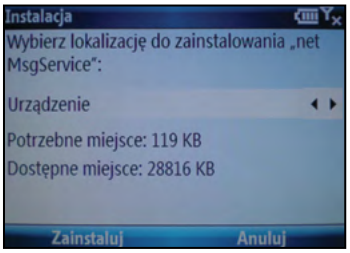


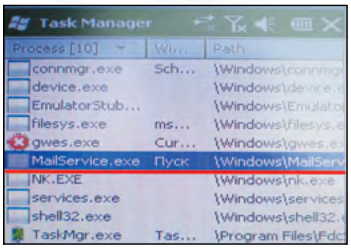




8.1.3 Windows Mobile

W przypadku telefonów z systemem operacyjnym Windows Mobile, plik instalacyjny z malware nazywał się cert.cab. Podczas instalacji ZITMO przedstawiał się jako „net MsgService". Po zainstalowaniu złośliwe oprogramowanie zapisywało ustawienia w czterech plikach: settings.xml, senders.xml, listnumbers.xml, messages.xml. Sam malware natomiast instalowany był w pliku c:\Windows\MailService.exe. Po uruchomieniu program ten nie był widoczny na liście zadań w standardowym (wbudowanym) menadżerze procesów. Dopiero zainstalowanie dodatkowego oprogramowania umożliwiło wyśledzenie działającego w tle szkodnika. Co ciekawe, tytuł głównego okna związanego ze szkodliwym procesem pisany był cyrylicą (jak na zdjęciu). Niestety oprogramowanie to nie jest również widoczne na liście zainstalowanych aplikacji - co znacznie utrudnia usunięcie szkodnika.





8.2 SpyEye w PDF

Dzięki współpracy polskich zespołów bezpieczeństwa, związanych inicjatywą Abuse-Forum, udało się wykryć oraz przeanalizować nowe zagrożenie. Na początku kwietnia do polskich internautów trafiała wiadomość e-mail zawierająca w załączniku złośliwy dokument PDF. Po jego otwarciu komputer infekowany był oprogramowaniem szpiegowskim SpyEye. Jego główne przeznaczenie to wykradanie poufnych informacji podawanych przez użytkownika na stronach internetowych (w tym systemach bankowości elektronicznej). Po otwarciu dokumentu i zainstalowaniu złośliwego oprogramowania komputer ofiary łączył się do serwera-kontrolera (C&C) znajdującego się pod adresem u-buntu.com. Po kilku dniach zainfekowanie ofiary były kierowane na nowy serwer kontrolera, wydający się być częścią większego botnetu.

Jak wyglądała złośliwa wiadomość?

Rozesłana wiadomości e-mail zawierała nastepujące pola:

Temat: `Your Order No ######## | Puremobile Inc.`
Nadawca: `PuremobileInc`
Załącznik: `Order_########.pdf`

W przeanalizowanych próbkach znajdowała się treść w języku polskim:

```
Dziekujemy za zamowienie
Twoje zamowienie zostalo przyjete.
Numer zamowienia 123-123456789.
Bedziesz musial podac ten numer w korespondencji.

Wybrales opcje platnosci karta kredytowa.
Twoja karta zostanie obciazona oplata
```

8. Najważniejsze zjawiska okiem CERT Polska

```
w wysokosci 1234,00 EUR.
Oplata za zamowienie bedzie opisana na
wyciagu bankowym z karty kredytowej
jako „Puremobile Inc.”

Ta wiadomosc nie jest dowod zakupu
Po otrzymaniu przez nas potwierdzenia
tej wplaty, wyslemy Ci list zwrotny.
W zaleznosci od tego jaka forme wysyl-
ki wybierzesz otrzymasz go wprost
na swoj adres e-mail lub na adres do-
mowy.
Puremobile Inc
```

Szczegółowa analiza złośliwego dokumentu PDF

Po otwarciu załączonego dokumentu PDF, program Adobe Reader rozpoczyna jego ładowanie i przetwarzanie. Struktura dokumentu PDF jest drzewem obiektów, z jednym obiektem typu Root jako korzeniem. Adobe Reader przetwarza kolejne obiekty, zgodnie z ich kolejnością i pozycją w drzewie. Część obiektów to skrypty JavaScript, które mogą być wykonywane przez silnik EScript (silnik JavaScript firmy Adobe). Do zbadania dokumentu PDF oraz wyświetlenia obiektów w nim zawartych można użyć programu PDFID (rysunek 8.2.1).

Na pierwszy rzut oka wydaje się, że ten dokument nie zawiera żadnych obiektów JavaScript. Jest to jednak nieprawda - skrypty ukryte są w skompresowanych strumieniach (stream). Są one zazwyczaj zaciemnione i trudne do zinterpretowania. Tak samo jest i w tym przypadku (fragment dekompresowanego kodu widoczny na rysunku 8.2.2).

Skrypt ukryty w skompresowanym strumieniu zostaje zdekompresowany i wykonany. Służy on do umieszczenia shellcodu w pamięci za pomocą techniki „heap spray”. Kiedy nastąpi włamanie (wykorzystanie luki w czytniku PDF), procesor ofiary rozpoczyna wykonywanie tego właśnie kodu.

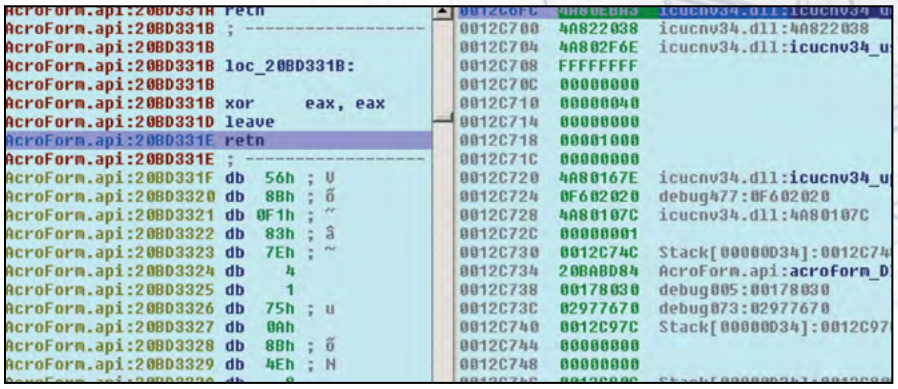
```
PDFiD 0.0.11 ./[redacted].pdf
 PDF Header: %PDF-1.5
 obj                    54
 endobj                 54
 stream                 20
 endstream              20
 xref                    1
 trailer                 1
 startxref               1
 /Page                   1
 /Encrypt                0
 /ObjStm                 0
 /JS                     0
 /JavaScript             0
 /AA                     0
 /OpenAction             0
 /AcroForm               1
 /JBIG2Decode            0
 /RichMedia              0
 /Launch                 0
 /Colors > 2^24          0
```

Rysunek 8.2.1. Analiza dokumentu PDF

```
function ttt4(zv, zt) {
    return ttt5(zv, zt);
}

function ttt5(zv, zt) {
    return f9FDCA5(zv, zt);
}



function f9FDCA5(zv, zt) {
    var c, gv, j, gf, zi, r, qd, qe, gm, qf, k, gm, qk, ql, v, qt, gp;
    p = 0.003;
    p++;
    q = 'XYiQBtme';
    g = 'seg';
    z = null;
```

Rysunek 8.2.2. Fragment kodu javascript

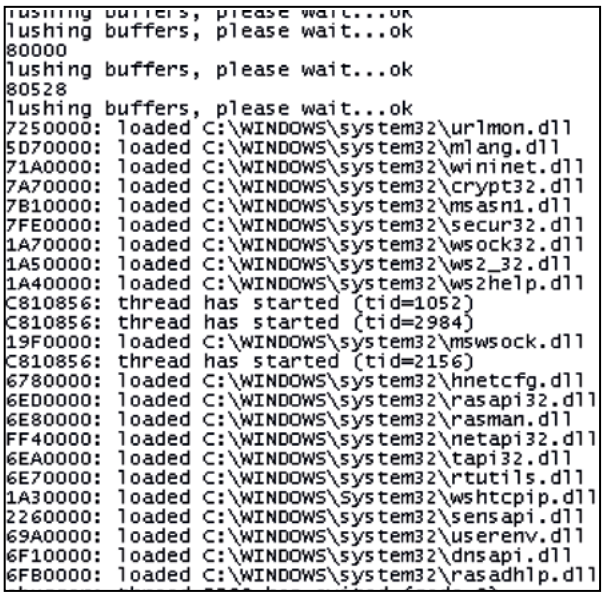
Jak dokładnie dochodzi do przejęcia kontroli nad przetwarzanym kodem? Biblioteka AcroForm.api zawiera błąd, który to umożliwia. W trakcie przetwarzania obiektu AcroForm (widocznego w listingu Programu PDFID), wykonywana procedura zakończy się przedwcześnie, co pozwala na wykonanie skoku do biblioteki icucnv34.dll (rysunek 8.2.3).



Rysunek 8.2.3. Kod biblioteki AcroForm podczas wykonywania

Biblioteka ta zostanie wykorzystana przez exploit typu ROP (o exploitach tego typu pisaliśmy w artykule z grudnia 2010 roku pod adresem: http://www.cert.pl/news/3078), który wcześniej został umieszczony w pamięci przez wspomniany JavaScript.

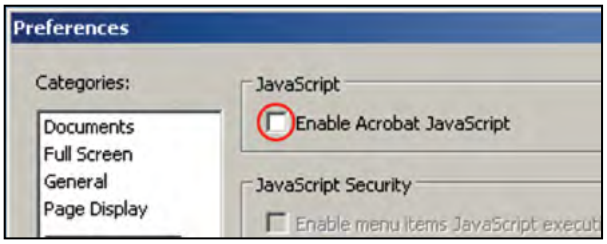
Jakie są konsekwencje wykonania złośliwego kodu? Przekonaliśmy się o tym przeprowadzając kontrolowane otwarcie badanego dokumentu na komputerze laboratoryjnym. Exploit ładuje biblioteki systemowe (rysunek 8.2.4) potrzebne do prowadzenia transmisji w sieci Internet i próbuje połączyć się z atakowanego komputera ze zdalnym serwerem. Po połączeniu pobiera oraz uruchamia plik typu EXE. Jest to trojan SpyEye, który jest następnie wykorzystywany do infiltrowania komputera ofiary i kradzieży jej danych (np. haseł bankowych).



Rysunek 8.2.4. Ładowanie nowych bibliotek

Jak się zabezpieczyć przed takim atakiem?

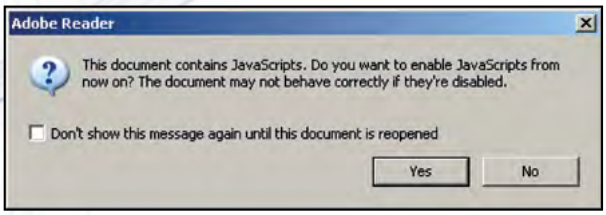
Aby zabezpieczyć się przed włamaniami tego typu, należy przestrzegać kilku reguł. Przede wszystkim nie należy otwierać załączników w wiadomościach e-mail od nieznanych osób. Oczywiście, czasem - niestety - możemy otrzymać maila od zaufanej osoby, która została już zainfekowana. W takiej sytuacji należy uważnie patrzeć, czy treść tego maila nie jest podejrzana. Dodatkowo dobrą praktyką jest wyłączenie obsługi JavaScript przez program Adobe Reader (rysunek 8.2.5).



Rysunek 8.2.5. Wyłączenie obsługi JavaScript

8. Najważniejsze zjawiska okiem CERT Polska

Jeśli w przyszłości Adobe Reader zapyta nas o pozwolenie na wykonywanie skryptów JavaScript zawartych w dokumencie, możemy mu odmówić (rysunek 8.2.6.)



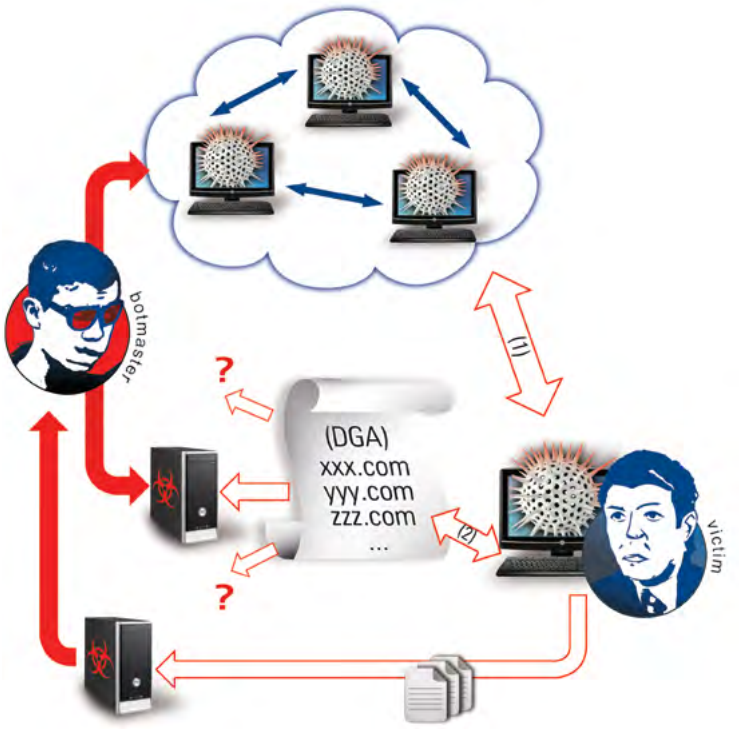
Rysunek 8.2.6

8.3 ZeuS - wariant P2P + DGA - analiza nowego zagrożenia

Jesienią 2011 roku zarejestrowano infekcje nowym złośliwym oprogramowaniem. Analiza mechanizmu uruchamiania złośliwego oprogramowania, proces jego ukrywania, czy też sposób składowania konfiguracji wskazywały na ZeuSa. Jednak podczas monitorowania zainfekowanych maszyn nie udało się zauważyć charakterystycznej dla tego trojana komunikacji z centrum C&C. Po głębszej analizie okazało się, iż próbka to najprawdopodobniej nowa wersja trojana ZeuS oparta na upublicznionym przypadkiem kodzie.W nowej wersji trojana autorzy skupili się na eliminacji najsłabszego ogniwa - scentralizowanego systemu dystrybucji informacji. Poprzednie wersje ZeuSa oparte były o jeden (lub kilka) zdefiniowanych adresów, pod którymi dostępne było centrum zarządzania C&C. Pozwalało to łatwo namierzyć takie adresy i poprzez ich blokowanie uczynić botnet bezużytecznym. Badany wariant trojana wykorzystuje dwa nowe kanały komunikacyjne do pobierania nowych rozkazów (rysunek 8.3.1):

1. Komunikacja w sieci peer-to-peer
2. Mechanizm Generowania Domen

W Internecie dostępne były już wcześniej informacje na temat nowego wariantu ZeuSa, ale - z informacji jakie posiadamy - dotychczasowa praca badawcza skupiała się na zarejestrowaniu i monitorowaniu ruchu do domen ZeuSowych.

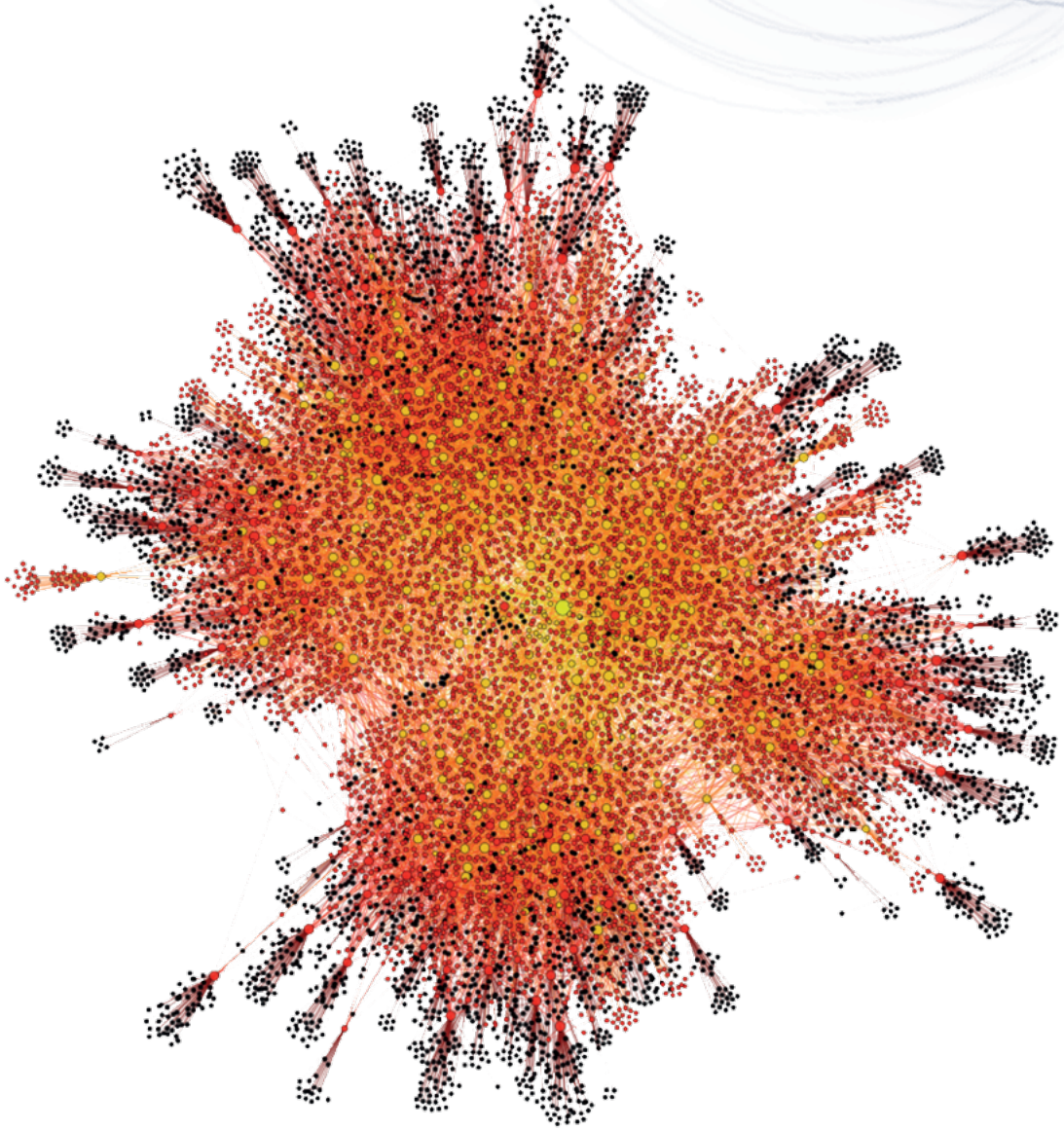


Rysunek 8.3.1.

