Zespół CERT Polska działa w ramach Naukowej i Akademickiej Sieci Komputerowej

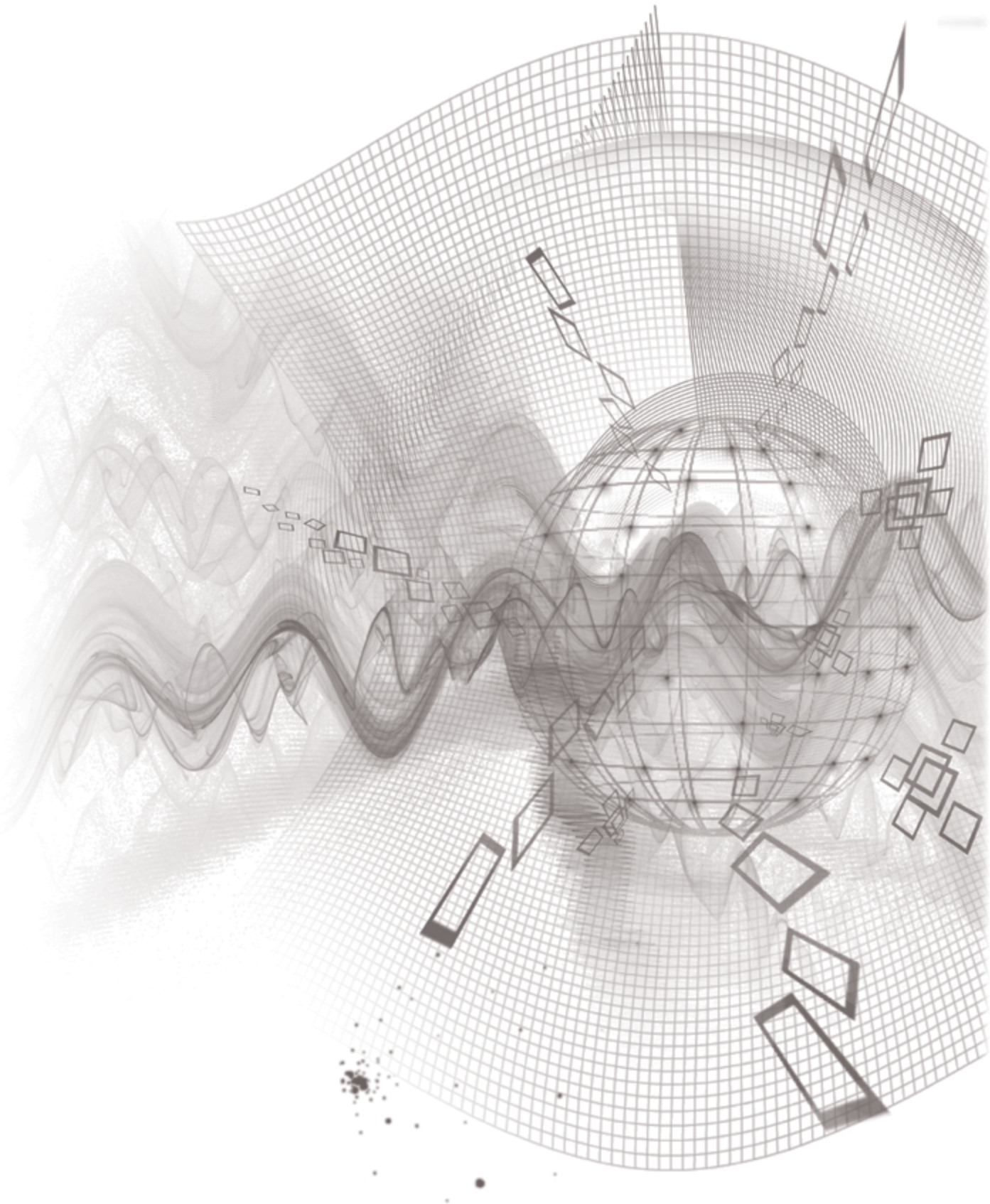
RAPORT 2010 CERT Polska

Zawiera raport z systemu ARAKIS

Analiza incydentów naruszających bezpieczeństwo teleinformatyczne

CERT POLSKA

NASK



Jak czytać ten dokument ?

Raport niniejszy przedstawia wybrane statystyki z danych zebranych przez zespół CERT Polska w 2010 r. wraz z omówieniem i wnioskami. Najważniejsze informacje znajdują się w rozdziałach 3, 4, 5 oraz 7.

W rozdziale 3 omawiamy 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.

Rozdziały 4 i 5 skupiają się na działalności operacyjnej CERT Polska. Dane w nich przedstawione pochodzą z systemu obsługi incydentów. Obejmują one takie zdarzenia, gdzie wymagana była interwencja CERT Polska. Używana przy obsłudze incydentów klasyfikacja umożliwia porównanie trendów w kolejnych latach, co uczyniliśmy w rozdziale 6.

Rozdział 7 omawia w szczegółach najważniejsze zjawiska, które pojawiły się bądź uaktywniły w sferze bezpieczeństwa w 2010 r.

Najważniejsze wnioski
podsumowujące raport

- Polska korzystnie wypada na tle innych państw jeśli chodzi o liczbę zagrożeń mających źródło w danym kraju. We wszystkich statystykach Polska jest poza pierwszą dziesiątką, za krajami porównywalnej wielkości i w podobnym stopniu zinformatyzowanymi.

- Pod względem źródeł spamu, Polska po raz pierwszy spadła poza pierwszą dziesiątkę – głównie dzięki działaniom prewencyjnym wprowadzonym przez Telekomunikację Polską. Przyjęcie podobnych rozwiązań przez innych operatorów bez wątpienia pomogłoby jeszcze bardziej zredukować ten problem.

- Zdecydowana większość zagrożeń związanych z usługą WWW – phishing i strony ze złośliwym oprogramowaniem ma swoje źródło w serwisach oferujących hosting oraz kolokację.

Streszczenie

Najważniejsze wnioski podsumowujące raport

- Co najmniej 9 proc polskich serwisów, na których znajdował się phishing należało do sklepów internetowych. Dostępność gotowych, łatwych w implementacji produktów wpływa na brak świadomości zagrożeń wynikających z ich stosowania.

- W statystykach zagrożeń, zarówno pod względem skanowań jak i spamu, coraz wyraźniej pojawiają się sieci mobilne.

- Ogromna większość ataków opartych o skanowanie uderza w port 445/TCP, co można w znacznej mierze przypisać aktywności robaka Conficker. Można przypuszczać, że polski użytkownik był w 2010 r. najczęściej infekowany właśnie przez tego robaka.

- Poważnym zagrożeniem stają się ataki na usługi Voice-over-IP. Zjawisko to można obserwować zarówno na poziomie skanowań jak i konkretnych przypadków skutecznych ataków, wiążących się często z poważnymi stratami finansowymi.

- Liczba spamu, zarówno na świecie jak i w Polsce, od dłuższego czasu nie wzrasta. W drugiej połowie 2010 r. widoczny był wyraźny trend spadkowy.

- Wśród polskich banków internetowych, które budziły największe zainteresowanie atakujących z użyciem oprogramowania Zeus dominowały ipko.pl oraz bsk.com.pl.

- Polskie serwisy przechowujące pliki (wrzuta.pl, przeklej.pl) zaczęły być wykorzystywane do dystrybucji złośliwego oprogramowania.

- Ataki DDoS, pomimo sporadycznych wystąpień (zgłoszeń), są bardzo groźne i brzemienne w skutkach. Odnotowaliśmy pierwszy przypadek połączony z próbą szantażu i uzyskania korzyści finansowych.

- W 2010 r. mieliśmy do czynienia z pierwszym poważnym zagrożeniem dla sieci instalacji przemysłowych – robakiem Stuxnet.

- Wciąż jednym z najpowszechniejszych sposobów infekcji użytkownika pozostaje technika drive-by download. Polega ona na umieszczeniu w kodzie strony złośliwego skryptu, który wykorzystując lukę w oprogramowaniu kieruje odwiedzającego, bez jego wiedzy, do serwera infekującego złośliwym oprogramowaniem.

Spis treści

Raport CERT Polska 2010

1	O zespole CERT Polska	6
2	Wstęp	7
3	**Statystyka zgłoszeń koordynowanych przez CERT Polska**	**8**
3.1	Ilość informacji we wszystkich kategoriach	8
3.2	„Tradycyjny" phishing	9
3.3	Strony związane ze złośliwym oprogramowaniem	11
3.4	Z piaskownicy do polskich sieci, czyli adresy odwiedzane przez malware	12
3.5	Spam z polskich sieci	14
3.6	Skanowania	14
3.7	Boty	17
3.8	Serwery command & control	17
3.9	Ataki DDoS	18
3.10	Serwery fast flux	18
3.11	Pozostałe	18
4.	**Statystyka incydentów obsłużonych przez CERT Polska**	**19**
4.1	Liczba przypadków naruszających bezpieczeństwo teleinformatyczne	19
4.2	Typy odnotowanych incydentów	19
4.3	Typy odnotowanych ataków	20
4.4	Zgłaszający, poszkodowani, atakujący	21
5.	**Statystyki dodatkowe**	**24**
5.1	Phishing w roku 2010	24
5.2	Liczba incydentów zgłaszanych tygodniowo z podziałem na główne kategorie	25
5.3	Liczba zgłoszeń a liczba incydentów	26
6.	**Trendy w kolejnych latach**	**27**
6.1	Liczba incydentów w latach 1996 – 2010	27
6.2	Rozkład procentowy podtypów incydentów w latach 2003-2010	27
7.	**Najważniejsze zjawiska okiem CERT Polska**	**29**
7.1	Rozwój spyware w 2010 roku	29
7.2	Zeus statystyki	32
7.3	Stuxnet – pierwszy znany robak atakujący instalacje przemysłowe	36
7.4	Ataki na VoIP	37
7.5	Pliki PDF nadal wykorzystywane jako nośniki złośliwego kodu	41
7.6	Politycznie motywowane ataki DDoS i Avenge Assange	43
8.	**Najciekawsze wydarzenia z działalności CERT Polska**	**44**
8.1	Społeczności CERT Polska	44
8.2	Doroczna konferencja FIRST i spotkanie CERTów narodowych w Miami	45
8.3	Zakończenie projektu HoneySpider Network	46
8.4	Konferencja SECURE 2010 pod znakiem zmian	47
	Raport ARAKIS 2010	**48**
	Wstęp	48
1.	Statystyki dotyczące alarmów	49
2.	Interesujące przypadki zaobserwowanych incydentów sieciowych	51
2.1	Atak na serwery Facebooka	51
2.2	HuaweiSymantecSpider – co to za pająk i dlaczego szuka phpMyAdmin?	52
2.3	Luka w aplikacji ProFTPd oraz jej wykorzystanie	53
	Podsumowanie	54

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.*

Wstęp

Zgodnie z założeniami programowymi wymienionymi na wstępie, CERT Polska co roku przygotowuje i udostępnia statystyki dotyczące przypadków naruszenia bezpieczeństwa teleinformatycznego w polskich zasobach internetowych[2], które zostały zgłoszone do naszego zespołu. Zespół prowadzi także prace w dziedzinie tworzenia wzorców rejestracji i obsługi przypadków naruszenia bezpieczeństwa teleinformatycznego (zwanych dalej incydentami), a także wzorców klasyfikacji incydentów oraz tworzenia statystyk.

Od kliku lat obserwujemy istotną dla profilu działalności zespołu 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 są 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 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. Dane te podajemy wraz z omówieniem w rozdziale 3, opisując je według kategorii informacji.

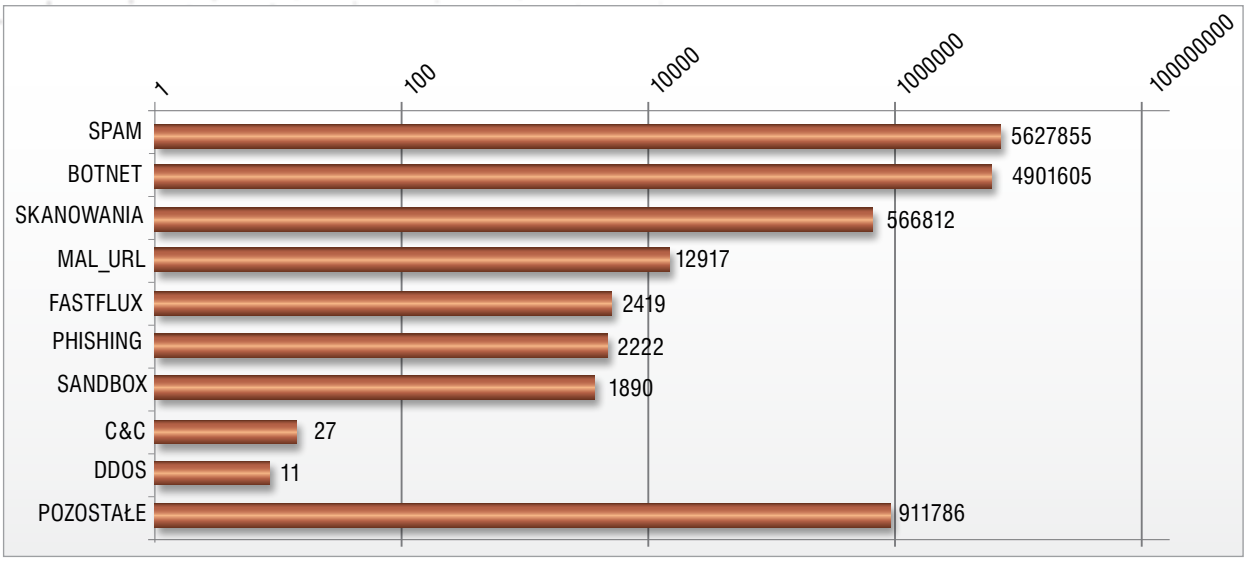
Dla danych pochodzących z obsługi incydentów, podobnie jak przez ostatnie pięć lat przygotowaliśmy statystyki zgodnie z klasyfikacją wypracowaną w ramach projektu eCSIRT.net (http://www.ecsirt.net/cec/service/documents/wp4-pub-userguide-v10.html#HEAD7). Umożliwia to porównanie trendów w kolejnych latach. Dane z incydentów, które zostały obsłużone wewnątrz zespołu znalazły się w rozdziale 4.

[2] *Niniejszy raport jest dwunastym z kolei raportem rocznym naszego zespołu. Dotychczasowe raporty (począwszy od roku 1996) dostępne są na stronie CERT Polska (http://www.cert.pl/raporty/).*

3. Statystyka zgłoszeń koordynowanych przez CERT Polska

3.1 Ilość informacji we wszystkich kategoriach

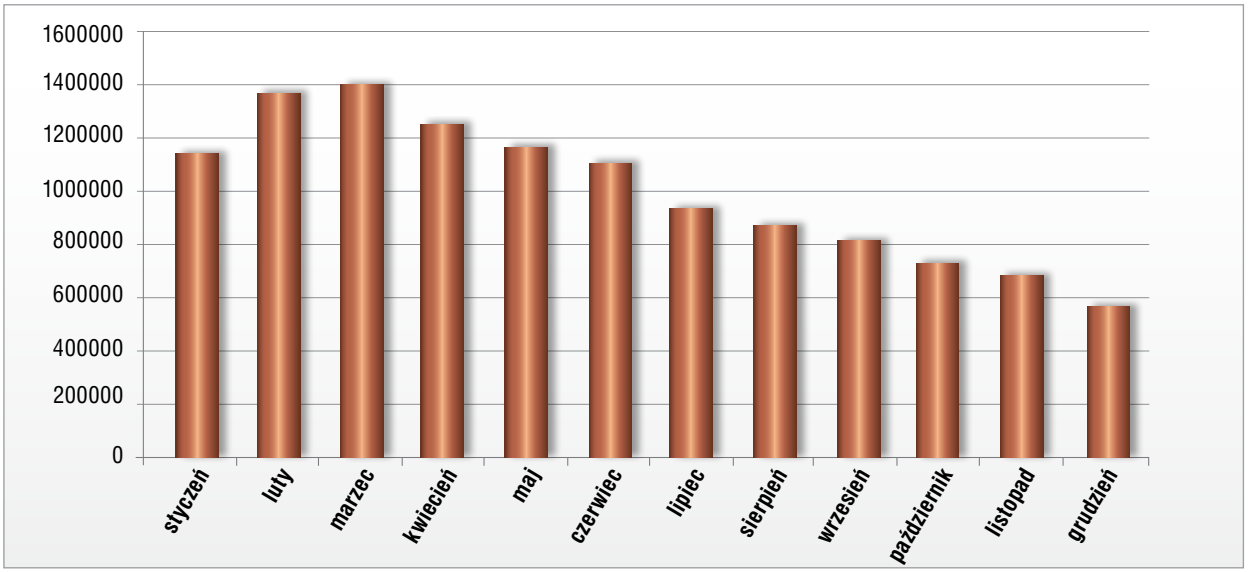
W 2010 r. otrzymaliśmy 12 027 544 zgłoszeń dotyczących Polski pochodzących z systemów automatycznych. Przeważająca większość dotyczyła rozsyłania spamu i innej działalności botnetów. Rozkład pozostałych kategorii, które wyróżniliśmy w raporcie przedstawia poniższy wykres (zwracamy uwagę na skalę logarytmiczną!).



Wykres 3.1.1. Liczba zgłoszeń automatycznych w wyróżnionych kategoriach

Dlatego sposoby ich zbierania oraz prezentacji znacznie różnią się między sobą. 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, fastflux, DDoS i pozostałe. Kategorie te są omówione w dalszej części.

Porównując liczbę zgłoszeń w poszczególnych miesiącach można zaobserwować wyraźny trend spadkowy, spowodowany przede wszystkim zmniejszającą się w drugiej połowie roku liczbą spamu oraz wygasającą aktywnością robaka Conficker.



Wykres 3.1.2. Liczba zgłoszeń automatycznych w poszczególnych miesiącach 2010 r.

3. Statystyka zgłoszeń koordynowanych przez CERT Polska

3.2 „Tradycyjny" phishing

W tej kategorii uwzględniamy zgłoszone przez automatyczne systemy adresy internetowe, pod którymi znajdowały się strony WWW podszywające się pod znane serwisy celem wyłudzenia danych dostępowych. Skupiamy się na stronach umieszczonych w sieciach polskich dostawców internetowych, przedstawiając je na tle zgłoszeń, dotyczących całego świata. Należy zwrócić uwagę, że tak rozumiany phishing (z wykorzystaniem fałszywej strony WWW) jest obecnie coraz rzadziej wykorzystywany ze względu na relatywnie niską skuteczność. Z jednej strony użytkownicy są coraz bardziej świadomi tego zagrożenia, z drugiej natomiast wiele systemów bankowych będących najczęstszymi celami phishingu, wymaga silniejszych form uwierzytelnienia niż sama nazwa użytkownika i hasło. Znacząco utrudnia to uzyskanie pełnego dostępu do konta z wykorzystaniem naiwnych metod phishingu bez jednoczesnego wzbudzania podejrzeń.

Tabela 3.2.1. Liczba przypadków „tradycyjnego" phishingu według lokalizacji geograficznej

1	US	189782	48,1%
2	CA	19240	4,9%
3	DE	17576	4,5%
4	GB	16404	4,2%
5	NL	15185	3,8%
6	FR	12179	3,1%
7	KR	10623	2,7%
8	RU	10124	2,6%
9	IT	8378	2,1%
10	CH	7587	1,9%
21	PL	2222	0,6%

Od kilku lat nasila się trend do wydobywania danych dostępowych przede wszystkim za pomocą złośliwego oprogramowania – snifferów, ale także koni trojańskich, przeprowadzających phishing wewnątrz przeglądarki klienta. Więcej na ten temat – p.5.1 oraz 7.1.

W 2010 r. ze źródeł automatycznych otrzymaliśmy 2 222 informacje o przypadkach phishingu umieszczonych w polskich sieciach. Zliczone zostały wszystkie przypadki stron wyłudzających dane dostępowe, umieszczone w sieciach dostawców zarejestrowanych w bazie RIPE z kodem kraju „PL" – bez względu na to, w jakiej domenie się znajdowały oraz z jakiego serwisu dane były wyłudzane. Zgłoszenia te dotyczyły 1 247 unikalnych adresów URL, znajdujących się w 843 domenach. Oznacza to, że na każde 100 serwisów WWW, w których celowo bądź w wyniku włamania umieszczono phishing przypadało średnio 148 różnych konkretnych stron wyłudzających dane. Wynika to z faktu, że częstą praktyką jest umieszczenie wielu stron podszywających się pod różne serwisy na jednym serwerze WWW.

Wykres 3.2.2. Kraje, w których najczęściej umieszczany był „tradycyjny" phishing

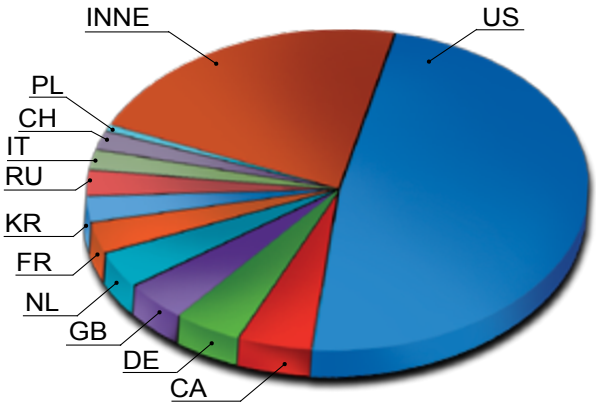


Tabela 3.2.3. Liczba przypadków „tradycyjnego" phishingu w Polsce według systemów autonomicznych

1	536	12824 (HOME.PL)
2	337	15967 (NETART)
3	158	5617 (TPNET)
4	114	29522 (KEI)
5	81	6714 (ATOM S.A.)

3. Statystyka zgłoszeń koordynowanych przez CERT Polska

Liczba zgłoszeń tradycyjnego phishingu przez cały rok utrzymywała się na podobnym poziomie. Nie został zaobserwowany wyraźny trend ani w skali globalnej, ani odnoszący się do Polski. Warto jednak zauważyć, że wspomniana liczba 2 222 zgłoszeń umieszcza Polskę dopiero na 21. miejscu krajów, w których najczęściej umieszczano strony phishingowe (zob. Tabela 3.2.1.). Choć wynik ten może być w pewnej mierze zaburzony rodzajem źródeł, z których otrzymujemy zgłoszenia automatyczne (głównie zagraniczne zespoły reagujące), uważamy go za w znacznym stopniu miarodajny.

Przyjrzeliśmy się z bliska temu, których dostawców internetowych najczęściej dotyka problem. W tabeli 3.2.3 przedstawiamy najczęściej pojawiające się polskie systemy autonomiczne.
Jak widać, strony phishingowe umieszczane są przede wszystkim w dużych serwisach hostingowych. Dzieje się tak ze względu na to, że najczęstszym sposobem umieszczenia phishingu jest skompromitowanie legalnego serwera WWW. Te natomiast częściej znaleźć można w serwisach hostingowych niż w sieciach operatorów obsługujących przede wszystkim indywidualnego użytkownika. Warto podkreślić, że statystyka ta nie upoważnia do wyciągania wniosków o tym, który z dostawców lepiej czy gorzej dba o bezpieczeństwo klientów. Różnice wynikać mogą przede wszystkim z liczby klientów, ale także z profilu klienta i wykorzystywanych przez niego usług (np. hosting współdzielony, dedykowany czy kolokacja).

Oprócz włamań na istniejące strony WWW, stosunkowo często stosowaną metodą „postawienia" phishingu jest wykorzystanie serwisów, w których można bezpłatnie zarejestrować dowolną poddomenę. Złodzieje często zakładają w nich aliasy o nazwie rozpoczynającej się np. od www.paypal.com [...]. Niemal co dziesiąta domena, w której umieszczono phishing w Polsce w 2010 r. została stworzona właśnie w ten sposób. Rozsądną rekomendacją dla firm prowadzących takie usługi jest więc moderacja lub weryfikacja nazw rejestrowanych bezpłatnie poddomen.
W grupie „inne/brak danych" znalazły się domeny, dla których nie byliśmy w stanie stwierdzić z całą pewnością, w jaki sposób został umieszczony phishing. Z pewnością także wiele z nich było ofiarami włamania. Mogą znajdować się w tej grupie także domeny zarejestrowane stricte w celu umieszczenia na nich phishingu.

