Zespół CERT Polska działa w ramach Naukowej i Akademickiej Sieci Komputerowej

RAPORT CERT Polska

za pierwsze półrocze **2011**

Analiza incydentów naruszających bezpieczeństwo teleinformatyczne

CERT POLSKA NASK

Statystyka zgłoszeń koordynowanych przez CERT Polska

Jak czytać ten dokument?

Niniejszy raport przedstawia wybrane statystyki z danych zebranych przez zespół CERT Polska w pierwszej połowie 2011 r. wraz z omówieniem i wnioskami. Jest to nasz pierwszy raport półroczny – dotychczas publikowaliśmy jedynie roczne analizy tego rodzaju. Dzięki raportowi czytelnicy mogą uzyskać bardziej aktualny obraz bezpieczeństwa w cyberprzestrzeni.

Główną treść niniejszego opracowania stanowią informacje na temat zagrożeń w polskich sieciach, przekazywane zespołowi CERT Polska przez różne podmioty związane z monitorowaniem i reagowaniem na zagrożenia. Ponieważ uwzględniają one wszystkich polskich operatorów, dają bardzo szeroki obraz tego, co naprawdę dzieje się w „polskim" Internecie. W raporcie porównujemy nasze obserwacje z tymi, których dokonaliśmy w raporcie za rok 2010.

Najważniejsze obserwacje podsumowujące raport

- Pomimo coraz większej liczby zautomatyzowanych źródeł informacji, otrzymaliśmy prawie o połowę mniej zgłoszeń dotyczących Polski niż się spodziewaliśmy.
- 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 zawarte w sms–ach m.in. te zawierające kody autoryzacji transakcji. Był to drugi, w pełni udokumentowany przypadek na świecie.
- W kwietniu nastąpił atak ukierunkowany na polskich 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 2011r. doszło do wielu poważnych 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 przypisawana jest grupom Anonymous oraz LulzSec.
- Choć hostownie w Polsce są w zdecydowanie większym stopniu dotknięte problemem phishingu, aniżeli dostawcy Internetu, to zdecydowanie skuteczniej sobie z nim radzą.

Streszczenie

Najważniejsze wnioski podsumowujące raport

- W Polsce częściej niż w co piątym przypadku (21%) domena, w której umieszczono phishing należała do sklepu internetowego. W polskich sieciach znajdowało się około 2% stron związanych ze złośliwym oprogramowaniem zauważonych na całym świecie. Procentowo jest to wzrost w stosunku do roku 2010 (1.4%).
- Wśród polskich operatorów, u których najczęściej umieszczane są złośliwe strony WWW dominują - co zaskakujące - najwięksi dostawcy internetu, a nie hostownie jak w roku ubiegłym.
- Wyodrębniliśmy 1 033 681 unikalnych incydentów dotyczących rozsyłania spamu z polskich sieci. Ponad połowa z nich (573 721) dotyczyła sieci Netii.
- W sieciach Telekomunikacji Polskiej zanotowaliśmy zaledwie 151 502 incydentów dotyczących spamu. Tak niski udział utrzymuje się od końca 2009 roku, kiedy to TP wdrożyła filtrowanie portu 25/TCP.
- Port 445/TCP był najczęstszym celem skanowań w polskich sieciach. Były one przeważnie związane z próbą wykorzystania luki związanej z błędem w obsłudze zapytań RPC - opisanej w biuletynie bezpieczeństwa Microsoft numer MS08-067.
- Lista dziesięciu najbardziej zainfekowanych sieci w Polsce odzwierciedla w dużej mierze wielkość operatorów pod względem użytkowników.
- W pierwszej połowie 2011 roku zauważyliśmy ponad 1 mln botów w polskich sieciach.
- Najczęściej występujące boty to Torpig oraz Rustock. Ich liczebność była co najmniej trzy razy wyższa niż pozostałych.
- Najwięcej botów zauważono w AS 5617 należącym do TP (blisko 560 tys.).
- Duża liczba botów w sieciach TP oraz mała liczba rozsyłanego spamu dobitnie wskazuje skuteczność blokowania portu 25/TCP i może być rekomendacją dla reszty ISP.
- Wzrost zgłoszeń sandboxowych wynika z aktywności trojana Sality, który wykorzystywał domeny Interii w celach zarządzania botnetem.
- Nie odnotowaliśmy żadnych ataków typu APT (Advanced Persistent Threat) skierowanych na podmioty w Polsce.
- Stany Zjednoczone i Kanada jeszcze wyraźniej niż w 2010 r. dominują wśród krajów, w których odnotowano phishing. Łącznie generowały one 60% zgłoszeń.
- Nastąpił wzrost udziału Chin w statystykach państw, w których zlokalizowane są złośliwe adresy URL. Procentowo mniej złośliwych adresów URL w stosunku do ubiegłego roku mają USA, które jednak pozostają liderem. W tych dwóch państwach znajduje się ponad 50% zgłaszanych do nas złośliwych stron WWW.
- W USA oraz Niemczech znajduje się prawie 50% kontrolerów C&C.

Informacje o zespole CERT Polska

CERT Polska (Computer Emergency Response Team Polska – http://www.cert.pl/) jest zespołem działającym w ramach Naukowej i Akademickiej Sieci Komputerowej (http://www.nask.pl/), zajmującym się reagowaniem na zdarzenia naruszające bezpieczeństwo w Internecie. CERT Polska działa od 1996 roku, a od 1997 jest członkiem FIRST (Forum of Incidents Response and Security Teams - http://www.first.org/) – największej na świecie organizacji zrzeszającej zespoły reagujące i zespoły bezpieczeństwa z całego świata. Od roku 2000 jest także członkiem inicjatywy zrzeszającej europejskie zespoły reagujące – TERENA TF-CSIRT (http://www.terena.nl/tech/task-forces/tf-csirt/) i działającej przy tej inicjatywie organizacji Trusted Introducer[1] (http://www.ti.terena.nl/). W ramach tych organizacji współpracuje z podobnymi zespołami na całym świecie, zarówno w działalności operacyjnej, jak też badawczo–wdrożeniowej.

Do głównych zadań zespołu CERT Polska należy:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci;
- alarmowanie użytkowników o wystąpieniu bezpośrednich dla nich zagrożeń;
- współpraca z innymi zespołami IRT (Incidents Response Team) – m.in. w ramach FIRST i TERENA TF-CSIRT;
- prowadzenie działań informacyjno-edukacyjnych, zmierzających do wzrostu świadomości na temat bezpieczeństwa teleinformatycznego (zamieszczanie aktualnych informacji na stronie http://www.cert.pl/, organizacja cyklicznej konferencji SECURE);
- prowadzenie badań i przygotowanie raportów dotyczących bezpieczeństwa polskich zasobów Internetu;
- niezależne testowanie produktów i rozwiązań z dziedziny bezpieczeństwa teleinformatycznego;
- prace w dziedzinie tworzenia wzorców obsługi i rejestracji incydentów, a także klasyfikacji i tworzenia statystyk;
- udział w krajowych i międzynarodowych projektach związanych z tematyką bezpieczeństwa teleinformatycznego.

[1] *Od 2001 r. zespół CERT Polska posiada najwyższy poziom zaufania Trusted Introducer Accredited Team.*

Wprowadzenie

Raport ten jest naszym pierwszym raportem półrocznym. Zdecydowaliśmy się na jego publikację, ponieważ uważamy, że dzięki niemu możliwe będzie lepsze zrozumienie tego, co dzieje się w kwestiach związanych z bezpieczeństwem w Internecie. Czytelnicy raportu będą bowiem dysponować bardziej aktualnymi danymi i analizami.

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 zespołu.Przede wszystkim takie zgłoszenia są przez nas rejestrowane, obsługiwane i wykazywane w statystykach. Otrzymujemy natomiast bardzo duże ilości danych dotyczących polskich sieci, pochodzące głównie z systemów automatycznych 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 abuse 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 „polskim" Internecie. Formuła jest zbliżona do naszego rocznego raportu za rok2010. Pozwala to na dokonywanie porównań i wychwycenie trendów w atakach. W odróżnieniu od naszych raportów rocznych skupiamy się przede wszystkim na danych otrzymywanych automatycznie („koordynowanych"). Zgłoszenia obsługiwane „ręcznie" będą podsumowane w raporcie za rok 2011.