Podczas naszej pracy skupiliśmy się na poznaniu oraz monitorowaniu mechanizmów wymiany informacji przez sieć P2P oraz próbie zebrania danych na temat jej kształtu.

Mechanizm wymiany informacji przez siec Zeus-peer-to-peer (dalej ZP2P)

W przypadku modelu opartego na centralnym (jednym lub wielu) punkcie zarządzania, z góry wiadomo jakie komputery wykorzystywane są do wydawania rozkazów. Nowy mechanizm dystrybucji informacji oparty jest o bezpośrednią wymianę danych między zainfekowanymi komputerami - czyli model komunikacji Peer-to-peer. Brak centralnego węzła zarządzającego w tym modelu powoduje, iż znacznie trudniej jest znaleźć komputery dystrybuujące nowe rozkazy, a zablokowanie kanału wymiany danych jest praktycznie niemożliwe. Dobrze ilustruje to wykres 8.3.2. Widać, iż w przedstawionej sieci brak jest centralnego punku (jednego czy też wielu), a połączenia między komputerami mają charakter losowy.



Wykres 8.3.2. Wizualizacja sieci ZP2P (10 000 węzłów)

8. Najważniejsze zjawiska okiem CERT Polska

Jak działa sieć ZP2P?

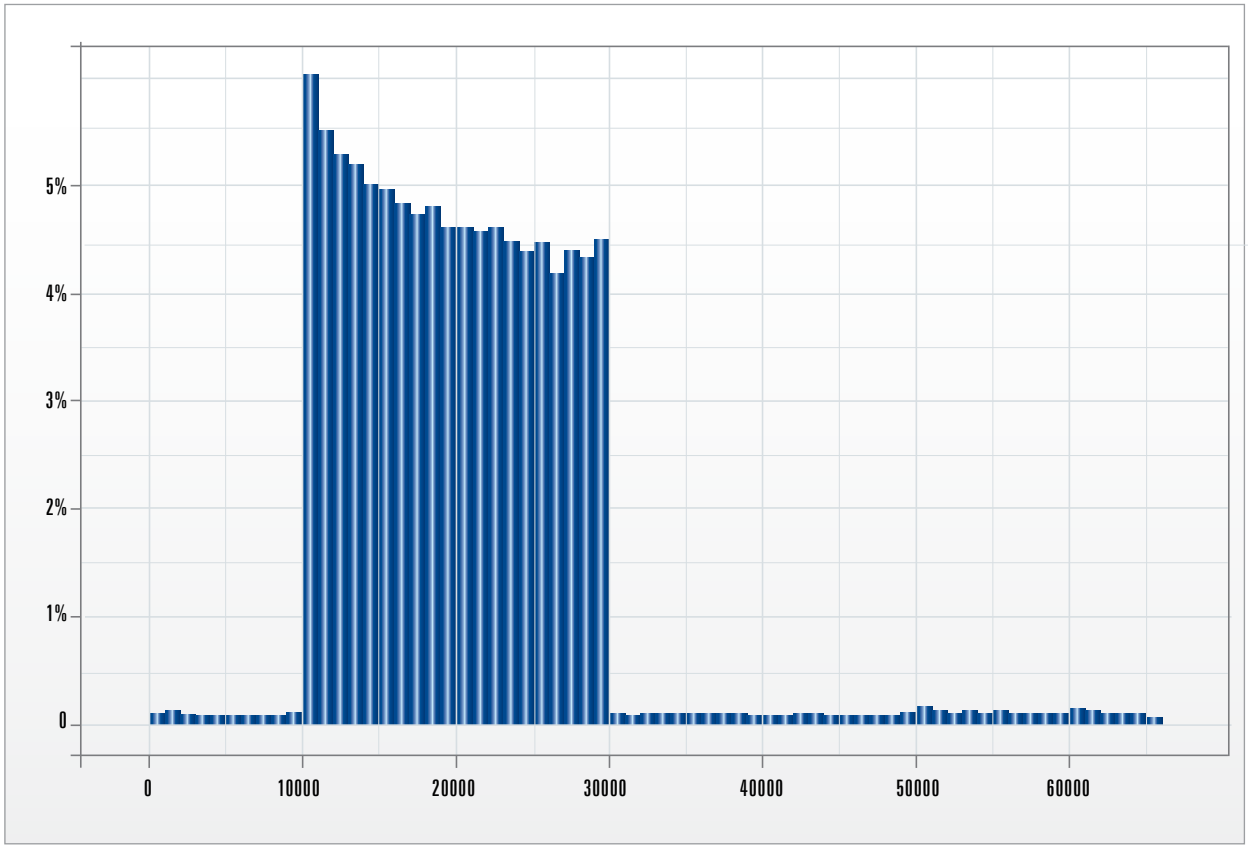
Sieć ta najprawdopodobniej jest oparta na standardzie protokołu Kademlia. Pojedynczy komputer (węzeł) w sieci ZP2P identyfikowany jest za pomocą unikalnego identyfikatora UID - który generowany jest podczas pierwszego uruchomienia złośliwego oprogramowania. Każdy z komputerów należących do sieci ZP2P posiada w pamięci „tablicę sąsiadów". Zawiera ona listę ok 30 pobliskich węzłów w sieci ZP2P - ich identyfikator UID, adres IP oraz numer portu UDP. Lista ta jest wykorzystywana do wymiany danych oraz informacji.

Wykresy 8.3.3 oraz 8.3.4 przedstawiają rozkład numerów portów wykorzystywanych do komunikacji w sieci ZP2P.

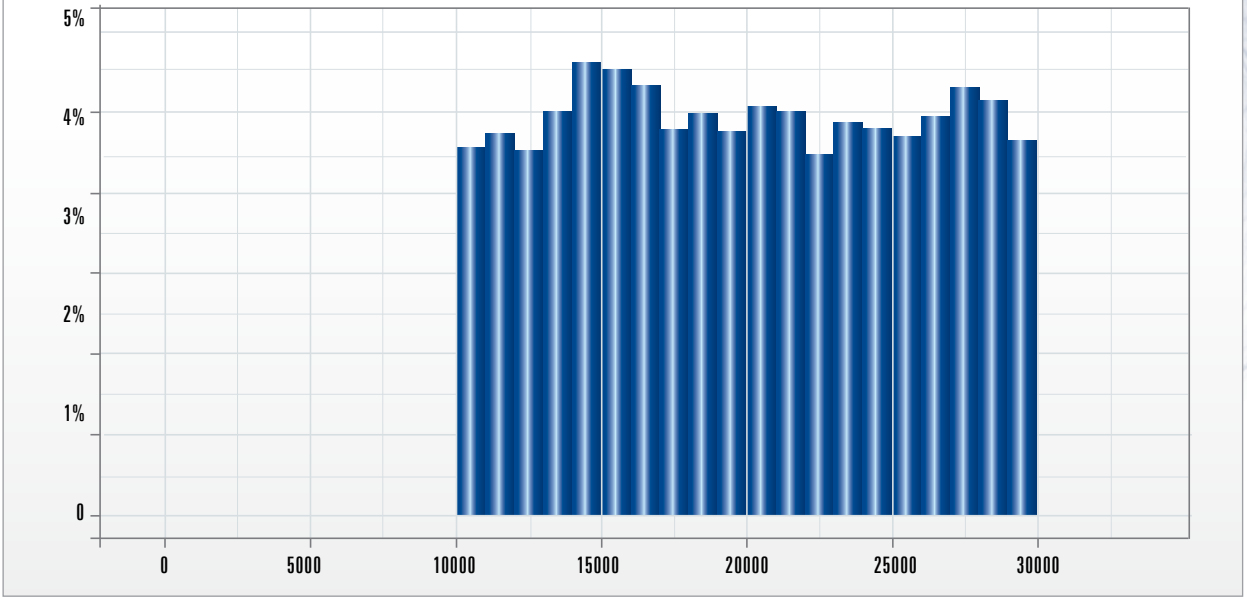
W sieci ZP2P możemy wyróżnić dwa rodzaje komunikacji:

- Wymiana informacji (z użyciem protokołu UDP):
  - (QV) Wymiana informacji o posiadane przez komputer wersji pliku konfiguracyj nego
  - (QN) Wymiana informacji o węzłach znajdujących się w „tablicy sąsiadów" danego komputera,
- Wymiana danych binarnych (z użyciem protokółu TCP),
  - Dystrybucja nowych plików konfiguracyjnych.

W przypadku komunikatu typu QN jednorazowo przesyłane jest tylko 10 rekordów z „tablicy sąsiadów". Ten rodzaj komunikacji służy uaktualnianiu lokalnej tablicy sąsiadów w sieci ZP2P. Po wykonaniu zapytania QN bot zapisuje informacje o sąsiednich węzłach, których identyfikator UID jest zbliżony do identyfikatora (w metrzce XOR) lokalnego komputera.



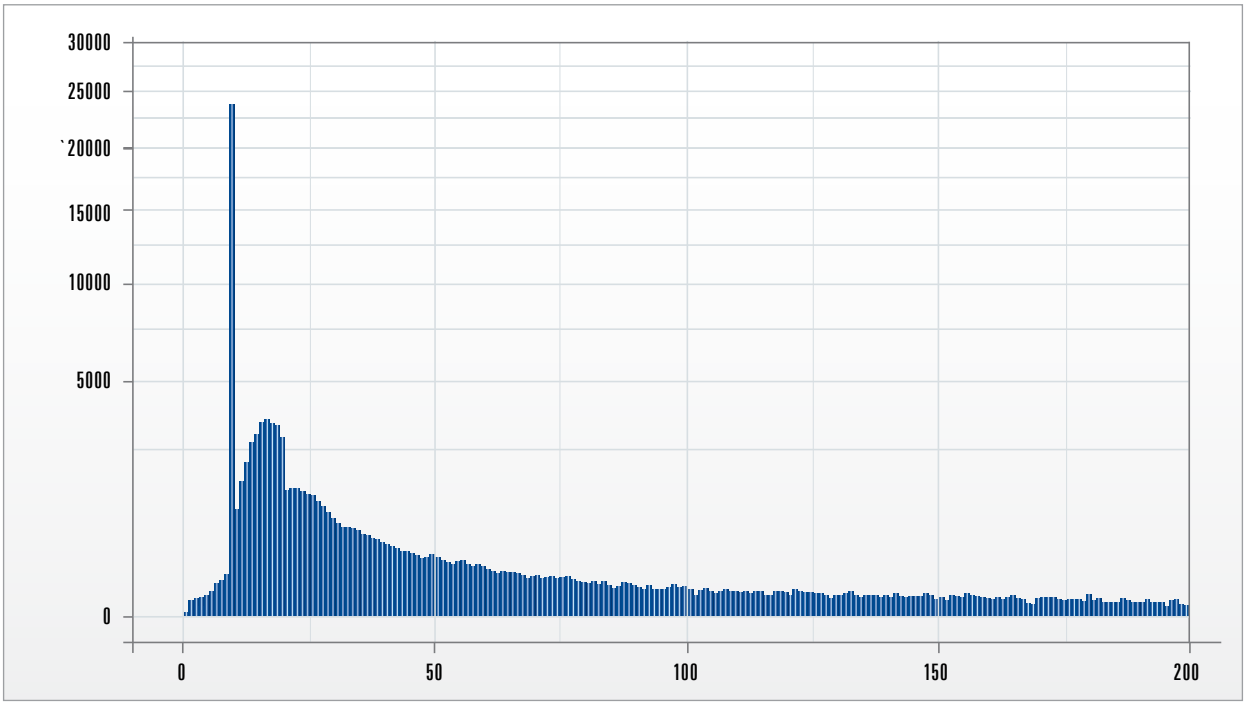
Wykres 8.3.3. Rozkład numerów portów UDP w sieci ZP2P (800 000 próbek)



Wykres 8.3.4. Rozkład numerów portów TCP w sieci ZP2P (100 000 próbek)

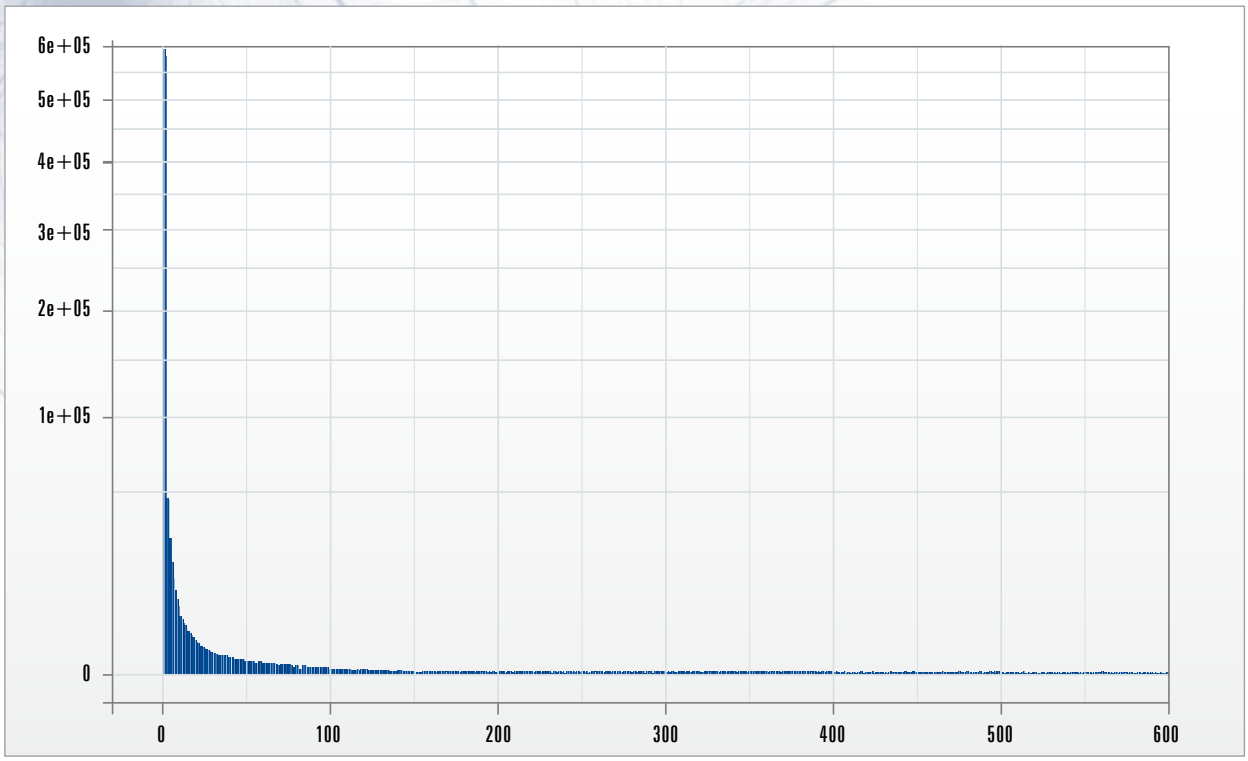
Komunikaty typu QV służą sprawdzeniu oraz propagacji informacji o nowych wersjach plików konfiguracyjnych. Jeżeli węzeł, który wykonał zapytanie QV posiada wersję konfiguracji starszą niż wersja podana w odpowiedzi na to zapytanie, wykona on połączenie TCP do zdalnego komputera prosząc o przesłanie nowszej wersji konfiguracji.

Wykresy 8.3.5 oraz 8.3.6 przedstawiają rozkład liczby dzieci i liczby rodziców w sieci ZP2P. Dane pochodzą z analizy odpowiedzi botów na zapytania typu QN w przeciągu 3 tygodni. Liczby dzieci (czyli liczba różnych wpisów w tablicy sąsiedztwa) może przekraczać wartość 30, ponieważ tablica sąsiedztwa ulegać może częstym aktualizacjom.



Wykres 8.3.5. Rozkład liczby dzieci

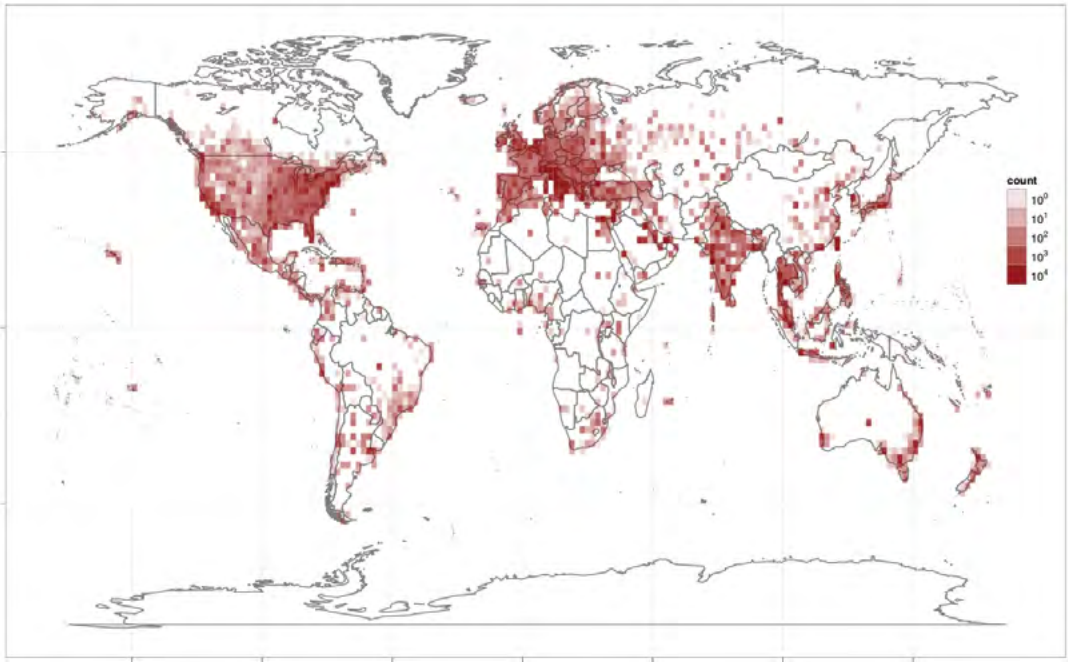
8. Najważniejsze zjawiska okiem CERT Polska



Wykres 8.3.6. Rozkład liczby rodziców

Monitorowanie sieci ZP2P

W laboratorium CERT Polska przeprowadziliśmy mapowanie sieci ZP2P poprzez monitorowanie odpowiedzi na komunikaty typu QN. Zebrane w ten sposób adresy IP naniesione zostały na mapę.