Tabela 3.2.4. Liczba przypadków „tradycyjnego" phishingu według użytych domen

unikalne domeny wykorzystane do phishigu w polskich sieciach:	843
w tym:	
darmowe poddomeny (aliasy):	81
treść umieszczona w wyniku włamania:	395
inne/brak danych:	367

Tabela 3.2.5. Słowa kluczowe „tradycyjnego" phishingu w polskich sieciach

457	PayPal
29	Ebay
19	MasterCard
1	Allegro

Smutną statystyką jest to, że aż 9 proc. stron, na których umieszczono phishing (79 z 843) należało do sklepów internetowych. Liczba ta jest w rzeczywistości zaniżona, ponieważ uwzględniliśmy wyłącznie te przypadki, gdy o rodzaju serwisu dało się wnioskować na podstawie adresu internetowego. Biorąc pod uwagę, że wiele sklepów zbiera przy składaniu zamówienia znacznie więcej danych niż niezbędne do jego realizacji (np. numer telefonu, adres email), można mieć poważne obawy co do bezpieczeństwa tych danych, skoro właściciel sklepu nie zadbał nawet o należyte zabezpieczenie własnego serwisu przed włamaniem. Przyczyną jest najczęściej wdrażanie gotowych, tanich lub bezpłatnych aplikacji do prowadzenia sklepu online, bez dodatkowego wkładu pracy wymaganego na odpowiednią konfigurację, oraz utrzymanie i bieżące aktualizacje tej aplikacji. Na pocieszenie, w przypadku umożliwienia płatności kartą kredytową, sama realizacja transakcji odbywa się zazwyczaj przez zaufanego pośrednika, którym jest jedna z kilku firm świadczących usługi płatności online.

Raport CERT Polska 2010

3. Statystyka zgłoszeń koordynowanych przez CERT Polska

W takim przypadku do właściciela sklepu trafia jedynie rezultat próby autoryzacji, a nie dane samej karty.

Sprawdziliśmy także, jakie serwisy były na celowniku złodziei, którzy swoje pułapki zastawiali w Polsce. Ponieważ nie mieliśmy dostępu do treści wszystkich stron, które znajdowały się pod adresami, skorzystaliśmy przede wszystkim z analizy słów kluczowych znajdujących się w samych odnośnikach URL (uwzględniając różne modyfikacje i wariacje pisowni).

Jak widać, zdecydowanie dominowały strony podszywające się pod serwis PayPal. Co interesujące, tradycyjne banki nie pojawiły się tutaj. Do wyłudzania danych do nich zdecydowanie częściej wykorzystuje się złośliwe oprogramowanie takie jak Zeus czy SpyEye (patrz 7.1). Niemal nie zaobserwowano też ataków, które byłyby w jakiś sposób specyficzne dla Polski. Wyjątkiem był pojedynczy incydent próby podszycia się pod serwis aukcyjny Allegro.

Ataki phishingowe dotyczące banków, zarówno tradycyjne jak i wykorzystujące złośliwe oprogramowanie były jednak wykrywane przez CERT Polska oraz zgłaszane do nas celem obsłużenia. Omówienie ich w kontekście innych incydentów obsłużonych przez zespół znajduje się w rozdziałach 4, 5.1 oraz 7.1.

3.3 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, pobierany w wyniku działania powyższego kodu,
- pliki konfiguracyjne służące do sterowania uruchomionym w systemie złośliwym oprogramowaniem.

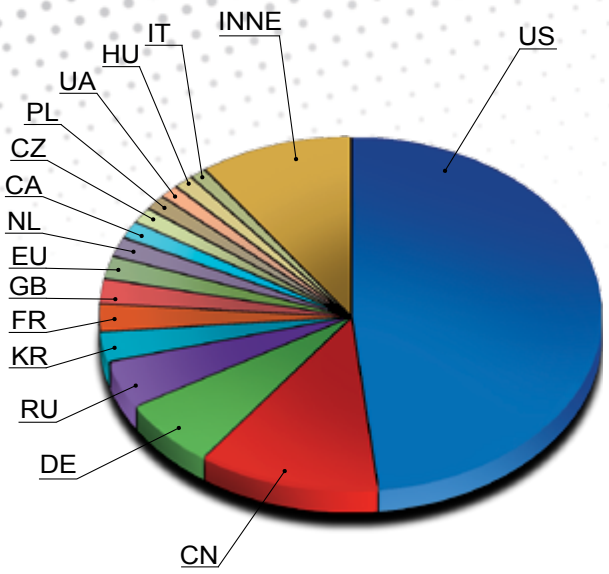
W 2010 r. trafiło do nas 12 917 zgłoszeń tego rodzaju dotyczących Polski. Stanowiło to około 1,4 proc. zgłoszeń dotyczących całego świata. Zgłoszenia te odnosiły się do 8 031 unikalnych adresów URL (1,61 zgłoszeń na każdy URL). Porównując między sobą poszczególne kraje, w których utrzymywane były pliki związane ze złośliwym oprogramowaniem warto zwrócić uwagę na wysoką pozycję Chin, Rosji i Ukrainy. Zestawiając poniższą tabelę 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. Polska zajmuje dwunastą pozycję – wyższą niż w przypadku phishingu, lecz z niewielką przewagą nad kolejnymi krajami.

Podobnie jak w przypadku phishingu, zadaliśmy sobie pytanie, w czyich sieciach najczęściej pojawiały się pliki związane ze złośliwym oprogramowaniem. Wyniki nie są zaskakujące – znów dominują najwięksi dostawcy usług hostingowych: Home.pl, Netart oraz Krakowskie E-Centrum Informatyczne Jump.

Warto zwrócić uwagę na znaczną liczbę adresów URL przypadających na pojedynczy adres IP – często po skompromitowaniu jednego serwisu WWW umieszczane jest na nim wiele plików. Zdarza się także nierzadko, że niektóre lub wszystkie

3. Statystyka zgłoszeń koordynowanych przez CERT Polska

Wykres 3.3.1. Kraje, w których najczęściej znajdowały się strony WWW ze złośliwym oprogramowaniem



legalne podstrony serwisu modyfikowane są w ten sposób, że w ich kodzie zagnieżdżona zostaje zawartość z kolejnych adresów serwujących złośliwe oprogramowanie. Takie wykorzystanie aktywnych mechanizmów stron WWW do instalacji złośliwego oprogramowania na komputerze użytkownika nosi nazwę drive-by download. Do infekcji dochodzi bez wiedzy i jakiejkolwiek świadomej akcji użytkownika, który zwyczajnie przegląda zawartość witryn WWW. Po stronie serwera do wstrzyknięcia kodu wykorzystywane są podatności aplikacji webowych lub dane dostępowe administratora wykradzione przez konia trojańskiego. Po stronie klienta natomiast atakowane są luki w przeglądarce lub, znacznie częściej, w silnikach przetwarzających aktywną zawartość np. Flash czy PDF. **Dlatego niezwykle istotne jest regularne aktualizowanie oprogramowania odpowiedzialnego za pobieranie i wyświetlanie treści pochodzących z Internetu.**

Tabela 3.3.2. Liczba przypadków złośliwego oprogramowania na stronach WWW według lokalizacji geograficznej

1	US	445653	48,2%
2	CN	110101	11,9%
3	DE	58265	6,3%
4	RU	41230	4,5%
5	KR	25772	2,8%
6	FR	22187	2,4%
7	GB	21336	2,3%
8	EU	19604	2,1%
9	NL	15635	1,7%
10	CA	15063	1,6%
11	CZ	13204	1,4%
12	**PL**	**12917**	**1,4%**
13	UA	11744	1,3%
14	HU	11555	1,2%
15	IT	9883	1,1%

Tabela 3.3.3. Liczba przypadków złośliwego oprogramowania na polskich stronach WWW według systemów autonomicznych

liczba zgłoszeń	system autonomiczny	URL / IP
3012	12824 (HOME.PL)	9,1
2417	29522 (KEI)	29,5
1211	15967 (NETART)	6,9
801	41079 (Superhost)	11,5

3.4 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. Na przestrzeni 2010 r. zaobserwowaliśmy 1 890 unikalnych polskich adresów WWW oraz FTP, do których łączyło się

3. Statystyka zgłoszeń koordynowanych przez CERT Polska

oprogramowanie uruchamiane w sandboxach. Do adresów tych odwoływało się w sumie 2 752 unikalnych plików. Ponad 32 proc. 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 adresy stat24.com oraz gemius.pl. Niestety w tym przypadku trudno ocenić jakie były powody odwiedzin adresów. Ponieważ programy antywirusowe nie wskazują na złośliwość plików, należy z dużym prawdopodobieństwem założyć, że był to normalny ruch. Zakładając scenariusz pesymistyczny, mógł to być wynik wyświetlania banerów reklamowych, celem uzyskania korzyści finansowych.
Do serwera appmsg.gadu-gadu.pl łączyło się 136 unikalnych plików, z czego ponad 42 proc. rozpoznano jako złośliwe oprogramowanie. Były to połączenia inicjujące komunikację z wykorzystaniem protokołu Gadu-Gadu. Jeżeli chodzi o połączenia do register.gadu-gadu.pl, to miały one format http://register.gadu-gadu.pl/regRndPictNew.php?tokenid=xxxxxxxxxxxxxxxxxxx, co oznacza pobranie tokenu używanego do rejestracji nowego konta. Tutaj unikalne pliki były zaledwie 3, za to wszystkie rozpoznano jako złośliwy kod. Można wysnuć kilka hipotez dotyczących takich połączeń. Możliwe, że Gadu-Gadu zostało wykorzystane jako medium do kontroli botnetu. Inny scenariusz to taki, że atakujący buduje bazę tokenów wyświetlanych przy rejestracji. Zakładane konta mogą być też wykorzystywane do rozsyłania spamu czy linków do złośliwego kodu.

Ciekawe wnioski odnoszą się do serwisów umożliwiających przechowywanie plików. Mowa o wrzuta.pl i przeklej.pl. Praktycznie wszystkie zauważone adresy zawierały złośliwe oprogramowanie. Serwisy te mogły być wykorzystywane do infekowania złośliwym oprogramowaniem nowych komputerów, bądź serwowania aktualizacji dla komputerów już zainfekowanych, będących częścią botnetu.

Na wrzuta.pl wiele z tych plików jest wciąż dostępnych. W przypadku przeklej.pl sprawa wygląda trochę lepiej, ponieważ pliki są usuwane automatycznie, jeśli nie były ściągane przez pewien okres. Niepokojący jest fakt, że złośliwe oprogramowanie w ogóle znajduje się w tego typu serwisach, co może świadczyć o niewystarczającej kontroli przesyłanej przez użytkowników zawartości przez programy antywirusowe, bądź też o ich słabej jakości.

Wiele z zauważonych adresów znajduje się na serwerach umożliwiających darmowy hosting stron WWW, takich jak np. interia.pl czy webpark.pl. Mogły one zostać umieszczone tam celowo lub też znaleźć się w wyniku niewielkiej wiedzy właścicieli takich stron na temat podstawowych zasad tworzenia bezpiecznych stron WWW.

W przypadku większości adresów niestety nie udało się jednoznacznie określić w jakim celu były one odwiedzane. Mógł to być np. atak typu DDoS, sprawdzanie przez malware połączenia z Internetem bądź też przypadkowa pochodna innej działalności złośliwego oprogramowania.

Tabela 3.4.1. Liczba unikalnych adresów w poszczególnych domenach

1	stat24.com	232
2	gemius.pl	196
3	appmsg.gadu-gadu.pl	77
4	register.gadu-gadu.pl	70
5	www.elitepvpers.pl	66
6	interia.pl	57
7	wrzuta.pl	45
8	www.accons.pl	43
9	pozwolenienabudowe.pl	41
10	www.swiatowapilka.pl	39
11	webpark.pl	34
12	bbelements.com	**34**
13	cagefight.pl	30
14	przeklej.pl	25
15	www.dialer.pl	24

3. Statystyka zgłoszeń koordynowanych przez CERT Polska

3.5 Spam z polskich sieci

W tej kategorii zawsze bierzemy pod uwagę źródła spamu, a nie poszczególne przesyłki z niezamawianą korespondencją. Dlatego wszelkie statystyki odzwierciedlają więc bardziej punkt widzenia dostawcy internetowego, który musi poradzić sobie z niepożądanym i niemile widzianym ruchem z jego sieci, niż użytkownika końcowego, dla którego problemem jest codzienne czyszczenie skrzynki odbiorczej.

Z systemów automatycznych trafiło do nas w 2010 r. 5 627 855 informacji o adresach IP w sieciach polskich dostawców, z których rozsyłany był spam. Na tej podstawie spróbowaliśmy oszacować, ile było rzeczywistych przypadków przejęcia maszyny do rozsyłania spamu. Przyjęliśmy metodę, w której powtarzające się zgłoszenia dotyczące tego samego adresu IP są ignorowane, o ile przerwa pomiędzy nimi była krótsza niż trzy dni. Oznacza to, że ten sam adres IP, który zamilkł na dłużej niż 3 dni i pojawił się ponownie, uznawaliśmy za nowy przypadek. Jesteśmy świadomi słabości i zaburzeń z niej wynikających – jak z każdej metody szacowania rzeczywistej liczby maszyn zainfekowanych, biorących udział w atakach, itp. Metoda ta faworyzuje sieci stosujące NAT kosztem tych, gdzie użytkownikom dynamicznie przydzielane są publiczne adresy IP. W przypadku tych pierwszych wiele maszyn wysyłających stale spam z wnętrza sieci NAT będzie uwzględnione tylko raz (nie ma przerwy). W drugim przypadku jedna zainfekowana maszyna, która odnawia codziennie swój adres IP, zostanie policzona wielokrotnie. Taka metoda liczenia jest jednak zbliżona do metod obliczania reputacji dla poszczególnych sieci przez zewnętrzne serwisy monitorujące bezpieczeństwo.

W 2010 r. wyodrębniliśmy korzystając z opisanej wyżej metody, 1 808 813 przypadków rozsyłania spamu. W skali długookresowej nasilenie spamu nie zwiększa się i utrzymuje się na mniej więcej stałym poziomie. Patrząc na kolejne miesiące 2010 r. widać jednak trend malejący w drugiej połowie roku. Ma on potwierdzenie w analizach globalnych, m.in. statystykach senderbase.org oraz spamcop.net. Od ubiegłego roku Polska zdecydowanie poprawiła swoje miejsce w tych statystykach, wypadając poza pierwszą dziesiątkę krajów, w których znajduje się najwięcej źródeł spamu. Dotyczy to w zasadzie wszystkich serwisów zwalczających i monitorujących spam, w tym Spamhaus, senderbase.org, spamcop.net czy UCEProtect. Jest to zasługą wdrożenia przez Telekomunikację Polską pod koniec 2009 r. mechanizmu blokowania portu 25 TCP dla użytkowników indywidualnych. Ruch ten znalazł też odzwierciedlenie w reputacji sieci Telekomunikacji Polskiej w wymienionych wyżej serwisach. Dzisiaj próżno szukać jej w pierwszej dziesiątce najbardziej „problematycznych" dostawców Internetu na świecie, choć jeszcze w 2009 r. miejsce w pierwszej trójce nie było rzadkością. Również w przypadku zgłoszeń otrzymanych przez CERT Polska, Telekomunikacja Polska została w 2010 r. wyprzedzona m.in. przez Netię oraz przez sieć iPlusa (!).

3.6 Skanowanie

Jedną z głównych kategorii zgłoszeń zewnętrznych, dotyczących złośliwej aktywności z Polski pozostaje skanowanie. Coraz rzadziej zdarzają się ręczne przypadki jego zgłaszania. W większości zgłoszenia są w pełni zautomatyzowane, wręcz hurtowe, przekazywane nam w dziennych, zbiorczych paczkach. Najczęściej są to dane z systemów honeypot. Ponieważ źródła zewnętrzne dostarczają nam dane w bardzo różnych formach, z różnych rodzajów systemów, a definicji skanowania można przyjąć bardzo wiele, przyjeliśmy jednolity sposób prezentacji danych. Zdecydowaliśmy się rozpatrzyć przypadki skanowania w kategorii unikalnych źródeł, które były rejestrowane przez systemy zgłaszające (globalnie lub per port docelowy) w przedziale całego roku chyba, że wskażemy inaczej.

3. Statystyka zgłoszeń koordynowanych przez CERT Polska

Najczęściej skanowane usługi

Pierwszą kategorię zgłoszeń, którą możemy rozpatrzyć, jest liczba unikalnych zgłoszonych zainfekowanych IP per port docelowy. Duża część obserwowanych komputerów jest częścią botnetów. Najczęściej atakowanym portem w chwili obecnej jest port 445, co nie jest nowością, ponieważ od lat wiele najpoważniejszych luk związanych z oprogramowaniem Microsoftu znajduje się w aplikacjach nasłuchujących na tym porcie. Jednakże przewaga ataków na tym porcie nad pozostałymi jest ogromna, o dwa rzędy wielkości. Nigdy wcześniej nie było aż takiej różnicy skali. Przypisujemy to przede wszystkim aktywności robaka Conficker. Luka z której korzysta (związana z błędem w obsłudze zapytań RPC), opisana w biuletynie bezpieczeństwa Microsoft numer MS08-067[3] była w roku 2010 najpopularniejszą luką wykorzystywaną do bezpośrednich ataków na komputery. Oczywiście luka ta jest obecnie powszechnie wykorzystywana również przez inne niż Conficker robaki i botnety.

Aktywność starszych robaków, od lat wpisujących się w „szum internetowy", takich jak Blaster, Sasser, Welchia czy Slammer jest jeszcze widoczna, ale już w coraz mniejszym stopniu. Port 1434/UDP – wykorzystywany przez słynnego Slammera z 2003 r., tak długo figurujący na listach TOP 10, pojawia się na nich coraz rzadziej (częściowo wynika to też z faktu, że jest w dalszym ciągu blokowany u wielu operatorów[4]).

Warta odnotowania jest także obecność w pierwszej dziesiątce portu 22/TCP. Wiąże się to w większości z atakami słownikowymi na usługę SSH. Celem jest zdobycie dostępu do systemu Unix/Linux, zazwyczaj na poziomie użytkownika root. Jest to najczęściej atakowany port „natywny" dla systemów Unix/Linux. Drugi jest związany z telnetem (port 23/TCP). Jego obecność w rankingu może się wydawać nieco zaskakująca, gdyż jest to usługa, która w świecie unixowym dawno została wyparta przez SSH. Odpowiedzi na zagadkę naszym zdaniem należy jednak szukać w innych urządzeniach: celem tych skanowań są routery, które często jeszcze nie wspierają SSH.

W porównaniu do większości w rankingu, port 5060/UDP jest stosunkowo nowym zjawiskiem. Kojarzony jest z usługą Voice-over-IP (VoIP) wykorzystującą do komunikacji protokół SIP. Ataki VoIP stają się coraz częstsze wraz ze wzrostem popularności tej usługi i są bardziej szczegółowo opisane dalej w rozdziale 7.4.

Tabela 3.6.1. TOP 10 portów docelowych pod kątem unikalnych skanujących źródłowych IP

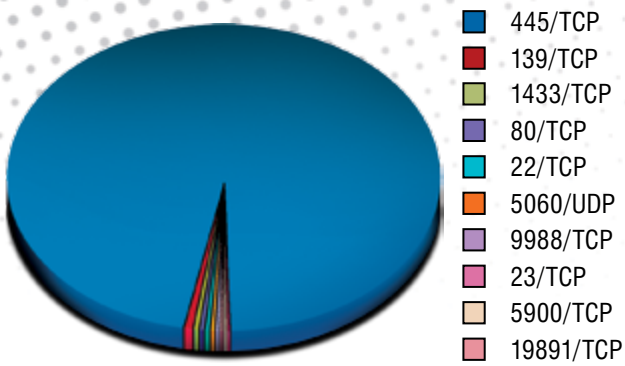
port docelowy / protokół	Liczba widzianych unikalnych IP	Prawdopodobny wiodący mechanizm ataków
445/TCP	288844	Ataki typu buffer overflow na usługi Windows RPC
139/TCP	1057	Ataki związane z usługą współdzielenie plików / drukarek Windows
1433/TCP	562	Ataki słownikowe na MS SQL
80/TCP	559	Ataki związane z aplikacjami webowymi
22/TCP	439	Ataki słownikowe na serwery SSH
5060/UDP	435	Ataki na VoIP
9988/TCP	363	Część innego ataku (ładowanie robaka przez zbindowany port)
23/TCP	314	Ataki słownikowe na usługę telnet
5900/TCP	311	Ataki na VNC
19891/TCP	296	Część innego ataku (ładowanie robaka przez zbindowany port)

[3] *http://www.microsoft.com/poland/technet/security/bulletin/MS08-067.mspx*

[4] *W przypadku systemu ARAKIS, port 1434/UDP nadal figuruje wysoko w rankingach*

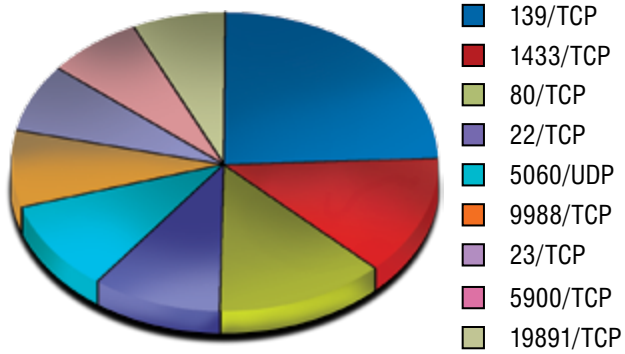
3. Statystyka zgłoszeń koordynowanych przez CERT Polska

Skalę dominacji ataków na port 445/TCP odwzorowują poniższe wykresy:



Wykres 3.6.2. TOP 10: unikalne źródłowe IP per port

Lepszy obraz udziału pozostałych portów w atakach daje usunięcie portu 445:



Wykres 3.6.3. TOP 9: Unikalne źródła per port (bez 445/TCP)

Obecność portów 9988/TCP i 19891/TCP jest niespodzianką. Nie są kojarzone z żadną znaną nam usługą. Wydaje się, że ich aktywność związana jest z kolejnym etapem infekcji komputera, gdzie do udanego ataku wykorzystano port 445/TCP, otworzono shell na wysokim porcie, po którym następnie załadowano główne „ciało" robaka. Taką aktywność na porcie 9988/TCP widzimy na własnych honeypotach ARAKISowych – na skutek działalności robaków Allaple i Virut. Port 19891/TCP pozostaje jednak zagadką.

Warto odnotować, że z listy TOP 10 wypadają ataki jeszcze niedawno dominujące – w szczególności na oprogramowanie antywirusowe (między innymi Symanteca – port 2967/TCP). Coraz rzadziej występują porty 1026 i 1027 UDP kojarzone ze spamem Windows Messenger Popup, który praktycznie zanika.

Nazwa operatora	Numer systemu autonomicznego	Liczba unikalnych skanujących IP
TPNET	5617	127810
NETIA	12747	56636
DIALOG	15857	47182
PTK CENTERTEL	43447	24592
PLUSNET	8374	18391
MULTIMEDIA	21021	16290
UPC Polska	9141	6018
ASK-NET	2538	4891
VECTRA	29314	4835
ATOM S.A.	6714	3277

Tabela 3.6.4. TOP 10 operatorów w Polsce pod kątem liczby skanujących IP

Najbardziej zainfekowane sieci w Polsce na bazie obserwowanych skanowań

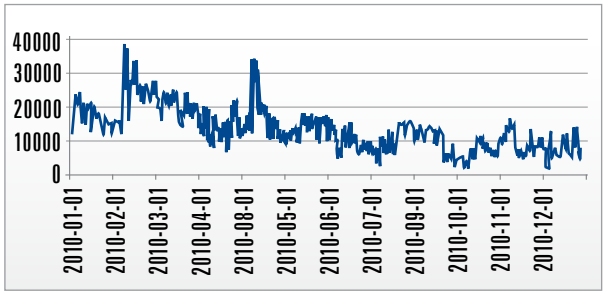
Innym ciekawym zestawieniem wydaje się być rozkład zainfekowanych unikalnych IP od poszczególnych polskich operatorów. Uświadamia to skalę infekcji złośliwym oprogramowaniem w Polsce. Powyżej prezentujemy tabelę dziesięciu najbardziej zainfekowanych sieci w przeciągu minionego roku.

W kategorii *najwięcej unikalnych atakujących IP* w Polsce króluje AS5617 – Telekomunikacja Polska SA. Druga, Netia, ma o połowę mniej - porównywalnie z trzecim operatorem Dialog. Ranking wydaje się odzwierciedlać największych operatorów w Polsce pod względem liczby użytkowników. Interesujący jest fakt obecności na liście operatorów sieci mobilnych. Przypuszczamy, że ich obecność będzie się z czasem stawać coraz bardziej znacząca. Operatorzy sieci kablowych z kolei znajdują się pod koniec pierwszej dziesiątki, co może być związane z architekturą sieci – wielu klientom sieci kablowych udostępniane są adresy prywatne ukryte za NAT. Oczywiście, w takim przypadku w statystykach pojawiają się jedynie publiczne adresy sieci.