Ilość informacji we wszystkich kategoriach

W pierwszym półroczu 2011 r. otrzymaliśmy 3 906 411 zgłoszeń pochodzących z systemów automatycznych. Przeważająca większość dotyczyła rozsyłania spamu i innej działalności botnetów. Rozkład pozostałych kategorii, które wyróżniliśmy w raporcie, przedstawia wykres na sąsiedniej stronie (zwracamy uwagę na skalę logarytmiczną!).

Dane pochodzą z wielu źródeł o bardzo zróżnicowanym charakterze. Dlatego sposoby ich zbierania i prezentacji znacznie różnią się między sobą. Tak jak w 2010 roku, zgłoszenia zostały pogrupowane na 10 kategorii, naszym zdaniem najlepiej opisujących ich wspólne cechy: spam, botnety, skanowanie, złośliwe adresy URL, serwery C&C, dane z sandboxów, phishing, fast flux, DDoS i pozostałe. Kategorie te są omówione poniżej.

Porównując powyższe dane z danymi z 2010 roku można zaobserwować spadek liczby zgłoszeń, pomimo faktu, że dysponujemy coraz większą liczbą źródeł informacji. Największy spadek odnotowaliśmy w kategorii botnetów – na podstawie danych z 2010 roku oczekiwalibyśmy co najmniej dwa razy więcej zgłoszeń. Otrzymaliśmy również prawie o połowę mniej zgłoszeń niż byśmy oczekiwali w kategoriach:

Statystyka zgłoszeń koordynowanych przez CERT Polska

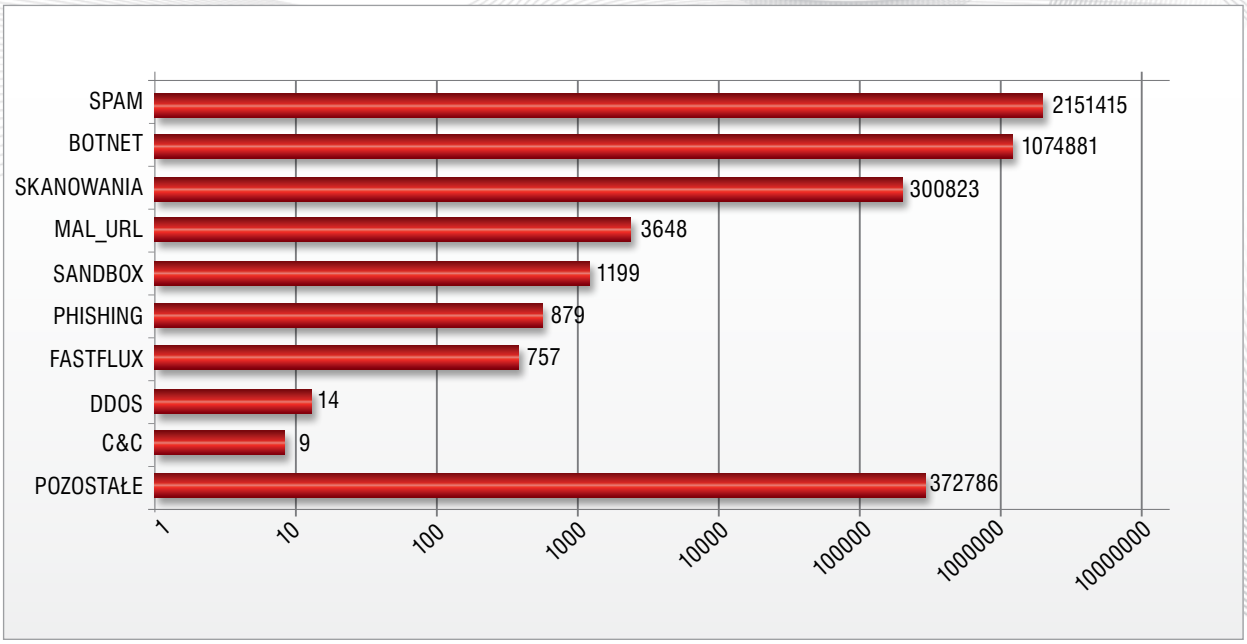


Tabela 1. Liczba zgłoszeń automatycznych w poszczególnych kategoriach

spam, phishing, złośliwe URL (mal_url), fastflux i serwerów C&C, zaś nieco więcej w kategoriach sandbox, ddos i skanowaniach.

„Tradycyjny" phishing

W tej kategorii zdarzeń nie zaszły znaczące zmiany względem tego, co działo się w roku 2010. Pozycja Polski na tle innych krajów niemal nie uległa zmianie. Choć o jedno miejsce pogorszyliśmy swoją pozycję w tabeli, Polska poprawiła swoje wyniki zarówno w liczbach bezwzględnych jak i w udziale procentowym wszystkich obserwacji phishingu, które zostały zaobserwowane w naszych źródłach. W pierwszej połowie 2011 roku mieliśmy 879 zgłoszeń phishingu w Polsce w porównaniu do 2 222 w całym ubiegłym roku. Stany Zjednoczone i Kanada jeszcze wyraźniej niż w 2010 r. dominują wśród krajów, w których znajdowano phishing. Łącznie w pierwszych sześciu miesiącach tego roku blisko 60% zgłoszeń dotyczyło właśnie tych dwóch krajów. W ubiegłym roku było to 53%. Porównanie liczby zgłoszonych przypadków phishingu w Polsce na tle innych krajów od stycznia do czerwca 2011 r. zawiera tabela 2.

1	US	91111	50,1%
2	CA	15567	8,6%
3	DE	9197	5,1%
4	GB	8703	4,8%
5	CL	7095	3,9%
6	RU	4813	2,6%
7	HK	4775	2,6%
8	FR	4311	2,4%
9	CZ	3925	2,2%
10	NL	3365	1,8%
20	PL	879	0,5%

Tabela 2. Liczba zgłoszonych przypadków phishingu według lokalizacji geograficznej

Statystyka zgłoszeń koordynowanych przez CERT Polska

Nie zmienił się także rozkład operatorów, u których najczęściej znajdowano phishing. Podobnie jak w ubiegłym roku, najczęściej problem dotyczył firm specjalizujących się w hostingu.

Powyższe dane mówią o liczbie zgłoszeń przypadków phishingu. Dotyczyły one 507 unikalnych adresów URL. Postanowiliśmy przyjrzeć się bliżej temu, jak wiele zgłoszeń dotyczy tych samych adresów URL. Biorąc pod uwagę, że najczęściej te same źródła raportują dany adres URL periodycznie, dopóki nie zostanie on „oczyszczony", jest to wyznacznik tego, jak długo dana strona phishingowa jest utrzymywana przed usunięciem. Średnio otrzymywaliśmy 1,72 zgłoszenia w przeliczeniu na adres URL. W najgorszych przypadkach jednego adresu URL dotyczyło aż 6 zgłoszeń. Przeprowadziliśmy porównanie tego wskaźnika pomiędzy operatorami, ograniczając je do tych, u których odnaleziono w ciągu półrocza więcej niż 5 adresów URL zawierających phishing. Wniosek, który nasuwa się z analizy tabeli 4 jest taki, że choć hostownie są w zdecydowanie większym stopniu dotknięte problemem phishingu, jednocześnie zdecydowanie skuteczniej sobie z nim radzą.