Wykres 8.3.7. Rozkład adresów IP po mapowaniu sieci ZP2P

Mechanizm wymiany informacji przez sieć ZP2P

Jeżeli mechanizm komunikacji w sieci ZP2P zostanie zablokowany (np. poprzez zablokowanie odpowiednich portów TCP i UDP na firewallu) - bot automatycznie przełącza się na zapasowy kanał komunikacyjny - DGA. Mechanizm DGA jest kolejnym elementem zaimplementowanym w nowej wersji trojana, który znacznie utrudnia poszukiwania oraz odcięcie osoby zarządzającej botnetem. Polega on na generowaniu pewnej długiej listy nazw domenowych w oparciu o określone parametry, a następnie próbie komunikacji z każdą z wygenerowanych domen. Parametry mechanizmu DGA umieszczone są w kodzie trojana - oraz znane tylko botmasterowi. Może on własnoręcznie wygenerować taką listę, wybrać z niej jedną pozycję - a następnie zarejestrować wybraną domenę i czekać na próby połączeń z zainfekowanych komputerów.

```
~ # ./dgaToday
DGA list for 2012-01-01 :
id:0000 : bse21bl8etduawivfuhugwjwaub68juiulv.ru
id:0001 : l68lscvkwlvc69gsc39c59l18gud60c59n20kqg53.com
id:0002 : h54i25l28i55b28m19l68gvb38o21orh34nwgtnrir.net
id:0003 : fro51owbyhsb48csi65avm39bqf22lygsjzmw.org
id:0004 : d20hxguf32n32quawixl28d10cxm20ngn32a37qw.info
```

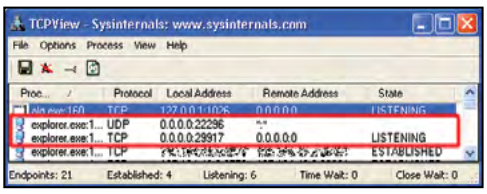
ZeuS-owe DGA

W przypadku botnetu ZeuS, parametrem dla mechanizmu DGA jest bieżąca data. Lista domen zawiera 1000 pozycji i zmienia się co 7 dni. Każda z nazw składa się z ciągu znaków o długości od 32 do 48 oraz jednej z TLD: .ru,.com,.biz,.info,.net lub .org. Warto zaznaczyć, iż w nazwie nie występuje znak „-”. Poniżej znajduje się wyrażenie regularne pozwalające na wyszukanie domen ZeuSowych w logach:

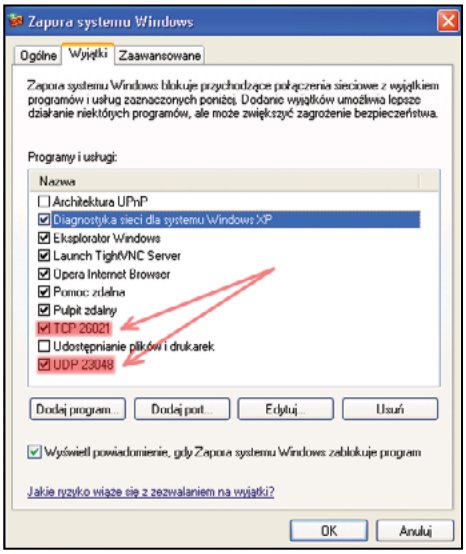
```
[a-z0-9]{32,48}\.(ru|com|biz|info|org|net)
```

Jak rozpoznać infekcję nowym ZeuSem?

Obecność nowego wariantu ZeuSa na komputerze można rozpoznać przede wszystkim poprzez monitorowanie ruchu sieciowego. Jak widać na rysunku 8.3.8., przy użyciu narzędzia TCPview (z pakietu SysInternals), można zauważyć nowe otwarte porty TCP i UDP procesu explorer.exe. Dodatkowo, aby umożliwić komunikację z siecią ZP2P, trojan dodaje do systemowego firewalla nowe reguły. Jak widać na rysunku 8.3.9. są to dwa nowe wyjątki pozwalające na nawiązywanie połączeń na określonych portach TCP i UDP. Zakres tych portów odczytać można z wykresów 8.3.2. i 8.3.3.



Rysunek 8.3.8. Otwarte porty TCP i UDP wykorzystywane do komunikacji P2P



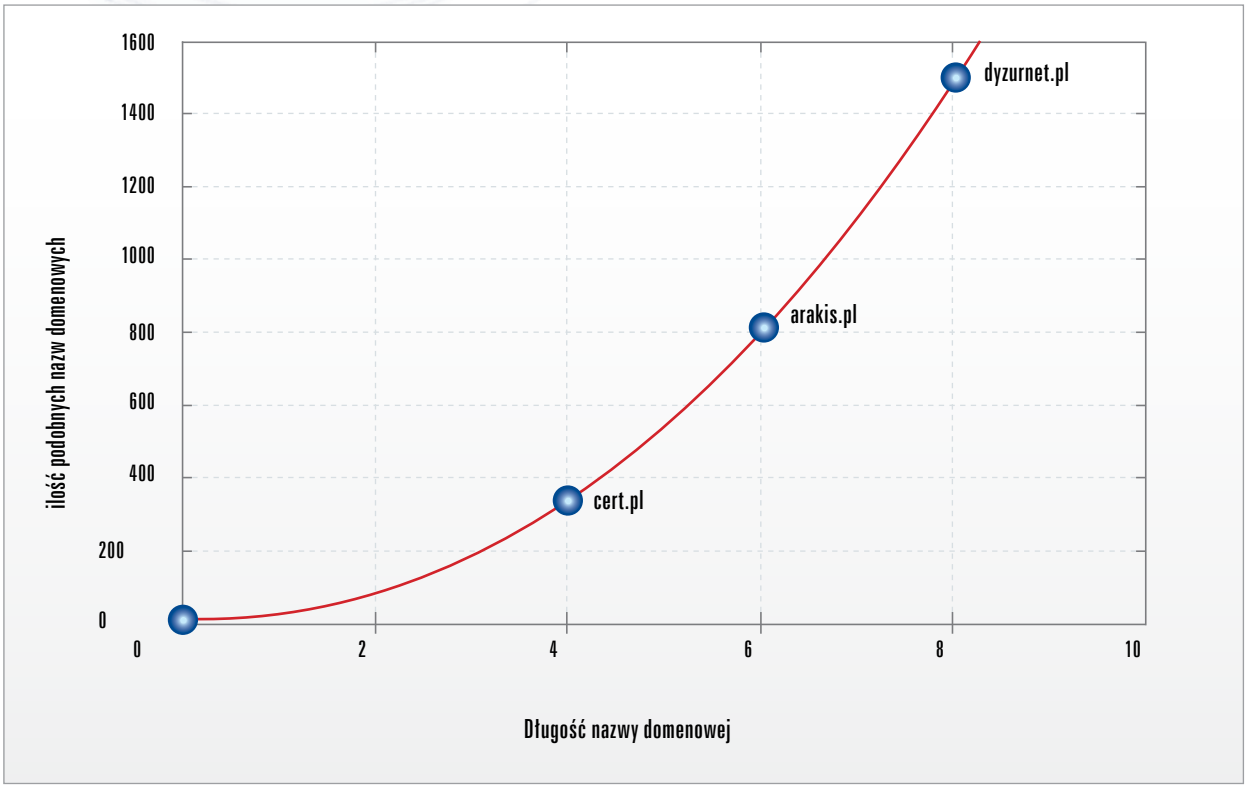
Rysunek 8.3.9. Dodane wyjątki w konfiguracji systemowego firewalla

8. Najważniejsze zjawiska okiem CERT Polska

8.4 Wygrałeś natychmiastową nagrodę

Typosquatting bazuje na omyłkowym wpisaniu nazwy domeny, którą internauta chce odwiedzić. Jest zjawiskiem obecnym od kilku lat. Wraz ze wzrostem popularności Internetu, rejestrowanie domen o nazwach nieznacznie różniących się od popularnych stało się całkiem lukratywnym biznesem. Możliwości popełnienia błędu podczas wpisywania adresu internetowego jest bardzo wiele, np. pominięcie kropki lub pojedynczej litery, wpisanie sąsiedniego znaku lub wpisanie dwukrotnie tego samego znaku. Oczywiście wraz ze wzrostem długości domeny, szansa na popełnienie pomyłki wzrasta. Wykres 8.4.1 przedstawia liczbę możliwych literówek w funkcji długości nazwy domenowej. Przykładowo dla domeny cert.pl możliwe jest zapisanie 341 nazw z literówką, dla domeny arakis.pl liczba literówek wzrasta do 826, zaś w przypadku dyzurnet.pl jest to aż 1 502.

Nazwy domenowe z literówkami zostały wygenerowane przy wykorzystaniu prostych podejść: zamiana znaku na znak sąsiadujący na klawiaturze, pominięcie znaku, dwukrotne wpisanie tego samego znaku oraz zastosowanie dwóch wyżej wymienionych podejść jednocześnie. Uwzględniono jedynie unikalne domeny.



Wykres 8.4.1. Liczba możliwych literówek w funkcji długości nazwy domenowej

Na stronie typosquattingowej można spotkać kilka rodzajów treści:

- witrynę zawierającą linki reklamowe,
- witrynę konkurencyjnego produktu,
- witrynę podszywającą się pod oryginalny serwis i wyłudzającą dane jego użytkowników (phishing),
- przekierowanie do oryginalnego serwisu,
- stronę innego produktu, nie związaną z tematyką oryginalnego serwisu.

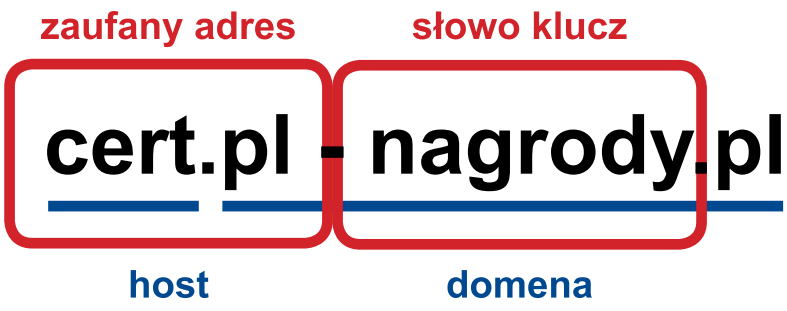
Najczęściej spotykane są linki reklamowe (bądź przekierowanie do strony zawierającej linki reklamowe). W takim wypadku zyski czerpane są na zasadzie pay-per-click (PPC) lub pay-per-visit (PPV). Aby dochód z wyżej wymienionych programów był większy od poniesionych kosztów, osoby trudniące się typosquattingiem rejestrują wiele domen. Istnieją serwisy oferujące całą infrastrukturę wymaganą do czerpania zysków z domen z literówkami (domain parking, partnerskie programy reklamowe).

Szczególnie niebezpieczne są strony podszywające się pod oryginalny serwis i wyłudzające dane jego użytkowników (klasyczny phishing). W tym przypadku cyberprzestępcy czerpią zyski bezpośrednio wykorzystując uzyskane dane (np. dane kart kredytowych, dane logowania do banku, itp.) bądź poprzez ich sprzedaż.

Często spotykane jest przekierowanie do oryginalnego serwisu. Taki przypadek wynika z wykupienia domeny przez oryginalny serwis bądź zawarcie umowy z właścicielem strony typosqauttingowej. Duże i popularne serwisy internetowe tworzą programy partnerskie, ułatwiające nawiązanie kontaktu właścicielom domen o podobnych nazwach. Realizowane jest to bezpośrednio lub przy pośrednictwie agencji PR. W takim wypadku właściciel portalu płaci za każde przekierowanie nieuważnego internauty na jego stronę.

Ciekawym zjawiskiem, jakie można zaobserwować począwszy od IV kwartału 2011 roku, było połączenie typosquattingu z płatnościami SMS Premium. Najczęściej witryna, na jaką trafia internauta, nie jest w jakikolwiek sposób powiązana z oryginalną witryną. Zawiera jednak potencjalnie interesujące treści, jak np. informacja o wygraniu atrakcyjnej nagrody. Aby „uwiarygodnić się" w oczach internauty, takie strony często nawiązują do witryn, których wizerunek wykorzystują poprzez zastosowanie łudząco podobnego szablonu graficznego bądź kolorystyki, symboli graficznych lub podobieństwa adresu (rysunek 8.4.2).

Takie połączenie jest wyjątkowo skuteczne, wiele osób nieświadomych zagrożenia wykona instrukcje zawarte na poszczególnych witrynach. Osoby te będą przekonane, że np. podanie swojego numeru telefonu i odesłanie wiadomości tekstowej jest nieszkodliwe, ponieważ cała komunikacja pochodzi z serwisu traktowanego przez nich jako zaufany. Dodatkowym czynnikiem motywującym jest chęć posiadania markowego gadżetu. Otrzymane później wiadomości tekstowe są najczęściej traktowane jako wiadomości reklamowe, jakie bardzo często otrzymujemy od operatorów telefonii komórkowej (a więc również nie są traktowane jako podejrzane). Tymczasem wysyłając wiadomość SMS na odpowiedni numer użytkownik wykupuje abonament, w ramach którego otrzymuje określoną liczbę informacji poprzez wiadomości Zwrotny SMS Premium. W przypadku wiadomości SMS Premium, stosowna opłata naliczana jest za wysłanie wiadomości. Natomiast w przypadku wiadomości typu Zwrotny SMS Premium, opłata naliczana jest za każdą otrzymaną wiadomość. Wysokość opłat może być różna, szczegółowe opłaty są przedstawione w tabeli 8.4.3.



Rysunek 8.4.2. Wykorzystanie podobieństwa adresu

8. Najważniejsze zjawiska okiem CERT Polska

Numer SMS Zwrotny	Cena netto	Cena brutto (VAT 23%)
70xx(x)	0,5 zł	0,62 zł
71xx(x)	1 zł	1,23 zł
72xx(x)	2 zł	2,46 zł
73xx(x)	3 zł	3,76 zł
74xx(x)	4 zł	4,92 zł
75xx(x)	5 zł	6,15 zł
76xx(x)	6 zł	7,38 zł
77xx(x)	7 zł	8,61 zł
78xx(x)	8 zł	9,84 zł
79xx(x)	9 zł	11,07 zł
8 000 - 8 099	bezpłatny	bezpłatny
80000 - 80999	bezpłatny	bezpłatny
81000 - 81099	0,10 zł	0,12 zł
81500 - 81599	0,15 zł	0,18 zł
82000 - 82099	0,20 zł	0,24 zł
82000 - 82099	0,25 zł	0,31 zł
83000 - 83099	0,30 zł	0,37 zł
83500 - 83599	0,35 zł	0,43 zł
84000 - 84099	0,40 zł	0,49 zł
84500 - 84599	0,45 zł	0,55 zł
85000 - 85099	0,50 zł	0,62 zł
910xx(x)	10 zł	12,30 zł
911xx(x)	11 zł	13,53 zł
912xx(x)	12 zł	14,76 zł
913xx(x)	13 zł	15,99 zł
914xx(x)	14 zł	17,22 zł
915xx(x)	15 zł	18,45 zł
916xx(x)	16 zł	19,68 zł
917xx(x)	17 zł	20,91 zł
918xx(x)	18 zł	22,14 zł
919xx(x)	19 zł	23,37 zł
921xx(x)	20 zł	24,60 zł
925xx(x)	25 zł	30,75 zł
50100 - 50199	0,01 zł	0,01 zł
50200 - 50299	0,02 zł	0,02 zł
50300 - 50399	0,03 zł	0,04 zł
50400 - 50499	0,04 zł	0,05 zł
50500 - 50599	0,05 zł	0,06 zł
50600 - 50699	0,06 zł	0,07 zł
50700 - 50799	0,07 zł	0,09 zł
50800 - 50899	0,08 zł	0,10 zł
50900 - 50999	0,09 zł	0,11 zł
51000 - 51099	0,10 zł	0,12 zł
52000 - 52099	0,20 zł	0,24 zł
53000 - 53099	0,30 zł	0,37 zł
54000 - 54099	0,40 zł	0,49 zł
55000 - 55099	0,50 zł	0,62 zł
56000 - 56099	0,60 zł	0,74 zł
57000 - 57099	0,70 zł	0,86 zł
58000 - 58099	0,80 zł	0,99 zł
59000 - 59099	0,90 zł	1,11 zł
60100 - 60199	1 zł	1,23 zł
60200 - 60299	2 zł	2,46 zł
60300 - 60399	3 zł	3,76 zł
60400 - 60499	4 zł	4,92 zł
60500 - 60599	5 zł	6,15 zł
60600 - 60699	6 zł	7,38 zł
60700 - 60799	7 zł	8,61 zł
60800 - 60899	8 zł	9,84 zł
60900 - 60999	9 zł	11,07 zł
61000 - 61099	10 zł	12,30 zł
61100 - 61199	11 zł	13,53 zł
61200 - 61299	12 zł	14,76 zł
61300 - 61399	13 zł	15,99 zł
61400 - 61499	14 zł	17,22 zł
61500 - 61599	15 zł	18,45 zł
61600 - 61699	16 zł	19,68 zł
61700 - 61799	17 zł	20,91 zł
61800 - 61899	18 zł	22,14 zł
61900 - 61999	19 zł	23,37 zł
62000 - 62099	20 zł	24,60 zł
62100 - 62199	21 zł	25,83 zł
62200 - 62299	22 zł	27,06 zł
62300 - 62399	23 zł	28,29 zł
62400 - 62499	24 zł	29,52 zł
62500 - 62599	25 zł	30,75 zł

Tabela 8.4.3. Opłaty za zwrotny SMS Premium

Najczęściej dopiero po otrzymaniu rachunku, rozpoczyna się dociekanie źródła wysokich opłat. Ustalenie źródła wysokiego rachunku i rezygnacja z usługi abonamentowej może potrwać nawet do kilku miesięcy.