3. Statystyka zgłoszeń koordynowanych przez CERT Polska

3.7 Boty

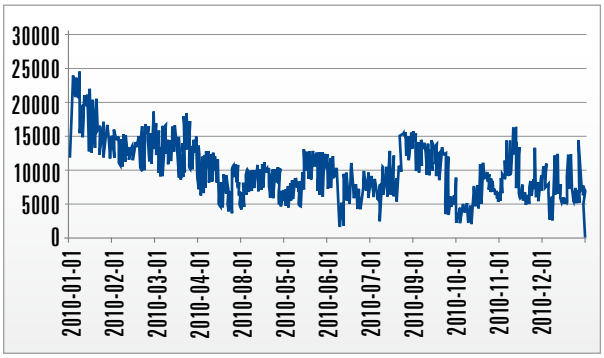
Kategoria ta uwzględnia komputery będące członkami botnetów znajdujące się w polskich sieciach, a nieuwzględnione w innych kategoriach. Choć najpopularniejszym zastosowaniem botnetów jest rozsyłanie spamu (patrz: 3.5), mogą one być wykorzystane do dowolnych innych zastosowań, wymagających dużego pasma lub dużej mocy obliczeniowej, albo po prostu jako dodatkowa warstwa anonimizacji.



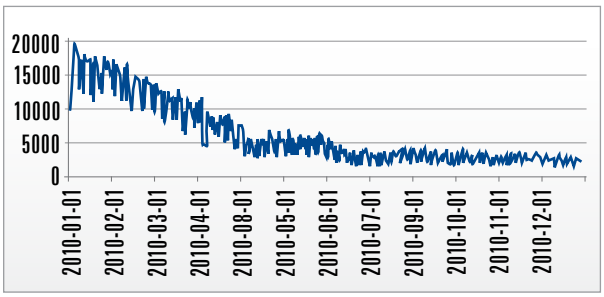
Wykres 3.7.1. Liczba botów w polskich sieciach

Na przestrzeni całego roku 2010 otrzymaliśmy 4 901 605 zgłoszeń dotyczących członków botnetów. W zgłoszeniach tych pojawiało się 269 635 unikalnych adresów IP – średnio 13,5 tys. zainfekowanych maszyn w ciągu dnia, zaś w momencie szczytowym prawie 40 tys. (wyk. 3.7.1.). Maksymalne wzrosty, które wystąpiły w lutym i maju, były wynikiem wzmożonej działalności złośliwego oprogramowania o nazwie Pushdo. Wykres aktywności dziennej bez niego wygląda nastepująco (wyk. 3.7.2.).

Po uwzględnieniu anomalii spowodowanych przez Pushdo, wyraźnie zaznacza się trend zniżkowy na przestrzeni całego roku. Tutaj niebagatelny wpływ miał Conficker, który maksimum aktywności wykazywał na początku roku, po czym wygasał z każdym kolejnym dniem. Pomimo tego, średnio stanowił ok. 40 proc. wszystkich botów w polskich sieciach. Aktywność Confickera na przestrzeni roku obrazuje wykres 3.7.3



Wykres 3.7.2. Liczba botów w polskich sieciach z wykluczeniem Pushdo



Wykres 3.7.3. Conficker w polskich sieciach

3.8 Serwery Command & Control

W roku 2010 otrzymaliśmy informacje z systemów automatycznych o 4 303 unikalnych serwerach Command & Control, wykorzystywanych do zarządzania botnetami. Były rozmieszczone w 90 krajach.

Najwięcej z nich umiejscowiono w USA – 1 493 serwery, co stanowi aż 34,7 proc. ogółu. Co ciekawe, w czołówce znajdują się państwa zachodnioeuropejskie takie jak Niemcy, Holandia, Wielka Brytania i Francja. Wbrew oczekiwaniom Chiny znalazły się dopiero na 11. miejscu. W Polsce odnotowaliśmy 27 serwerów, co daje nam 25. miejsce na liście i stanowi zaledwie 0,6 proc. ogółu.

Większość z tych serwerów działała w oparciu o protokół IRC. Jedenaście z nich znajdowało się w sieci Telekomunikacji Polskiej (na adresach należących do usługi Neostrada/Neostrada Plus). Pozostałe były rozproszone w wielu różnych systemach autonomicznych.

3. Statystyka zgłoszeń koordynowanych przez CERT Polska

1	US	1493	34,7%
2	DE	435	10,1%
3	NL	227	5,3%
4	GB	208	4,8%
5	FR	205	4,8%
6	RU	139	3,2%
7	LU	126	2,9%
8	TR	96	2,2%
9	UA	90	2,1%
10	CA	85	2,0%
11	CN	77	1,8%
12	CL	76	1,8%
13	JP	66	1,5%
14	EU	62	1,4%
15	IL	54	1,3%
-	-	-	-
25	**PL**	**27**	**0,6%**

Tabela 3.8.1. Serwery Command & Control według lokalizacji geograficznej

3.9 Ataki DDoS

W roku 2010 otrzymaliśmy 11 zgłoszeń zawierających informacje o atakach DDoS na serwery znajdujące się w polskich sieciach. Były to przypadki wydania rozkazu, zauważone na inwigilowanych serwerach C&C. Większość z nich była skierowana na użytkowników indywidualnych (w odróżnieniu od zgłoszeń przekazywanych ręcznie, gdzie poszkodowanym jest najczęściej firma komercyjna). Nie poznano motywów działania atakujących. Nie udało się zidentyfikować zleceniodawcy ataku. Pomimo niewielkiej liczby zgłoszeń, problem jest poważny i może mieć duże konsekwencje, szczególnie w przypadku podmiotów, dla których Internet jest głównym narzędziem prowadzenia wszelakiego rodzaju działalności.

3.10 Serwery fast flux

Fast flux jest techniką polegającą na rozproszonym hostowaniu treści (zazwyczaj nielegalnych bądź związanych z nielegalną działalnością) przez utrzymywanie wielu kopii serwisu na przejętych maszynach, posiadających publiczne adresy IP. Rekordy A domeny kontrolowanej przez właściciela takiego serwisu są często aktualizowane (nawet co kilka minut) i w każdej chwili zwracają wiele adresów IP (przy każdej aktualizacji innych). W ten sposób skutecznie utrudnia się zablokowanie bądź oczyszczenie wszystkich maszyn służących w roli serwerów, ponieważ każda z nich może znajdować się u innego dostawcy, w innych rejonach świata. Często w charakterze serwerów fast flux wykorzystywane są części botnetów.

W 2010 r. otrzymaliśmy informacje o 2 419 przypadkach użycia polskich komputerów w charakterze serwerów fast flux dla 82 domen (średnio 29 adresów na domenę). Co ciekawe, dla każdej domeny adresy rozrzucone są pomiędzy różnymi operatorami, co wyklucza interpretację, że być może te same maszyny pojawiały się z różnymi adresami IP. Brak danych spoza polskich sieci uniemożliwia przesądzenie czy z jakichś powodów właściciele tych domen upodobali sobie akurat polskie sieci, czy też miały one tak wiele serwerów, że 29 adresów w Polsce można wyjaśnić statystycznie.

Znaczna większość adresów znajdowała się w sieci Telekomunikacji Polskiej, co należy wytłumaczyć efektem skali. Niestety, w tym przypadku wprowadzone przez TP mechanizmy służące poprawie bezpieczeństwa, takie jak blackholing, filtrowanie portów typowych usług systemu Windows czy blokowanie portu 25 TCP, nie mają zastosowania.

Mimo wszystko niewielka liczba domen wykorzystujących fast flux w skali roku może być wytłumaczona faktem, że technika ta nie przyjęła się tak mocno jak się spodziewano. Domeny wykorzystujące ją są bowiem łatwe do wykrycia przez obserwację odpowiedzi na zapytania o rekord A.

3.11 Pozostałe

W kategorii *Pozostałe* znalazły się wszystkie zgłoszenia nie objęte powyższą klasyfikacją, takie jak informacje o otwartych resolwerach DNS (ponad 500 tys.) a także np. próbach włamania się do serwerów SSH za pomocą brute force. Ze względu na dużą różnorodność zdecydowaliśmy się nie umieszczać analizy tych zdarzeń w raporcie za 2010 r. – dane te będą przedmiotem odrębnej analizy.

4. 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.

4.1 Liczba przypadków naruszających bezpieczeństwo teleinformatyczne

W roku 2010 obsłużyliśmy 674 incydentów. W następnych rozdziałach znajduje się ich szczegółowa klasyfikacja .

4.2 Typy odnotowanych incydentów

Poniższa tabela przedstawia zbiorcze zestawienie statystyk odnotowanych incydentów. Nasza klasyfikacja zawiera osiem głównych typów incydentów oraz kategorię *Inne*. Każdy z głównych typów zawiera podtypy incydentów, które najczęściej stanowią bardziej precyzyjny opis incydentu, z jakim mieliśmy do czynienia.

Tabela 4.2.1. Incydenty obsłużone przez CERT Polska według typów

Typ/Podtyp incydentu	Liczba	Suma	Procent
Obraźliwe i nielegalne treści	2	195	28,93 %
Spam	2		
Dyskredytacja, obrażanie	2		
Pornografia dziecięca, przemoc[5]	2		
Złośliwe oprogramowanie	90	91	13,50 %
Wirus	0		
Robak sieciowy	0		
Koń trojański	1		
Oprogramowanie szpiegowskie	0		
Dialer	0		
Gromadzenie informacji	8	66	9,79 %
Skanowanie	54		
Podsłuch	1		
Inżynieria społeczna	3		
Próby włamań	16	42	6,23 %
Wykorzystanie znanych luk systemowych	12		
Próby nieuprawnionego logowania	14		
Wykorzystanie nieznanych luk systemowych	0		

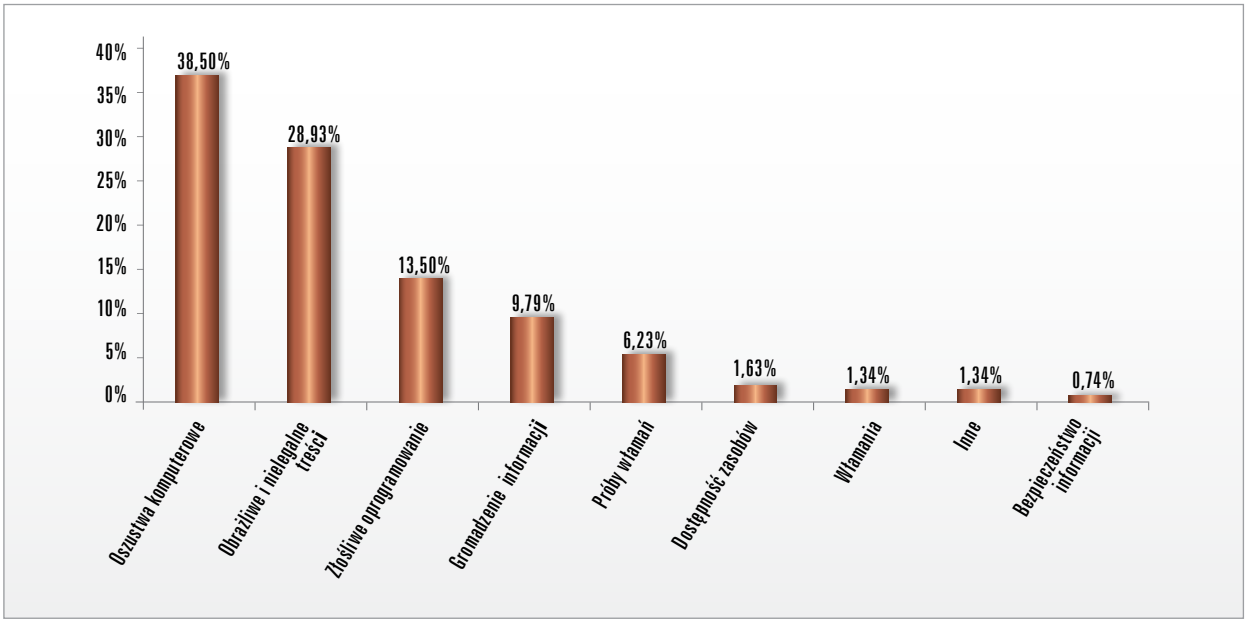
[5] *Wszelkie zgłoszenia dotyczące nielegalnych treści w rozumieniu polskiego prawa, kierowane są do zespołu Dyżurnet.pl, również działającego w ramach NASK (http://www.dyzurnet.pl/)*

4. Statystyka incydentów obsłużonych przez CERT Polska

Włamania	2	9	1,34 %
Włamanie na konto uprzywilejowane	1		
Włamanie na konto zwykłe	3		
Włamanie do aplikacji	3		
Atak na dostępność zasobów	0	11	1,63 %
Atak blokujący serwis (DoS)	1		
Rozproszony atak blokujący serwis (DDoS)	10		
Sabotaż komputerowy	0		
Atak na bezpieczeństwo informacji	0	5	0,74 %
Nieuprawniony dostęp do informacji	5		
Nieuprawniona zmiana informacji	0		
Oszustwa komputerowe	3	246	36,50 %
Nieuprawnione wykorzystanie zasobów	1		
Naruszenie praw autorskich	1		
Kradzież tożsamości, podszycie się (w tym Phishing)	241		
Inne	9	9	1,34 %
Suma	674	674	100 %

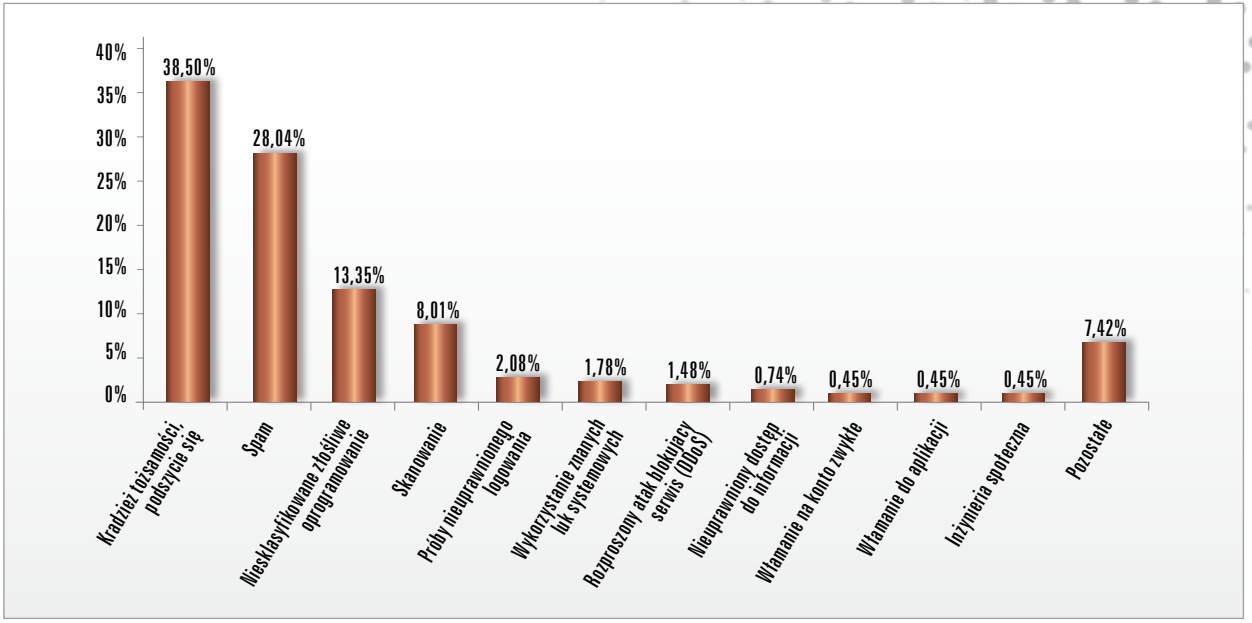
4.3 Typy odnotowanych ataków

Przedstawione wykresy prezentują rozkład procentowy typów i podtypów incydentów.



Wykres 4.3.1. Rozkład procentowy typów incydentów

4. Statystyka incydentów obsłużonych przez CERT Polska



Wykres 4.3.2. Rozkład procentowy podtypów incydentów

W roku 2010 najczęściej występującym typem incydentów były *Oszustwa komputerowe* (36,50 proc.). Jest to pochodna dużej ilości zgłoszeń dotyczących *Kradzieży tożsamości, podszycia się,* szczególnie tych dotyczących zagranicznych podmiotów. Na drugim miejscu uplasowały się *Obraźliwe i nielegalne treści* (28,93 proc.). W tym przypadku mieliśmy w głównej mierze do czynienia ze zgłoszeniami *Spamu*. W porównaniu do roku poprzedniego nastąpiła zmiana miejsc oraz nieznaczne zwiększenie dystansu pomiędzy nimi. Nadal stanowią one około 2/3 wszystkich zgłoszeń. Trzecim najczęściej zgłaszanym typem incydentów były te dotyczące *Złośliwego oprogramowania* (13,50 proc.).

W przypadku podtypów incydentów najczęściej występowała *Kradzież tożsamości, podszycie się* (35,76 proc.). Praktycznie wszystkie zgłoszone incydenty dotyczyły *Phishingu* umieszczonego na polskich serwerach. Ofiarami były zarówno instytucje finansowe z Polski jak i z zagranicy. 28,04 proc. incydentów dotyczyło *Spamu*. Były to w głównej mierze zgłoszenia pochodzące ze SpamCopa, dotyczące polskich komputerów, które wysyłały niezamówioną ofertę handlową. Tak jak w roku poprzednim występowały spore problemy z zaszeregowaniem złośliwego oprogramowania jako robak, koń trojański itp., w związku z czym stworzyliśmy dodatkowy podtyp, który nazwaliśmy *Nieskla-syfikowane złośliwe oprogramowanie.* Stanowi on 13,35 proc. wszystkich zgłoszonych incydentów.

4.4 Zgłaszający, poszkodowani, atakujący

Na potrzeby statystyki 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. Poniższa tabela przedstawia zbiorcze zestawienie danych dotyczących podmiotów incydentu.

W roku 2010 najczęściej otrzymywaliśmy zgłoszenia *od Innej instytucji ds. bezpieczeństwa* (38,43 proc.). W większości dotyczyły one rozsyłania spamu przez polskich użytkowników i pochodziły ze SpamCopa. W drugiej kolejności odnotowaliśmy zgłoszenia pochodzące od *Firm komercyjnych* (34,27 proc.). Dotyczyły one głównie *Phishingu* i były przesłane przez instytucje finansowe bądź też podmioty je reprezentujące. 18,84 proc. zgłoszeń zostało przekazanych przez zespoły typu CERT

4. Statystyka incydentów obsłużonych przez CERT Polska

Podmiot	Zgłaszajacy	%	Poszkodowany	%	Atakujący	%
Osoba prywatna	39	**5,79**	28	**4,15**	11	**1,63**
CERT[6]	127	**18,84**	0	**0,00**	0	**0,00**
ISP Abuse	0	**0,00**	0	**0,00**	0	**0,00**
Inna instytucja ds. bezpieczeństwa	259	**38,43**	0	**0,00**	0	**0,00**
Firma komercyjna	231	**34,27**	294	**43,62**	0535	**79,38**
Ośrodek badawczy lub edukacyjny	11	**1,63**	13	**1,93**	29	**4,30**
Instytucja niekomercyjna	4	**0,59**	5	**0,74**	5	**0,74**
Jednostka rządowa	1	**0,15**	7	**1,04**	11	**1,63**

Tabela 4.4.1. Rodzaje podmiotów ujętych w klasyfikacji incydentów

(również te pochodzące z systemów automatycznych oraz z systemu ARAKIS). W 45,99 proc. przypadków niemożliwe było ustalenie rodzaju *Poszkodowanego* podmiotu. Były to w głównej mierze zgłoszenia przesyłane przez SpamCopa oraz zespoły reagujące w imieniu osób trzecich. Jest to wynik nieznacznie niższy niż w roku 2009. Aż 43,62 proc. poszkodowanych to *Firmy komercyjne.* Chodzi tutaj o zgłoszenia dotyczące *Phishingu*, gdzie jako poszkodowanego przyjmujemy instytucje finansową. Należy tutaj wyraźnie podkreślić, że w tym szczególnym przypadku występuje wielu innych poszkodowanych, przy czym takie informacje nie są CERT Polska udostępniane.

Aż w 79,38 proc. 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 ostatnie znane ogniwo czyli *Firmę komercyjną.* 12,31 proc. atakujących pozostaje *Nieznanych.* W porównaniu do roku poprzedniego jest prawie o połowę mniej, co nie zmienia faktu, że często nie jesteśmy w stanie zidentyfikować prawdziwego źródła ataku. *Atakujący* ukrywa się za serwerem proxy, botnetem, TOR-em czy przejętą maszyną nieświadomej ofiary.

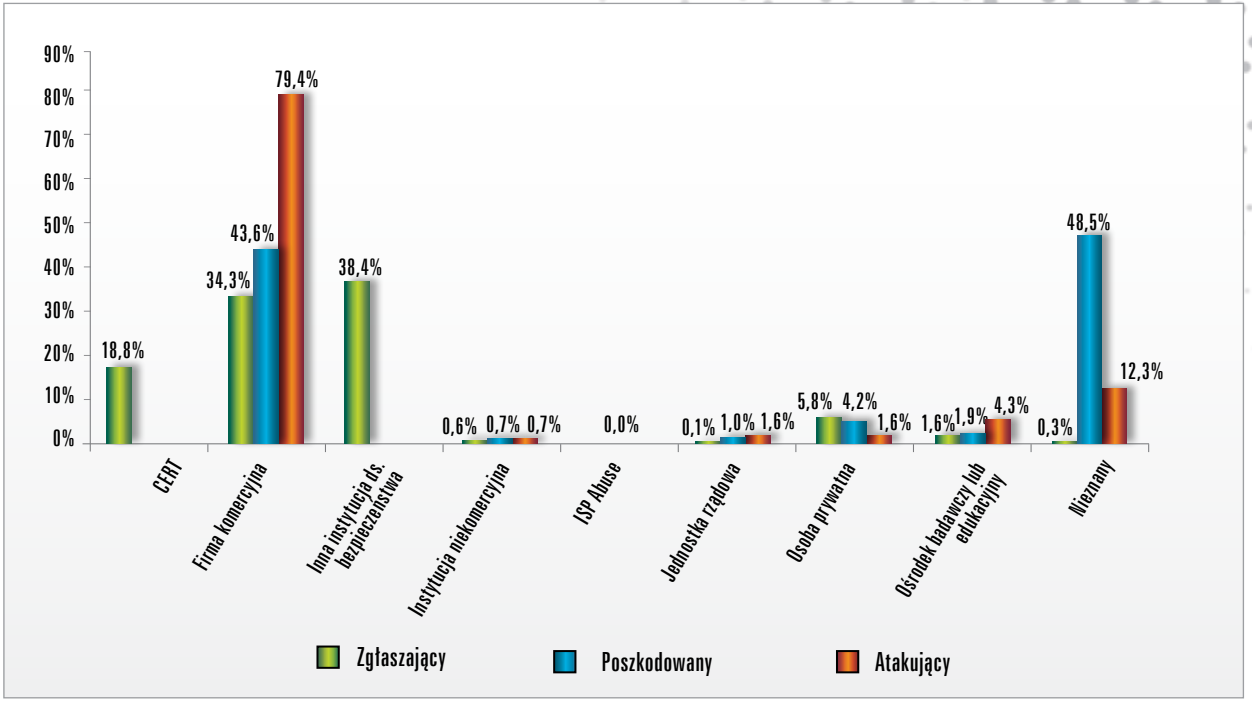
Zgłaszający aż w 76,26 proc. przypadków pochodził z zagranicy, co jest bezpośrednio spowodowane dużą liczbą zgłoszeń *Spamu* ze SpamCopa oraz phishingu dotyczącego zagranicznych podmiotów. 23,59 proc. *Zgłaszających* pochodziło z Polski.

Z tych samych przyczyn co w przypadku rodzaju podmiotu, niemożliwe było określenie kraju pochodzenia dla 45,99 proc. *Poszkodowanych.* 39,91 proc. *Poszkodowanych* pochodziło z zagranicy, co oznacza ponad 13 proc. wzrost w stosunku do roku 2009. Jest to bezpośrednie odzwierciedlenie trendu zwyżkowego dotyczącego *Phishingu* zagranicznych instytucji. 14,09 proc. stanowili *Poszkodowani* pochodzący z Polski.