Średnia liczba zgłoszeń / URL	Liczba adresów URL	ASN
2,94	16	31242 (TKP)
2,83	6	6714 (GTS)
2,67	12	41508 (IWACOM)
2,50	20	49102 (CONNECTED)
2,38	8	29314 (VECTRA)
2,32	19	21021 (MULTIMEDIA)
2,03	36	5617 (TP)
1,85	26	29522 (KEI)
1,78	23	16265 (LEASEWEB)
1,63	8	12968 (CROWLEY DATA POLAND)
1,42	110	15967 (NETART)
1,40	10	43470 (NETWORK COMMUNICATION)
1,33	9	47544 (IQ PL)
1,33	61	12824 (HOME.PL)
1,25	12	44514 (INOTEL)
1,18	11	41079 (SUPERHOST.PL)
1,13	15	16138 (INTERIA)
1,00	15	9085 (SUPERMEDIA)

Tabela 4. Liczba zgłoszeń/URL według systemów autonomicznych

156	15967 (NETART)
81	12824 (HOME.PL)
73	5617 (TP)
50	49102 (CONNECTED)
48	29522 (KEI)

Tabela 3. Liczba przypadków phishingu w Polsce według systemów autonomicznych

Strony phishingowe umieszczone były w 346 różnych domenach. Ponownie jak w roku ubiegłym, oszacowaliśmy metody, z których skorzystali przestępcy. Nadal ogromna większość stron zostaje umieszczona w wyniku włamania. Tak było w przypadku 228 (65,9%) domen. Aż 55 (15,9%) domen zostało jednak zarejestrowanych w serwisach oferujących bezpłatną rejestrację poddomen, np.: www.paypal.de.blo.pl. Częściej niż w co piątym przypadku (73; 21%) domena, w której umieszczono phishing należała do sklepu internetowego.

Wśród najczęściej podrabianych stron nadal króluje PayPal (85 adresów URL), lecz coraz częściej pojawia się także Western Union (9 adresów) czy Amazon (6 adresów). Banki pojawiły się w sumie w 24 przypadkach.

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:

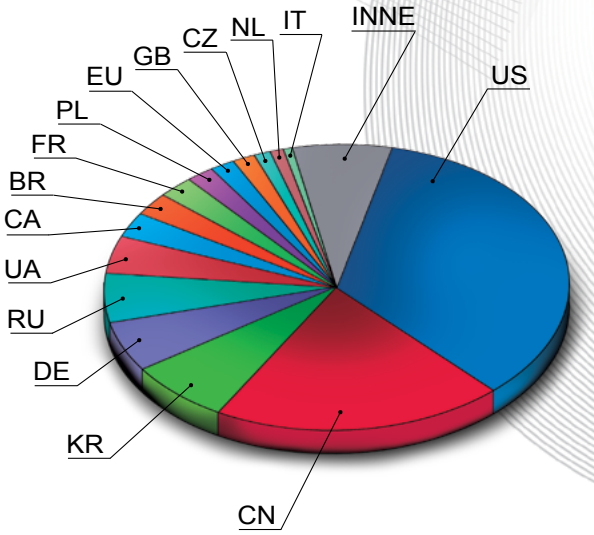
- kod służący przełamaniu zabezpieczeń przeglądarki lub jednego z jej rozszerzeń,
- plik wykonywalny (w tym pobierany w wyniku działania powyższego kodu) ,
- pliki konfiguracyjne służące do sterowania uruchomionym w systemie złośliwym oprogramowaniem.

Zgłoszenia nie dotyczą phishingu, który jest rozpatrywany w innej kategorii, tak jak w raporcie za rok ubiegły.

W tym półroczu trafiło do nas mniej zgłoszeń dotyczących złośliwych stron (liczonych jako unikalne kombinacje – dzień zgłoszenia /IP/URL) niż się spodziewaliśmy. Bazując na statystykach z roku ubiegłego spodziewaliśmy się co najmniej dwukrotnie więcej zgłoszeń. Ponieważ statystyki tworzymy na podstawie zewnętrznych źródeł, trudno nam dokładnie określić przyczynę tego zjawiska.

Wpierwszej połowie 2011 r. trafiło do nas 3 648zgłoszeń dotyczących Polski (w całym zeszłym roku mieliśmy 12 917 zgłoszeń). Stanowiło to około 2% zgłoszeń dotyczących całego świata. Procentowo jest to wzrost w stosunku do danych z 2010 roku (wtedy było to 1.4% zgłoszeń z całego świata).

Co interesujące, o ile USA pozostają liderem (w ubiegłym roku aż 48,2% zgłoszeń), nastąpił znaczący spadek ich procentowego udziału, przede wszystkim na skutek znaczącego wzrostu Chin (w ubiegłym roku również drugie miejsce, ale zaledwie z 11,9% udziałem).



Wykres 1. Kraje, w których najczęściej znajdowały się złośliwe strony WWW (wg. liczby zgłoszeń)

1	US	61187	34%
2	CN	36134	20%
3	KR	12867	7%
4	DE	10127	6%
5	RU	10039	6%
6	UA	7501	4%
7	CA	5078	3%
8	BR	4567	3%
9	FR	4213	2%
10	**PL**	**3648**	**2%**
11	EU	2949	2%
12	GB	2875	2%
13	CZ	1991	1%
14	NL	1671	1%
15	IT	1148	1%

Tabela 5. Liczba przypadków złośliwego oprogramowania na stronach WWW według lokalizacji geograficznych

Statystyka zgłoszeń koordynowanych przez CERT Polska

Podobnie jak w ubiegłym roku, porównując między sobą poszczególne kraje, w których utrzymywane były pliki związane ze złośliwym oprogramowaniem, warto zwrócić uwagę na wysoką pozycję Chin, Rosji i Ukrainy. Zestawiając tabelę nr 6 z podobną tabelą dla phishingu widać, że pozycje tych krajów (w szczególności Chin) są istotnie wyższe w kategorii związanej ze złośliwym oprogramowaniem. Możliwą interpretacją jest to, że pliki ze złośliwym oprogramowaniem w tych krajach nie pojawiają się wyłącznie w wyniku ślepych na geografię 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 statystycznie nadzwyczaj wysokiej pozycji tych trzech krajów w tabeli.

Kiedy przyjrzeliśmy się bliżej wynikom dla Polski, okazały się one zaskakujące. W czołówce zestawienia dominują najwięksi ISP tacy jak Telekomunikacja Polska, Netia i ATM. Tymczasem spodziewaliśmy się zestawienia zbliżonego do zeszłego roku, w którym z kolei dominowali najwięksi dostawcy usług hostingowych – HOME.PL, Netart czy KEI. Także znacząco zmalała średnia liczba URL przypadająca na pojedynczy adres. Spadek ten może wynikać z faktu dominacji największych dostawców usług. Być może do hostowania złośliwych stron wykorzystywane są przejęte komputery użytkowników domowych. Ponieważ czas życia tych stron jest krótki, niewiele URL jest na nie przekierowywanych.

liczba zgłoszeń	system autonomiczny	operator	liczba Url/IP
986	5617	TP	3,5
415	6714	ATOM	6,9
344	12741	NETIA	5,1
257	12824	HOME.PL	2,7
231	15694	ATMAN	2,9

Tabela 6. Liczba przypadków złośliwego oprogramowania na polskich stronach WWW według systemów autonomicznych

Podsumowując, nie jesteśmy w stanie określić dlaczego nastąpiły zmiany w rankingu operatorów – czy są one spowodowane sposobem zbierania danych o złośliwych stronach przez nasze źródła, czy też wynikają z wprowadzenia lepszych polityk bezpieczeństwa u dostawców usług hostingowych, co z kolei zaowocowało zmianą strategii podziemia cyberprzestępczego.

Z piaskownicy do polskich sieci, czyli adresy odwiedzane przez malware

Ta kategoria informacji jest w zasadzie rozszerzeniem poprzedniej i uwzględniamy w niej adresy, które odwiedzane były przez złośliwe oprogramowanie zainstalowane w laboratoriach wewnątrz sandboxu, czyli w dużym skrócie specjalnie przygotowanego środowiska, służącego do kontrolowanego uruchamiania wszelakiej maści podejrzanego oprogramowania. Zaobserwowaliśmy 1199 unikalnych adresów WWW oraz ftp, do których łączyło się oprogramowanie uruchamiane w sandboxach. Jeżeli w przyszłym półroczu zanotujemy podobną skalę zjawiska, to należy się spodziewać ok. 25% wzrostu w porównaniu do roku 2010.