Podsumowanie

Połączenie cybersquattingu z typosquattingiem jest wyjątkowo niebezpieczne z punktu wiedzenia internauty. Podstawową metodą obrony jest uważne wpisywanie adresów. Można również skorzystać z komercyjnych rozwiązań oferowanych przez producentów oprogramowania antywirusowego. Dodatkowo można skorzystać z serwerów nazw OpenDNS. Niestety często wykupywane są linki reklamowe, aby dodatkowo zwiększyć szansę odwiedzenia „witryny konkursowej". Należy wystrzegać się podawania swoich danych (jak np. numer telefonu bądź adres e-mail) oraz poświęcić chwilę i zapoznać się z regulaminem.

9. Najciekawsze wydarzenia z działalności CERT Polska

9.1 Społeczności CERT Polska

CERT Polska jest obecny w serwisach społecznościowych od 2010 roku. Nasz profil na Facebooku śledzi już ponad 300 użytkowników, natomiast kanały Twitter cert_polska i anglojęzyczny cert_polska_en stały się doskonałym uzupełnieniem obszernych wiadomości i raportów publikowanych na stronie www.cert.pl. W 2011 roku umieściliśmy po kilkaset krótkich notek w każdym z nich, informując o istotnych podatnościach, ciekawostkach czy spektakularnych wydarzeniach. Cieszy nas, że wiele z nich spotyka się z żywym zainteresowaniem i są cytowane także przez wpływowych blogerów. Co ciekawe, zdecydowanie większą popularnością cieszy się kanał cert_polska_en prowadzony po angielsku. Jest on obserwowany przez przeszło 460 użytkowników, ponad dwukrotnie więcej niż wersja polskojęzyczna.

Jesienią 2011 nasza obecność w mediach społecznościowych została rozszerzona także o profil konferencji SECURE na portalu Facebook. Publikujemy tam informacje praktyczne związane z konferencją, odnośniki do artykułów, zdjęcia, a także wybrane prezentacje. Po raz pierwszy przeprowadziliśmy także konkurs dla fanów profilu, w którym można było zdobyć bezpłatne zaproszenie na konferencję.

Zapraszamy do dołączenia oraz do kontaktu i dyskusji z nami na łamach tych serwisów.

http://fb.com/CERT.Polska
http://twitter.com/cert_polska
http://twitter.com/cert_polska_en
http://fb.com/Konferencja.SECURE

9.2 Konferencja SECURE 2011

Konferencja SECURE 2011, która odbyła się w dniach 24-26 października 2011 r., była wyjątkowa pod wieloma względami. Pierwszego dnia udostępnione zostały aż cztery warsztaty Hands-on, co było rezultatem bardzo wysokiego zainteresowania taką formą udziału w poprzedniej edycji. Dwa z nich prowadzone były przez CERT Polska. Także program konferencji był bardzo bogaty.

Wśród najlepiej ocenionych prelegentów znaleźli się Raoul Chiesa, który w prezentacji „Cyber Weapons in 2011: An F16 Just Flew Over a 1st World War Battlefield" opowiadał o tym, jak zmieniły się układy sił w obliczu cyberkonfilktów a także Dick Hardt - współautor specyfikacji OpenID 2.0 i OAuth 2.0 oraz ekspert od tożsamości online i Piotr Konieczny - założyciel i właściciel portalu niebezpiecznik.pl, na co dzień zajmujący się szkoleniami z dziedziny bezpieczeństwa.

W sumie gościliśmy 38 prelegentów, którzy wygłosili łącznie 33 prezentacje, przez większość czasu podzielone na trzy równoległe sesje. W sesjach plenarnych wystąpili między innymi Brian Krebs

9. Najciekawsze wydarzenia z działalności CERT Polska

- znany bloger, były dziennikarz śledczy The Washington Post oraz Ryan Seu z zespołu bezpieczeństwa portalu Facebook. Gościem specjalnym konferencji był Robert Korzeniowski - wielokrotny mistrz świata, mistrz Europy oraz mistrz olimpijski w chodzie sportowym, który opowiedział o związkach odpowiedzialności i rozliczalności sportowców za doping ze światem online.

Niemniej interesujące okazały się prezentacje w sesjach równoległych. Mocnym akcentem były prezentacje dotyczące zagrożeń przedsiębiorstw, w tym ataków APT, o których mówił m.in. Gavin Reid z Cisco Systems czy Wojciech Ledzion i Marcin Siedlarz z rządowego zespołu CERT.GOV.PL. W tym samym czasie techniczne tematy zdominowane przez złośliwe oprogramowanie poruszali Tomasz Bukowski i Tomasz Sałaciński z CERT Polska. Po obiedzie jedna z sesji poświęcona była w całości zagadnieniom prawnym. Na niej obok Aleksandra Gacka i Macieja Kołodzieja z portalu społecznościowego nk.pl pojawili się Michał Kluska i Grzegorz Wanio z kancelarii Olesiński i Wspólnicy. Ci ostatni przedstawili błyskotliwy pomysł na ściganie przestępstw popełnianych na blogach i forach w warunkach polskiego systemu prawnego. Drugiego dnia można było wybierać między prezentacjami o bezpieczeństwie VoIP (Sandro Gauci i Joffrey Czarny) i tymi o obecnych i przyszłych narzędziach armii i agencji wywiadu (Michał Młotek i wspomniany wcześniej Raoul Chiesa). Nie zabrakło także prezentacji CERT Polska - Paweł Krześniak opowiadał o wykorzystaniu pasywnych danych z systemów DNS do analizy zagrożeń.

Podobnie jak w ubiegłym roku, pod koniec drugiego dnia oddaliśmy głos uczestnikom konferencji, dając każdemu okazję do wygłoszenia krótkiej prezentacji „lightning talk". Mieliśmy dzięki temu okazję do posłuchania kolejnych ośmiu dynamicznych i bardzo zróżnicowanych prelekcji.

Uczestnicy konferencji pozytywnie ocenili bogactwo tematów, a także unikatowe prezentacje, spośród których wiele zawierało opisy konkretnych, rzeczywistych przypadków.

Konferencji towarzyszyła impreza wieczorna w restauracji Vapiano, która zapewniła okazję do luźniejszych rozmów, nawiązania kontaktów, a także nabycia sprawności we własnoręcznym przygotowywaniu pizzy i makaronu.

9.3 Raport CERT Polska dla ENISA „Proactive Detection of Network Security Incidents"

W grudniu 2011 roku Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA) opublikowała przygotowany przez CERT Polska raport dotyczący metod wykrywania sieciowych incydentów bezpieczeństwa - „Proactive detection of network security incidents".

Proaktywne wykrywanie incydentów to proces odnajdywania złośliwej aktywności w sieci, za którą dany CERT jest odpowiedzialny, przy pomocy narzędzi monitorujących lub z wykorzystaniem zewnętrznych usług dostarczających informacje o wykrytych incydentach, jeszcze zanim właściciele atakowanych sieci staną się tego świadomi. Zwiększenie efektywności tych działań jest fundamentem prężnego funkcjonowania zespołów CERT i zwiększenia ich możliwości obsługi incydentów.

W dokumencie dokonano analizy sposobów, w jaki CERTy, w szczególności narodowe i rządowe, wykrywają incydenty w swoich obszarach działalności. Raport zawiera również zestaw najlepszych praktyk i użytecznych narzędzi dla nowo powstałych zespołów typu CERT, analizę problemów jakim muszą stawić czoła i zestaw rekomendacji dla usprawnienia obsługi incydentów przez zespoły CERT.

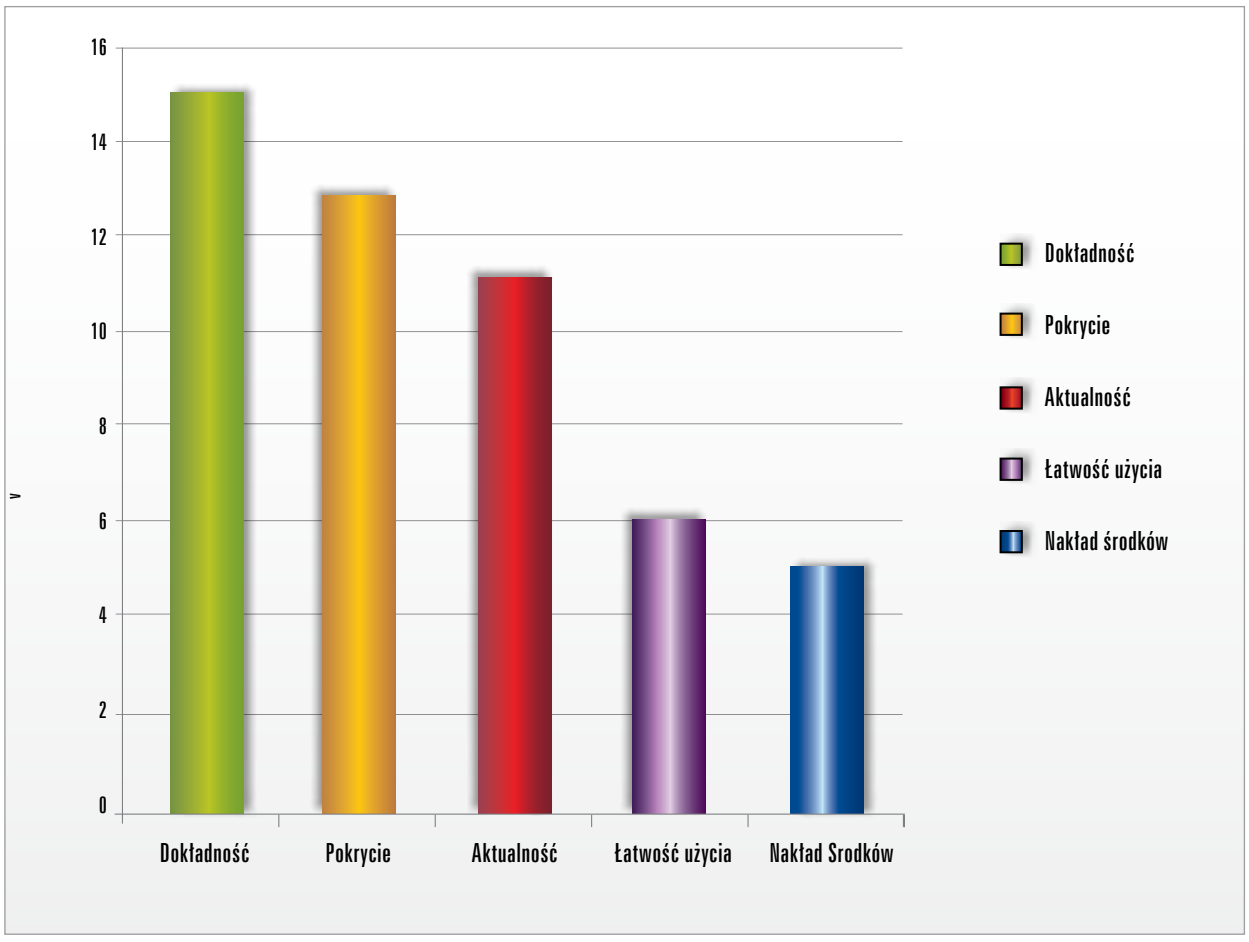
Istotnym w tym opracowaniu jest fakt, że w jego powstanie zaangażowani byli praktycy głównie

9. Najciekawsze wydarzenia z działalności CERT Polska

z europejskich zespołów CERT i uznani eksperci z dziedziny bezpieczeństwa. Raport opiera się na gruntownym badaniu ankietowym przeprowadzonym pośród 45 zespołów CERT oraz toczącej się przez cały czas tworzenia dokumentu dyskusji ekspertów. Ich znaczny wkład, obok doświadczenia i pracy autorów, pozwolił na stworzenie wyczerpującej publikacji o obsłudze incydentów przez zespoły CERT.

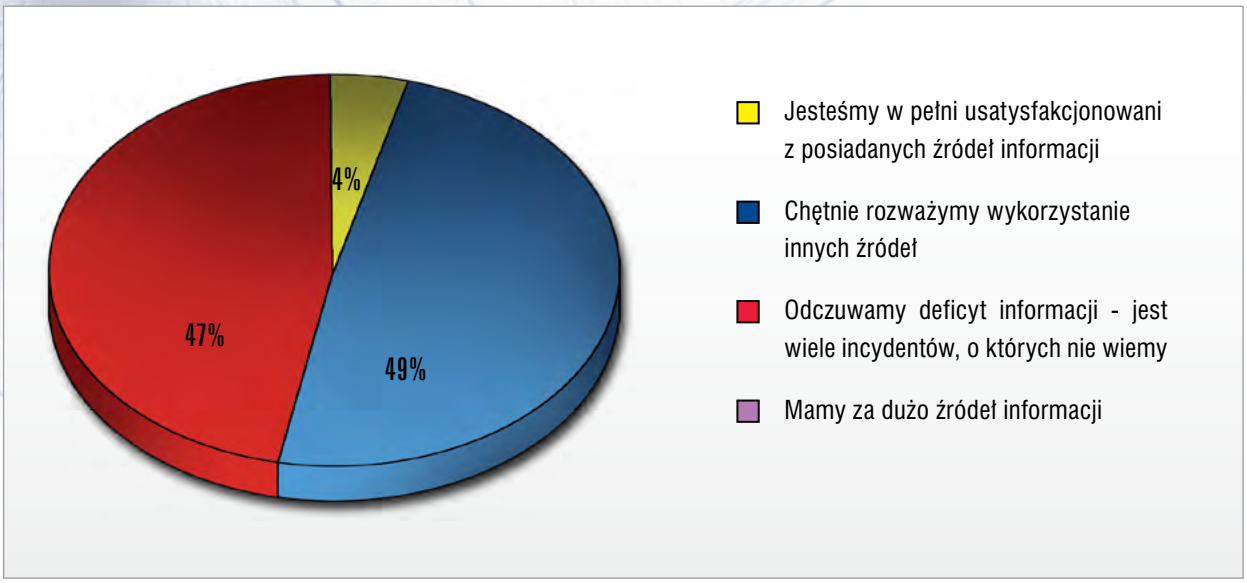
W raporcie można znaleźć oceny i opisy zewnętrznych źródeł informacji o incydentach oraz wewnętrznych narzędzi monitorujących, z których CERTy mogą korzystać, aby zwiększyć swoje możliwości detekcji incydentów bezpieczeństwa w codziennej działalności.

Podczas zbierania materiału do raportu zostało zidentyfikowanych i przeanalizowanych 16 poważnych przeszkód w procesie wykrywania incydentów dotyczących zarówno kwestii technicznych, jak i prawno-organizacyjnych. Pośród przeszkód technicznych najczęściej wymieniane były słaba jakość danych, brak automatyzacji w ich przetwarzaniu i korelacji. W kwestiach prawnych problemem są regulacje dotyczące prywatności i ochrony danych osobowych, które uniemożliwiają wymianę danych. Dla każdego ze zidentyfikowanych problemów zaproponowany został szereg potencjalnych rozwiązań i rekomendacji dla podmiotów dostarczających dane o incydentach, dla ich odbiorców i dla organizacji europejskich lub krajowych.



Wykres 9.3.1. Właściwości źródeł danych o incydentach, które według zespołów reagujących wymagają poprawy

9. Najciekawsze wydarzenia z działalności CERT Polska



Wykres 9.3.2. Opinie zespołów CERT dotyczące zadowolenia ze źródeł informacji z obszaru ich działania

Wyniki opublikowanego raportu pomogą zarówno nowopowstałym, jak i już istniejącym zespołom CERT znaleźć i skorzystać z wcześniej nieużywanych, a wartych uwagi źródeł informacji, a także rozważyć wykorzystanie dodatkowych narzędzi w swojej organizacji. Usprawnienie proaktywnego wykrywania i przetwarzania danych o incydentach wpływa na sprawność funkcjonowania nie tylko pojedynczego CERTu, ale również wszystkich, których dane te dotyczą. To z kolei pozwala zacieśniać współpracę i wymianę informacji pomiędzy zespołami CERT, które dużo szybciej są w stanie reagować i rozwiązywać problemy zwiększając bezpieczeństwo Internetu.

Po pełną informację odsyłamy do raportu na stronie: http://www.enisa.europa.eu/act/cert/support/proactive-detection
oraz do wyników badania przeprowadzonego wśród zespołów CERT:
http://www.enisa.europa.eu/act/cert/support/proactive-detection/survey-analysis

9.4 CERT Polska dołącza do APWG

Pod koniec 2010 roku CERT Polska przystąpił do inicjatywy Anti-Phishing Working Group. Jest to forum dla podmiotów zajmujących się zwalczaniem przestępczości elektronicznej, ze szczególnym uwzględnieniem wyłudzania danych. W ramach APWG aktywne są zarówno jednostki naukowo-badawcze czy zespoły reagujące typu CERT, jak i wiele podmiotów komercyjnych, w szczególności producentów komercyjnych systemów filtrowania ruchu, antywirusów itp. Zewnętrzne cele APWG to przede wszystkim analiza trendów zagrożeń oraz edukacja - zarówno decydentów stanowiących o prawie czy regulacjach (np. w zakresie rejestracji domen), jak i końcowych żytkowników. Dobrym przykładem jest realizowana w Stanach Zjednoczonych wspólnie z NCSA kampania „STOP. THINK. CONNECT". Nie da się ukryć, że dla wszystkich członków APWG co najmniej równie ważnym celem jest nawiązywanie kontaktów oraz stała wymiana wiedzy, której sprzyja połączenie środowiska akademickiego, telekomunikacyjnego i komercyjnego. CERT Polska ma w APWG status „research member".

9. Najciekawsze wydarzenia z działalności CERT Polska

W 2011 roku CERT Polska wziął udział w dwóch spotkaniach organizowanych przez APWG - eCrime Researchers Sync Up w marcu w Dublinie oraz eCrime Research Summit w listopadzie w San Jose, w Kalifornii. Na tej ostatniej konferencji Przemysław Jaroszewski zaprezentował studium przypadku infekcji Zeusem mobilnym (ZITMO).

Więcej informacji o Anti-Phishing Working Group można znaleźć na stronie http://www.apwg.org/.