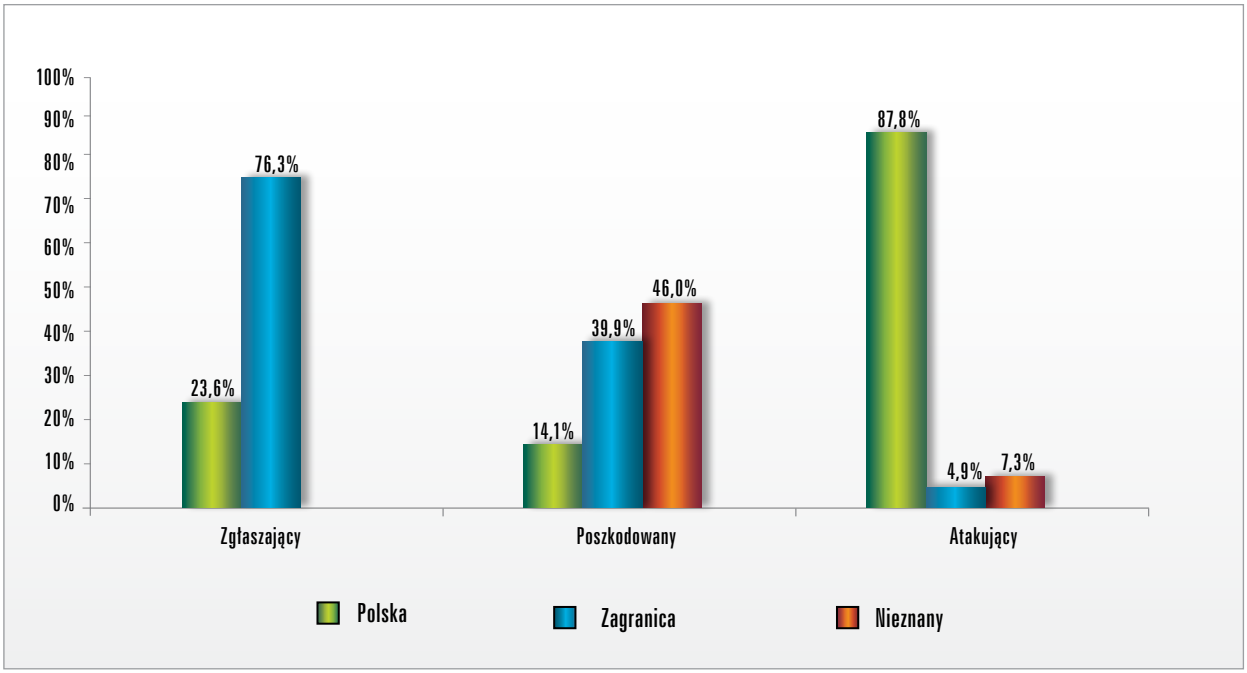
Atakujący w większości pochodził z Polski (87,83 proc.), co jest naturalną konsekwencją obsługi zgłoszeń dotyczących domeny .pl. Sporadycznie zdarzają się incydenty, w których *Atakujący* pochodzi z zagranicy. Są to zazwyczaj sprawy dotyczące phishingu polskich banków. Tylko w 7,3 proc. przypadków umiejscowienie *Atakującego* w kraju lub zagranicą było niemożliwe.

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

4. Statystyka incydentów obsłużonych przez CERT Polska



Wykres 4.4.2. Źródła zgłoszeń, ataków i poszkodowani

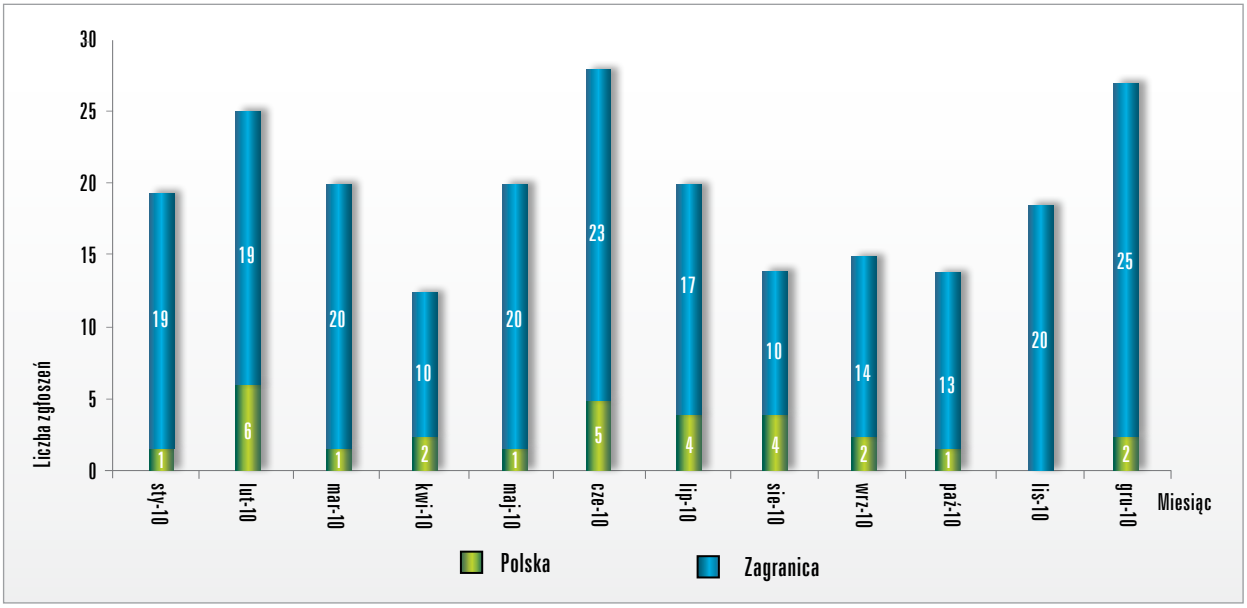


Wykres 4.4.3. Pochodzenie *Zgłaszającego, Poszkodowanego i Atakującego*

5. Statystyki dodatkowe

5.1 Phishing w roku 2010

Poniższy wykres przedstawia liczbę incydentów dotyczących phishingu w poszczególnych miesiącach 2010 r. W odróżnieniu od statystyk zaprezentowanych w rozdziale 3.2, mówimy tu o przypadkach wyłudzania danych dotyczących polskich instytucji (bez względu na metodę i lokalizację serwera lub innych narzędzi), a także takich przypadkach phishingu w polskich sieciach, gdzie niezbędna była interwencja CERT Polska. Zazwyczaj dzieje się tak wtedy, gdy zagraniczny podmiot działający na rzecz instytucji, której dane są wykradane nie jest w stanie skontaktować się z odpowiednim administratorem. Wykres ten pokazuje mniej więcej podział pomiędzy tymi rodzajami incydentów phishingu, dzieląc je ze względu na kraj pochodzenia instytucji będącej celem phishingu na polskie i zagraniczne.



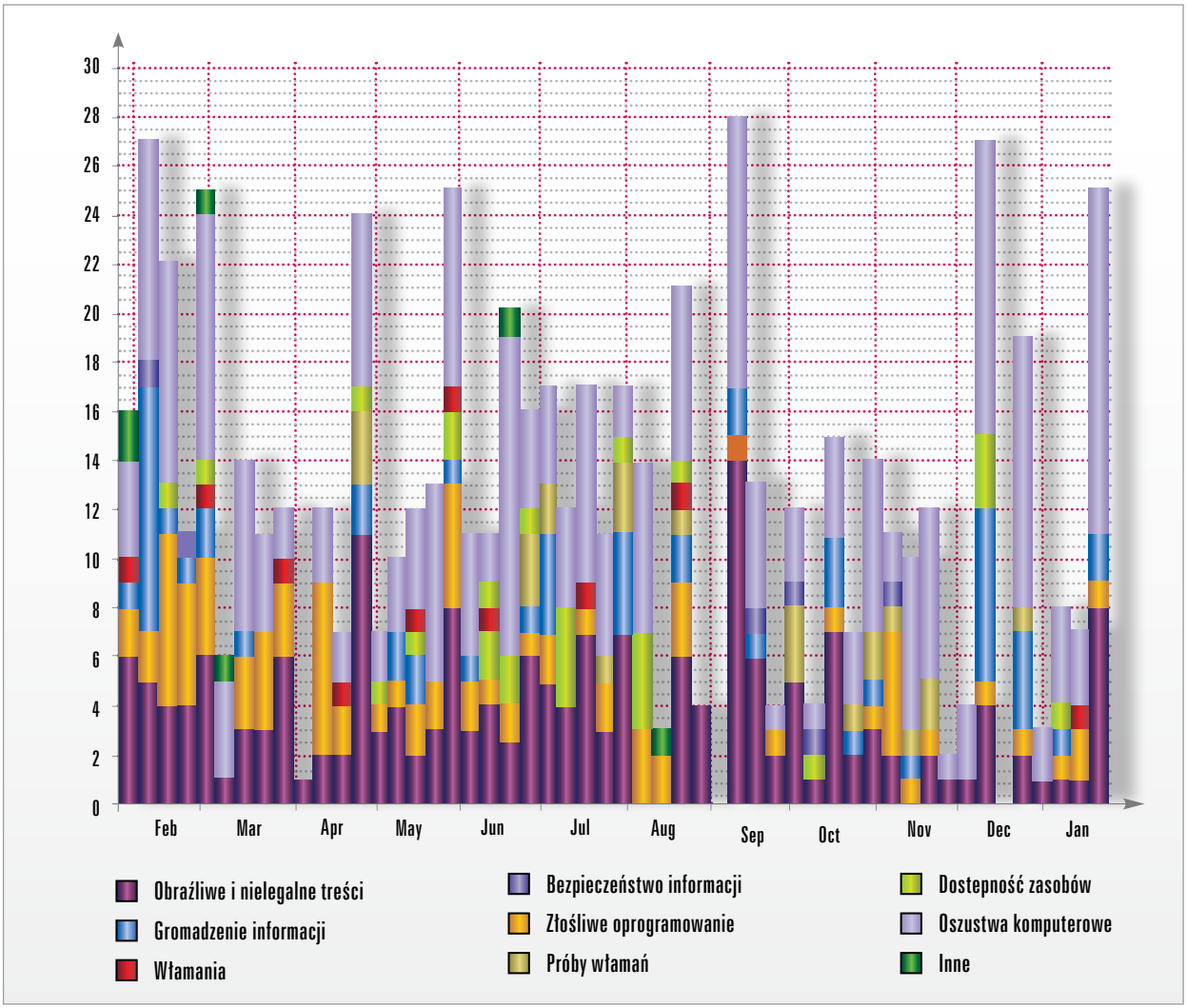
Wykres 5.1.1. Phishing 2010

W większości odnotowanych przypadków phishing dotyczył podmiotów zagranicznych, przy czym fałszywe strony znajdowały się na polskich serwerach. Praktycznie w 100 proc. był to wynik włamania, a cały proceder odbywał się bez wiedzy właściciela serwera. W przypadku phishingu polskich instytucji, fałszywe strony umieszczano na całym świecie, włącznie z Polską. Najwięcej odnotowaliśmy ich w lutym. Dotyczyły one prób wyłudzenia danych klientów polskich banków. Wykorzystano wówczas najstarszą metodę, masowe rozsyłanie w mailu adresów do fałszywych stron. Zgłaszane do nas nadużycia dotyczą zauważonych fałszywych stron. Wiele z nich jest pokłosiem działalności mutacji *Złośliwego oprogramowania* o nazwie Zeus. Należy podkreślić, że zauważone incydenty to tylko „wierzchołek góry lodowej". Najpoważniejsze z nich, za którymi stoi Zeus, dzieją się bezpośrednio na komputerze ofiary i są często zauważone dopiero po wypłynięciu środków z konta lub ich blokadzie przez bankowe mechanizmy wykrywające naruszenia. Więcej danych dotyczących działalności Zeusa znajduje się w p.7.1.

5.2 Liczba incydentów zgłaszanych tygodniowo z podziałem na główne kategorie

Wykres 5.2.1 przedstawia liczbę incydentów zarejestrowanych w okresie tygodnia, z wyszczególnieniem głównych kategorii.

Rejestrowaliśmy od 10 do 28 incydentów tygodniowo. Liczba przypadków dotyczących *Obraźliwych i nielegalnych* treści była bardzo zróżnicowana. Były to w większości przypadki rozsyłania spamu. Począwszy od 4 incydentów w drugim tygodniu marca, a kończąc na 22 w trzecim tygodniu kwietnia. Notowaliśmy dość dużą aktywność na tym polu do połowy września, po czym nastąpił spadek do około 5 incydentów tygodniowo. W pierwszym kwartale notowaliśmy dużą aktywność dotyczącą *Oszustw komputerowych*. Były to zazwyczaj przypadki phishingu, zarówno polskich jak i zagranicznych banków. W ostatnim kwartale liczba tych incydentów nieznacznie zmalała.



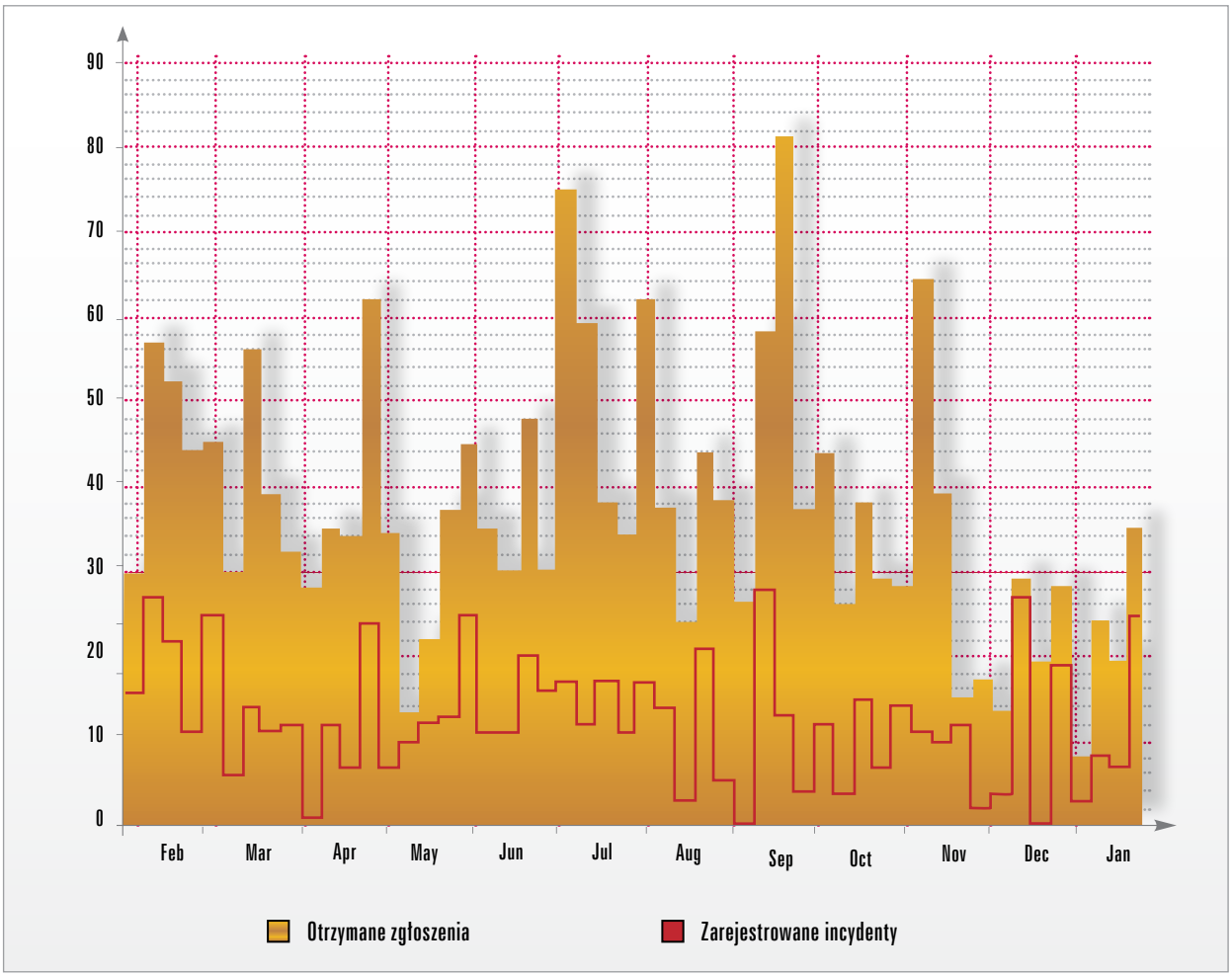
Wykres 5.2.1. Główne kategorie incydentów w 2010 r.

5. Statystyka dodatkowe

5.3 Liczba zgłoszeń a liczba incydentów

Wykres 5.3.1 przedstawia liczbę zgłoszeń w stosunku do liczby incydentów.

Jak można zauważyć, nie każda informacja trafiająca do naszego systemu obsługi jest w rzeczywistości incydentem. Większość odrzuconych przypadków to oczywiście spam. Bardzo często zdarza się, że informacja o incydencie trafia do naszego zespołu z wielu źródeł. Niejednokrotnie otrzymujemy niezależne zgłoszenia tego samego przypadku (np. zainfekowanego komputera będącego źródłem spamu) z automatycznych systemów detekcji oraz od użytkowników indywidualnych. Statystycznie otrzymywaliśmy 2,97 zgłoszenia na jeden incydent.

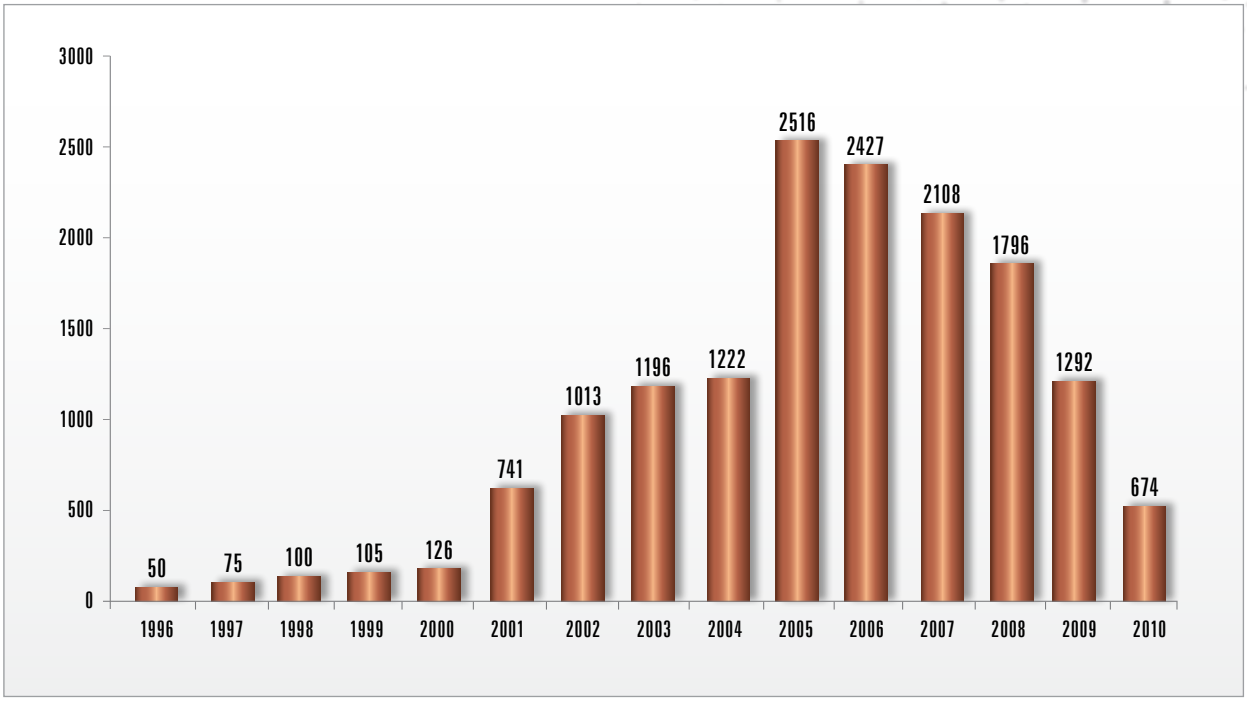


Wykres 5.3.1. Otrzymane zgłoszenia i zarejestrowane incydenty w 2010 r.

6. Trendy w kolejnych latach

6.1 Liczba incydentów w latach 1996 - 2010

Wykres 6.1.1 przedstawia liczbę incydentów w latach 1996 – 2010.



Wykres 6.1.1. Liczba incydentów 1996 - 2010

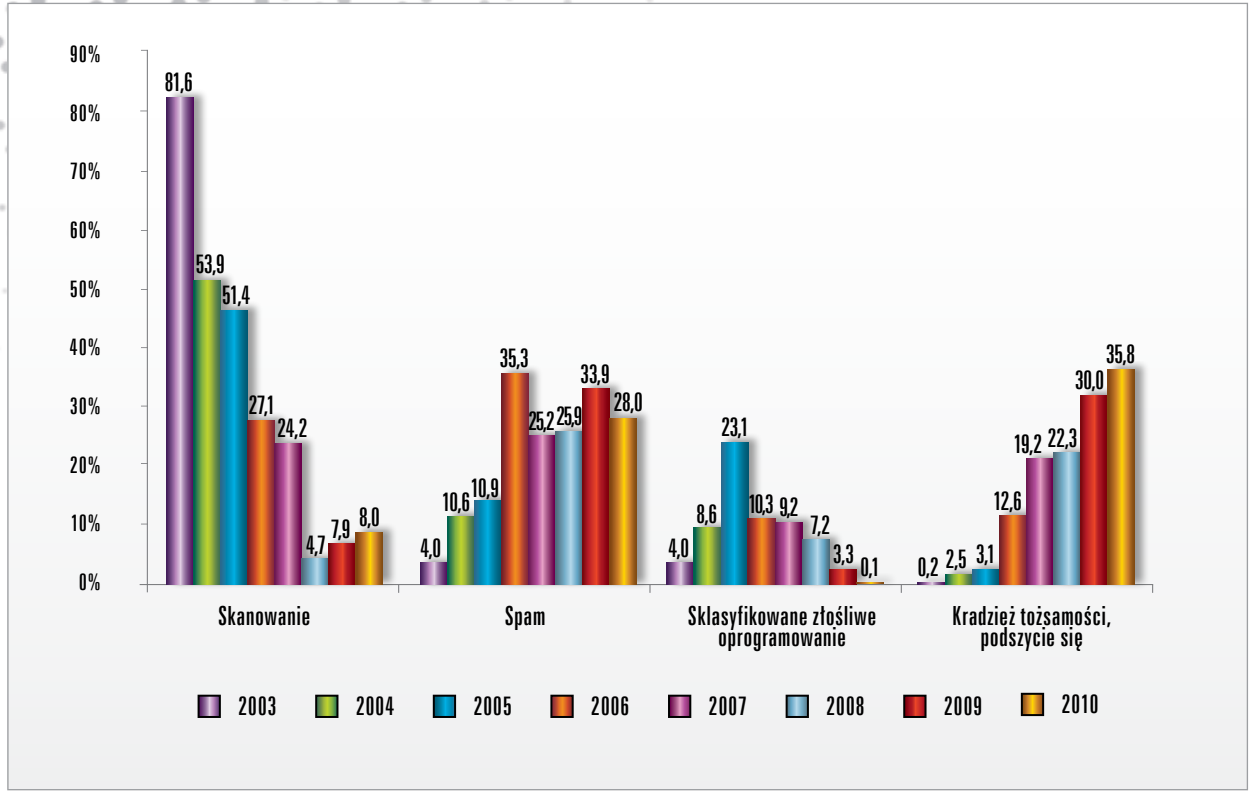
Rok 2010 okazał sie kolejnym, w którym zanotowaliśmy mniejszą liczbę incydentów. Wynika to z wielu przyczyn. Zgłoszenia trafiają coraz częściej bezpośrednio do właściciela sieci a poziom obsługi incydentów przez dużych dostawców Internetu i treści oraz firmy hostingowe, jest z roku na rok wyższy. Nierzadko CERT Polska pełni rolę pomocniczą, działając jako krajowy punkt kontaktowy, przez który informacje są przekazywane (patrz: rozdział 3). Otrzymujemy jednak coraz mniej próśb o interwencję z powodu braku reakcji właściwego zespołu, co jest spowodowane wspomnianym już wzrostem jakości obsługi incydentów u dostawców Internetu. Pojawiające się incydenty są za to coraz poważniejsze i bardziej skomplikowane, np. te dotyczące phishingu, a proces ich obsługi znacznie się wydłużył. Obsługa spraw dotyczących kontrolerów odpowiedzialnych za ataki na użytkowników polskich banków potrafi zająć nawet kilka tygodni.

6.2 Rozkład procentowy podtypów incydentów w latach 2003-2010

Od roku 2003 statystyki są tworzone w oparciu o tę samą klasyfikację. Umożliwia to porównanie rozkładu procentowego incydentów na przestrzeni czasu (patrz wykres 6.2.1).