Do adresów tych łączyło się w sumie 1 302 (2 752 w całym 2010 roku) unikalnych plików. Około 25% (32% wroku 2010) z nich zostało rozpoznanych przez programy antywirusowe jako złośliwe oprogramowanie (na podstawie Cymru Malware Hash Registry – http://www.team-cymru.org/Services/MHR/).

Statystyka zgłoszeń koordynowanych przez CERT Polska

Najczęściej obserwowaliśmy połączenia do serwera o adresie IP 212.33.79.77. Wyodrębniliśmy aż 275 unikalnych zapytań. To o ponad 40 więcej niż w najliczniejszym przypadku z 2010 roku. Odpowiedzialny za to jestkoń trojański, który po zainstalowaniu w systemie ofiary łączył się do centrum zarządzającego. Żaden z dostawców oprogramowania antywirusowego nie przydzielił mu indywidualnej nazwy.

Bardzo ciekawa sytuacja dotyczy adresów w domenie interia.pl: pelcpawel.fm.interia.pl, radson_master.fm.interia.pl, aanna74.eu.interia.pl oraz mattfoll.eu.interia.pl. We wszystkich przypadkach winowajcą był koń trojański o nazwie Sality. Tak jak w powyższym 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 poprzednim roku, mieliśmy do czynienia z połączeniami inicjującymi do sieci gadu-gadu. 23% łączących się plików zostało rozpoznanych jako złośliwe oprogramowanie.

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 sandboxie.

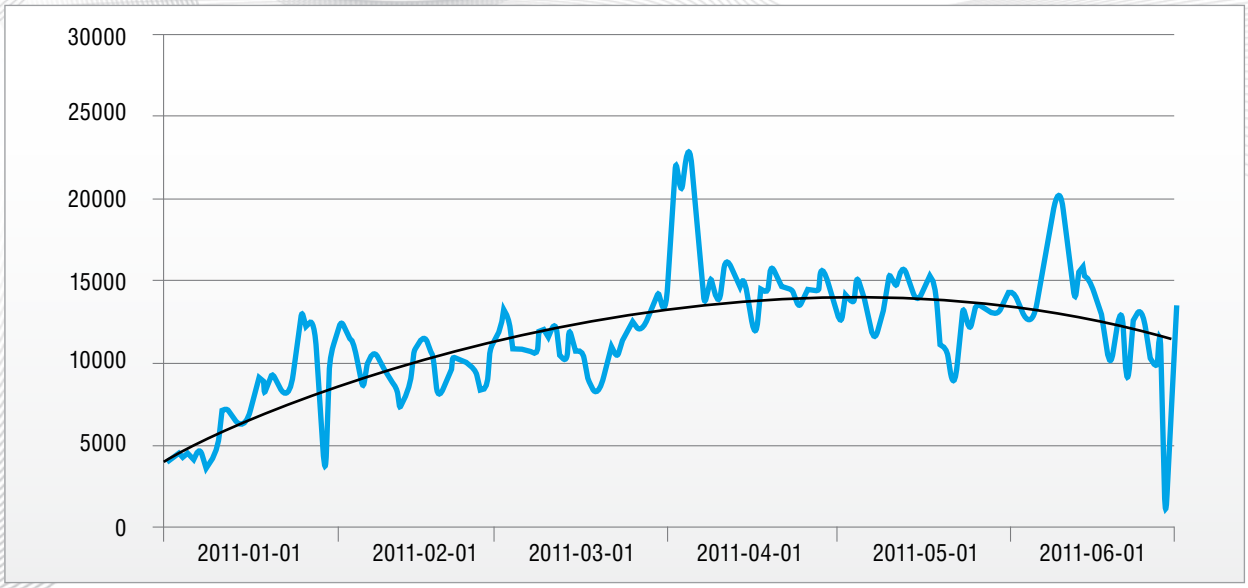
1	212.33.79.77	275
2	pelcpawel.fm.interia.pl	85
3	radson_master.fm.interia.pl	50
4	webpark.pl	46
5	footballteam.pl	38
6	aanna74.eu.interia.pl	30
7	appmsg.gadu-gadu.pl	30
8	www.odlotek.ugu.pl	26
9	s1.footballteam.pl	25
10	hit.stat24.com	22
11	ftp.webpark.pl	18
12	uaneskeylogger.hdo01.pdg.pl	**18**
13	mattfoll.eu.interia.pl	17
14	kluczewsko.gmina.pl	16
15	www.hotgame.za.pl	16

Tabela 7. Liczba unikalnych adresów w poszczególnych domenach

Spam z polskich sieci

W pierwszej połowie 2011 r. otrzymaliśmy 2 151 415 informacji o hostach wysyłających spam z polskich sieci. Uznając wszystkie zgłoszenia dotyczące jednego adresu IP, pomiędzy którymi nie wystąpiła przerwa dłuższa niż 3 dni za jeden incydent, wyodrębniliśmy 1 033 681 takich incydentów. Ponad połowa z nich (573 721) dotyczy sieci Netii. Dla porównania, z Telekomunikacji Polskiej, która wprowadziła filtrowanie portu 25 tcp dla swoich klientów pod koniec 2009 roku, pochodziło jedynie 151 502 incydentów, niemal tyle samo, co z sieci Plus (138 591 incydentów).

Pierwszy kwartał 2011 r. przyniósł wzrost liczby przypadków wysyłania spamu z Polski. Na przełomie kwietnia i maja liczba ta powróciła do poziomu zbliżonego do połowy 2010 r. Od tego czasu obserwujemy lekki spadek.



Wykres 2. Liczba informacji o hostach rozsyłających spam z polskich sieci

Skanowanie

Tak jak w latach ubiegłych, jedną z głównych kategorii zgłoszeń w pierwszej połowie 2011 rokupozostaje skanowanie. Skanowanie zazwyczaj jest związane z aktywnością botnetów lub robaków, czasami też z dedykowanymi narzędziami służącymi do mapowania sieci.Skanowanie od wielu lat wpisuje się w szum internetowy co sprawia, że często jest ignorowane przez wielu użytkowników, a nawet przez dedykowane zespoły bezpieczeństwa. Wiele organizacji wykrywa i przetwarza informacje o skanowaniach w sposób w pełni zautomatyzowany. Jeżeli zgłoszenie jest dokładniej przeanalizowane, może być powiązane z aktywnością konkretnego botnetu i robaka, i jest jako takie do nas przekazywane – takie zgłoszenia nie są rozpatrywane w tej kategorii.

W tym raporcie przeanalizujemy zgłaszane automatycznie do nas skanowania pod kątem najczęściej atakowanych portów TCP/UDP (a więc tak naprawdę aplikacji na nich nasłuchujących) oraz pod kątem najbardziej zainfekowanych sieci w Polsce. Rozpatrzymy przypadki skanowania w kategorii unikalnych źródłowych IP, które były rejestrowane przez systemy zgłaszające w pierwszym półroczu 2011 r. (globalnie lub per port docelowy) a także licząc unikalne kombinacje IP/port docelowy skanowań widzianych w danym dniu. Pierwsza kategoria umożliwi orientację co do skali ilości zainfekowanych komputerów, druga z kolei zilustruje, z jakich sieci ta aktywność jest najbardziej agresywna.

Najczęściej skanowane usługi

Podobnie jak w całym 2010 roku, w pierwszej połowie 2011 widzimy wyraźnie dominujący port 445, który jest w chwili obecnej najczęściej atakowanym portem. Nie jest to zaskoczeniem - większość najpoważniejszych luk związanych z oprogramowaniem Microsoftu znajduje się w aplikacjach nasłuchujących na tym porcie (obecnie najczęściej jest wykorzystywana luka związana z błędem w obsłudze zapytań RPC - opisana w biuletynie bezpieczeństwa Microsoft numer MS08-067).