9.5 Publiczne wydanie Capture-HPC w ramach Honeynet Project

Organizacja The Honeynet Project zrzesza ekspertów z różnych domen bezpieczeństwa komputerowego i umożliwia im łatwą wymianę wiedzy oraz wspólne tworzenie rozwiązań, których celem jest poprawa bezpieczeństwa użytkowników Internetu. Udział w organizacji opiera się na wolontariacie - poświęceniu własnego wolnego czasu na analizę i rozpoznawanie nowych zagrożeń, tworzenie narzędzi, materiałów edukacyjnych oraz udział w dyskusjach. Od momentu powstania w 1999 jest jedna z najlepiej rozpoznawanych organizacji w międzynarodowym środowisku security.

Eksperci zrzeszeni w The Honeynet Project podejmują wspólny wysiłek mający na celu wzbogacanie istniejącej wiedzy o zagrożeniach i metodach jakich można użyć, aby je zwalczać. Owocem ich prac jest zbiór blisko trzydziestu artykułów noszących wspólny tytuł „Know Your Enemy" („Poznaj swojego wroga"). Seria opisuje zagadnienia takie, jak śledzenie botnetów, przedstawia architektury honeypotów i możliwości ich zastosowania, opisuje zagrożenia typu phishing, robaki internetowe, złośliwe strony WWW oraz wiele innych. Odbiorcami artykułów są najczęściej eksperci codziennie stykający się z zagadnieniami bezpieczeństwa komputerowego, jednakże bardziej zaawansowani użytkownicy także znajdą w nich bogate źródło informacji.

Dynamiczny charakter zagrożeń, z jakimi eksperci bezpieczeństwa stykają się na co dzień wymaga, aby ciągle doskonalili swoje umiejętności związane z ich rozpoznawaniem i ich analizą. Najlepszą drogą do osiągnięcia tego celu są praktyczne ćwiczenia. The Honeynet Project udostępnia zbiór zaawansowanych zadań, dzięki którym każdy może sprawdzić swoje siły w analizie zagrożeń takich jak złośliwe pliki PDF, zagrożenia związane z VoIP, analiza z wykorzystaniem technik reverse-engineering oraz wiele innych. Każde z zadań bazuje na rzeczywistym przypadku ataku, który został wnikliwie zbadany przez ekspertów. Podsumowanie zadania wskazuje kroki, jakie należało podjąć w celu wykrycia ataku oraz przedstawia przykładowe narzędzia pomocne w jego analizie. Dodatkowym atutem udziału w zadaniu, które ma formę konkursu, są drobne nagrody fundowane przez organizatorów.

Wiedza, jaką gromadzi organizacja, ma bezpośrednie przełożenie w postaci narzędzi tworzonych przez jej członków. W chwili obecnej zbiór projektów prowadzonych przez The Honeynet Project przekracza 20. Ze względu na to, że jest to działalność non-profit, a jedynym źródłem, z jakiego może się utrzymywać, są dotacje, narzędzia jakie powstają, są owocem prac wolontariuszy lub częściami większych projektów prowadzonych przez niezależne jednostki, które zgodziły się je upublicznić. Od kilku lat The Honeynet Project jest także aktywnym członkiem programu Google Summer of Code, umożliwiającego studentom z całego świata pracę nad tworzeniem narzędzi open source. Dzięki tego typu inicjatywom powstały nowe, a także zostały rozwinięte już istniejące projekty, które są pod opieką organizacji.

The Honeynet Project jest organizacją międzynarodową, składającą się z ponad 40 kapituł rozsianych po całym globie. W Polsce od listopada 2011 roku, dzięki zaangażowaniu członków CERT

9. Najciekawsze wydarzenia z działalności CERT Polska

Polska, działa Polska Kapituła The Honeynet Project. W skład kapituły wchodzi grupa ekspertów z CERT Polska, dodatkowo wspieranych przez ekspertów z Zespołu Metod Bezpieczeństwa Sieci i Informacji działającego w Pionie Naukowym NASK. Misją kapituły jest propagowanie wiedzy o zagrożeniach napotykanych we współczesnej sieci Internet oraz tworzenie narzędzi wspomagających wykrywanie i analizę ataków. Dotychczasowym wkładem w rozwój organizacji jest stworzenie nowszej i stabilniejszej wersji wysoko -interaktywnego klienckiego Honeypota Capture -HPC. Prace zostały wykonane w ramach rozwoju projektu HoneySpider Network - wspólnego przedsięwzięcia zespołów CERT Polska, GOVCERT.NL oraz SURFnet. Autorem oryginalnego oprogramowania jest Christian Seifert, a modyfikacje zostały wprowadzone przez Dział Rozwoju Oprogramowania NASK. Capture-HPC z projektu HoneySpider Network to nowa wersja, która wprowadza szereg ulepszeń oraz pozwala na zastosowanie maszyn wirtualnych VirtualBox oraz KVM (oryginał opierał się na VMware). Oprogramowanie zostało ustabilizowane oraz udostępnione na licencji GPL 2.0. Kod źródłowy honeypota oraz instrukcje instalacji i użytkowania można pobrać ze strony kapituły.

Kapituła liczy ośmiu członków, głównie zaangażowanych w rozwój projektów związanych z wykorzystaniem technologii honeypotów do wykrywania i analizy różnego rodzaju ataków. Eksperci z CERT Polska prowadzą także wiele szkoleń i kursów przybliżających zagadnienia związane z bezpieczeństwem w sieci Internet. Więcej informacji o misji Polskiej Kapituły The Honeynet Project dostępnych jest na stronach internetowych http://cert.pl oraz http://pl.honeynet.org. Wszystkich zainteresowanych rozwojem kapituły oraz narzędziami, jakie udostępniamy, zapraszamy do kontaktowania się poprzez email hnp@cert.pl.

9.6 Zakończenie projektu WOMBAT

W kwietniu 2011 roku zakończył się projekt WOMBAT - Worldwide Observatory of Malicious Behaviour and Attack Threats. Projekt wystartował w styczniu 2008 roku w ramach 7. Programu Ramowego Unii Europejskiej. Celem projektu WOMBAT było utworzenie platformy systemu monitorowania i analizy zagrożeń internetowych, w szczególności złośliwego oprogramowania, które w ostatnich latach stało się potężnym narzędziem w rękach cyberprzestępców. Obok NASK w projekcie brali udział specjaliści ds. bezpieczeństwa z firm takich jak: France Telecom R&D, Symantec, Hispasec Sistemas (twórcy projektu Virustotal) oraz instytucji naukowo-badawczych: Institut Eurecom, FORTH, Politecnico di Milano, Technical University Vienna, Vrije i Universiteit Amsterdam. Prace projektowe były kierowane przez zespół CERT Polska przy współpracy Działu Naukowego NASK.

Prace w projekcie były prowadzone wokół trzech różnych obszarów:

- zbierania informacji o złośliwym oprogramowaniu za pomocą crawlerów i honeypotów (w tym udoskonalania tych technik i zaproponowanie nowych),
- rozwojem nowych technik wzbogacania zbieranych informacji,
- zaawansowana analiza zagrożeń, na podstawie korelacji informacji od partnerów projektu w celu identyfikacji przyczyn i zrozumienia charakterystyki zjawiska.

Stworzono WAPI (WOMBAT API), który w łatwy i przystępny sposób umożliwia dostęp do danych z wielu systemu uczestniczących i rozwijanych w ramach projektu (m.in. Virustotal, SGNET, Shelia, Wepawet, HoneySpider Network, HARMUR, Anubis). Kod WAPI został udostępniony na licencji BSD: http://sourceforge.net/projects/wombat-api/. Kod jest stale udoskonalany.

9. Najciekawsze wydarzenia z działalności CERT Polska

Wkład NASK w projekt dotyczył:

- przeprowadzenia analizy obecnego stanu rzeczy oraz sporządzenia założeń dla środowiska WOMBAT,
- pracę nad wspólnym API (WAPI),
- udoskonalenia i rozwoju systemu klienckich honeypotów - HoneySpider Network,
- opracowania narzędzia w oparciu o techniki maszyn uczących się w celu redukcji fałszywych alarmów dla systemu Capture-HPC,
- opracowania narzędzia do wizualizacji i analizy powiązań pomiędzy wykrytymi złośliwymi adresami URL.

Ponadto niektóre instancje systemu HoneySpider Network zasilały nowo powstały w ramach projektu system wykrywania zagrożeń FIRE (FInding Rogue Networks): http://maliciousnetworks.org/.

Poza rozwojem i opracowaniem narzędzi i systemów przez partnerów projektu, przeprowadzono również wiele prezentacji na temat osiągnięć projektu na konferencjach naukowych (np. RAID, DIMVA) i technicznych (np. BlackHat, FIRST, Honeynet Project Workshop). Dokumentację projektową zamieszczono na oficjalnej stronie projektu: http://www.wombat-project.eu.

9.7 Zakończenie projektu FISHA, przygotowania do projektu NISHA

Projekt FISHA to przedsięwzięcie, w ramach którego opracowano prototyp europejskiego systemu wymiany informacji o bezpieczeństwie komputerowym oraz ostrzegania przed zagrożeniami pojawiającymi się w Internecie - EISAS (European Information Sharing and Alerting System). Projekt był realizowany w latach 2009 − 2011 w ramach programu Komisji Europejskiej „Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" we współpracy pomiędzy CERT Polska, węgierskim zespołem CERT (CERT-Hungary) oraz niemieckim instytutem badawczym Internet Security Centre z Uniwersytetu Gelsenkirchen.

Nadrzędnym celem projektu jest wzrost świadomości w kwestii bezpieczeństwa on-line wśród użytkowników oraz kadry pracowniczej sektora małych i średnich przedsiębiorstw. Skupienie się na tych grupach wynika z faktu, że poprzez swoją liczebność odgrywają one kluczową rolę w bezpieczeństwie Internetu, będąc jednocześnie łatwym celem ataków z powodu niskiej znajomości zagadnień bezpieczeństwa.

W ramach projektu prowadzono zarówno działania techniczne, mające na celu wytworzenie platformy do wymiany i rozgłaszania informacji, jak i działania polegające na opracowaniu sposobów dotarcia z przystępną informacją do grup docelowych. Owocem współpracy konsorcjum jest prototyp modelowego portalu internetowego oraz autorskiej implementacji sieci P2P do wymiany informacji pomiędzy podmiotami z krajów członkowskich Unii Europejskiej, a także plan komunikacji z odbiorcami.

Stworzony w ramach FISHA prototyp systemu będzie bazą do kontynuacji prac w postaci projektu NISHA (Network for Information Sharing and Alerting) w latach 2012-2014 przez trzech dotychczasowych partnerów oraz przez nowego członka konsorcjum - fundację FCCN (Foundation for National Scientific Computing) z Portugalii.

ARAKIS

Raport roczny 2011

Wstęp

System ARAKIS (AgRegacja, Analiza i Klasyfikacja Incydentów Sieciowych) jest projektem zespołu CERT Polska działającego w strukturach NASK. System rozwijany jest we współpracy z Działem Rozwoju Oprogramowania oraz z Działem Naukowym NASK. Jego głównym zadaniem jest wykrywanie i opisywanie zagrożeń występujących w sieci na podstawie agregacji i korelacji danych z różnych źródeł, w tym rozproszonej sieci honeypotów (pułapek), darknetu, firewalli oraz systemów antywirusowych. W przypadku podstawowego źródła danych - honeypotów - system bazuje na danych pozyskanych z ruchu nieprodukcyjnego. W związku z tym nie jest możliwe wykrywanie i analizowanie ataków precyzyjnych wycelowanych jedynie w serwery produkcyjne (np. DDoS). ARAKIS sprawdza się natomiast w analizowaniu zagrożeń (głównie automatycznych) propagujących się poprzez aktywne skanowanie sieci (w takim przypadku jest duża szansa, że zostanie nawiązane połączenie do honeypota), np. robaki sieciowe.

Szczególną implementacją systemu ARAKIS jest projekt ARAKIS-GOV wykorzystywany do ochrony zasobów teleinformatycznych administracji publicznej. Jest on obecnie wdrożony w siedemdziesięciu pięciu instytucjach administracji publicznej we współpracy z polskim CERTem rządowym CERT.GOV.PL działającym w strukturach Departamentu Bezpieczeństwa Teleinformatycznego ABW.

Niniejsze roczne podsumowanie jest czwartym tego typu. Głównym celem systemu jest ochrona zasobów sieciowych uczestników projektu poprzez wykrywanie źródeł infekcji będącej we wczesnym stadium. Dzięki pozyskanym informacjom możliwe było również poznanie mechanizmów działania zarówno nowych jak i aktualnych ataków na aplikacje serwerowe. Projekt ARAKIS był prezentowany na wielu krajowych i międzynarodowych konferencjach poświęconych bezpieczeństwu IT. Wielokrotnie był także wymieniany przez polskich i zagranicznych naukowców oraz specjalistów od bezpieczeństwa IT w ich publikacjach.

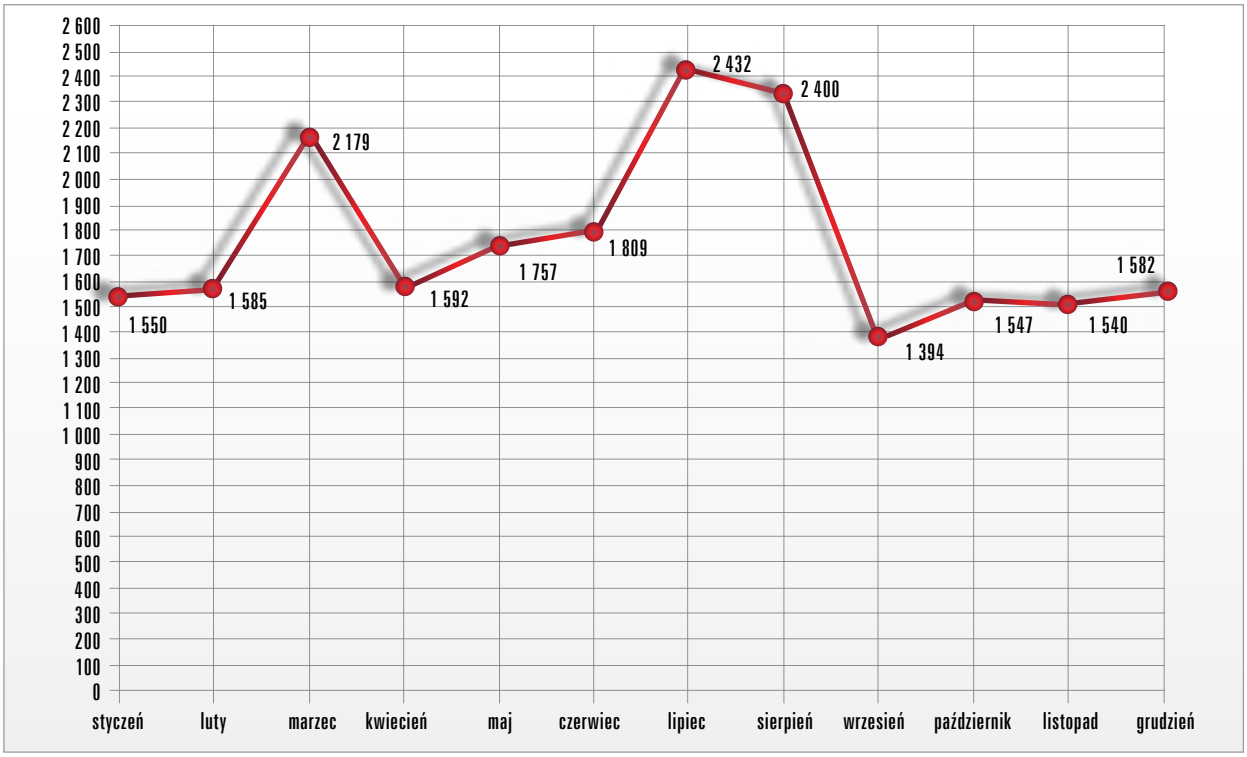
W raporcie zamieszczono m.in. statystyki dotyczące alarmów generowanych przez system. Są one kluczowe z punktu widzenia obsługi systemu, ponieważ zawiadamiają operatorów opisując - zależnie od swojego typu i priorytetu - zagrożenia i zdarzenia mające znamiona incydentu związanego z naruszeniem bezpieczeństwa sieciowego. Inne statystyki dotyczą źródeł oraz rodzajów zagrożeń. Ponadto opisano kilka interesujących przypadków obserwacji dokonanych przez system ARAKIS.

1. Statystyki dotyczące alarmów

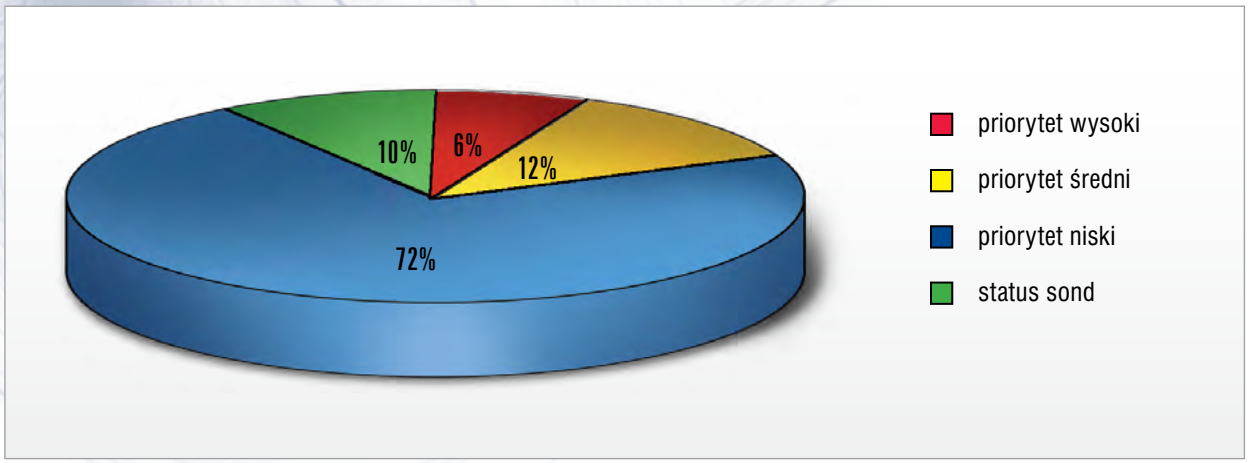
W roku 2011 w systemie ARAKIS zostało wygenerowanych 21 307 alarmów - jest to o ponad 6 000 mniej niż w roku 2010. Spadek spowodowany był m.in. ogólnoświatowym trendem związanym z odchodzeniem cyberprzestępców od ataków propagujących się przez skanowanie na korzyść atakowania aplikacji klienckich (przeglądarek internetowych, czytników PDF, itd.), oraz precyzyjnych i ukierunkowanych ataków na wcześniej rozpoznane cele. Wykres 1.1 przedstawia roczne zestawienie wszystkich alarmów bez podziału na typy.