Rok 2010 nie przyczynił się do znacznej zmiany trendu w żadnej z obserwowanych kategorii. Skanowania utrzymały się na podobnym poziomie co rok temu. W porównaniu do roku 2003 nastąpiła

6. Trendy w kolejnych latach



Wykres 6.2.1. Rozkład procentowy podtypów incydentów w latach 2003 - 2010

marginalizacja tego podtypu. Na taki stan rzeczy mają wpływ głównie dwa czynniki. Po pierwsze do dystrybucji złośliwego oprogramowania wykorzystuje się inne metody, np. złośliwe JavaScripty umieszczone na skompromitowanych stronach WWW. Po drugie *skanowania* na tyle spowszechniały, że są traktowane jako zło konieczne, którego nie da się uniknąć i nie są w związku z tym zgłaszane. O trafności drugiej obserwacji świadczyć może rzeczywista skala obserwowanych (a nie zgłaszanych do obsługi) skanowań, opisana w rozdziale 3.6.

Niezmiennie od 4 lat na wysokim poziomie utrzymuje się odsetek incydentów dotyczących *Spamu* (około 30 proc.). Należy podkreślić, że skala zjawiska jest o wiele większa. CERT Polska odnotowuje tylko zgłoszone przypadki spamu rozsyłanego przez maszyny znajdujące się w obrębie .pl. Dokładniejszą analizę zjawiska spamu z domeny .pl na podstawie automatycznie zgłaszanych (nie obsługiwanych ręcznie) zdarzeń znaleźć można w rozdziale 3.5.

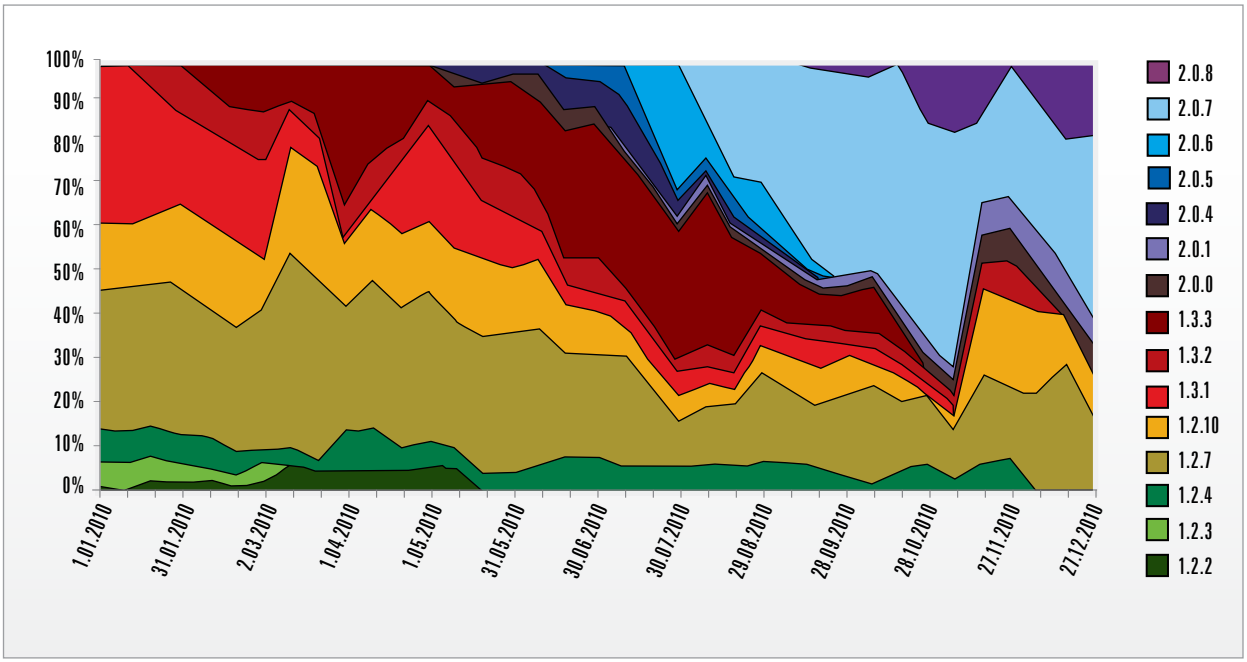
Z roku na rok mamy coraz większy problem z klasyfikacją *Złośliwego oprogramowania*. Trudno jednoznacznie opisać je jako *Wirusa*, *Robaka sieciowego* czy *Konia trojańskiego*, ponieważ zawiera ono w sobie elementy charakterystyczne dla każdego z nich. W takim ujęciu przełomowy był rok 2005, kiedy to praktycznie każdy przypadek był przez nas sklasyfikowany (większość stanowiły *Robaki sieciowe*). Każdy kolejny rok przynosił spadek aż do 0,1 proc. w roku bieżącym.

Od 2003 r. notujemy regularny wzrost incydentów dotyczących *Kradzieży tożsamości*, *podszycia się*. Są to w większości przypadki phishingu. W roku 2010 stanowiły one ponad 1/3 wszystkich incydentów. Dotyczą zarówno instytucji polskich jak i zagranicznych (patrz 5.1.1).

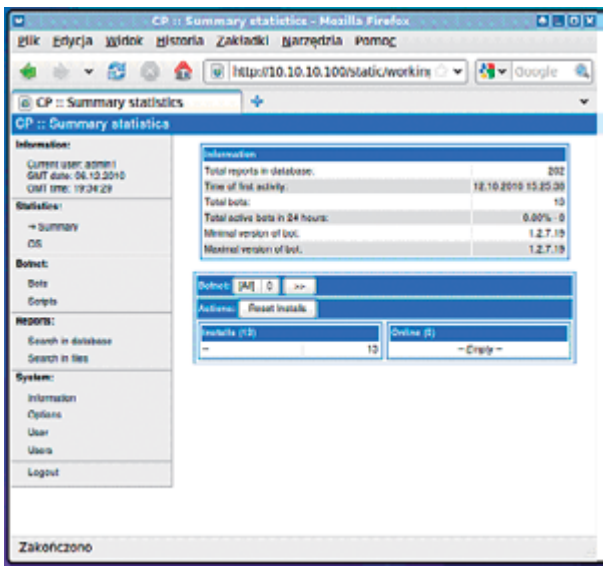
7. Najważniejsze zjawiska okiem CERT Polska

7.1 Rozwój spyware w 2010 roku

Dużym zainteresowaniem na podziemnym rynku malware w 2010 cieszył się Zeus. Jest on klasycznym przykładem oprogramowania typu spyware. Jego funkcjonalność skupia się na śledzeniu działań użytkownika, zbieraniu (podsłuchiwaniu) poufnych danych oraz przesyłaniu ich z zainfekowanego komputera (bota) do centrum zarządzania (C&C). Posiada on również funkcje pozwalające na zmianę treści strony internetowej, wyświetlanej w przeglądarce na zainfekowanym komputerze.



Wykres 7.1.1. Rozbicie „rynku Zeusa" na wersje



Rysunek 7.1.2. Okno główne panelu zarządzającego

Na początku 2010 r. „zeusowy" rynek podzielony był między dwie wersje (1.2 oraz 1.3). Jedną z najpopularniejszych jest wersja 1.2.7. Może być to spowodowane tym, że można ją znaleźć za darmo w sieci. Nowsze wersje wymagają dokonania zakupu na podziemnym rynku. Na początku lata zaobserwowano pojawienie się pierwszych instancji sygnowanych wersją 2.0. Na przełomie lipca i sierpnia można było zaobserwować silną ekspansję wersji 2.0.7, która do końca roku niechlubnie cieszyła się największą „popularnością". Na wykresie 7.1.1 widać, że przestępcy dość szybko aktualizują wykorzystywane wersje złośliwego oprogramowania. Anomalię w październiku można skorelować z aresztowaniem przez FBI osób związanych z zeusem.

7. Najważniejsze zjawiska okiem CERT Polska

Zeus nie posiada zaimplementowanych mechanizmów infekowania i rozprzestrzeniania się. Na komputerze ofiary musi zostać zainstalowany przez „pomocnicze" oprogramowanie zwane często „dropper". Po zainstalowaniu ukrywa swoją obecność w systemie poprzez utworzenie nowych wątków oraz wstrzyknięcie swojego kodu do jednego z procesów systemowych.

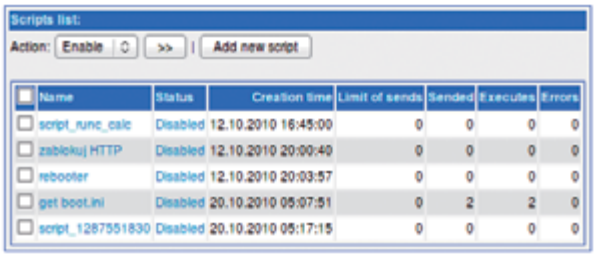
Zainfekowany komputer pobiera nowe pliki konfiguracyjne oraz komunikuje się z C&C poprzez wysyłanie żądań HTTP (podobnie jak przeglądarka internetowa). Treść komunikacji szyfrowana jest algorytmem RC4. Algorytm ten wykorzystuje 256 - bajtowy klucz, co stanowczo wyklucza możliwość monitorowania oraz dekodowania komunikacji metodą brute-force. Plik konfiguracyjny zeusa może zawierać między innymi:

- adres URL do nowej wersji malware
- adresy URL do plików konfiguracyjnych
- hasło-klucz do botnetu
- adresy stron internetowych oraz opis akcji podejmowanych dla każdej z osobna
- wartości interwałów czasowych między komunikacją z C&C

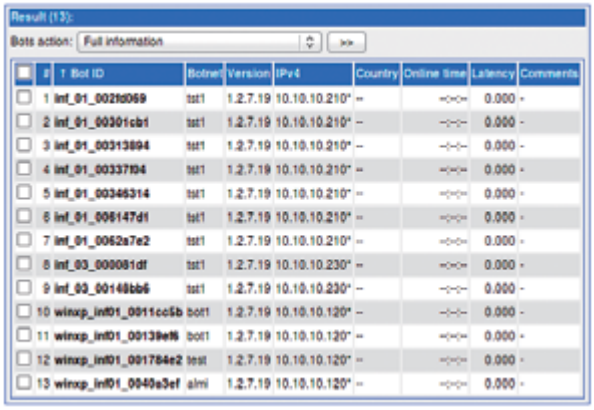
Podczas komunikacji z C&C, bot wysyła raport ze swojej aktywności. Raport taki zawiera wszystkie podsłuchane dane (loginy, hasła i inne) oraz informacje na temat komputera ofiary (np.: wersja systemu operacyjnego). W odpowiedzi bot może otrzymać zestaw poleceń do wykonania, takich jak:

- ponowne uruchomienie komputera
- wysłanie dowolnego pliku z komputera ofiary do C&C
- pobranie dowolnego pliku z Internetu na komputer ofiary
- uruchomienie dowolnego programu
- zabicie systemu operacyjnego

Zarządzanie botnetem opartym na Zeusie odbywa się przy pomocy panelu napisanego w języku PHP. Podczas konfiguracji panelu istnieje możliwość wybrania, czy zbierane dane mają być zapisywane w bazie danych (MySQL) czy też w zwykłych plikach. Po zalogowaniu do panelu, atakujący ma możliwość przeglądania statystyk dotyczących funkcjonowania botnetu, takich jak ilość aktualnie

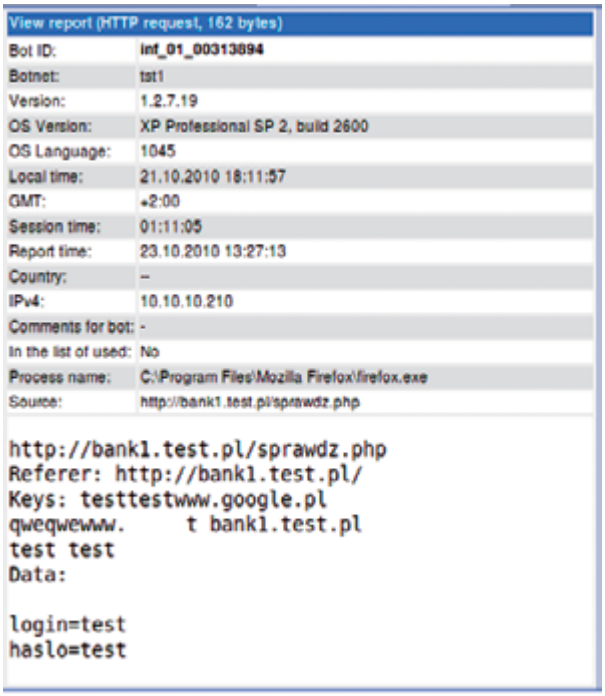


Rysunek 7.1.3. Panel zarządzania skryptami



Rysunek 7.1.4. Lista zainfekowanych komputerów

aktywnych botów, ilość komputerów w sieciach lokalnych czy wersje zainfekowanych systemów operacyjnych. Znajduje się tam również formularz umożliwiający przeszukiwanie zebranych danych po dacie, bądź dowolnym słowie kluczowym. Przykładowy raport przedstawia rysunek 7.1.5.



Rysunek 7.1.5. Przykładowy raport Zeusa

Jedną z ciekawszych, innowacyjnych funkcji Zeusa, jest możliwość robienia zrzutów ekranu dla wybranej strony internetowej. Zrzut wykonywany jest za każdym razem, kiedy po otwarciu określonego adresu internetowego użytkownik zainfekowanego komputera kliknie myszką. Pozwala to przechwytywać poufne informacje nawet w przypadku wykorzystania mechanizmu klawiatury ekranowej. Rysunek 7.1.6 przedstawia przykładowy zrzut ekranu wykonany podczas wpisywania hasła na testowej stronie.

Rysunek 7.1.6. Zrzut ekranu podczas korzystania z klawiatury ekranowej

Pod koniec 2010 r. (głównie w związku z aresztowaniami przeprowadzonymi przez FBI) popularność zaczął zyskiwać główny konkurent Zeusa - SpyEye. Oprogramowanie to w swoim działaniu jest bardzo podobne do Zeusa - komunikuje się ono przez protokół HTTP, pobiera konfigurację, wysyła zebrane dane do C&C. Rzeczą która zwróciła uwagę podczas analizy SpyEye, jest możliwość wykrycia oraz usunięcia Zeusa na zainfekowanym komputerze. Jest to dość innowacyjna metoda na pozbycie się niechcianej konkurencji.

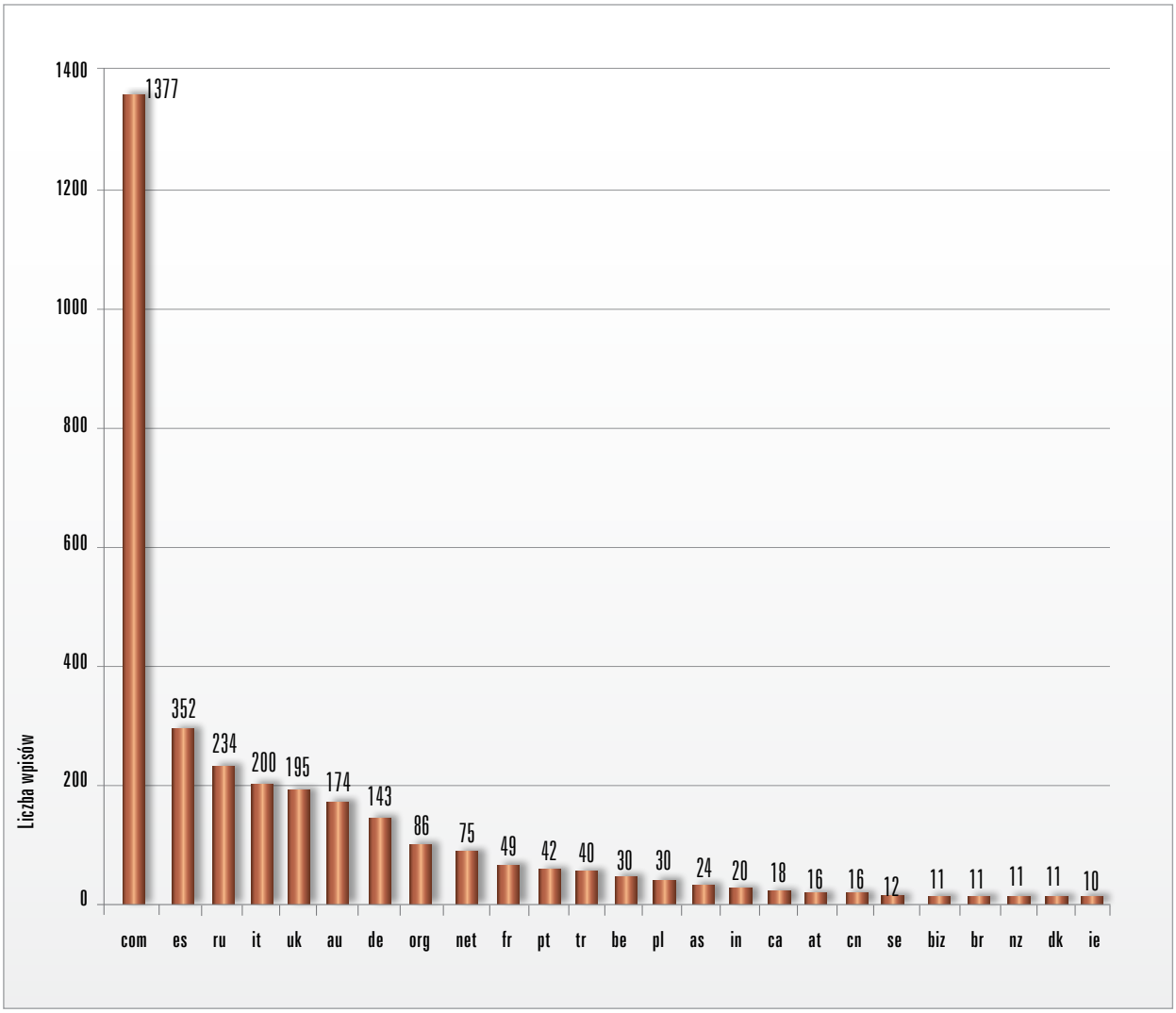
Zimą na forach internetowych pojawiły się informacje o połączeniu Zeusa oraz SpyEye i pracach nad nowym (ulepszonym) złośliwym oprogramowaniem. Jest to chyba najlepszy dowód na to, że spyware cieszy się dużym zainteresowaniem na podziemnym rynku. Zapowiada się, że w nadchodzącym roku będziemy mogli zaobserwować pojawienie się nowych rodzajów oprogramowania, którego jedynym celem jest inwigilacja użytkowników.

Rysunek 7.1.7. SpyEye - konfiguracja oraz budowa bota

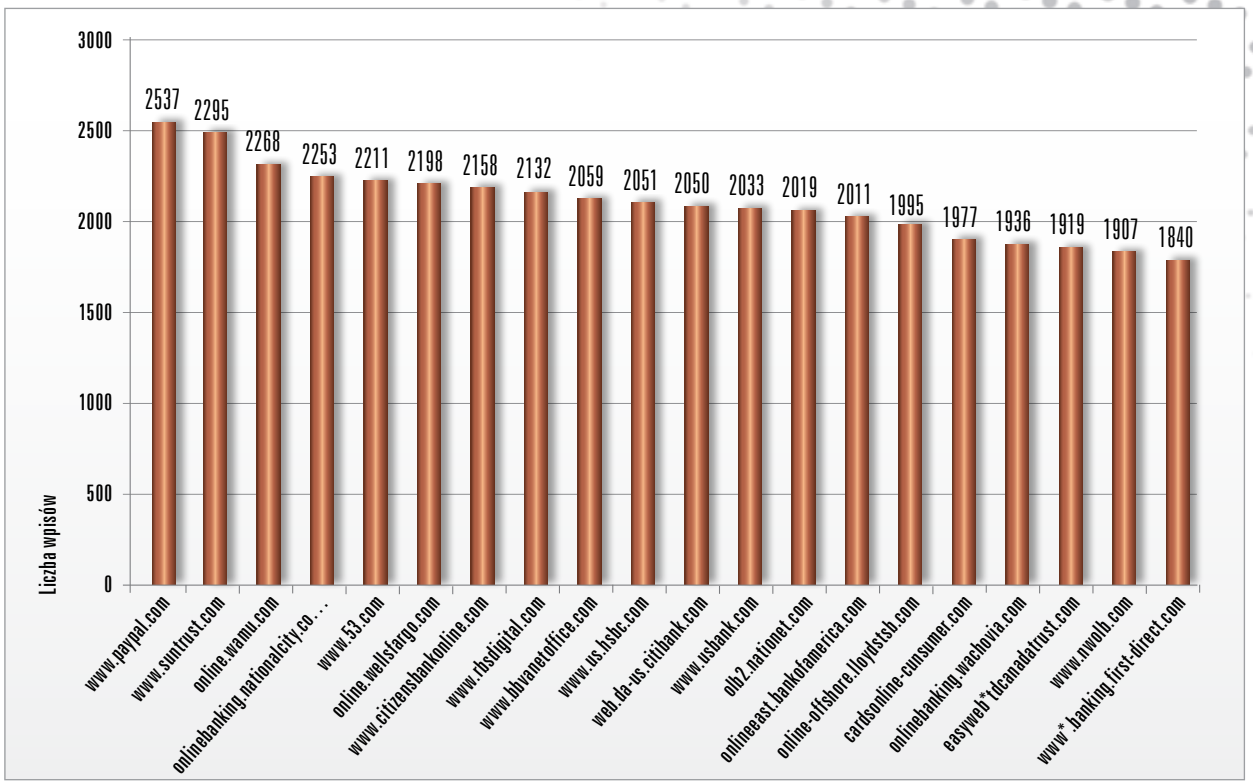
7. Najważniejsze zjawiska okiem CERT Polska

7.2 Zeus - statystyki

Zespół CERT Polska dokonał analizy działalności Zeusa na przestrzeni dwóch ostatnich lat. Statystyki opracowano na podstawie bazy zawierającej ponad 7 tysięcy plików konfiguracyjnych. Dotyczą one okresu od stycznia 2009 r. do października 2010 r. Definicje ataków znalezione w plikach konfiguracyjnych dotyczą blisko 100 państw. Zawierają około 3 tysięcy unikalnych wpisów dotyczących atakowanych instytucji. Fakt wystąpienia danej domeny w pliku konfiguracyjnym świadczy o przygotowywanym ataku, polegającym na modyfikacji stron znajdujących się w tej domenie podczas wyświetlania ich na zainfekowanym komputerze. Liczba wystąpień domeny to swoisty wskaźnik „popularności", mówiący o tym, jak często była ona uwzględniana w konkretnych mutacjach Zeusa. Może on być związany z popularnością konkretnego serwisu, ukierunkowaniem przestępców na szczególny rodzaj stosowanych rozwiązań bądź na szczególny rodzaj klientów. Może być także związany ze szczególną aktywnością przestępców w konkretnych krajach. Nie jest to więc w żadnym