Lp.	Liczba widzialnych unikalnych IP	Port docelowy /protokół	Prawdopodobny wiodący mechanizm ataków
1	143009	445/TCP	Ataki typu buffer overflow na usługi Windows RPC
2	774	139/TCP	Ataki związane z usługą współdzielenie plików/drukarek Windows
3	752	1433/TCP	Ataki słownikowe na MS SQL
4	648	135/TCP	Ataki na usługę Microsoft Endpoint Mapper
5	645	80/TCP	Ataki związane z aplikacjami webowymi
6	341	25/TCP	Prawdopodobnie próby rozsyłania spamu
7	268	4899/TCP	Ataki na aplikację do zdalnego zarządzania, radmin
8	245	5900/TCP	Ataki na VNC
9	165	23/TCP	Ataki słownikowe na usługę telnet
10	152	9988/TCP	Część innego ataku (ładowanie robaka przez zbindowany port)

Tabela 8. TOP 10 portów docelowych pod kątem unikalnych źródłowych skanujących IP

W porównaniu do 2010 roku, zaobserwowano mniej hostów skanujących port 22/TCP (usługę SSH, na którą często przeprowadzano ataki słownikowe). Z listy TOP 10 wypadł też port 5060/TCP (protokół SIP). Z kolei pojawił się port 135/TCP (Microsoft RPC Endpoint Mapper), oraz port 25/TCP związany z usługą SMTP (pocztą elektroniczną).

Najbardziej zainfekowane sieci w Polsce

Innym ciekawym zestawieniem wydaje się być rozkład zainfekowanych unikalnych IP od poszczególnych polskich operatorów. Uświadamia to skalę infekcji złośliwym oprogramowaniem w Polsce. Poniżej prezentujemy tabelę dziesięciu najbardziej zainfekowanych sieci w przeciągu minionej pierwszej połowy roku 2011.

Lp.	Liczba unikalnych IP	Numer systemu autonomicznego	Nazwa operatora
1	52834	5617	TP
2	27788	12741	NETIA
3	26340	15857	DIALOG
4	11691	43447	PTK CENTERTEL
5	11215	8374	PLUSNET
6	8876	21021	MULTIMEDIA
7	1950	25388	ASK-NET
8	1570	29314	VECTRA
9	1338	6714	ATOM
10	727	12912	PTC

Tabela 9. TOP 10 operatorów w Polsce pod względem liczby źródłowych skanujących IP

Statystyka zgłoszeń koordynowanych przez CERT Polska

Podobnie jak w zeszłym roku, uważamy, że ranking odzwierciedla w dużej mierze wielkość operatorów pod względem użytkowników – pozycja Telekomunikacji Polskiej nie jest więc zaskakująca. Ranking jest identyczny jak w ubiegłym roku, za wyjątkiem zmiany jednego operatora - z rankingu wypadło UPC (7. pozycja na liście z ubiegłego roku, w tym roku pozycja 12.), a na miejscu 10. tegorocznej listy zadebiutowało PTC.

Sporządziliśmy też ranking operatorów pod kątem częstości obserwowanych skanowań – w tym celu podsumowaliśmy sumę wszystkich źródłowych IP zgłaszanych do nas w paczkach dziennych (czyli IP, które są najczęściej do nas zgłaszane).

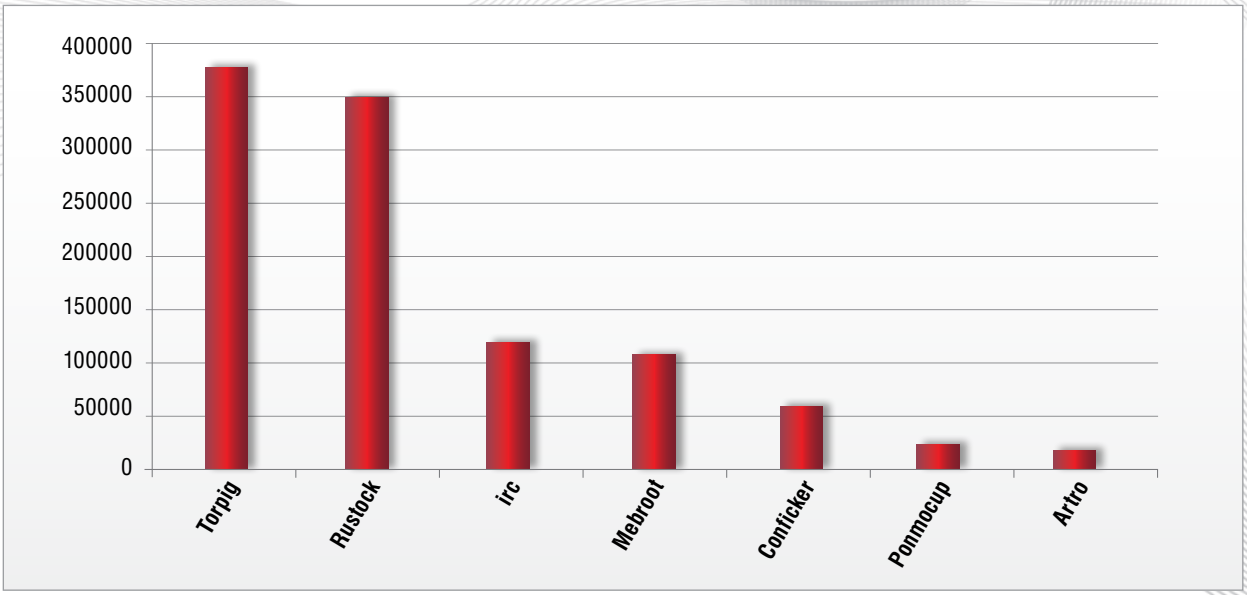
Suma wszystkich zgłaszanych IP/dzień	Numer systemu autonomicznego	Nazwa operatora
77287	5617	TP
36171	15857	DIALOG
32564	12741	NETIA
15691	29314	VECTRA
14041	21021	MULTIMEDIA
12553	43447	PTK CENTERTEL
11827	8374	PLUSNET
10220	25388	ASK-NET
9315	35191	ASTA-NET
9140	16265	LEASEWEB

Tabela 10. Ranking operatorów pod kątem częstości obserwowanych skanowań

Boty

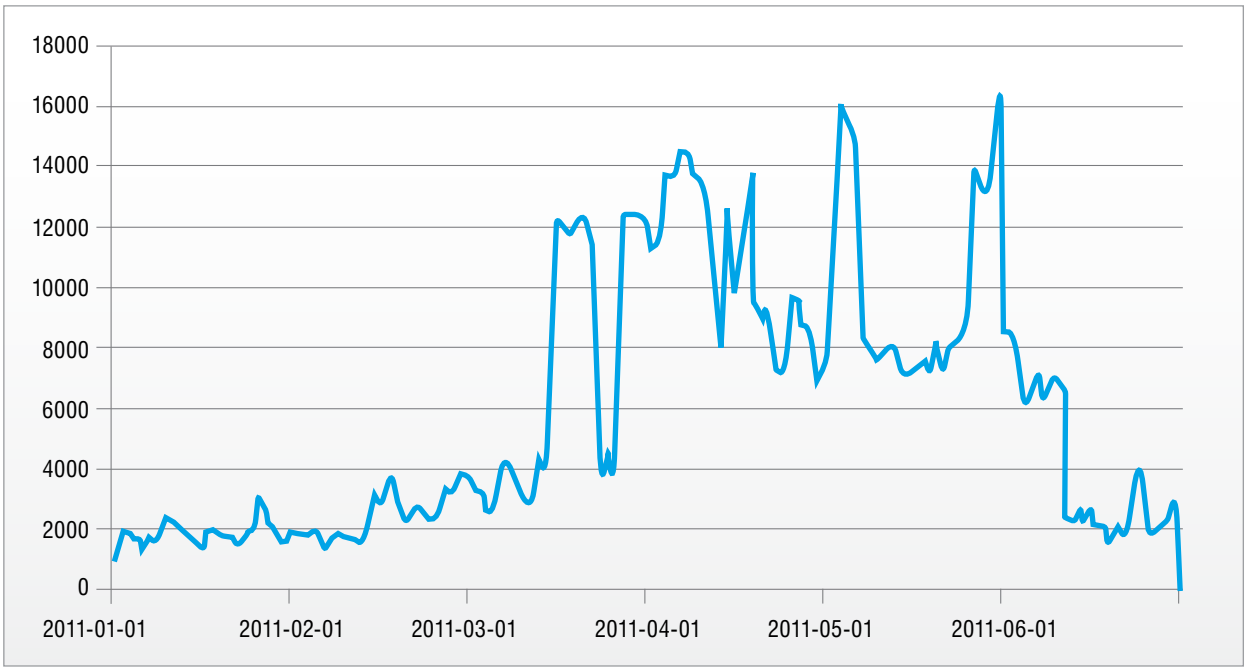
Kategoria ta uwzględnia komputery będące członkami botnetów znajdujące się w polskich sieciach, a nieuwzględnione w innych kategoriach. Choć najpopularniejszym zastosowaniem botnetów jest rozsyłanie spamu (patrz strona 11), mogą one być wykorzystane do dowolnych innych zastosowań, wymagających dużego pasma lub dużej mocy obliczeniowej, albo po prostu jako dodatkowa warstwa anonimizacji.