Największą liczbę alarmów odnotowano głównie w miesiącach wakacyjnych. Złożyły się na nie przede wszystkim alarmy o priorytecie niskim związane ze wzrostem trendu anomalnego ruchu na poszczególnych portach. Alarmy te dotyczyły zdarzeń pochodzących z sieci Internet (nie były to infekcje stacji roboczych uczestników systemu). Nagły i tymczasowy wzrost liczby alarmów w marcu związany był z problemami z łączem między sondami a centrum (alarmy diagnostyczne są powiązane ze statusem sond) i nie dotyczył zdarzeń związanych z bezpieczeństwem.

Znaczna większość wygenerowanych alarmów w roku 2011 miała niski priorytet (72%). Alarmy o niskim priorytecie świadczą zazwyczaj o anomaliach w ruchu i nie są bezpośrednio związane z incydentami. Następne w kolejności były alarmy o priorytecie średnim (12%) oraz te opisujące stan poszczególnych sond. Najmniej było alarmów opisujących wykrycie poważnych zagrożeń w sieci (6%). W stosunku do zeszłorocznego zestawienia widać wyraźny wzrost procentowych udziałów alarmów o wysokim i niskim priorytecie. Należy jednak wyraźnie zaznaczyć, że znaczna większość alarmów o wysokim priorytecie, które wystąpiły w roku 2011, nie oznaczała rzeczywistego ataku bądź infekcji, a jedynie wynikała ze specyficznej konfiguracji urządzeń sieciowych, użycia pewnych protokołów bądź narzędzi do aktywnego monitoringu sieci.

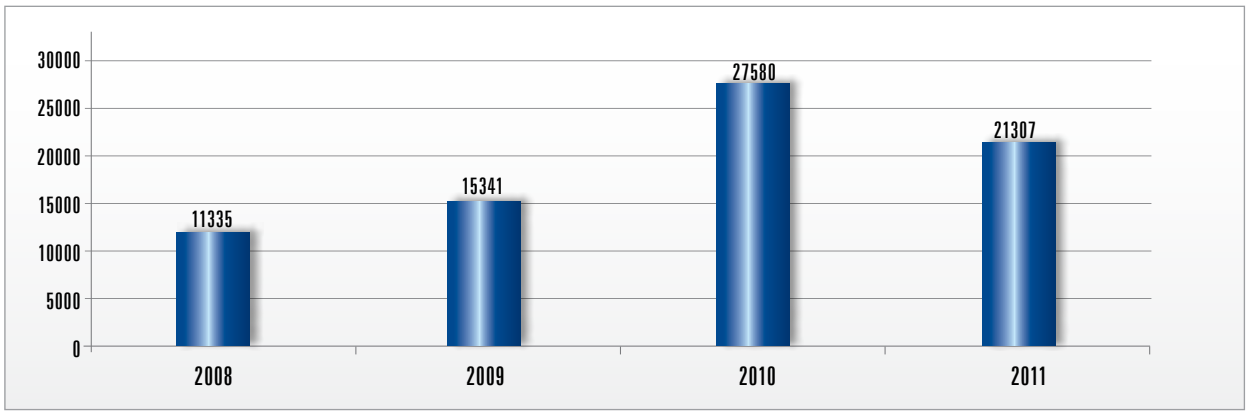


Wykres 1.1. Alarmy wygenerowane przez system ARAKIS w roku 2011

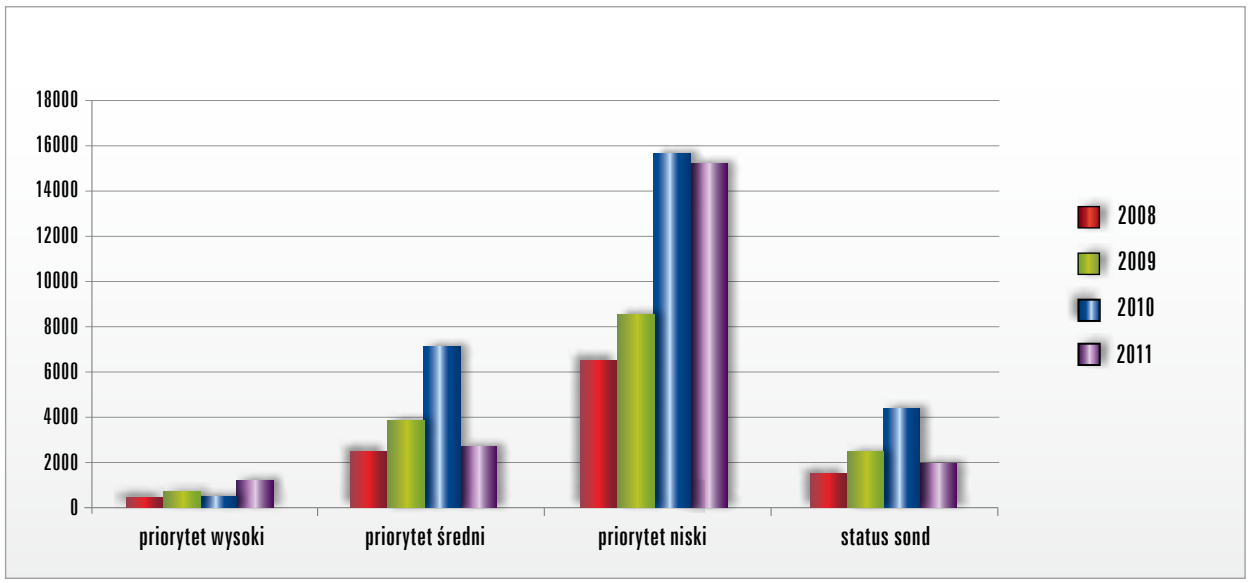


Wykres 1.2. Rozkład procentowy alarmów ze względu na priorytety w roku 2011

Poniżej znajdują się wykresy porównujące alarmy z ostatnich 4 lat:



Wykres 1.3. Liczba wszystkich alarmów



Wykres 1.4. Alarmy systemu ARAKIS

2. Statystyki dotyczące ataków

Jedną z ważniejszych kategorii związanych z atakami wykrywanymi przez honeypoty systemu ARAKIS jest skanowanie portów. Ranking przedstawia liczbę unikalnych w skali całego roku adresów IP, które próbowały łączyć się na poszczególne porty. Obrazuje to bezpośrednio skalę zainteresowania konkretnymi portami (a więc usługami słuchającymi na nich) przez złośliwe oprogramowanie bądź narzędzia typu skanery bezpieczeństwa. Na pierwszym miejscu znajduje się port 445/TCP. Na nim nasłuchuje wiele aplikacji związanych z oprogramowaniem Microsoft, które miało wiele efektownych luk wykorzystywanych przez takie robaki, jak Sasser czy Conficker. Ciekawostką jest drugie i czwarte miejsce, na którym znajdują się porty związane z natywnymi dla systemów Unix usługami: telnet i SSH.

Innym ciekawym zestawieniem wydają się być statystyki Top 10 najczęściej dopasowanych reguł systemu Snort. W tym przypadku także wyznacznikiem były unikalne w skali roku źródłowe adresy IP. Prawie wszystkie reguły poza jedną dotyczą ataków na usługi windowsowe. Pierwsze trzy reguły dotyczą połączenia RDP na port 3389/TCP (używany jest przez usługę „zdalny pulpit") i mogą być powiązane z robakiem Morto, który pojawił się w roku 2011.

Pozycja	Docelowy port / protokół	Liczba widzianych unikalnych IP	Opis
1	445/TCP	79 925	Ataki typu buffer overflow na usługi Windows RPC
2	23/TCP	56 908	Ataki na usługę telnet
3	135/TCP	18 799	Ataki na usługę Windows DCE/RPC
4	22/TCP	15 665	Ataki słownikowe na serwery SSH
5	139/TCP	11 273	Ataki na usługę NetBIOS / współdzielenie plików i drukarek
6	1433/TCP	9 125	Ataki na MS SQL
7	80/TCP	7 677	Ataki na aplikacje webowe
8	3389/TCP	6 798	Ataki słownikowe na RDP (zdalny pulpit) - w dużej mierze aktywność robaka Morto
9	5060/UDP	3 375	Ataki na VoIP
10	4899/TCP	3 010	Ataki na usługę Radmin

Tabela 2.1. Najczęściej atakowane porty

Pozycja	Reguła Snort	Liczba unikalnych IP
1	ET POLICY RDP connection request	85 994
2	MISC MS Terminal server request	80 910
3	ET POLICY Radmin Remote Control Session Setup Initiate	77 748
4	ET SCAN DCERPC rpcmgmt ifids Unauthenticated BIND	48 450
5	ATTACK-RESPONSES Microsoft cmd.exe banner	24 480
6	ET ATTACK_RESPONSE Possible MS CMD Shell opened on local system	22 487
7	ET POLICY Suspicious inbound to MSSQL port 1433	21 485
8	NETBIOS SMB-DS IPC$ unicode share access	20 183
9	ET SCAN Potential SSH Scan	16 617
10	ET EXPLOIT LSA exploit	16 479

Tabela 2.2. Najczęściej dopasowywane reguły Snort

Rozpatrując statystyki geograficznych lokalizacji źródeł ataków otrzymujemy ciekawe zestawienie: w kontekście unikalnych adresów IP na pierwszym miejscu są USA, na drugim Rosja, na trzecim Turcja, a Chiny dopiero na piątym. Jeżeli natomiast rozpatrzona zostanie sama liczba połączeń, bez kontekstu unikalnego adresu IP, na pierwszym miejscu znajdą się Chiny, a następnie USA i Rosja. Wynika stąd, że najwięcej ataków jest z Chin, ale pochodzą one ze stosunkowo niewielu adresów IP.

Pozycja	Kraj	Liczba unikalnych adresów IP
1	US	19 313
2	RU	18 317
3	TR	16 102
4	KR	13 384
5	CN	11 866
6	PL	9 015
7	TW	8 450
8	UA	8 358
9	AE	7 873
10	DE	7 790

Tabela 2.3. Najbardziej zainfekowane kraje pod względem unikalnych adresów IP

Pozycja	Kraj	Liczba połączeń
1	CN	2 149 387
2	US	1 641 497
3	RU	631 184
4	UA	450 243
5	KR	432 089
6	TR	418 869
7	PL	386 186
8	DE	323 129
9	TW	207 125
10	GB	195 262

Tabela 2.4. Najbardziej zainfekowane kraje pod względem liczby przepływów

Zestawienie najbardziej zainfekowanych systemów autonomicznych ujawnia, że najwięcej unikalnych w skali roku źródłowych adresów IP pochodziło z sieci tureckiego operatora Turk Telekomunikasyon Anonim Sirketi (numer AS: 9121).

Na drugim miejscu znajduje się sieć koreańskiego ISP Korea Telecom (AS: 4766), a na trzecim Emirates Telecommunications Corporation (AS: 5384) ze Zjednoczonych Emiratów Arabskich.

Pozycja	Liczba unikalnych adresów IP	Numer AS	Kraj	Nazwa operatora
1	12 416	AS9121	TR	TTNET Turk Telekomunikasyon Anonim Sirketi
2	10 406	AS4766	KR	KIXS-AS-KR Korea Telecom
3	7 841	AS5384	AE	EMIRATES-INTERNET Emirates Telecommunications Corporation
4	6 767	AS12741	PL	INTERNETIA-AS Netia SA
5	6 174	AS3462	TW	HINET Data Communication Business Group
6	5 767	AS4134	CN	CHINANET-BACKBONE No.31,Jin-rong Street
7	4 632	AS6147	PE	Telefonica del Peru S.A.A.
8	2 862	AS8452	EG	TE-AS TE-AS
9	2 845	AS24863	EG	LINKdotNET-AS
10	2 602	AS5483	HU	HTC-AS Magyar Telekom plc.

Tabela 2.5. Najbardziej zainfekowane systemy autonomiczne pod względem unikalnych adresów IP

Jeżeli zestawimy liczbę połączeń (bez uwzględniania unikalności nadawcy), to - podobnie jak w zestawieniu najbardziej zainfekowanych krajów - czołowe pozycje będą zajmować operatorzy chińscy. Potwierdza to fakt, że z Chin widocznych było w systemie ARAKIS dużo ataków ale pochodziły one ze stosunkowo niewielkiej liczby IP.

Pozycja	Liczba połączeń	Numer AS	Kraj	Nazwa operatora
1	983 239	AS4134	CN	CHINANET-BACKBONE No.31,Jin-rong Street
2	328 667	AS4837	CN	CHINA169-BACKBONE CNCGROUP China169 Backbone
3	290 53	AS9121	TR	TTNET Turk Telekomunikasyon Anonim Sirketi
4	270 021	AS4766	KR	KIXS-AS-KR Korea Telecom
5	219 077	AS23650	CN	CHINANET-JS-AS-AP AS Number forCHINA-NET jiangsu province backbone
6	153 623	AS5384	AE	EMIRATES-INTERNET Emirates Telecommunications Corporation
7	144 942	AS12741	PL	INTERNETIA-AS Netia SA
8	130 050	AS3462	TW	HINET Data Communication BusinessGroup
9	116 941	AS36351	US	SOFTLAYER - SoftLayer Technologies Inc.
10	114 696	AS5483	HU	HTC-AS Magyar Telekom plc.

Tabela 2.6. Najbardziej zainfekowane systemy autonomiczne pod względem liczby przepływów

Innym ciekawym zestawieniem jest rozkład zainfekowanych IP w polskich sieciach. Inaczej niż w statystykach opisanych w głównej części raportu CERT Polska (dane pochodzące z kilku systemów raportujących, nie tylko z ARAKIS-a) na pierwszym miejscu nie znajduje się Telekomunikacja Polska, lecz Netia z ogromną przewagą unikalnych w skali roku adresów IP. Co ciekawe, w rankingu nie ma żadnych operatorów mobilnych. Ponadto w stosunku do ogólnego obrazu przedstawionego w rozdziale 1, pojawiają się mniej znani lub lokalni operatorzy.

Pozycja	Liczba unikalnych IP	Numer AS	Nazwa operatora
1	6 767	AS12741	NETIA
2	744	AS5617	TP
3	201	AS21021	MULTIMEDIA
4	167	AS15857	DIALOG
5	69	AS12476	ASTER
6	65	AS29314	VECTRA
7	58	AS35007	MICRONET
8	56	AS42709	BIELSAT
9	43	AS34337	ELPOS Cable TV
10	39	AS6714	GTS

Tabela 2.7. Zainfekowane adresy IP w polskich sieciach

3. Interesujące przypadki zaobserwowanych incydentów sieciowych

Oprócz ochrony, jaką system ARAKIS zapewnił sieciom, w których zainstalowane są sondy, przyczynił się także do zrozumienia wielu rodzajów zagrożeń powszechnie występujących w Internecie. Dalej w skrócie opisane zostały ciekawsze, naszym zdaniem, obserwacje dokonane przez ARAKIS w minionym roku 2011.

3.1 Morto - nowy robak sieciowy

W połowie marca 2011 roku „narodził" się nowy robak sieciowy nazwany Morto. Atakuje on źle zabezpieczone systemy Microsoft Windows wykorzystując do tego celu protokół RDP (Remote Desktop Protocol) wykorzystywany przez tzw. zdalny pulpit. Morto nie wykorzystuje żadnej luki w oprogramowaniu, a atak polega na próbie odgadnięcia nazwy użytkownika i hasła. Po infekcji robak szuka w sieci kolejnych komputerów z uruchomioną usługą RDP i próbuje je zainfekować. Powoduje to znaczący wzrost ruchu sieciowego na typowym dla tej usługi porcie 3389/TCP. W zainfekowanym systemie Morto zabija procesy, które uznaje (po nazwach) za aplikacje związane z bezpieczeństwem. Jest to bardzo popularne działanie wykonywane po infekcji przez złośliwe oprogramowanie. Masową propagację Morto od jej początku obserwujemy dzięki systemowi ARAKIS.

Regularny wzrost ruchu na porcie 3389/TCP pojawił się 15 sierpnia 2011 r., natomiast 24 sierpnia nastąpił nagły i wyraźny skok, który utrzymywał się do 26 sierpnia.