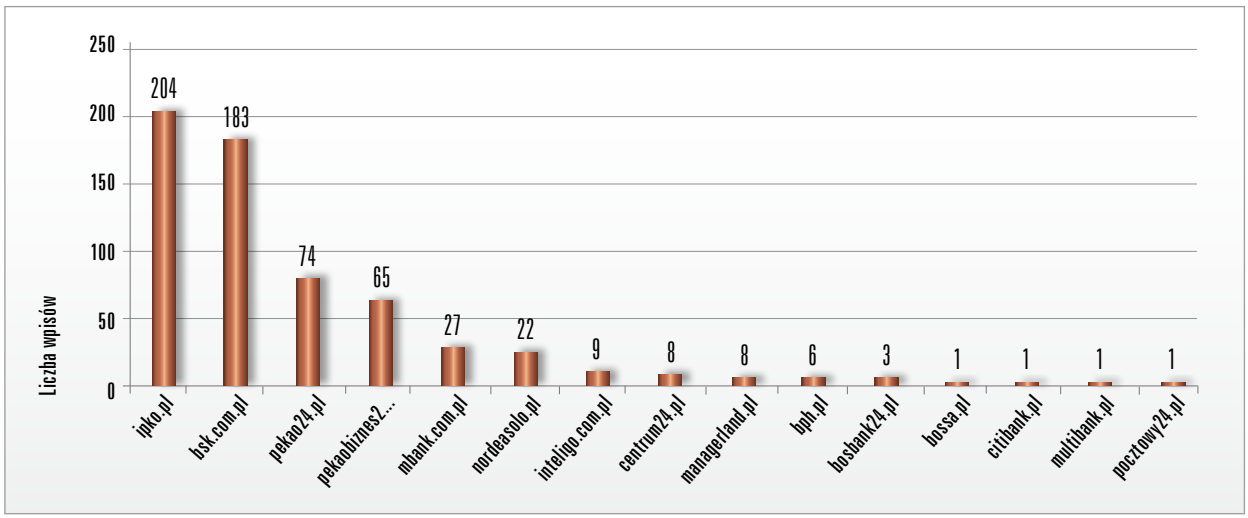


Wykres 7.2.1. Liczba unikalnych wpisów dla poszczególnych krajów



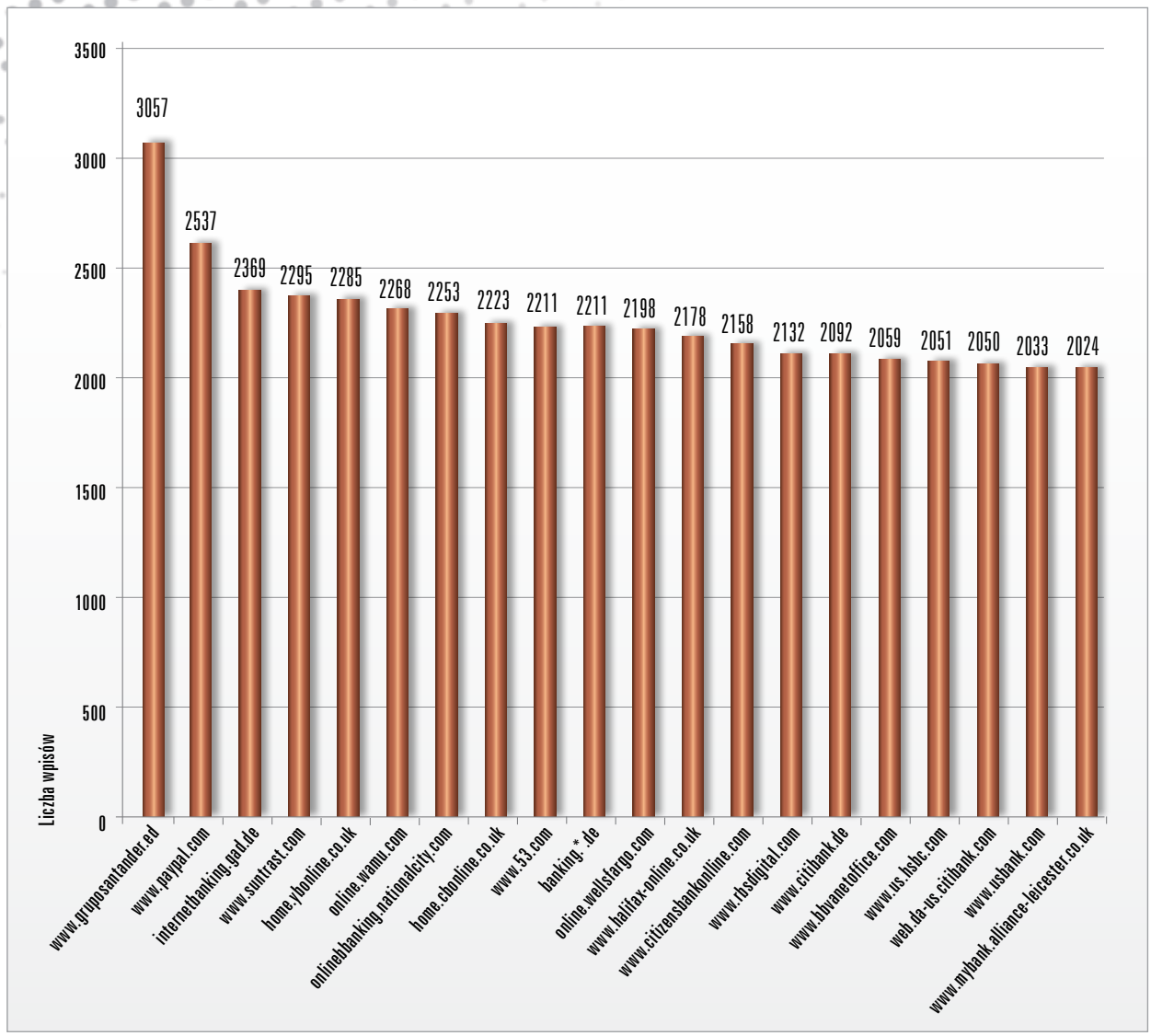
Wykres 7.2.2. TOP 20 unikalnych wpisów dla domeny .com

wypadku wyznacznik większej podatności, słabości zabezpieczeń czy też skuteczności działania Zeusa w tej domenie. Najczęściej pojawiającą się w konfiguracjach domeną jest .com, aż 1 z 377 unikalnych wpisów. W większości są to ataki na amerykańskie podmioty. Na drugim miejscu znajdują się serwisy hiszpańskie (352 unikalne wpisy). Następnie w kolejności pojawiają się instytucje rosyjskie, włoskie, brytyjskie, australijskie oraz niemieckie. Szczególnie częste występowanie tych domen może wskazywać na to, że wielu z przestępców korzystających z Zeusa związanych jest z tymi krajami lub przynajmniej korzysta z „usług" środowisk przestępczych w tych krajach. Przygotowanie ata-



Wykres.7.2.3. Polskie serwisy w plikach konfiguracyjnych

7. Najważniejsze zjawiska okiem CERT Polska



Wykres 7.2.4. TOP 20 wpisów w plikach konfiguracyjnych Zeus

ku na konkretną witrynę wymaga bowiem dobrego jej rozpoznania zarówno od strony funkcjonalnej jak i technicznej. W plikach konfiguracyjnych znalazło się 30 unikalnych wpisów dotyczących domeny .pl (13 miejsce).

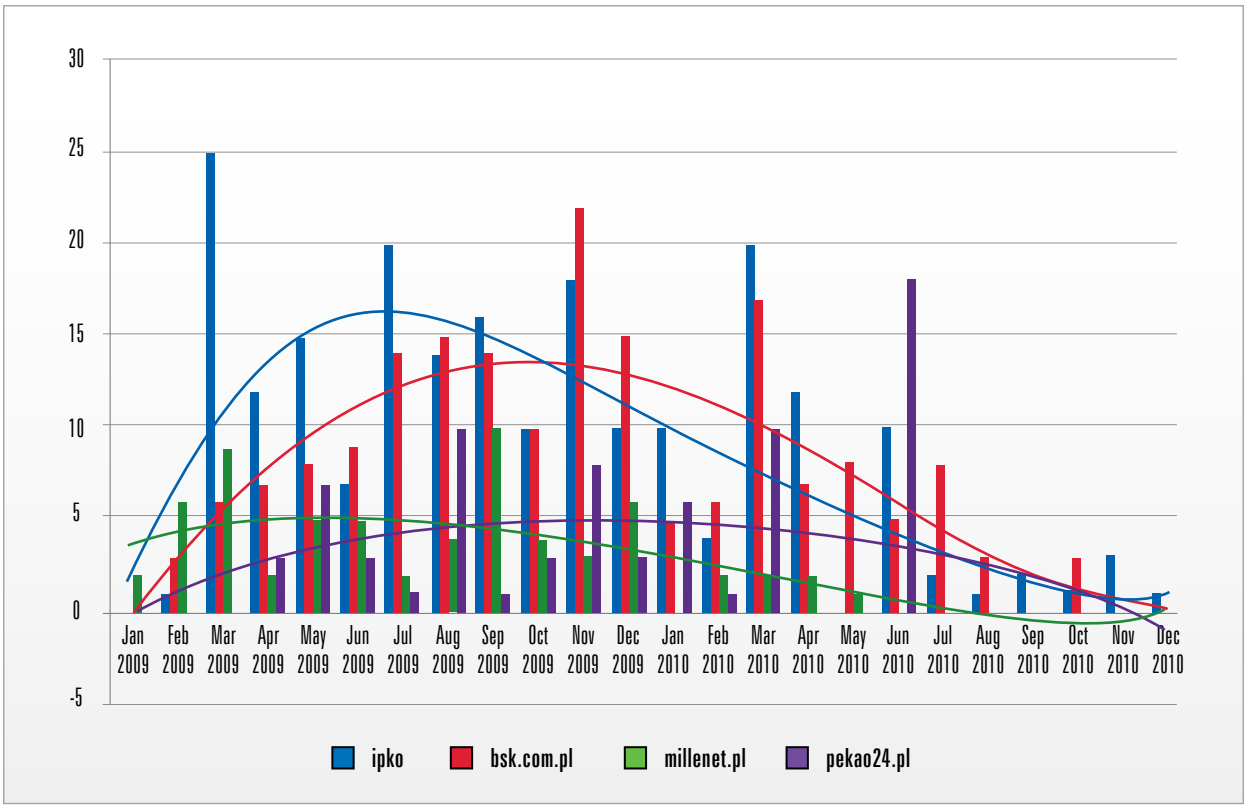
Podmiotem najpopularniejszym pod względem wpisów w konfiguracjach Zeusa wśród domen .com jest PayPal. Dotyczące go wpisy pojawiły się w 2 537 plikach konfiguracyjnych. Zainteresowanie PayPalem wśród przestępców korzystających z Zeusa jest zgodne z obserwowanym zainteresowaniem tym serwisem w klasycznych przypadkach phishingu (zob. rozdział 3.2). Wszystkie instytucje które znalazły się w „.com – TOP 20" znajdują się w USA.

Najczęściej występującą instytucją spośród wszystkich, które znaleźliśmy w konfiguracjach Zeusa, jest hiszpański bank Santander. Zliczono 3057 przypadków dotyczących tego podmiotu, aż o ok. 500 więcej niż w przypadku drugiego poszkodowanego PayPal. Wśród 20 najczęściej atakowanych znajdują się instytucje z Hiszpanii, USA, Niemiec oraz Wielkiej Brytanii.

7. Najważniejsze zjawiska okiem CERT Polska

Wśród polskich serwisów, którymi interesowali się przestępcy korzystający z Zeusa najczęściej pojawiały się dwa: ipko.pl, będący własnością PKO BP oraz należący do ING Banku Śląskiego bsk.com.pl. Obydwa znalazły się w blisko 200 plikach konfiguracyjnych. Kolejne pozycje, z istotnie mniejszą liczbą wpisów w plikach konfiguracyjnych zajęły: serwis internetowy Pekao SA - pekao24.pl i millenet.pl, czyli bankowość elektroniczna Millenium. W sumie w plikach konfiguracyjnych Zeusa znaleźliśmy wpisy dotyczące 16 polskich instytucji.

W ostatnim okresie notuje się mniejszą liczbę wpisów dotyczących polskich instytucji. Nie oznacza to bynajmniej mniejszej aktywności przestępców czy liczby incydentów. Po pierwsze zmianie uległy mechanizmy wykradania danych. Fałszywe strony są generowane bezpośrednio na komputerze ofiary, co eliminuje serwer zewnętrzny, który był słabym ogniwem w całym procederze. Nie ma w związku z tym konieczności generowania nowych plików konfiguracyjnych po zamknięciu takiego serwera. Po drugie serwery zarządzające, hostujące pliki konfiguracyjne oraz zbierające wykradzione dane, są umieszczane w tzw. bulletproof hostingu, gdzie nie można ich zablokować. Jeden plik konfiguracyjny jest wykorzystywany przez stosunkowo długi okres czasu.



Wykres 7.2.5. Polskie instytucje I 2009 - XII 2010

7. Najważniejsze zjawiska okiem CERT Polska

7.3 Stuxnet – pierwszy znany robak atakujący instalacje przemysłowe

Stuxnet jest robakiem internetowym atakującym systemy Windows. Po raz pierwszy wykryty został przez białoruską firmę antywirusową VirusBlokAda w czerwcu 2010 r. pod nazwą RootkitTmpHider. Robak posiada wiele charakterystycznych cech. Jego wyróżnieniem jest jednak obiekt ataku – to pierwszy znany robak, który został napisany w celu włamywania się, obserwacji i przejmowania kontroli nad systemami przemysłowymi sterującymi pracą maszyn, wykorzystywanych np. do kierowania pracą pomp, silników, zaworów itp. w elektrowni, rafinerii czy fabryce.

Uzyskanie dostępu do systemu sterującego pracą maszyn w sposób bezpośredni nie jest łatwy – najlepiej dotrzeć do niego przez systemy pośredniczące. Pierwszym działaniem robaka jest więc udane włamanie się do systemu Windows, licząc na to, że system będzie podłączony do instalacji przemysłowej. Atak następuje na kilka sposobów, w tym:

- poprzez zainfekowane podręczne pamięci USB, które muszą być fizycznie włożone do komputera ofiary, a następnie automatyczne uruchomienie robaka przez wykorzystani luki typu 0-day umożliwiającej automatyczne uruchamianie plików na skutek niepoprawnej obsługi skrótów LNK/PIF (Microsoft Windows Shortcut ‚LNK/PIF' Files Automatic File Execution Vulnerability - CVE-2010-2568),

- poprzez sieć lokalną korzystając ze zdalnej luki 0-day w usłudze buforującej drukowanie (Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability - CVE-2010-2729) umożliwiającej uzyskanie przywilejów na poziomie SYSTEM,

- poprzez wykorzystanie znanej zdalnej luki (Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability -CVE-2008-4250) umożliwiającej uzyskanie przywilejów na poziomie SYSTEM,

- poprzez wykorzystanie dwóch innych lokalnych luk 0-day umożliwiających podniesienie uprawnień opisanych w Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege – MS10-073, CVE-2010-2743 oraz Vulnerability in Task Scheduler Could Allow Elevation of Privilege –MS10-092, CVE-2010-3338.

Wykorzystanie czterech luk typu 0-day w robaku internetowym jest niespotykane. Luki tego typu uchodzą za niezwykle cenne, gdyż znacznie poszerzają możliwości ofensywne, dając dostęp do większej grupy potencjalnych ofiar, w tym tych dobrze chronionych. Wykorzystanie nieznanych wcześniej luk w robaku oznacza ich szybkie „spalenie". Rzadko więc zdarza się wykorzystanie nawet jednej tego typu luki w robaku. Stuxnet posiada funkcjonalność rootkita. Sterowniki instalowane przez Stuxneta są podpisane dwoma skompromitowanymi certyfikatymi wykradzionymi z firm na Tajwanie, utrudniając tym samym rozpoznanie go jako złośliwego oprogramowania.

Po udanym dostaniu się do systemu, Stuxnet wyszukuje i podmienia bibliotekę należącą do oprogramowania SIMATIC WinCC/Step 7 firmy Siemens. WinCC jest oprogramowaniem typu SCADA (ang. Supervisory Control and Data Acquisition) nadzorującym przebieg procesu technologicznego. Podmiana biblioteki s7otbxdx.dll umożliwia Stuxnetowi przechwycenie komunikacji pomiędzy układem programującym (systemem Windows z WinCC/Step 7) a układem PLC (ang. Programmable Logic Controller) przeznaczonym do sterowania procesem technologicznym. Nowa, złośliwa biblioteka zezwala również na przeprogramowanie sterownika a także ukrycie faktu infekcji PLC.

Stuxnet starannie dobiera sterowniki PLC, które chce przeprogramować. Atakowane są tylko systemy, do których podpięte są napędy o zmiennej częstotliwości (ang. variable frequency drives - urządzenia wykorzystywane do sterowania pręd-

kością innych urządzeń, np. do sterowania prędkością silnika, gdzie wzrost częstotliwości oznacza zwiększenie jego szybkości, spadek zaś jego zmniejszenie) dwóch konkretnych producentów – Vacon z Finlandii oraz Fararo Paya z Iranu. Monitorowane są również zakresy częstotliwości działania silników, które podpięte są do sterowników – atakowane są jedynie te działające w określonym zakresie (od 807 do 1210 Hz). Zainfekowane PLC są tak przeprogramowywane aby od czasu do czasu zmieniać częstotliwość kręcenia się silników poza ich normalne parametry pracy – a co za tym idzie, potencjalnie uszkadzając je lub inne komponenty przez nie sterowane. Urządzenia taki mogą być wykorzystywane między innymi do sterowania szybkością wirówek np. służących do wzbogacania uranu.

Chociaż działania Stuxneta były z góry zaprogramowane, robak mimo wszystko posiadał mechanizmy aktualizacji, zarówno przez sieć P2P jak i bezpośrednio przez węzły C&C – działające w Internecie. Być może więc twórcy robaka przyjęli założenie, że sieci przemysłowe również – wbrew częstym zapewnieniom – mogą mieć dostęp do Internetu. Po identyfikacji węzłów C&C możliwe stało się ich przejęcie i monitorowanie. Monitoring pozwolił na zebranie statystyk infekcji – które, według Symanteca na początku października 2010 wynosiły około 100 tysięcy komputerów, z czego większość – ponad 60 proc. znajdowały się w Iranie (drugie w kolejności były Indie, z kilkunastoma procentami).

Ponieważ większość zainfekowanych maszyn znajduje się w Iranie, w mediach pojawiły się spekulację, że Stuxnet został stworzony przez Izrael z myślą o zaatakowaniu irańskich reaktorów atomowych, w celu powstrzymania lub opóźnienia irańskiego programu nuklearnego. Spekulacje te zostały podsycone pojawiającymi się doniesieniami mediów o kłopotach w elektrowniach w Iranie, w tym uszkodzeniach wirówek, wypowiedziach wysokich przedstawicieli rządu irańskiego o problemach z wirusami, a nawet o zabójstwie naukowca irańskiego pracującego przy programie. Doniesienia sugerują, że atak Stuxneta nie jest jednorazowy, ale wręcz długofalowy. Spekuluje się, że pierwotnie robak mógł się dostać do wewnętrznych sieci w elektrowniach za pośrednictwem zainfekowanych laptopów należących do pracowników rosyjskiej firmy wykonującej prace kontraktowe.

Wielu ekspertów od bezpieczeństwa sieciowego uważa, że oprogramowanie tak skomplikowane jak Stuxnet mogło zostać stworzone tylko za wsparciem zasobów państwowych. W styczniu 2011 r. w „New York Times" ukazał się artykuł opisujący wyniki śledztwa dziennikarskiego – zdaniem autorów, za stworzeniem Stuxneta stał nie tylko Izrael ale i Stany Zjednoczone[7]. Jeżeli faktycznie tak było i powyższe spekulacje są prawdziwe, Stuxnet to pierwszy zwiastun prawdziwej cyberwojny w historii ludzkości.

CERT Polska nie otrzymał żadnych zgłoszeń dotyczących aktywności robaka w Polsce.

7.4 Ataki na VoIP

Telefonia VoIP (Voice over IP) cieszy się coraz większą popularnością i jest coraz powszechniej wykorzystywana. Niestety, wzrostowi popularności ze strony użytkowników towarzyszy wzrost popularności ze strony cyberprzestępców. Źle zabezpieczone centralki mogą być m.in. źródłem poważnych strat finansowych, ponieważ przestępcy mogą wykorzystywać je do wykonywania połączeń telefonicznych w dowolne miejsce na świecie lub na specjalne dodatkowo płatne numery. Tego typu ataki opisywaliśmy już w roku 2008 na blogu cert.pl. Innym zagrożeniem jest dzwonienie do końcowego numeru z

[7] *http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1*

niezamówionymi ofertami handlowymi (tzw. SPIT: Spam over Internet Telephony). Najprostszą formą ataku jest atak odmowy usługi (DoS), który może sparaliżować sieć telefoniczną np. w całej firmie.

Dane zbierane przez rozproszoną sieć sond systemu ARAKIS potwierdzają, że problem ataków na telefonię IP w polskiej przestrzeni Internetu jest bardzo realny i ciągle się pogłębia. Poniżej przybliżone zostaną obserwacje incydentów, których w drugiej połowie 2010 r. świadkiem był system ARAKIS. Ataki przeprowadzane były z wykorzystaniem protokołu SIP (Session Initiation Protocol).

Protokół SIP w telefonii IP

Jednym z najpowszechniej używanych protokołów w technologii VoIP jest SIP opisany w RFC 3261. Służy on do kontrolowania sesji pomiędzy klientami VoIP, w szczególności do nawiązywania, modyfikowania oraz kończenia połączeń głosowych i wideo. Protokół SIP ma zdefiniowany zestaw metod (żądań). Przyjrzyjmy się bliżej czterem z nich, które wykorzystywane były w obserwowanych przez nas atakach.

- **OPTIONS** – zapytanie o możliwości/funkcjonalności; serwer SIP na tego typu żądanie powinien zwrócić informacje o dostępnych usługach. Często wykorzystywane w masowych skanowaniach do szukania urządzeń VoIP.

- **REGISTER** – tym poleceniem klient rejestruje się w serwerze rejestrującym SIP (tzw. SIP Registrar), który dodaje jego dane do bazy obsługiwanych adresów. SIP Registrar działa podobnie jak serwer DNS: mapuje nazwy SIP-owe (tzw. SIP URI) na adresy IP klientów. Dzięki temu użytkownik zyskuje możliwość odbierania połączeń w konkretnej podsieci (konieczne, gdy telefonia IP pracuje w trybie klient-serwer, a nie peer-to-peer, oraz gdy adres IP klienta jest zmienny lub pochodzi z puli prywatnej, a chce on przyjmować rozmowy spoza sieci lokalnej). Nierzadko zdarza się łączenie różnych funkcji serwerowych SIP w obszarze jednego serwera, przez co dany serwer może pełnić jednocześnie funkcje SIP Registrara oraz SIP Proxy czy SIP Redirecta

- **INVITE** – zaproszenie do nawiązania sesji (lub dołączenia do już istniejącej), skutkuje np. rozpoczęciem połączenia bezpośrednio do klienta VoIP lub przez serwer SIP Proxy. Mówiąc kolokwialnie: rozpoczęcie procesu dzwonienia.

- **CANCEL** – anulowanie poprzedniego żądania wysłanego z danego urządzenia.

Urządzenia korzystające z tego protokołu domyślnie komunikują się na porcie 5060/UDP. Dlatego wszystkie ataki z wykorzystaniem SIP widziane przez system ARAKIS kierowane były tylko na ten port. Poniżej wykres przedstawiający liczbę unikalnych adresów IP łączących się na port 5060/UDP do honeypotów ARAKISa.

Głębszej analizie poddane zostały dane tylko z okresu pięciu dni. Nie oznacza to, że dopiero niedawno pojawiły się te ataki – wzmożony ruch widziany jest na mniej więcej na stałym poziomie cały czas od lipca 2010 r. W ciągu pięciu dni ruch ten:

- widziany był na wszystkich sondach systemu ARAKIS (oznacza to, że celem nie jest konkretna sieć/dostawca usług, ale cała przestrzeń polskiego Internetu);

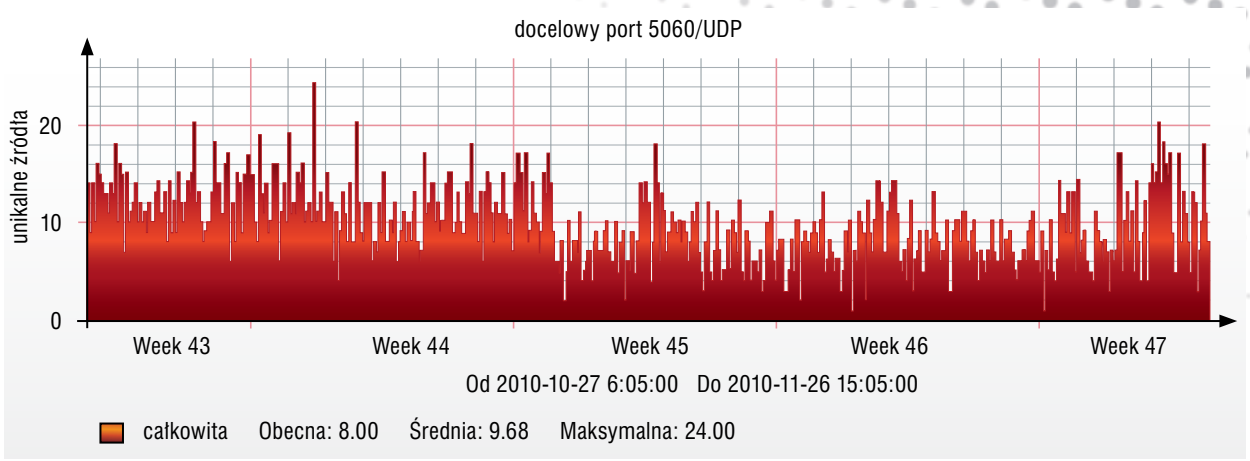
- odbyło się ok. 45 000 połączeń;

- połączenia były nawiązywane z ok. 440 unikalnych adresów IP;

- źródła połączeń należały do ok. 200 różnych systemów autonomicznych (AS)

- źródłowe adresy IP były rozmieszczone w ok. 50 różnych krajach na całym świecie

- najbardziej aktywnymi krajami były (w kolejności malejącej): Chiny (60 proc. unikalnych źródeł ataków), USA (11 proc.) i Francja (5 proc.)