W pierwszej połowie 2011 roku zauważyliśmy ponad 1 mln botów. Bezsprzecznie dominowały dwa z nich: Torpig oraz Rustock. Ich liczebność była co najmniej trzy razy wyższa niż pozostałych. Zauważyliśmy prawie 380 tys. maszyn zainfekowanych Torpigiem oraz prawie 350 tys. Rustockiem. Poza nimi znaczący udział miały boty ircowe, mebroot oraz Conficker. W przypadku botów ircowych mamy do czynienia ze składową wielu odmian botów. Jedną wspólną wyróżniającą je cechą był kanał zarządzania, jakim był IRC. Na szczególną uwagę zasługuje mebroot, który jest wykorzystywany do wykradania danych klientów instytucji finansowych. Co prawda chociaż w większości przypadków poważne, dedykowane ataki są ukierunkowane na podmioty zagraniczne, to jednak istnieje duże prawdopodobieństwo trafienia do botnetu, którego celem jest polski użytkownik.

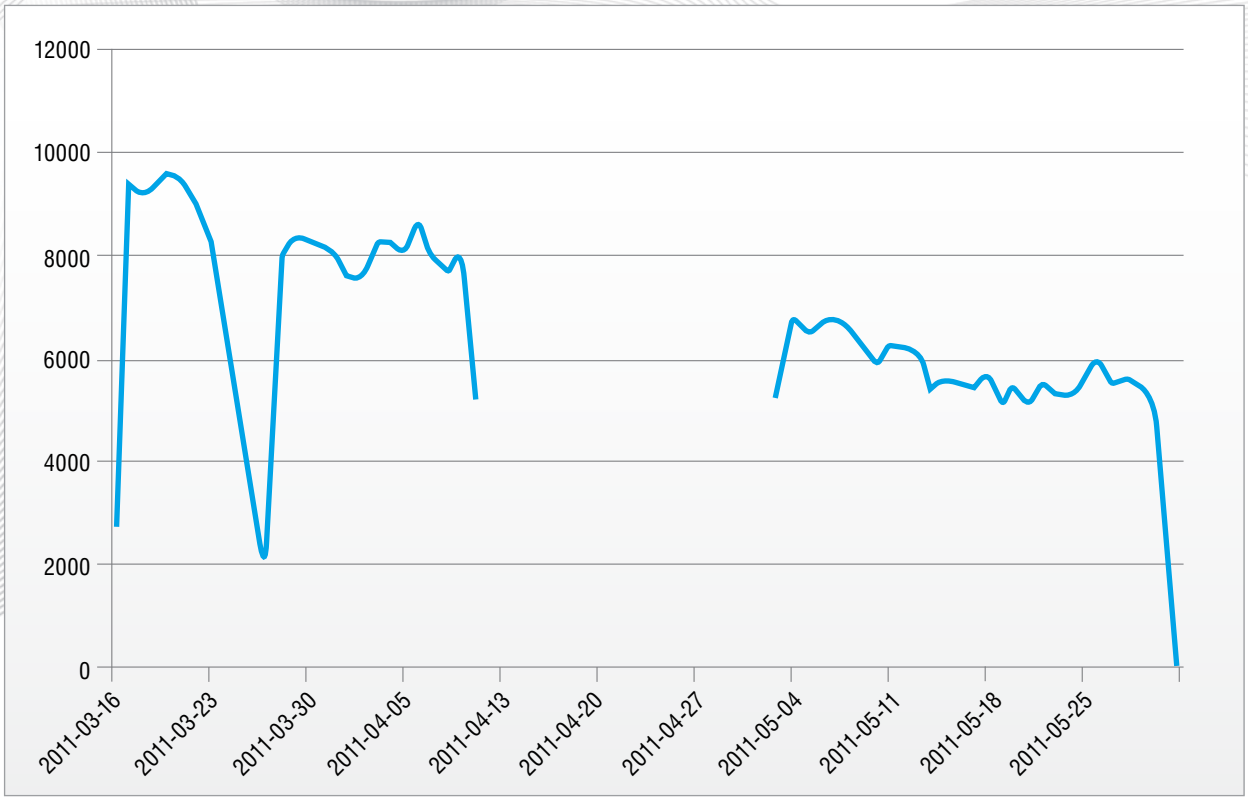


Wykres 3. Liczba botów według typów

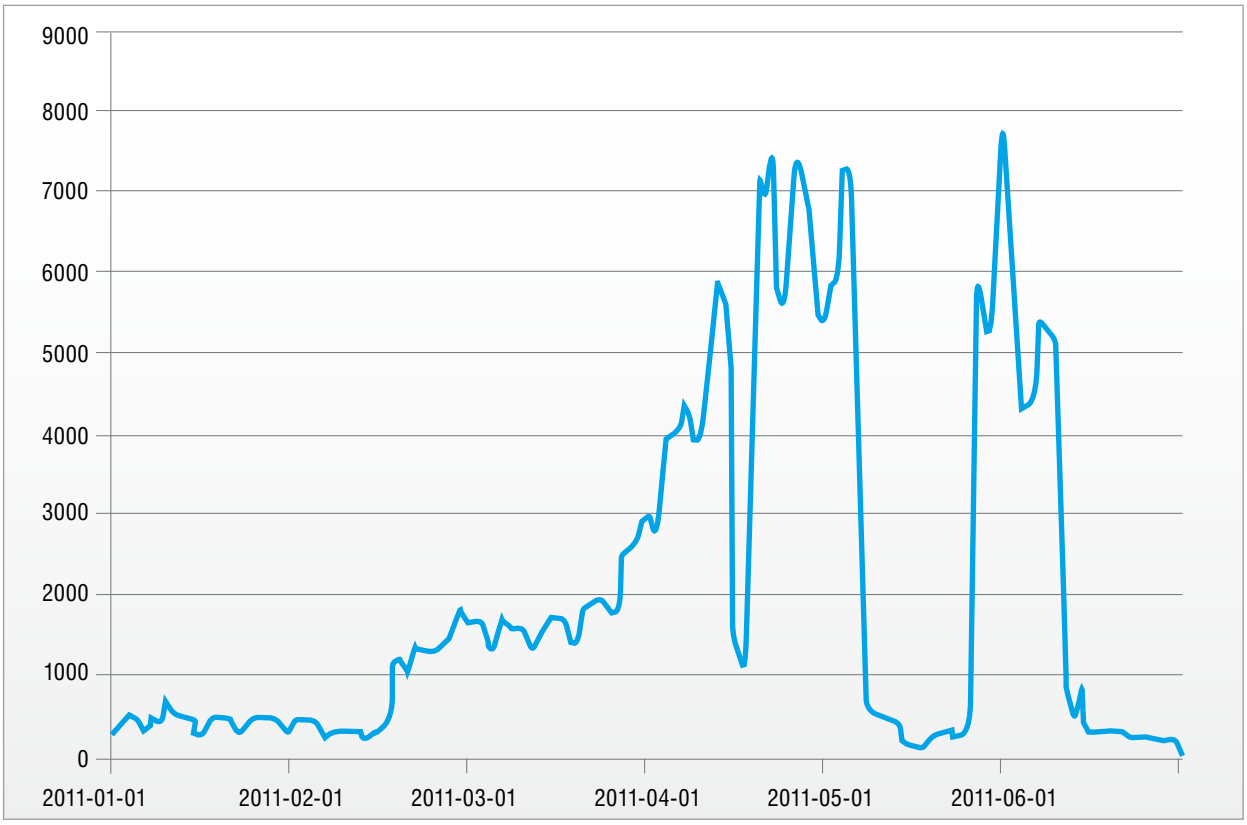
Dzienny rozkład botów w pierwszym półroczu 2011 roku (wyk. 3) utrzymywał się na poziomie pomiędzy dwoma a czterema tysiącami maszyn. W połowie marca wzrósł nagle do około 12 tys. Jest to związane z danymi dotyczącymi Rustocka, które zaczęliśmy otrzymywać począwszy od 16 marca (patrz wyk. 5).Na przełomie kwietnia i maja miało miejsce kolejne ważne wydarzenie, które spowodowało przekroczenie progu 14 tys. Było ono związane z działaniami grupy ekspertów z Uniwersytetu Kalifornijskiego w Santa Barbara, która dokonała udanej próby przejęcia botnetu Torpig. Od tego momentu rejestrowano ofiary, które łączyły się do przejętych serwerów. Jeszcze wyraźniej widać to na wykresie 6. przedstawiającym liczbę komputerów zainfekowanych Torpigiem. Kolejne maksima widoczne na przestrzeni maja i czerwca są spowodowane głównie sumaryczną działalnością obydwu botnetów.