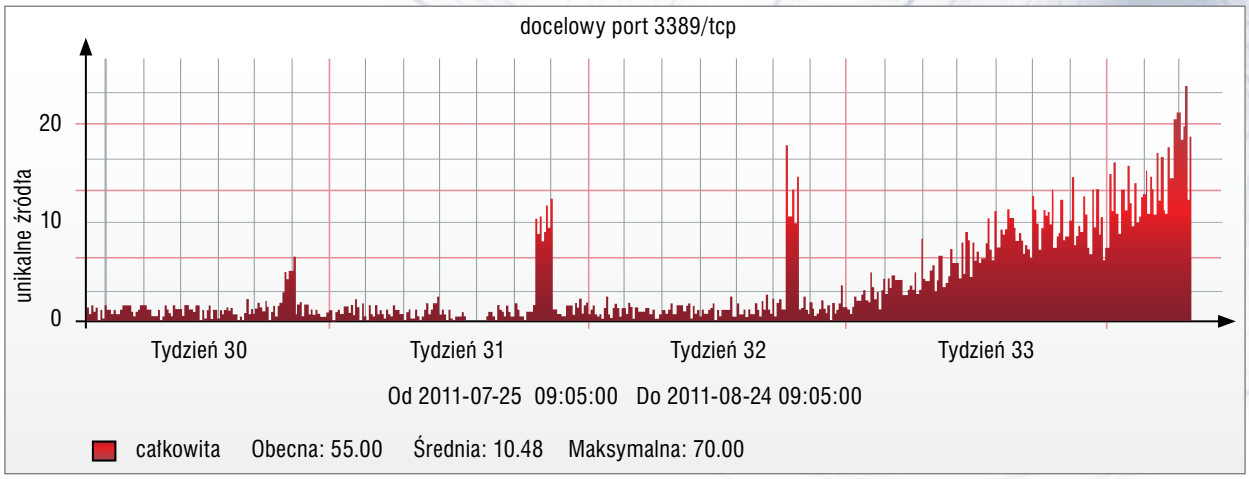


Tabela 3.1.1. Ruch RDP w sieci honeynet (unikalne źródła)

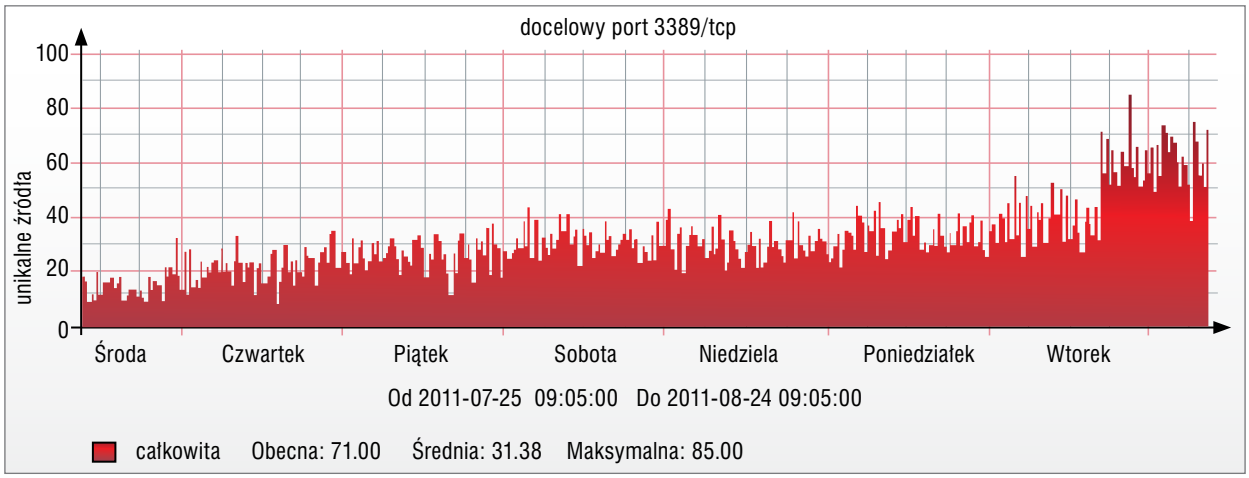


Tabela 3.1.2. Ruch RDP w sieci honeynet (unikalne źródła)

28 sierpnia 2011 r. aktywność na porcie wróciła do normy sprzed masowej propagacji Morto. Po kilku tygodniach robak znowu był widoczny i jego aktywność - już nieco mniejsza - obserwowana jest do chwili obecnej.

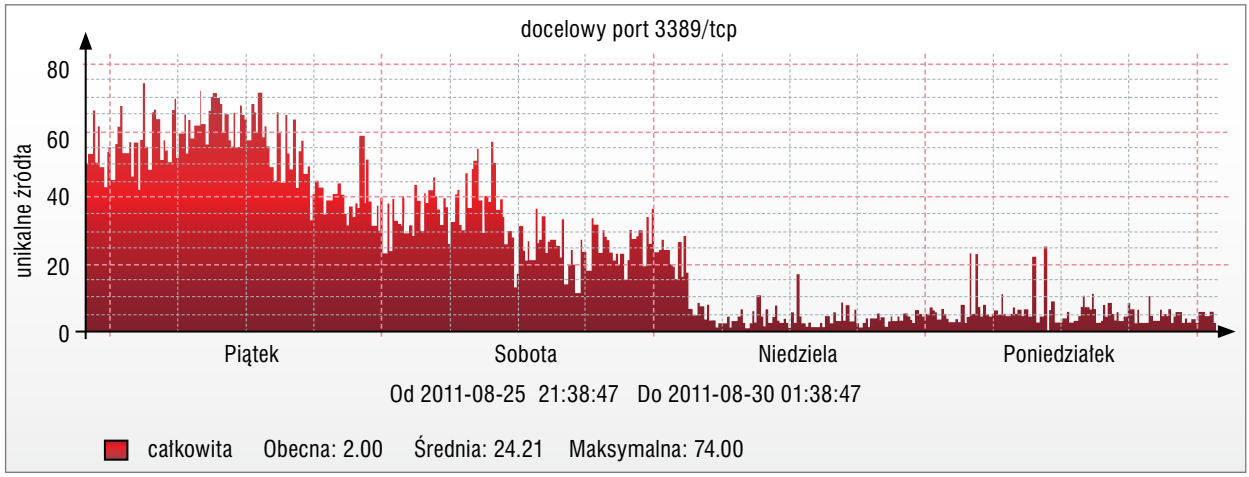


Tabela 3.1.3. Ruch RDP w sieci honeynet (unikalne źródła)

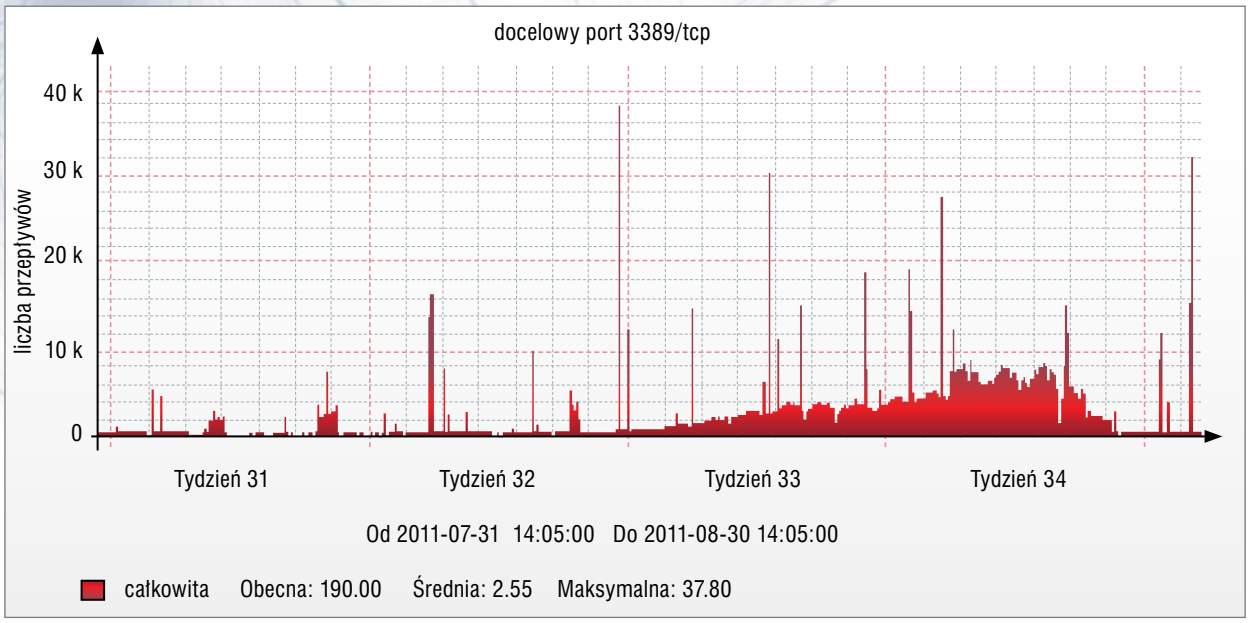


Tabela 3.1.4. Ruch RDP w sieci darknet (liczba przepływów)

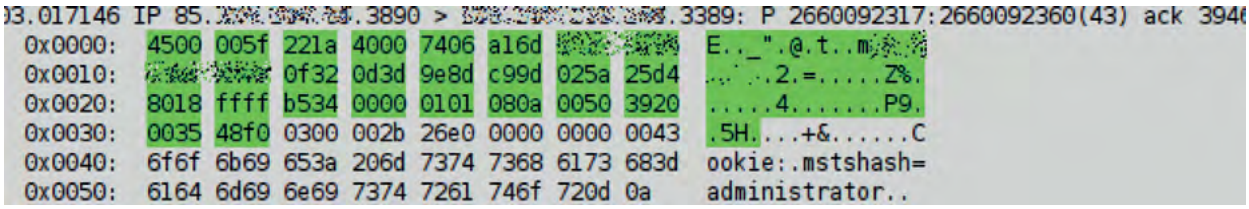
Skanowania RDP widziane były zarówno w honeynecie (wykresy na str. 65), jak i w darknecie (wykres 3.1.4).

Warto zauważyć, że w chwili obecnej aktywność robaka Morto jest nadal stosunkowo wysoka, a port 3389/TCP cały czas znajduje się w TOP 10 najczęściej skanowanych portów.

Rysunek 3.1.5. przedstawia próbkę surowego ruchu sieciowego - pakietu „connection request”[1] komponentu X.224 służący do nawiązania połączenia (faza inicjacji połączenia RDP). Widać w nim ustawione „user cookie”[2] (rozpoczynające się od „mstshash”), które zawiera nazwę użytkownika.

Specjaliści z innych zespołów zajmujących się analizą robaka Morto twierdzili, że próbuje się łączyć zawsze na konto „administrator” z użyciem zestawu predefiniowanych haseł. Do honeypotów ARAKIS-a trafiały jednakże próby połączeń zawierające nazwę nie tylko tego użytkownika (chociaż w znacznej większości). Nie jesteśmy pewni, czy próby połączeń RDP na konta innych użytkowników są też efektem działania tego robaka, czy raczej jest to inne zagrożenie. Stosowane w systemie ARAKIS nisko-interaktywne pułapki nie pozwalają nawiązać pełnej sesji z atakującymi (usługa Remote Desktop nie jest w pełni symulowana), przez co nie możemy stwierdzić, czy za wszystkimi próbami włamań stoi Morto.

Z powodu ogromnej ilości danych w dalszych analizach wykorzystaliśmy pełny zapis ruchu sieciowego z pięciu najczęściej atakowanych sond systemu ARAKIS od 20 do 28 sierpnia, chyba że zostanie napisane inaczej.



Rysunek 3.1.5. Pakiet nawiązujący połączenie RDP

[1] http://msdn.microsoft.com/en-us/library/cc240470%28v=prot.10%29.aspx

[2] http://www.snakelegs.org/2011/02/06/rdp-cookies-2/

Tabela 3.1.6 przedstawia listę najczęściej wykorzystywanych nazw użytkowników.

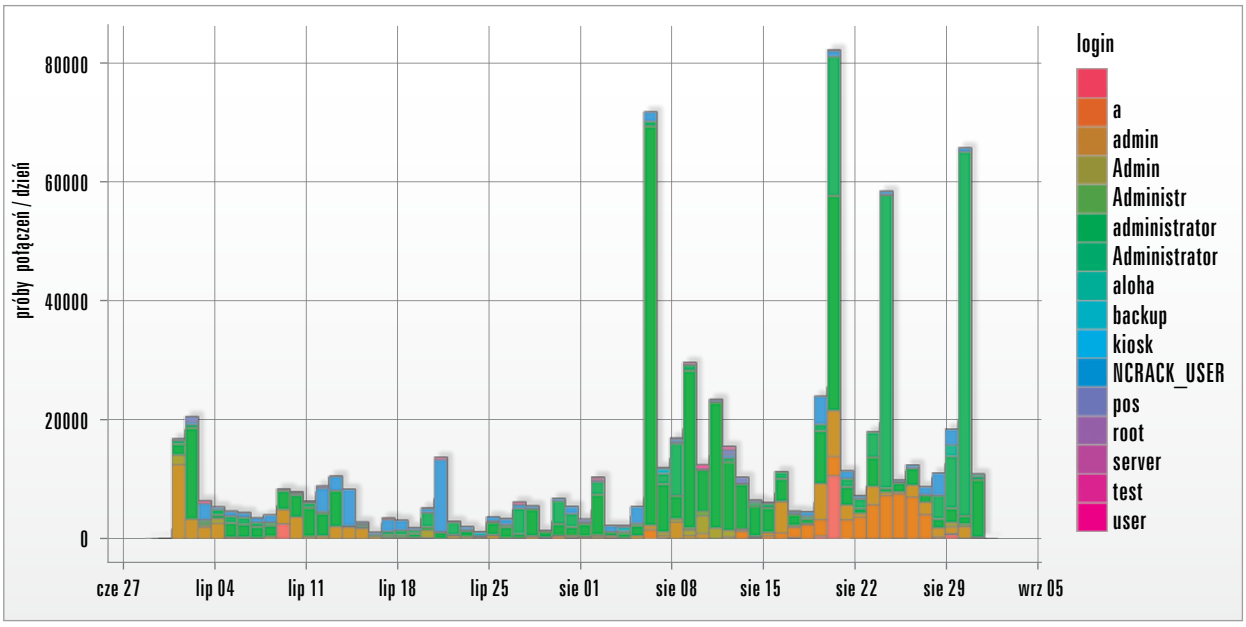
Pozycja	Liczba wystąpień	Nazwa użytkownika
1	33 692	Administrator
2	18 070	administrator
3	11 804	a
4	4 612	admin
5	3 474	..a (\xFF\xFE\x61)
6	3 265	usuario
7	2 884	support
8	2 074	NCRACK_USER
9	644	micros
10	624	pos1
11	369	adm
12	322	aloha
13	230	skannata
14	178	pos
15	129	Admin
16	126	fax
17	100	administrateur

Tabela 3.1.6. Najczęściej używane nazwy użytkowników

Interesujący ciąg znaków znajduje się na piątej pozycji - jest to znak drukowalny („a”) poprzedzony dwoma niedrukowalnymi („FF” i „FE” w kodzie szesnastkowym). Ciekawe wydaje się także użycie „NCRACK_USER” - najprawdopodobniej ktoś nieumiejętnie skorzystał z automatycznego skanera (najprawdopodobniej był to ncrack[3]). Wśród nazw użytkowników znalazły się także słowa w wielu innych niż angielski językach, np. „usuario” (hiszpański), „skannata” (fiński), „administrateur” (francuski), czy „Verwalter” (niemiecki).

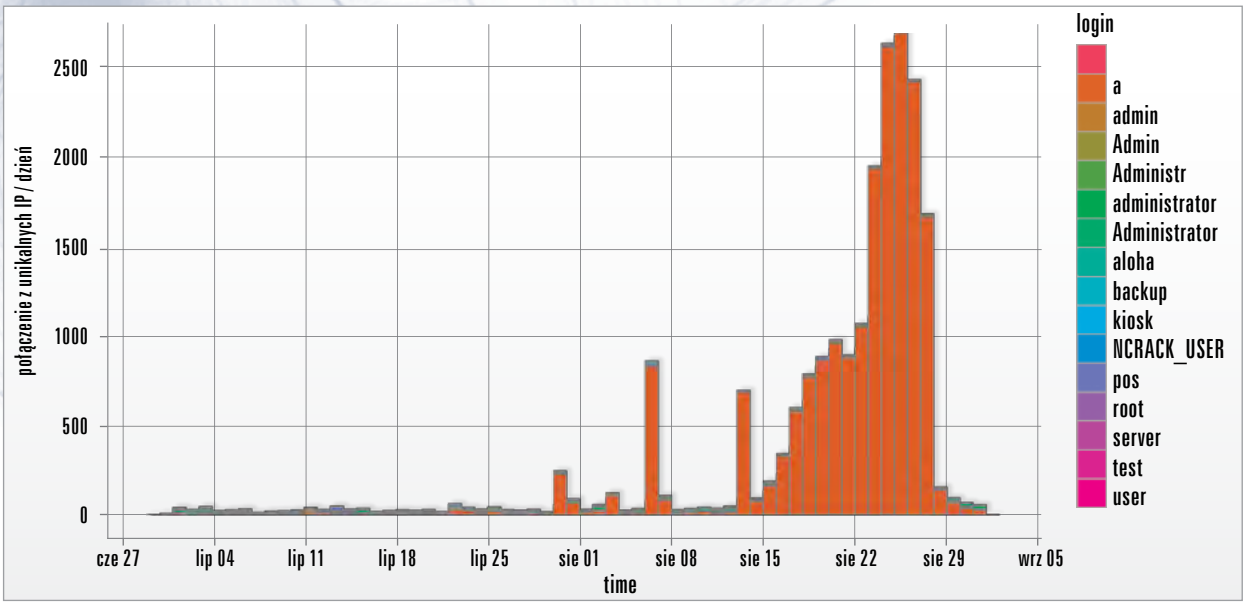
Po przeanalizowaniu kompletnych danych z systemu ARAKIS z lipca i sierpnia 2011 r. wyłoniły się nowe ciekawe wnioski. W przypadku zdecydowanej większości skanowań, pojedynczy źródłowy adres IP próbował łączyć się do wielu adresów docelowych przy użyciu pojedynczej nazwy użytkownika. Na 1 800 adresów źródłowych, jedynie 24 łączyło się na więcej niż jedną nazwę użytkownika, z tego 21 na jedynie dwie różne nazwy. Nasze obserwacje nie są więc do końca zgodne z wcześniejszymi raportami innych zespołów monitorujących Morto, według których robak próbuje zalogować się na wielu różnych użytkowników.

Następnym krokiem była analiza natężenia ruchu w całym badanym okresie. Wykres 3.1.7 przedstawia wszystkie połączenia RDP zarejestrowane przez nasze honeypoty w rozbiciu na nazwy użytkownika, jakie próbowano wykorzystać.



Wykres 3.1.7. Nazwy użytkowników użyte podczas prób połączeń RDP

[3] http://nmap.org/ncrack/

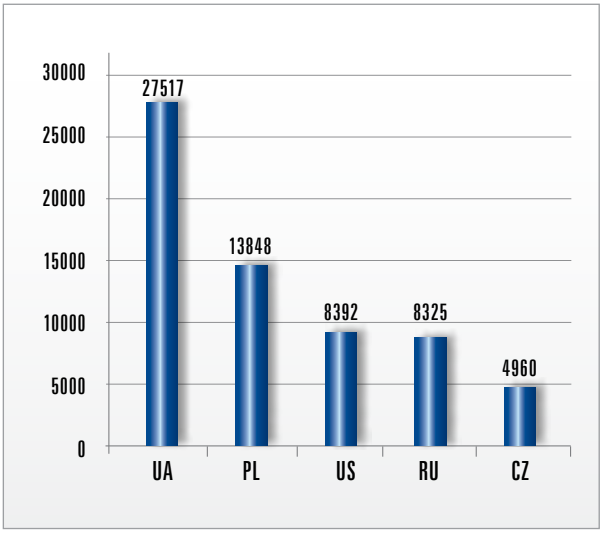


Wykres 3.1.8. Nazwy użytkowników użyte w pierwszym połączeniu każdego unikalnego adresu IP

Maksymalna liczba połączeń dziennie przekracza 80 000, jednak nie widać istotnego trendu. Okazało się, że większość ruchu generowana jest przez pojedyncze źródła, które atakują duże zakresy adresów IP. Dlatego zbadaliśmy jak rozkładały się w czasie połączenia od unikalnych źródłowych adresów IP - powyższy wykres zawiera dane wyłącznie o pierwszym połączeniu z danego adresu IP (nowi atakujący).