Wykres 7.4.1 Liczba unikalnych adresów IP skanujących port 5060/UDP

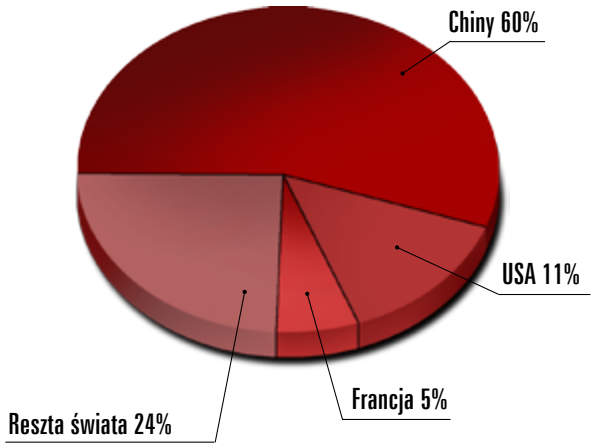
Istnieje prawdopodobieństwo, że źródłowe adresy IP mogą być sfałszowane (UDP spoofing), lecz to nie miałoby sensu, gdyż atakujący nie mógłby poznać odpowiedzi na żądanie SIP. Bardziej realne wydaje się użycie tych adresów IP jako ostatnich spośród łańcuszka kolejnych pośredników (pośrednicy działają jak proxy), by ukryć rzeczywiste źródło ataku. Wobec tego nie możemy postawić tezy, że inicjatorzy ataków znajdują się w krajach wymienionych powyżej.

Pozycja	Państwo
1	Chiny
2	USA
3	Francja
4	Nigeria
5	Niemcy
6	Egipt
7	Rosja
8	Korea
9	Irlandia
10	Rumunia

Tabela 7.4.2 Kraje, z których obserwowano skanowania SIP

Skanowania SIP Options

Najczęściej widziane skanowania SIP w systemie ARAKIS to te z użyciem żądań OPTIONS. W tym wypadku atakujący, jeżeli trafi na serwer SIP który obsłuży to żądanie, pozna jego możliwości. Jest to więc typowy rekonesans. Pozyskane w ten sposób informacje najprawdopodobniej służą do stworzenia listy potencjalnych dostępnych publicznie serwerów SIP wraz z ich możliwościami. Taka lista może posłużyć do dalszych ataków, niosących już konkretne zagrożenie. De facto to żądanie jest obecnie powszechnie wykorzystywane przy masowych poszukiwaniach „na ślepo" urządzeń VoIP – coś jak ping na poziomie protokołu SIP (odpowie tylko aktywne urządzenie). Takie skanowanie jest w miarę dyskretne – nie powoduje na docelowym urządzeniu efektu dzwonienia. Dodatkowo na podstawie odpowiedzi łatwo poznać z jakim oprogramowaniem/producentem urządzenia atakujący ma do czynienia (tzw. fingerprinting), a jak wiadomo każda aplikacja posiada luki (tylko nie zawsze są



Wykres 7.4.3 Udział poszczególnych krajów w skasowaniach SIP obserwowanych w ARAKIS-ie

7. Najważniejsze zjawiska okiem CERT Polska

one odkryte). Wolumen tych skanowań obserwowany przez ARAKIS-a cały czas utrzymuje się na mniej więcej stałym poziomie – w zależności od konfiguracji sondy średnio dziennie widzianych jest od kilkudziesięciu do kilkuset tego typu ataków. Szczegóły pakietów wskazują, że najprawdopodobniej do przeprowadzenia skanowań użyte zostały dwa popularne narzędzia do audytu urządzeń VoIP opartych na protokole SIP: Sipvicious oraz Sundayddr.

Skanowania SIP Register

W sierpniu roku 2010 w honeypotach kilku sond zostały zaobserwowane żądania REGISTER. Atakujący szukał „na ślepo" serwerów typu SIP registrar i próbował się zarejestrować. Nie wiemy do końca co miał na celu ten atak. Prawdopodobnie – gdyby rejestracja się powiodła – mógł w ten sposób uzyskać dostęp do pozostałych klientów zarejestrowanych w tym rejestratorze (atak typu rekonesans). To z kolei pozwala na przeprowadzenie dalszych ataków. Za pomocą odpowiednio spreparowanych żądań REGISTER można także przejmować rejestracje innych klientów (tzw. registration hijacking) co skutkuje przejmowaniem połączeń telefonicznych. Znane są też przypadki „zalewania" urządzenia dużą ilością żądań REGISTER, co skutkuje paraliżem sieci telefonicznej (tzw. REGISTER flooding należący do ataków typu DoS). Informacje zawarte w pakietach sugerują, że do przeprowadzonego skanowania użyto aplikacji eyeBeam, która jest komunikatorem VoIP. Należy jednak pamiętać, że taki nagłówek łatwo można spreparować. Nigdy nie była użyta autoryzacja, więc atak był skierowany na niezabezpieczone rejestratory SIP.

Skanowania SIP INVITE + CANCEL

W połowie listopada 2010 r. w systemie ARAKIS zaobserwowany został znaczący, ponad kilkuset procentowy, wzrost żądań INVITE oraz CANCEL. Poprzez polecenia INVITE atakujący próbował nawiązać połączenie VoIP do docelowego adresu. W rzeczywistym środowisku telefonii IP, gdy taki pakiet trafi do telefonu VoIP, ten powinien zacząć dzwonić. Żądania INVITE mogą być także kierowane do centralek VoIP – gdy urządzenie będzie odpowiednio skonfigurowane (a właściwie błędnie skonfigurowane), połączenie zostanie przekazane dalej (w ten sposób można na czyjś koszt dzwonić na płatne numery). Honeypoty ARAKIS-owe należą do grupy nisko-interaktywnych, przez co żaden nie wszedł w dalszą interakcję z atakującym. Najprawdopodobniej w wyniku braku wspomnianej interakcji atakujący po pewnym czasie przerwał próbę ustanowienia połączenia telefonicznego wysyłając żądanie CANCEL. Najprawdopodobniej użyte było rzeczywiste narzędzie, jakim jest centrala telefoniczna oparta na bardzo popularnym open source-owym oprogramowaniu Asterisk. Próby wywołania połączenia (INVITE) trwały raptem jeden dzień, lecz było ich bardzo dużo – pojedyncza sonda zarejestrowała ich ok. 4 800.

Jak się bronić?

W sytuacji wysokiego stanu zagrożenia zabezpieczenie własnej infrastruktury VoIP jest bardzo ważne. Najlepiej w tym celu zajrzeć do dokumentacji i zaleceń producenta rozwiązań używanych we własnej sieci. Na poziomie ogólnym użytkownikom telefonii IP opartej na SIP możemy zasugerować:

- podczas rejestracji urządzeń VoIP w registrarze SIP używać autoryzacji i uwierzytelniania (wprawdzie nie jest to metoda gwarantująca w stu procentach bezpieczeństwo – przesyłane są skróty MD5 z haseł – jednak lepsze to niż nic)
- skonfigurować centralki i proxy VoIP-owe tak, by nie obsługiwały połączeń telefonicznych inicjowanych przez nieuprawnione adresy IP
- jeżeli to możliwe używać narzędzi, które będą wykrywać i blokować urządzenia, które będą wykazywać cechy skanerów (np. wiele prób wysłania żądań SIP w krótkim przedziale czasu)

7.5 Pliki PDF nadal wykorzystywane jako nośniki złośliwego kodu

Złośliwe oprogramowanie stanowi jedno z największych zagrożeń współczesnego Internetu. Wirusy, konie trojańskie oraz robaki internetowe nie są już tylko pojęciami znanymi wąskiemu gronu specjalistów. Coraz częściej pojawiają się w mediach, przez co trafiają do zbiorowej świadomości użytkowników Internetu. Powoduje to, że oni sami starają się coraz lepiej zabezpieczać przed działaniem tego typu oprogramowania poprzez instalację programów antywirusowych oraz osobistych firewalli. Pozwala to osiągnąć pewien poziom ochrony przed znanymi zagrożeniami, lecz ciągle nie daje gwarancji bezpieczeństwa w przypadku, gdy w sieci pojawiają się nowe, wyróżniające się cechami takimi jak niezwykły dynamizm i polimorfizm. Taką charakterystykę mają złośliwe pliki PDF. Artykuł stara się opisać metody ataków zaobserwowane przez Zespół CERT Polska, które wykorzystują ten rodzaj plików osadzonych na stronach skompromitowanych serwisów WWW.

Charakterystyka ataków

Jednym z najszerzej i najczęściej wykorzystywanych sposobów infekowania komputerów użytkowników jest atak z wykorzystaniem skompromitowanych serwisów WWW. Jest on przeprowadzany poprzez umieszczenie w nich złośliwej treści, najczęściej w postaci zaciemnionego kodu JavaScript. Trudny do interpretacji kod jest umieszczany celowo, aby oszukać silniki antywirusowe, których działanie jest oparte na wykrywaniu złośliwej treści za pomocą dopasowania przez sygnatury. Nawet drobna zmiana w oryginalnym kodzie JavaScript może prowadzić do powstania zupełnie nowej wersji, która nie była do tej pory widziana przez program antywirusowy i nie może być poprawnie zaklasyfikowana. Przykład prezentowany poniżej pokazuje, jak ze zrozumiałej dla każdego linijki kodu otrzymać postać, która na pierwszy rzut oka wykonuje bliżej nieokreślone operacje.

Czytelna linijka kodu JavaScript.

```
document.write(„I am evil!”);
```

Ta sama linijka kodu JavaScript przetworzona przez jeden z publicznie dostępnych pakerów.

```
eval(function(p,a,c,k,e,d)
{e=function(c){return c};if(!’’.
replace(/^/,String)){while(c--)
{d[c]=k[c]||c}k=[function(e){re-
turn d[e]}];e=function(){return’\\
w+’};c=1};while(c--){if(k[c])
{p=p.replace(new RegExp(,\\b’+e-
(c)+’\\b’,’g’),k[c])}}return p}
(,0.1(„2 3 4!”);’,5,5,’document|w-
rite|I|am|evil’.split(,|’),0,{}))
```

Osadzony na skompromitowanej stronie kod JavaScript nie musi być koniecznie złośliwy. W większości przypadków jest to zaciemniony kod, który jedynie przekierowuje użytkownika dalej do kolejnego serwera, który z kolei może go odsyłać także do następnego. Przekierowania mogą się wielokrotnie rozwidlać utrudniając w ten sposób analizę obserwowanego ruchu. Liczba i zawiłość przekierowań zależy wyłącznie od inwencji autora oraz liczby maszyn jaką udało mu się przejąć. Ostatecznie przeglądarka użytkownika trafia na serwer, który ma na celu infekcję komputera złośliwym oprogramowaniem. Sam proces infekcji może przebiegać w różny sposób, który jest zależny od użytej metody. W artykule prezentowany jest proces infekcji z użyciem plików PDF, które są jednym z najpopularniejszych wektorów ataku.

Cała seria przekierowań, jakie się z reguły spotyka w czasie odwiedzin skompromitowanego serwisu, prowadzi przeglądarkę użytkownika do złośliwej strony. Umieszczony na niej kod JavaScript ma za zadanie wykorzystać lukę w przeglądarce lub

zainstalowanych dodatkach. Ogromna większość złośliwych stron WWW stara się wykorzystać luki m.in. właśnie we wtyczce umożliwiającej wyświetlanie treści plików PDF. Po otwarciu złośliwej strony, osadzany jest w niej obiekt odpowiedzialny za uruchomienie odpowiedniej wtyczki oraz pobranie pliku PDF zawierającego tzw. exploit, czyli kod wykorzystujący podatność umożliwiającą wstrzyknięcie dowolnego kodu maszynowego i infekcję maszyny użytkownika. Zdarza się, że w wyniku działania exploita możliwe jest do zaobserwowania chwilowe spowolnienie działania przeglądarki lub zawieszenie się całego programu. Nietypowe zachowanie przeglądarki jest związane z procesem infekcji jaki zachodzi po otwarciu pliku PDF skażonego złośliwym kodem.

Podatności najczęściej opierają się na przepełnieniach buforów, czyli niszczeniu wewnętrznych struktur danych programu oraz przejmowaniu kontroli nad jego wykonaniem. Jest to w większości przypadków proces nieodwracalny i robiony „na ślepo" przez tzw. exploit. Wstrzyknięty kod maszynowy wprawdzie jest wykonywany poprawnie, lecz później powrót do oryginalnej ścieżki wykonania programu jest z reguły niemożliwy i powoduje zawieszenie się aplikacji.

Otwarcie pliku przez wtyczkę powoduje uruchomienie w tle procesu, który przetwarza pobrane dane i ma za zadanie wyświetlić je użytkownikowi. W tym momencie złośliwy kod, wykorzystując lukę, infekuje komputer. Systemy antywirusowe nie zawsze są w stanie zapobiec tego typu działaniom. Wynika to głównie ze sposobu przemycania takiego kodu. Format plików PDF umożliwia zmianę reprezentacji danych w sposób, z którym silnik antywirusowy nie zawsze jest w stanie sobie poradzić. Podobnie jak w przykładzie z kodem JavaScript, gdzie pojedyncza linijka była zamieniana w ciąg, który był dosyć odmienny od oryginału, także format plików PDF umożliwia szeroko pojętą konwersję danych. Opiera się on głównie na użyciu tak zwanych filtrów, które są w stanie odtworzyć oryginalne dane z zakodowanej postaci. Jest kilka dopuszczalnych formatów w jakich mogą być przenoszone dane. Poza standardową formą, która zachowuje dane oryginalne, możliwa jest ich kompresja, zamiana na tekstowy łańcuch kodów heksadecymalnych odpowiadających wartościom kolejnych bajtów oryginału, kodowanie algorytmem Base85, RLE, a nawet szyfrowanie. Ponadto metody te można łączyć w kaskady otrzymując coraz to nowe reprezentacje tych samych danych. Tego typu właściwość nazywa się polimorfizmem, a kod powstały w ten sposób kodem polimorficznym.

W plikach PDF może zostać przemycony kod JavaScript, który będzie uruchomiony automatycznie wraz z otwarciem i wyświetleniem treści. Jest to właściwy kod (exploit), który ma za zadanie wykorzystać podatność w czytniku plików PDF. Wstrzykuje on do pamięci przydzielonej aplikacji złośliwy kod maszynowy, tzw. shellcode, który najczęściej pobiera z Internetu jakiś rodzaj wirusa i instaluje go w systemie operacyjnym użytkownika. W tym momencie proces infekcji dobiega końca, a wykorzystana aplikacja najczęściej przestaje odpowiadać, co wymusza jej ręczne zamknięcie.

Metody obrony

Walka ze złośliwym oprogramowaniem staje się coraz trudniejsza. Dzieje się tak głównie ze względu na ogromną ilość wirusów jakie powstają każdego dnia. Programy antywirusowe mają coraz większe problemy z rozpoznawaniem nowych zagrożeń, których forma jest coraz bardziej złożona i dynamiczna. Pomimo trudności są jednak ciągle pierwszą linią frontu i używanie jednego z nich daje pozytywne rezultaty nawet jeżeli nie wykrywa 100 proc. zagrożeń. Na szczęście istnieją sposoby, aby ograniczyć ryzyko zarażenia komputera.
Jednym z najważniejszych są aktualizacje systemu operacyjnego, a także każdej aplikacji, która komunikuje się z Internetem lub przetwarza dane pobrane z sieci. Ręczne zarządzanie aktualizacjami dla czasem dziesiątków aplikacji jest z praktycznego punktu widzenia niewykonalne. Z pomocą przychodzą nam monitory aktualizacji. Sprawdzają one za użytkownika, czy pojawiły się nowe wydania lub poprawki dla oprogramowania zainstalowanego na komputerze. Przykładem takiej aplikacji może

być Personal Software Inspector opracowany przez firmę Secunia. Istnieje wersja online narzędzia, która potrafi szybko ocenić ilość potrzebnych aktualizacji. Specjalnie przygotowaną dla polskich użytkowników można znaleźć pod adresem http://www.cert.pl/sprawdz-aktualizacje.

W przypadku gdy jesteśmy zmuszeni pracować z dokumentami lub plikami pochodzącymi z niepewnego źródła, dobrym nawykiem jest przeglądanie ich zawartości z wykorzystaniem zewnętrznych serwisów. Prawdopodobnie najpopularniejszym jest Google Docs. Umożliwia on podgląd plików z pakietu MS Office, a także plików PDF. Przeglądając je na zdalnym serwerze nie narażamy się na wykonanie złośliwego kodu, nawet jeżeli taki w pliku się znajdował. W przypadku gdy otwarcie pliku się nie powiodło możemy podejrzewać, że plik mógł być niebezpieczny. VirusTotal jest jednym z serwisów, który może pomóc w określeniu, czy przesłana próbka może zawierać wirusa. Umożliwia on przeskanowanie pliku ponad 40 silnikami antywirusowymi jednocześnie i prezentuje w wyniki w zrozumiałej nawet dla laika postaci.

Podsumowanie

Internet to środowisko niezwykle dynamiczne, nie tylko ze względu na ciągle zmieniające się treści jakie są w nim dostępne, lecz także ze względu na rodzaje niebezpieczeństw, które czyhają na użytkowników. One także podlegają ewolucji i ciągłym zmianom. Nowe sposoby prezentacji danych, stając się popularne, przyciągają uwagę twórców złośliwego oprogramowania. Poszukują oni luk, dzięki którym będą mogli użyć komputerów zwykłych użytkowników do własnych przestępczych celów. Tak było w przypadku plików PDF. Gdy tylko format zyskał na popularności, a później także na funkcjonalności, stał się wykorzystywanym na szeroką skalę wektorem ataków. Podobnie stało się z plikami Flash oraz wcześniej z plikami aplikacji biurowych. Wirusy zwykle kojarzą się jedynie z plikami wykonywalnymi. Należy jednak pamiętać, że ze względu na rozbudowaną funkcjonalność popularnych formatów wymiany danych mogą się znajdować niemalże w każdym ich rodzaju. Najskuteczniejszą formą obrony pozostaje zawsze doświadczenie i zdrowy rozsądek użytkownika komputera.

7.6 Politycznie motywowane ataki DDoS i Avenge Assange

WikiLeaks

Julian Assange, redaktor naczelny serwisu WikiLeaks, opublikował na jego łamach treść ponad 250 000 tajnych depesz amerykańskiego rządu (w większości z ostatnich trzech lat). Zdarzenie to miało miejsce 28 listopada 2010 r. i zapoczątkowało bezprecedensowy, ogólnoświatowy kryzys dyplomatyczny. Depesze te stanowiły treść transmisji pomiędzy Rządem USA a amerykańskimi ambasadami. Komunikacja dotyczyła na przykład: Pakistanu, Iranu, Chin, Wielkiej Brytanii, ONZ, w tym znanych polityków i członków rządu. Zawierała również fragmenty współpracy pomiędzy Polską a USA, a także wzmianki o wstawiennictwie Gordona Browna w sprawie ekstradycji hakera Garry'ego McKinnona do USA.

Reakcja

Oprócz ostrej krytyki działań Assange'a przez władze Stanów Zjednoczonych i wielu innych państw w mediach publicznych, WikiLeaks został także zaatakowany w bardziej brutalny sposób przez nieznane podmioty. Niemal jednocześnie z chwilą opublikowania treści depesz serwis WikiLeaks stał się celem zmasowanego ataku DDoS. Do udziału w atakach na WikiLeaks przyznał sie między innymi haker o pseudonimie th3j35t3r (użył on własnego narzędzia o nazwie XerXes).

Operacja Avenge Assange

Na operację Avenge Assange prowadzoną przez aktywistów z Anonymous składały się serie ataków typu DDoS, których cele ustalane i dystrybuowane były na bieżąco za pośrednictwem serwisu twitter.com oraz sieci IRC.

8. Najciekawsze wydarzenia z działalności CERT Polska

Jedną z pierwszych ofiar operacji był serwis PayPal, a właściwie jego blog firmowy – thepaypalblog.com. Atak nastąpił 4 grudnia 2010 r. jako odpowiedź na wstrzymanie transakcji prowadzonych na konto WikiLeaks. Od dnia 6. grudnia rozpoczął się atak na serwisy postfinance.ch, Aklagare.se, EveryDNS.com, lieberman.senate.gov (pierwsza zaatakowana strona rządowa), w tym czasie nastąpił także kontratak na serwis AnonOps.net, o który podejrzewany jest th3j35t3r. Usługi firm MasterCard i Visa stały się celem ataków od 8. grudnia, na kanale koordynującym ataki znajdowało się wtedy ponad 2200 osób.

LOIC

Do prowadzenia ataków zaprzęgnięto szereg technik, z dużym prawdopodobieństwem wykorzystane były również botnety. Wyróżniającym się narzędziem w arsenale aktywistów jest aplikacja LOIC (ang. Low-Orbit Ion Cannon), aplikacja zmieniająca komputer, na którym jest zainstalowana, w część botnetu. Obecnie najczęściej wykorzystywana jest jej wersja napisana w języku JavaScript, z wprowadzonymi modyfikacjami umożliwiającymi koordynację swoich działań przez kanał C&C (ang. Command and Control), którym w tym przypadku był kanał na serwerze IRC AnonOps. W odróżnieniu od tradycyjnego botnetu, którego elementami są nieświadome swojej roli ofiary, użytkownicy LOIC dobrowolnie „oddawali" swoje komputery na użytek ataku. Warto też zauważyć, że o ile do przeprowadzeniu ataku z użyciem botnetu przejętych maszyn konieczne jest zazwyczaj spore doświadczenie, LOIC może być wykorzystywany przez praktycznie każdego użytkownika. Przyłączający się do ataku nowicjusze są jednak zazwyczaj nieświadomi faktu, że zostawiają w sieci ślad umożliwiające szybkie i dokładne ich zidentyfikowanie.

Ataki DDoS

Ataki typu DDoS stają się coraz bardziej popularne i stanowią coraz większe zagrożenie dla praktycznie każdego użytkownika sieci Internet - od instytucji rządowych, poprzez przedsiębiorstwa, aż po zwykłego użytkownika. Najgorsze są zazwyczaj skutki ataków na serwisy utrzymujące się ze swojej obecności online - czyli sklepy internetowe, kasyna, elementy infrastruktury bankowej. Metody stawiania czoła atakom DDoS są zróżnicowane. Są wśród nich metody prewencyjne, polegające na blokowaniu ataków u ich źródła - czyli podejmowania działań przez IAP (ang. Internet Access Provider) wobec swoich klientów bądź śledzenie i rozbijanie botnetów używanych do prowadzenia ataków, są także metody opierające się na nowoczesnych rozwiązaniach programowych i sprzętowych odróżniających atak od zwykłego ruchu, a także zwyczajny „wyścig zbrojeń" - czyli zwiększanie pojemności sieci przez zakup nowego sprzętu. Mniejsze przedsiębiorstwa mogą skorzystać z usług firm i specjalistów specjalizujących się w powstrzymywaniu ataków DDoS. Obecnie nie istnieje jednak ogólna, skuteczna metoda obrony przed odpowiednio przygotowanym atakiem.

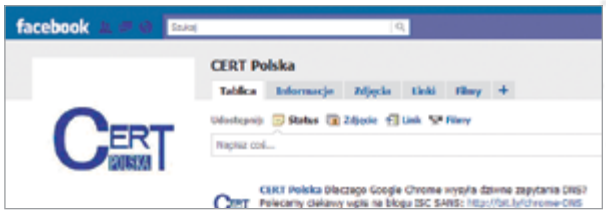
8.1 Społeczności CERT Polska

Rok 2010 zaowocował wyjściem wizerunkowym zespołu CERT Polska poza portal www.cert.pl. Pozostał on głównym miejscem publikacji większych opracowań czy raportów na podstawie autorskich badań i przemyśleń. Luźniejsze i mniej formalne informacje znalazły swoje miejsce w serwisach Twitter oraz Facebook.

CERT Polska zadebiutował na Twitterze w marcu 2010 r. zarówno w wersji polskiej oraz angielskiej. Twitty ukazują się często i regularnie w obu wersjach i zawierają wybrane spostrzeżenia lub wiadomości, którymi chcemy podzielić się „na gorąco". Co ciekawe, na koniec 2010 roku, popularniejsza okazała się wersja angielska.

Strona CERT Polska w serwisie społecznościowym Facebook została stworzona zaraz po konferencji SECURE 2010 (patrz: 8.4). Oprócz okolicznościowych zdjęć i komentarzy pojawiają się na niej kopie wiadomości z serwisu Twitter oraz artykułów ze strony www.cert.pl.