Wykres 4. Dzienny rozkład botów w pierwszym półroczu 2011 roku

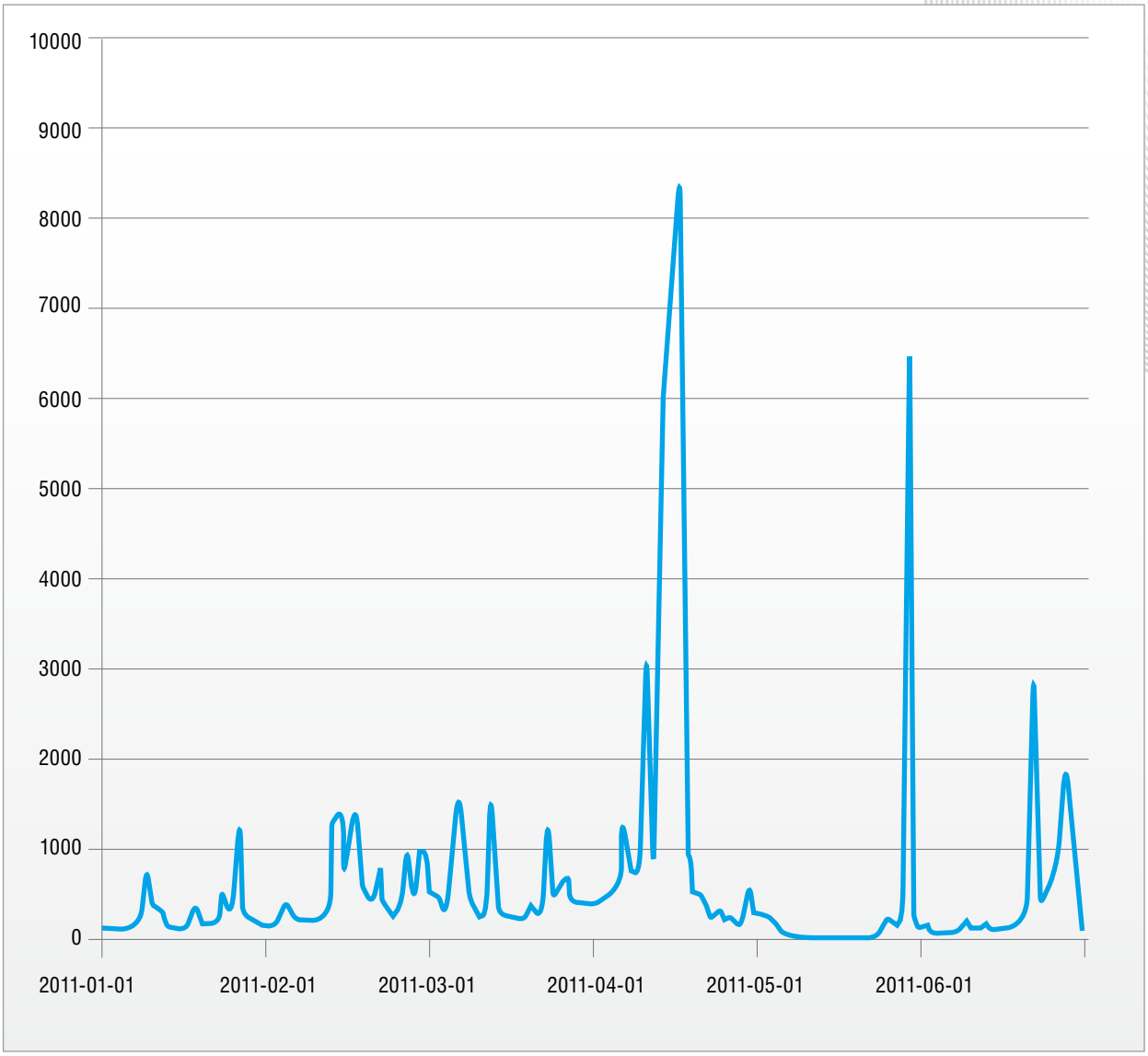


Wykres 5. Dzienny rozkład botnetu Rustock w pierwszym półroczu 2011 roku



Wykres 6. Dzienny rozkład botnetu Torpig w pierwszym półroczu 2011 roku

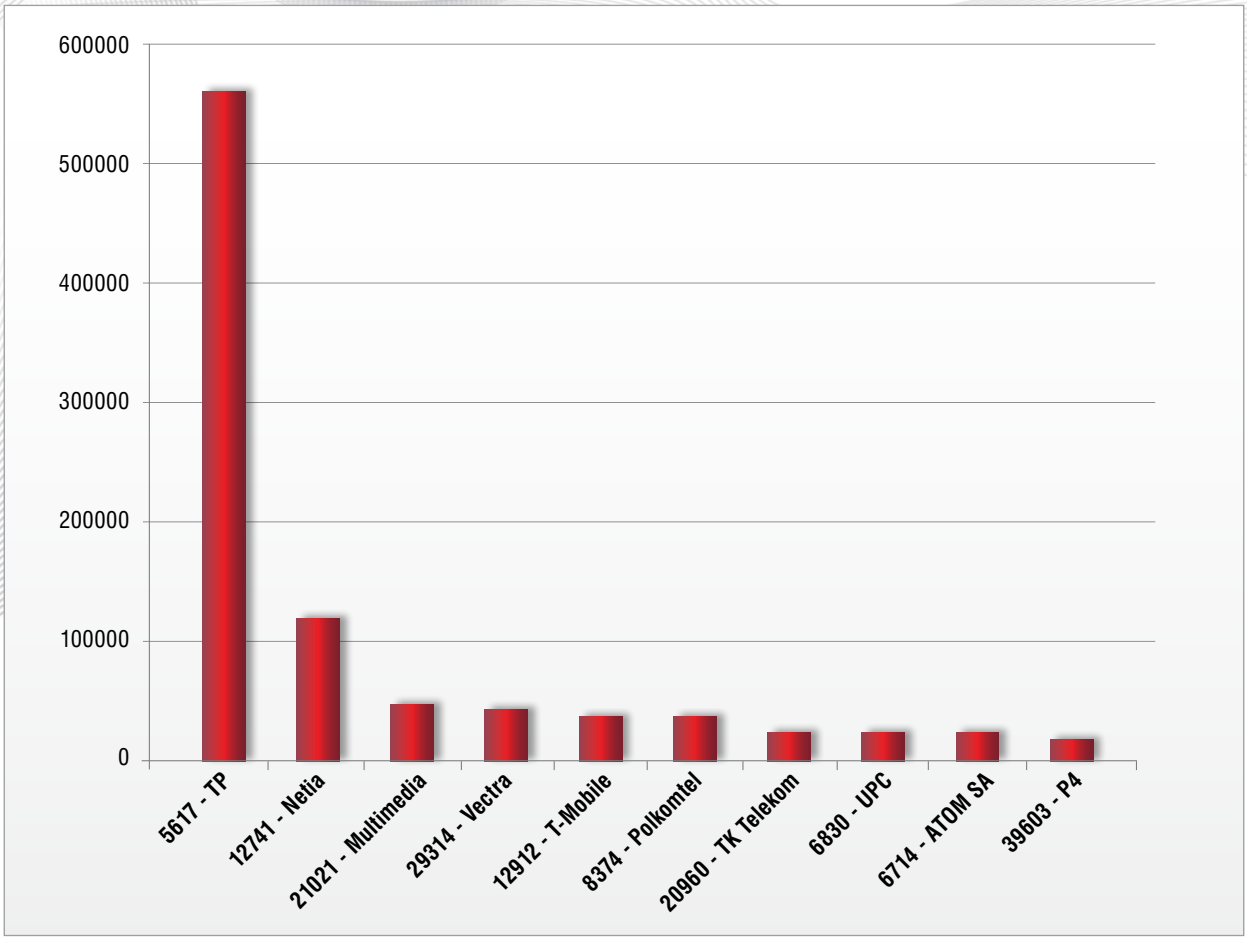
W przypadku botów ircowych notowaliśmy średnio 800 zainfekowanych maszyn dziennie. Jeśli chodzi o mebroota (wyk. 7.), to przez większość czasu zarażonych było od kilkuset do 1 500 maszyn w jednym dniu. Wyjątkiem są tutaj dwa zdarzenia. Pierwsze, mające miejsce pomiędzy 15 a 20 kwietnia (ponad 8 500 komputerów), drugie 31 maja (ponad 6 500 komputerów). W obydwu przypadkach miał prawdopodobnie miejsce atak ukierunkowany na polskich użytkowników lub instytucje finansowe.