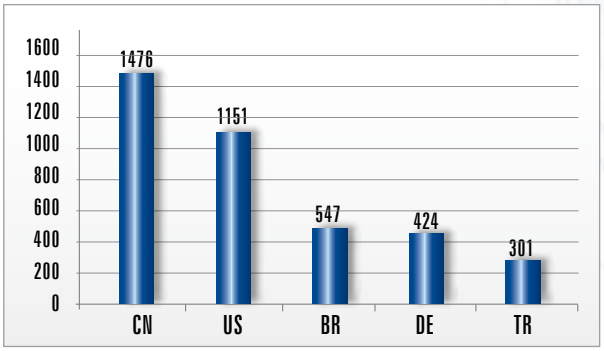
Łatwo zaobserwować, że od ok. 15 sierpnia lawinowo narastała liczba unikalnych źródeł ataków, które wykorzystywały login „a". Atakujący posługujący się innymi nazwami zostali w tym ujęciu całkowicie zmarginalizowani. Lawinowo narastająca liczba źródeł ataków to charakterystyczna cecha szybko rozprzestrzeniających się robaków, więc można przypuszczać, że obserwowany ruch pochodził od Morto. Nazwa „a" była znana jako jedna z wykorzystywanych przez Morto, jednak nie jesteśmy pewni, czemu zaobserwowaliśmy wzrost ataków jedynie z tą nazwą, a nie innymi (np. „Administrator"). Istnieje prawdopodobieństwo, że robak nie nawiązawszy pełnego połączenia na poziomie warstwy aplikacji RDP (wspomniana wcześniej kwestia nisko-interaktywnych honeypotów), zaprzestał dalszych prób z inną nazwą użytkownika.

Obok znajduje się klasyfikacja państw, z których widzianych było najwięcej prób połączeń RDP (ataków). Dane znowu zostały ograniczone do pięciu najczęściej atakowanych sond systemu ARAKIS od 20 do 28 sierpnia. Warto pamiętać, że choć w liście uwzględniono tylko połączenia, w których przesłana była nazwa użytkownika (odrzuciliśmy sprawdzania otwartości portu 3389/TCP), to, jak wspomniane było wyżej, nie mamy pewności, czy wszystkie połączenia związane są z robakiem Morto. Ponadto istnieje prawdopodobieństwo, że źródłowe adresy IP nie są jednoznacznie źródłem ataku - mogą być to pośrednicy, za którymi ukrywa się prawdziwy atakujący. Należy pamiętać, że większe sieci z racji efektu skali mogą być wyżej.



Wykres 3.1.9. Liczba skanowań per kraj (robak Morto)

Poniżej znajduje się klasyfikacja państw, z których widzianych było najwięcej unikalnych atakujących adresów IP.



Wykres 3.1.10. Unikalne adresy IP per kraj

Zarówno aktywność robaka Morto, jak i pozostałe skanowania RDP mogą zostać wykryte za pomocą reguł Snort. W systemie ARAKIS najczęściej dopasowywaną reguła na porcie 3389/TCP jest:

- „ET POLICY RDP connection request" (sid:2001329),
- „ET POLICY MS Remote Desktop Administrator Login Request" (sid:2012709),
- „MISC MS Terminal server request" (sid:1448),
- „ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection" (sid:2001972).

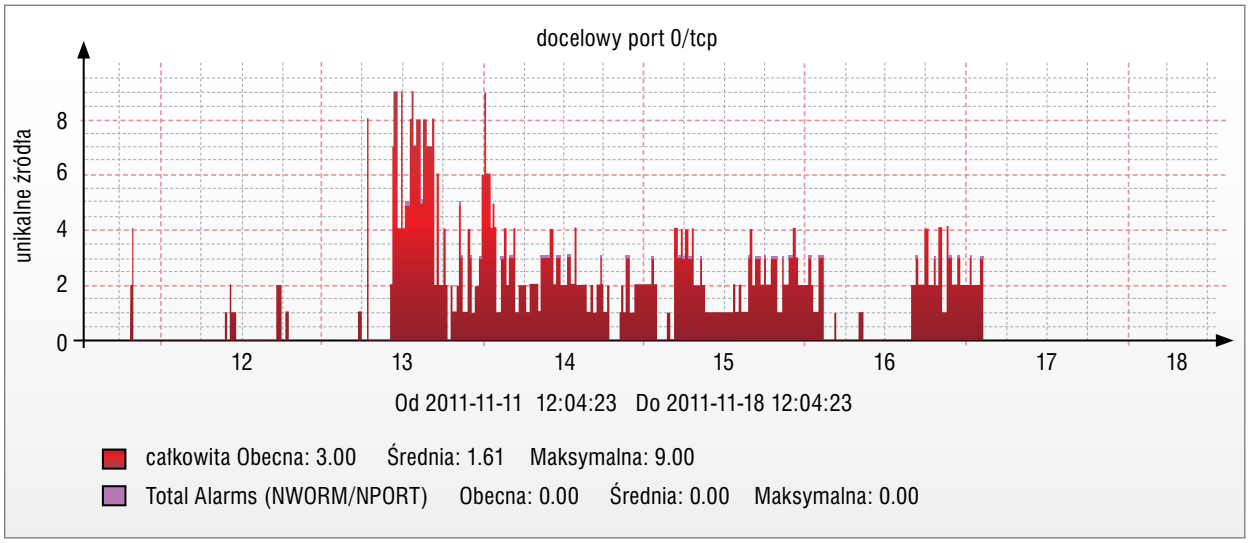
3.2 Dziwny ruch na porcie 0/TCP

Port 0/TCP jest wg rejestru IANA[4] portem zarezerwowanym. Oznacza to, że żadna usługa nie powinna korzystać z tego portu do komunikacji sieciowej. Gdy w dniu 13 listopada 2011 roku do sond systemu ARAKIS zaczęła napływać wzmożona liczba pakietów TCP kierowanych na port 0, wzbudziło to nasze zainteresowanie. Próby połączeń na ten port były widziane zarówno przez honeypoty, jak i w sieci darknet. Znaczna większość pakietów zarejestrowanych w honeypotach była zniekształcona. Ruch wrócił do normy z dniem 17 listopada 2011 r.

Zarejestrowaliśmy jeszcze krótkotrwały wzrost w dniach 30 listopada - 1 grudnia 2011 r.
Nasze obserwacje w tych okresach pokrywają się z danymi pochodzącymi z systemu DSHIELD[5], co świadczy o globalnym zasięgu tej anomalii.

Obserwacje w honeypotach

Wykres 3.2.1 przedstawia liczbę unikalnych adresów IP w pięciominutowym oknie czasowym, które próbowały łączyć się na port 0/TCP do honeypotów systemu ARAKIS.



Wykres 3.2.1. Unikalne adresy IP łączące się na port 0/TCP

[4] http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml
[5] http://www.dshield.org/

Liczba pakietów	Payload (hex)
640	00000000A0027D78
615	0000000000000000A0027D78
602	A0027D78
534	00000000000000000000000000A0027D78
26	DB19F91B00000000000000000000000000A0027D78
7	ED8DDA5E00000000000000000000000000A0027D78
7	CE537D4600000000000000000000000000A0027D78
7	C9A7340E00000000000000000000000000A0027D78
6	F080F25D00000000000000000000000000A0027D78
6	F02FD77C00000000000000000000000000A0027D78

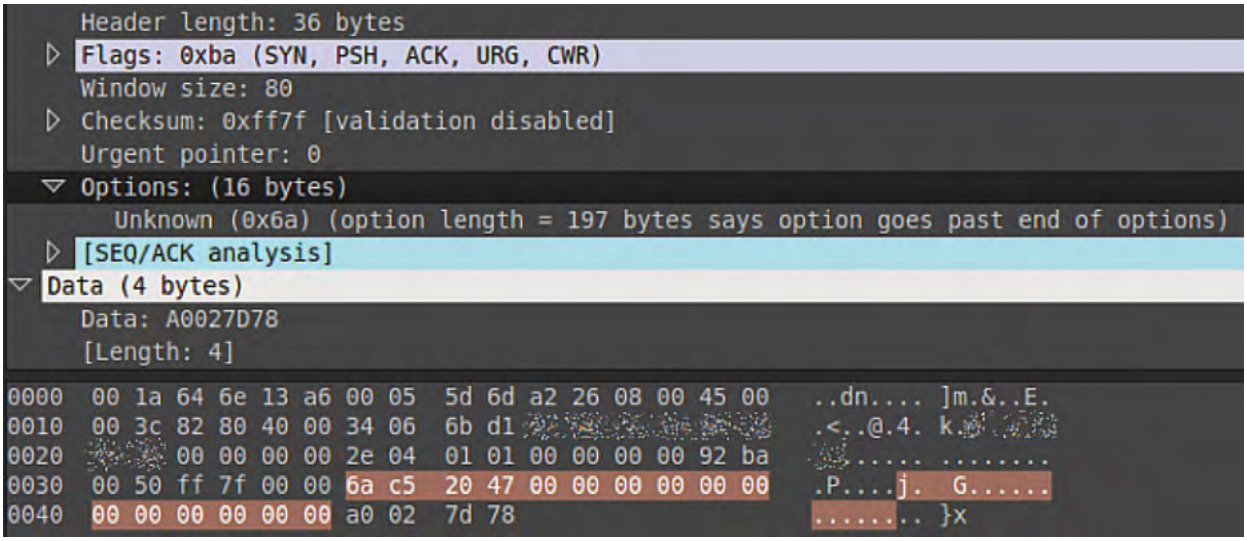
Tabela 3.2.2. Zestawienie zawartości danych w pakietach kierowanych do port 0/TCP

W okresie od 13 do 17 listopada 2011 r. zostało zaobserwowanych przez honeypoty ok. 15 000 pakietów kierowanych na port 0/TCP. Znaczna większość z nich (ok. 14 200) miała w nagłówku ustawiony port źródłowy także 0. Same nagłówki TCP w większości były zniekształcone (np. niepoprawna długość nagłówka) lub nie miały sensu (np. w kontekście ustawionych flag). Również kombinacje flag wydawały się pozbawione sensu.

Jeżeli poza nagłówkiem pakiet TCP zawierał jeszcze dane (tzw. payload), to zawsze występował w nim ciąg heksadecymalny `A0027D78` (zazwyczaj ciąg ten występował sam lub poprzedzony był ciągiem różnej długości składającym się z zer oraz ewentualnie losowych liczb heksadecymalnych - wyrażenie regularne opisujący ten ciąg, to `[0-9A-F]*0*A0027D78`).

Tabela 3.2.2. przedstawia statystyki widzianego payloadu (TOP 10).

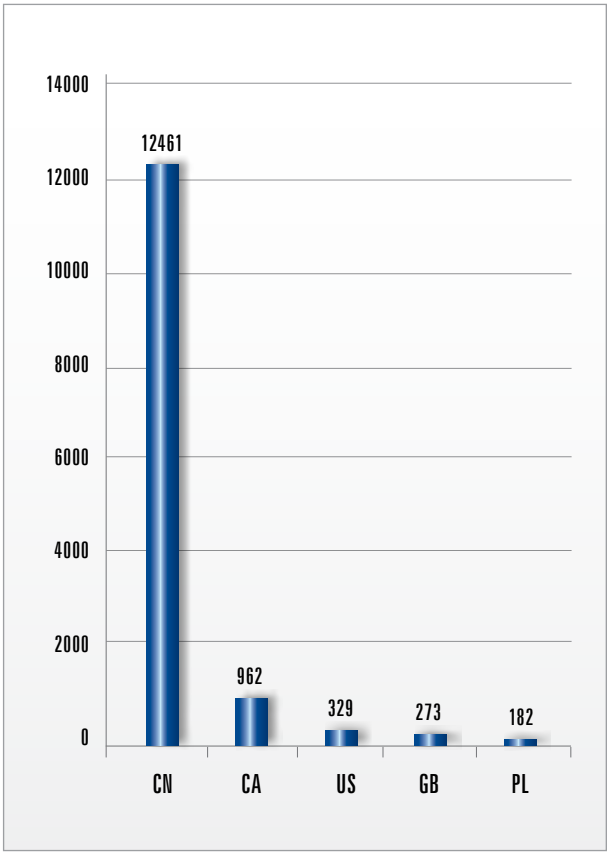
W charakterystyce ruchu można zauważyć, że ciąg `0000000000000000000000000A0027D78` występuje zawsze, tylko nieraz jest przesunięty do początku pakietu (na tyle, że pole „dane” jest puste, zawiera jedynie 4 bajty `A0027D78` lub ciąg zer jest krótszy niż 12 bajtów), ewentualnie przesunięcie ma miejsce w prawo (wtedy ciąg zer jest poprzedzony losowymi bajtami). Losowe bajty wpływają na zniekształcenie nagłówka TCP, w tym nietypowe ustawienie flag. Rysunek 3.2.3. prezentuje przykład pakietu, którego ciąg przesunięty jest w sposób zniekształcający pole „opcje” (zaznaczone) oraz flagi nagłówka TCP.



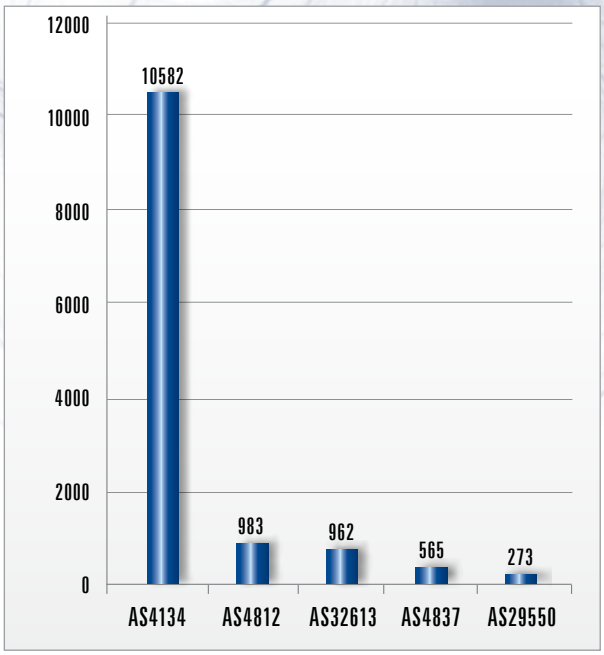
Rysunek 3.2.3. Zniekształcony pakiet kierowany na 0/TCP

Może to oznaczać, że bajty powyżej nagłówka IP nie są protokołem TCP (pomimo tego, że w nagłówku IP w polu „protocol" ustawiona jest wartość 0x06). Jeżeli tak, to albo ktoś testował jakiś swój protokół warstwy czwartej, albo testowane były zachowania różnych stosów TCP/IP na zniekształcone w odpowiedni sposób dane.

Źródłem skanowań w 84% były adresy należące do chińskich ISP (głównie pochodzące z jednego systemu autonomicznego AS4134). Na drugim miejscu pojawiła się Kanada (6%), a na trzecim USA (2%). Należy jednak zaznaczyć, że źródłowe adresy IP mogą być zespoofowane. Próby nawiązania połączenia TCP na port 0 zazwyczaj nie powinny spotkać się z odpowiedzią (tak też było w przypadku naszych honeypotów). Jeżeli osoby odpowiedzialne za wytworzenie takiego ruchu do Internetu wiedziały o tym, to nie oczekiwały żadnych pakietów zwrotnych od docelowego adresu IP, więc adres źródłowy mógł zostać sfałszowany. Wykres 3.2.4. przedstawia statystyki związane ze źródłami anomalnego ruchu.



Wykres 3.2.4. Liczba pakietów per kraj (ruch na port 0/TCP)



Wykres 3.2.5. Liczba pakietów per ASN (ruch na portach TCP)

Poniżej przedstawiamy regułę dla systemu Snort dopasowującą charakterystyczny ciąg bajtów. Ponieważ opisany ruch jest mocno osobliwy, nie wykluczamy, że może się także pojawić na innych portach. Dlatego przedstawiamy postać najbardziej ogólną:

```
alert tcp any any -> any any
msg:"Suspicious 0/TCP payload";
content:"|a0 02 7d 78|"; sid: 120003;
rev: 1;)
```

Wykres 3.2.6. Reguła Snort opisująca anormalny ruch na 0/TCP

Podsumowanie

Nie mamy pewności co do przyczyny ani celu generowania anomalnego ruchu na port 0/TCP. Z jednej strony mogła być to zwykła pomyłka, błąd lub jakaś forma projektu badawczego, a z drugiej mogły być to testy zachowania stosów TCP/IP na zniekształcone pakiety TCP. Ponieważ honeypoty, jak i większość standardowych usług bądź systemów, nie generują odpowiedzi na tego typu ruch, nie wiadomo czy źródłowe adresy IP nie były sfałszowane (brak jakiejkolwiek interakcji). Obecnie ruch na porcie 0/TCP jest znikomy i nie wyróżnia się z tzw. „szumu tła".

Kontakt

Adres:	NASK / CERT Polska
	ul. Wąwozowa 18
	02-796 Warszawa
tel.:	+48 22 3808 274
fax:	+48 22 3808 399

Zgłaszanie incydentów:	cert@cert.pl
Zgłaszanie spamu:	spam@cert.pl
Informacja:	info@cert.pl
Klucz PGP:	http://www.trusted-introducer.org/teams/0x553FEB09.asc
Strona WWW:	http://www.cert.pl/
	http://facebook.com/CERT.Polska
RSS Feed:	http://www.cert.pl/rss
Twitter:	@CERT_Polska http://twitter.com/CERT_Polska
	@CERT_Polska_en http://twitter.com/CERT_Polska_en