Wykres 7. Dzienny rozkład botnetu Mebroot w pierwszym półroczu 2011 roku

Najwięcej botów zauważono w AS 5617 należącym do TP (wyk. 8.). Była to liczba bliska 560 tys. i aż czterokrotnie przewyższa liczbę botów w AS 12741 należącym do Netii (tutaj ok. 140 tys.). W sieciach kolejnych operatorów znajdowało się poniżej 50 tys. zainfekowanyh komputerów. Nie ulega wątpliwości, że najwięcej botów znajduje się w sieciach operatorów, którzy dostarczają internet odbiorcom indywidualnym. Są to duże telekomy takie jak TP czy Netia, dostawcy internetu w sieciach kablowych - Multimedia i Vectra oraz dostawcy internetu mobilnego – T-Mobile i Polkomtel. Ponad połowa wszystkich botów (ok. 55%) znajdowało się w sieci TP, zaś 15% w sieci Netii.

Statystyka zgłoszeń koordynowanych przez CERT Polska



Wykres 8. Rozkład botów w poszczególnych ASach

Serwery command & control

W pierwszej połowie 2011 roku otrzymaliśmy informacje z systemów automatycznych o 1 565 unikalnych serwerach Command&Control wykorzystywanych do zarządzania botnetami. Były rozmieszczone w 68 krajach.

Najwięcej z nich znajdowało się w USA – 32,1% ogółu. Razem z Niemcami hostują prawie 50% kontrolerów C&C. Podobnie jak w zeszłym roku, w czołówce znajdują się państwa zachodnioeuropejskie, takie jak Wielka Brytania, Holandia i Francja. Chiny znajdują się relatywnie nisko – dopiero na 10. pozycji. Według danych nam dostępnych również Polska pod tym względem prezentuje się bardzo korzystnie, dopiero na 30. miejscu z 9 kontrolerami– jeszcze niżej niż w roku ubiegłym (wtedy było miejsce 25.).

Liczba C&C	AS	Operator
3	12741	NETIA
2	5617	TP
2	16265	LEASEWEB
1	29314	VECTRA
5	8256	LODMAN

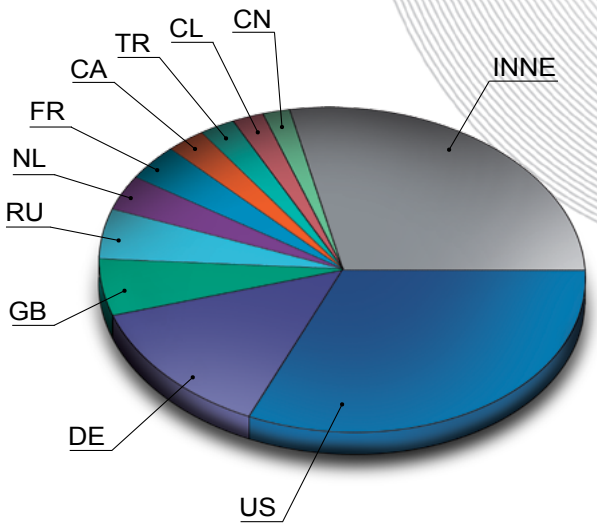
Tabela 11. Liczba unikalnych serwerów C&C według operatorów działających w Polsce

Statystyka zgłoszeń koordynowanych przez CERT Polska

Pozycja	Kraj	Liczba C&C	Procentowy udział
1	US	502	32,1
2	DE	209	13,4
3	GB	86	5,5
4	RU	78	5,0
5	NL	57	3,6
6	FR	57	3,6
7	CA	41	2,6
8	TR	37	2,4
9	CL	34	2,2
10	CN	29	1,9
11	CY	28	1,8
12	UA	25	1,6
13	LU	25	1,6
14	SG	22	1,4
15	KR	21	1,3
-	-	-	-
30	PL	9	0,6

Tabela 12. Serwery C&C według lokalizacji geograficznej

Większość zgłoszeń z Polski dotyczyła serwerów IRC.W porównaniu z ubiegłym rokiem liderem jest NETIA, a nie Telekomunikacja Polska, jednak z racji niewielkiej liczby zgłoszeń, trudno jest wyciągać z tego jednoznaczne wnioski. Interesujący jest fakt odnotowania kontrolerów w sieciach holenderskiego operatora Leaseweb, którego niektóre sieci są wpisane w RIPE jako będące w Polsce.



Wykres 9. Kraje, w których najczęściej znajdowały się serwery C&C

Ataki DDoS, serwery fast flux i pozostałe zgłoszenia

W tym podpunkcie raportu przedstawiamy krótki przegląd pozostałych rodzajów zgłoszeń, z których wyróżniliśmy dwie ważne kategorie: ddos oraz fastflux.

W pierwszej połowie 2011 roku otrzymaliśmy 14 automatycznych zgłoszeń zawierających informacje o atakach DDoS na serwery znajdującesię w polskich sieciach. Były to przypadki wydania rozkazu, zauważone na inwigilowanych serwerach C&C. Cztery ataki były wykonywane na serwery gier. Pozostałe według naszych analiz dotyczyły użytkowników indywidualnych.Jest to więcej niż w 2010 roku, w którym otrzymaliśmy 11 takich przypadków, jednak w dalszym ciągu niewiele w porównaniu do innych kategorii zgłoszeń.

W pierwszej połowie 2011 roku otrzymaliśmy 757 zgłoszeń (każde o innym numerze IP) dotyczących użycia polskich komputerów w charakterze serwerów fast flux dla 17 domen. Podobnie jak w zeszłym roku, przypadki te dotyczyły sieci z dużą liczbą użytkowników indywidualnych – prawie połowa adresów IP należała do Telekomunikacji Polskiej. Ogólnie jednak liczba zgłoszeń jest niższa niż w 2010 roku co naszym zdaniem wynika z coraz mniejszej popularności tej techniki.

Pozostałe zgłoszenia, które otrzymaliśmy, dotyczyły takich zagadnień, jak np. otwarte resolwery DNS i ataki typu brute force. Zagadnienia te poddamy analizie w raporcie na koniec tego roku.

Kontakt

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:	http://twitter.com/CERT_Polska
	http://twitter.com/CERT_Polska_en

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