8. Najciekawsze wydarzenia z działalności CERT Polska



Facebook:	http://www.facebook.com/CERT.Polska
Twitter (PL):	http:// twitter.com/cert_polska
Twitter (EN):	http://twitter.com/cert_polska_en

8.2 Doroczna konferencja FIRST i spotkanie CERT - ów narodowych w Miami

W dniach 13-18 czerwca 2010 r. odbyła się 22. doroczna konferencja FIRST. Jest to najważniejsze w roku wydarzenie dla ogólnoświatowego forum zespołów reagujących, zrzeszającego w tej chwili ponad 220 zespołów z sześciu kontynentów, od rządowych, przez uczelniane i akademickie, po bankowe i te należące do wielkich korporacji. Tegoroczna edycja miała miejsce w Miami na Florydzie i zgromadziła przeszło 450 uczestników. CERT Polska jest jednym z aktywnych członków forum. W tym roku, oprócz trzyosobowej reprezentacji wśród uczestników, miał także znaczący wkład merytoryczny w program konferencji. Byliśmy autorami lub współautorami aż czterech wygłoszonych prezentacji:

- *R&D projects launched in response to the dynamic evolution of Internet security threats – CERT view* - wygłoszona przez Krzysztofa Silickiego i Piotra Kijewskiego (współautor: Mirosław Maj)
- *Cooperation and self-regulation of Polish ISPs in combating online crime* – wygłoszona przez Przemysława Jaroszewskiego
- *FISHA – A Framework for Information Sharing and Alerting in Europe* – współautorstwa Piotra Kijewskiego i Katarzyny Gorzelak
- *WOMBAT API: handling incidents by querying a world-wide network of advanced honeypots* wygłoszona przez Piotra Kijewskiego (współautor: Adam Kozakiewicz)

Znaczący udział wśród pozostałych prezentacji miały tematy związane z bezpieczeństwem i prywatnością w systemach cloud computing. Pojawiły się także interesujące prezentacje dotyczące ataków dedykowanych oraz mnóstwo ciekawych przykładów rozwiązań organizacyjnych i technicznych związanych z bezpieczeństwem i reagowaniem na incydenty. Bardzo ciekawy program sprawiał, że często trudno było dokonać wyboru między trzema ścieżkami tematycznymi.

Bezpośrednio po konferencji odbyło się spotkanie zespołów narodowych, organizowane przez CERT/CC od kilku lat. Spotkania te są doskonałą okazją do wymiany kontaktów oraz zapoznania się z wyzwaniami, które stoją przed zespołami CERT działającymi na szczeblu narodowym. W trakcie spotkania w Miami Piotr Kijewski, kierownik CERT Polska, zaprezentował projekt WOMBAT oraz przeprowadził demonstrację API, służącego do pozyskiwania danych z wielu źródeł zajmujących się analizą i obserwacją złośliwego oprogramowania.

8. Najciekawsze wydarzenia z działalności CERT Polska

8.3 Zakończenie projektu HoneySpider Network

W grudniu 2010 r. zakończył się projekt HoneySpider Network. HoneySpider Network był wspólnym projektem działającego w ramach NASK zespołu CERT Polska, rządowego CERT - u holenderskiego GOVCERT.NL oraz akademickiego operatora w Holandii, SURFnet. Projekt miał na celu zbudowanie nowych oraz wykorzystanie istniejących technik klienckich honeypotów do wykrywania ataków na aplikacje klienckie, w szczególności przeglądarki WWW. Projekt powstał w odpowiedzi na obserwacje nowego trendu w propagacji zagrożeń internetowych poprzez luki w aplikacjach klienckich, a nie jak dotychczas, w aplikacjach serwerowych. W szczególności zagrożeniem są ataki typu drive-by download, które do skutecznego zarażenia systemu operacyjnego wymagają jedynie odwiedzenia odpowiednio spreparowanej strony, bez jakiejkolwiek dodatkowej interakcji z użytkownikiem.

W ramach projektu stworzono nowy system zdolny do przetwarzania hurtowej ilości adresów URL pod kątem zbadania ich złośliwości. Rozwiązanie bazuje zarówno na rozwiązaniach wysokointeraktywnych (roboty emulujące przeglądarki) jak i na rozwiązaniach wysokointeraktywnych (przeglądarki uruchamiane i automatycznie sterowane z poziomu rzeczywistych systemów operacyjnych). W ramach rozwiązania niskointeraktywnego stworzono własny autorski system oceny złośliwości stron wykorzystujący techniki maszyn uczących się. W ramach rozwiązań wysokointeraktywnych dokonano dużej przebudowy istniejącego rozwiązania Capture-HPC, w tym przeniesienia go do środowiska VirtualBox, rozbudowania funkcjonalności w zakresie logowania i usunięcia wielu poważnych błędów. Dzięki temu w ramach systemu dysponujemy stabilnym wysokointeraktywnym klienckim honeypotem. Do integracji obu rodzajów honeypotów stworzono nowy framework odpowiedzialny za zarządzanie adresami URL, oraz GUI dla operatorów.

Tabela 7.4.2 Kraje, z których obserwowano skanowania SIP

System prezentowany był na wielu światowych konferencjach na świecie, zarówno technicznych jak i akademickich. Był wielokrotnie cytowany w literaturze akademickiej, w tym także przez wiodące firmy z branży na świecie, takie jak Microsoft – Microsoft Research.

W chwili obecnej na świecie funkcjonuje już kilka instalacji tego systemu – także w CERT Polska. Pod koniec ubiegłego roku nasz zespół zaangażowany był w kilka wdrożeń, między innymi w Dubaju na zlecenie rządu Emiratów Arabskich. Obecnie system wytworzony w ramach projektu znajduje się w fazie utrzymaniowej. W 2011 r. rusza kolejny projekt: HoneySpider Network 2.0, który będzie naszą odpowiedzią na ciągłe zmiany w technikach ataków na aplikacje klienckie. Dzięki niemu mamy nadzieję rozszerzyć nasze możliwości ich detekcji.

8. Najciekawsze wydarzenia z działalności CERT Polska

8.4 Konferencja SECURE 2010 pod znakiem zmian

25-27 października 2010 r. w centrum konferencyjnym Adgar Plaza w Warszawie odbyła się XIV edycja organizowanej przez CERT Polska i NASK konferencji SECURE. Przygotowując ją postawiliśmy na wiele zmian, więc nie obyło się bez obaw, czy wszystko pójdzie tak, jak sobie to wyobrażaliśmy.

W poniedziałek, 25 października, zorganizowane zostały warsztaty z limitowaną liczbą miejsc. Do wyboru zaproponowaliśmy zajęcia prowadzone przez Tomasza Grudzieckiego i Pawła Jacewicza z CERT Polska o zagadkowej nazwie „Duchy w przeglądarkach" oraz szkolenie z tworzenia reguł snorta i zastosowań tego oprogramowania, prowadzone przez Piotra Linke z Sourcefire. Na każdy z warsztatów dostępne było jedynie 30 miejsc i zostały one zapełnione długo przed konferencją. Uczestnicy byli zadowoleni, więc uznajemy, że ta nowość była krokiem w dobrym kierunku i zapewne skorzystamy z tej nauki w przyszłości.Oficjalnego otwarcia konferencji we wtorkowy poranek dokonał dyrektor operacyjny NASK, dr Tomasz Kruk. Chwilę później swoją prezentację rozpoczął Lance Spitzner – postać znana w świecie bezpieczeństwa m.in. jako wykładowca SANS, założyciel The Honeynet Project oraz autor książki „Honeypots: Tracking Hackers". Znanych nazwisk było więcej. Drugi dzień konferencji rozpoczęła prezentacja Mikko Hypponena z F-Secure, a w sesjach plenarnych wystąpili także m.in. Julio Canto z hiszpańskiego Hispasec, prowadzącego serwis VirusTotal, oraz Udo Helmbrecht – dyrektor wykonawczy europejskiej agencji bezpieczeństwa sieci i informacji ENISA. Chcemy, by przybliżanie znanych postaci ze świata bezpieczeństwa IT oraz ich myśli nie przestało być wizytówką SECURE'a.

Dużym zainteresowaniem pierwszego dnia cieszyły się także prezentacje Dominica Storey'a z Sourcefire (z barwnie przedstawionymi przykładami ataków APT) oraz Macieja Kołodzieja i Michała Kluski z NK (poświęcona ściganiu spamerów na portalu). Zainteresowanie dopisało też na prezentacjach naszego zespołu (było ich aż cztery!), a oddziałujące na wyobraźnię przykłady wziętych z życia kłopotów po kradzieży konta email prezentowane przez Rafała Tarłowskiego oraz demonstracja możliwości złośliwego oprogramowania

Zeus w wykonaniu Tomka Bukowskiego rozbudziły emocje. Na szczęście można je było uspokoić w trakcie wieczornego spotkania w restauracji Akashia, gdzie oprócz pokazu filetowania łososia i nauki przygotowywania sushi, uczestnicy konferencji mieli doskonałą okazję do rozmów i wymiany kontaktów w niezobowiązującej atmosferze.

Na środowej sesji, w której wystąpili Wojciech Dworakowski („Bankowość elektroniczna kontra malware") oraz Piotr Konieczny („Kulisy ataków na polskie serwisy internetowe") trudno było znaleźć wolne miejsca. Niewątpliwie jednym z silnych punktów tego dnia były także „lightning talks". To kolejna z nowości, które zaproponowaliśmy w tym roku – obarczona sporym ryzykiem, ponieważ wszystko zależało od aktywności samych uczestników. Formuła tych „prezentacji błyskawicznych" zakładała krótkie (do 5 minut) wystąpienia na dowolny temat. Tymczasem do końca pierwszego dnia pojawił się tylko jeden chętny do udziału… W okolicach środowego obiadu lawina jednak ruszyła i tuż przed sesją mieliśmy aż dwanaście zgłoszeń! Żywiołowa atmosfera i ciekawe tematy wystąpień dopełniły bardzo pozytywnego efektu.

Mimo, że drugi (a dla niektórych trzeci) dzień dobiegał końca, sala nie przerzedziła się przed prezentacją Ryana McGeehana z Facebooka „Defending a Social Network". Jej uzupełnieniem była dyskusja panelowa poświęcona prywatności oraz zagrożeniom w dobie sieci społecznych. Udział w niej, oprócz przedstawicieli Facebooka i NK, wzięli także Katarzyna Szymielewicz z Fundacji „Panoptykon" oraz Przemysław Jaroszewski z CERT Polska.

ARAKIS

Raport roczny 2010

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, darknet, firewalli oraz systemów antywirusowych. Szczególną implementacją systemu ARAKIS jest projekt ARAKIS-GOV wykorzystywany do ochrony zasobów teleinformatycznych administracji publicznej. Jest on obecnie wdrożony w około siedemdziesięciu instytucjach administracji publicznej we współpracy z polskim CERT-em rządowym CERT.GOV.PL, działającym w strukturach Departamentu Bezpieczeństwa Teleinformatycznego ABW.

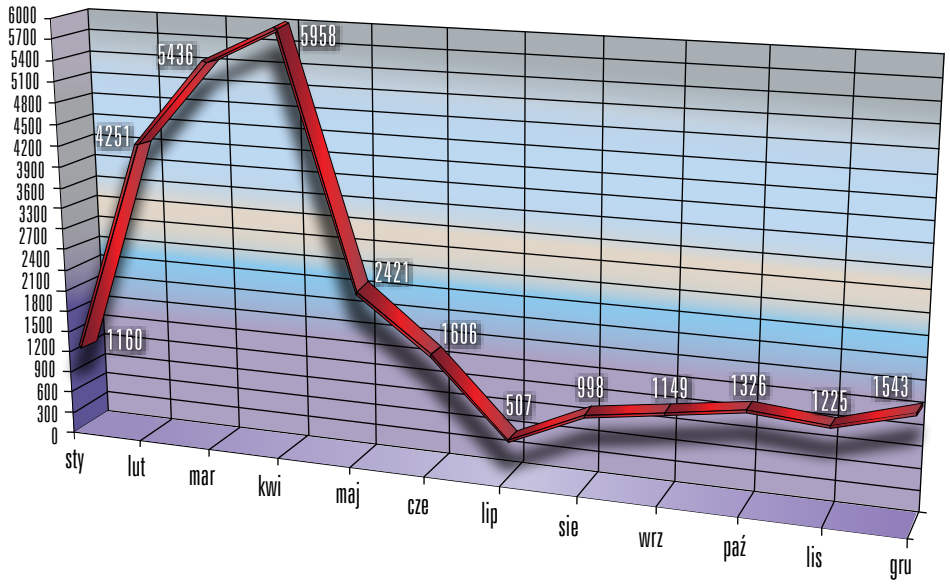
Niniejsze roczne podsumowanie jest trzecim tego typu w historii systemu. System przede wszystkim sprawdził się w ochronie zasobów sieciowych uczestników projektu, wykrywając źródła infekcji we wczesnym stadium, dzięki czemu można było szybko zapobiec jej rozprzestrzenianiu się. Dzięki pozyskanym informacjom możliwe było również poznanie mechanizmów działania zarówno nowych, jak i aktualnych ataków na aplikacje serwerowe. Projekt ARAKIS był wielokrotnie prezentowany na wielu krajowych i międzynarodowych konferencjach poświęconych bezpieczeństwu IT. Co więcej, był także wymieniany przez polskich i zagranicznych naukowców oraz specjalistów od bezpieczeństwa IT w ich publikacjach.

W raporcie zamieszczono 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. Ponadto opisano kilka interesujących przypadków obserwacji dokonanych przez system ARAKIS.

1. Statystyki dotyczace alarmów

W roku 2010 w systemie ARAKIS zostało wygenerowanych 27 580 alarmów – jest to o ponad 12 000 więcej niż w roku 2009. Tak duży wzrost spowodowany był wieloma czynnikami. Oprócz zwiększenia liczby incydentów i zdarzeń do wzrostu przyczynił się także fakt opracowania i wdrożenia kolejnych typów alarmów, oraz dodanie nowych sond.

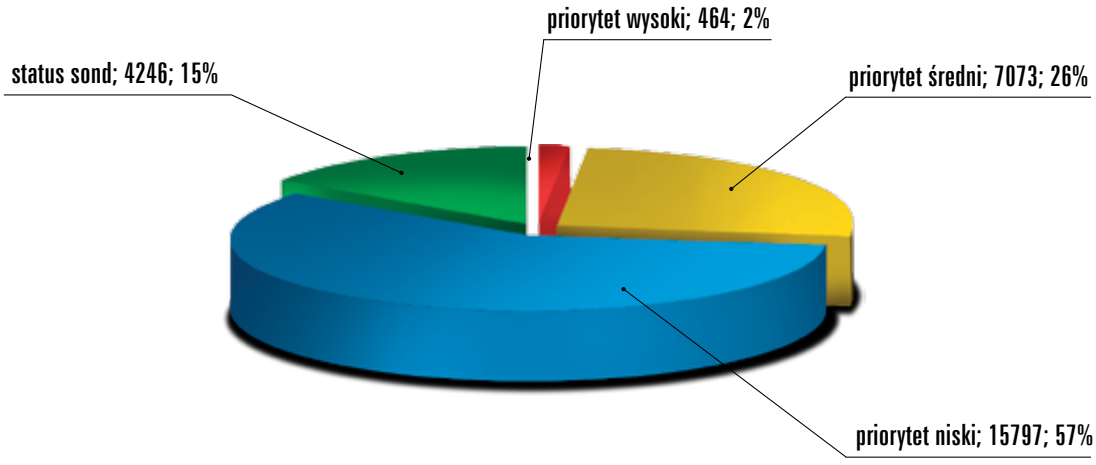
Największą liczbę alarmów odnotowano w pierwszych czterech miesiącach roku 2010. Złożyły się na nie przede wszystkim alarmy o priorytecie niskim oraz średnim, które w znacznej większości dotyczyły zdarzeń pochodzących z sieci Internet (nie były to infekcje stacji roboczych uczestników systemu).



Wykres 1.1. Alarmy wygenerowane przez system ARAKIS w roku 2010

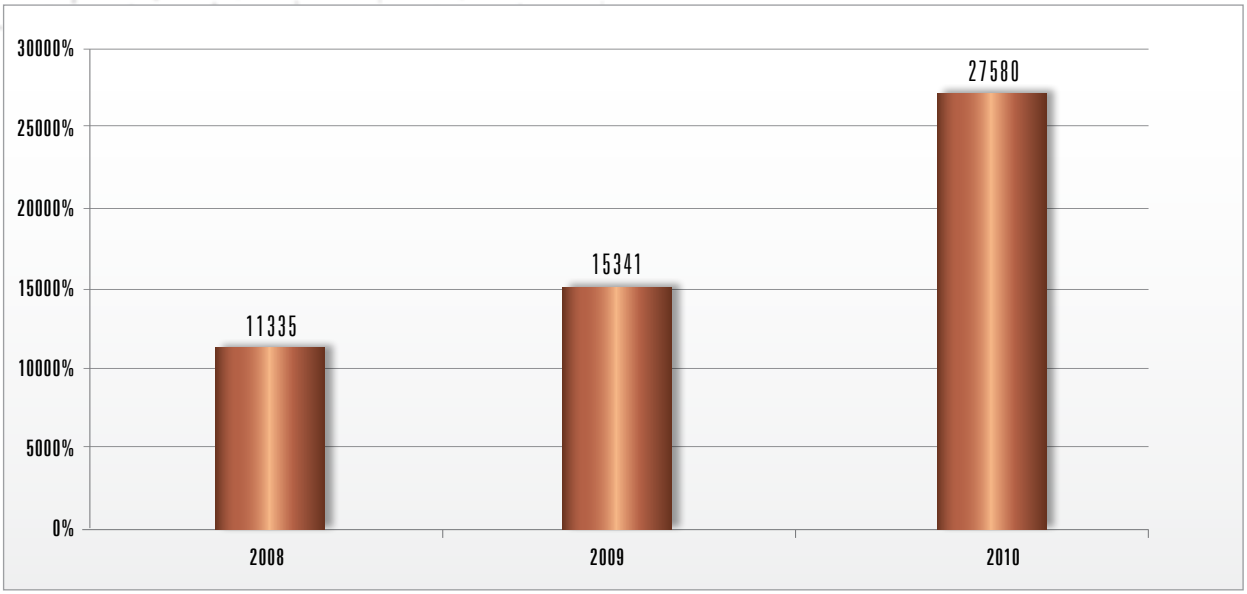
Wykres powyżej przedstawia roczne zestawienie wszystkich alarmów bez podziału na typy.

Większość wygenerowanych alarmów w roku 2010 miała niski priorytet (57 proc.). Następne w kolejności były alarmy o priorytecie średnim (26 proc.),

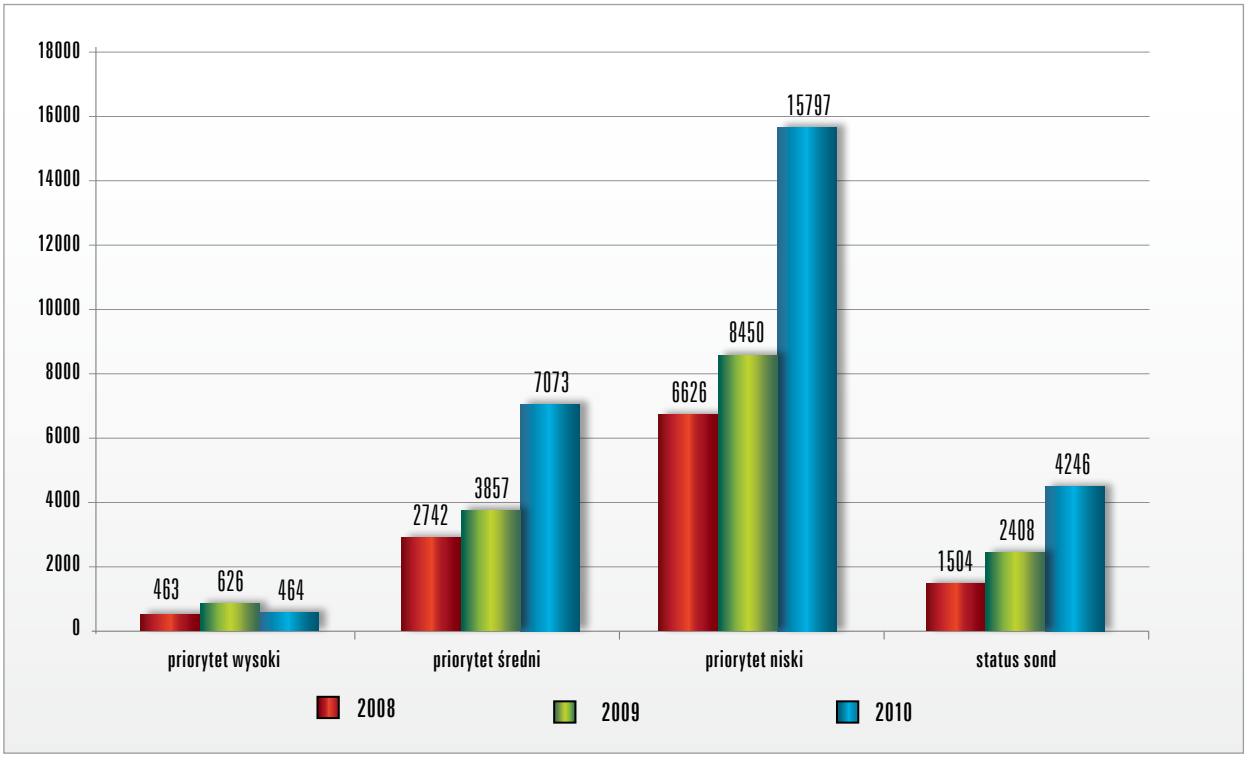


Wykres 1.2. Alarmy wygenerowane przez system ARAKIS w roku 2010

oraz te opisujące stan poszczególnych sond ARAKISowych (15 proc). Najmniej było alarmów opisujących wykrycie poważnych zagrożeń w sieci (2 proc). Rozkład ten jest bardzo podobny do zeszłorocznego, a więc zwiększyła się tylko liczba alarmów – proporcje pozostały niezmienione. Jedynym odstępstwem są alarmy najważniejsze, czyli o najwyższym priorytecie. Tych alarmów w stosunku do innych typów było mniej o połowę (w zeszłym roku stanowiły one 4 proc. wszystkich alarmów), ale gdy porównamy liczbowo okazuje się, że ich liczba zmalała o ok. ¼.



Wykres 1.3. Liczba wszystkich alarmów



Wykres 1.4. Alarmy systemu ARAKIS

2. Interesujące przypadki zaobserwowanych incydentów sieciowych

Oprócz ochrony, jaką dostarczył sieciom z zainstalowanymi sondami, system ARAKIS przyczynił się także do zrozumienia wielu rodzajów zagrożeń powszechnie występujących w Internecie. Poniżej skrótowo opisane zostały ciekawsze, naszym zdaniem, obserwacje dokonane przez ARAKIS-a w roku 2010. W rozdziale 7 raportu CERT Polska zostały dodatkowo szerzej opisane obserwacje ataków na telefonię internetową (VoIP) dokonane dzięki systemowi ARAKIS.

2.1 Atak na serwery Facebooka

Pod koniec sierpnia w systemie ARAKIS zaobserwowany został atak typu DDoS na serwery Facebooka. Dnia 24. sierpnia 2010 r. o godzinie 21:00 został wygenerowany alarm NSNORT mówiący o dopasowaniu reguły Snort do przepływu. Oznacza to zwykle jakąś znaną formę ataku, która jednak nie była ostatnio rejestrowana przez system ARAKIS. Tą regułą była: ET POLICY facebook activity. Okazało się jednak, że to serwery Facebooka przesyłały pakiety do honeypota ARAKIS.

Patrząc na szczegóły pozyskanych przepływów widać, że najpierw miało miejsce połączenie z adresu IP 69.63.181.11 należącego do Facebooka. Pierwszy pakiet jest pakietem protokołu TCP z ustawionymi flagami SYN (synchronize) oraz ACK (acknowledge), czyli jest najprawdopodobniej drugą fazą nawiązania połączenia TCP (three-way handshake). Adres docelowy wskazuje na jeden z ARAKIS-owych honeypotów, które same nie nawiązują połączeń. W związku z tym, że honeypot nie rozpoczął tego połączenia, odpowiedział, zgodnie z RFC793, pakietem z flagą RST (reset). Na tej podstawie można wywnioskować, że atakujący DOS-ując serwery Facebooka fałszował adresy źródłowe. Niektóre z nich wskazywały na honeypoty ARAKIS-a, dzięki czemu mogliśmy zaobserwować ten atak.

Poniższej widać listę przepływów świadczących o omawianym ataku (zawiera jedynie unikatowe adresy źródła):

Data	Źródło	Port	Cel	Port	Protokół
2010-08-23 11:16:55	69.63.189.34	80	XXX.XX.XX.66	41145	TCP
2010-08-23 11:53:15	69.63.190.22	80	XXX.XX.XX.95	4496	TCP
2010-08-24 07:58:15	69.63.190.18	80	XXX.XX.XX.89	1392	TCP
2010-08-24 08:10:25	69.63.189.16	80	XXX.XX.XX.89	2382	TCP
2010-08-24 08:27:13	69.63.190.10	80	XXX.XX.XX.89	3295	TCP
2010-08-24 08:50:21	69.63.181.52	80	XXX.XX.XX.66	27897	TCP
2010-08-24 09:29:59	69.63.189.11	80	XXX.XX.XX.66	47827	TCP
2010-08-24 14:48:19	69.63.181.16	80	XXX.XX.XX.66	10042	TCP
2010-08-24 22:46:10	69.63.181.11	80	XXX.XX.XX.8	1225	TCP
2010-08-25 08:52:49	69.63.181.15	80	XXX.XX.XX.66	12361	TCP
2010-08-25 09:24:32	69.63.181.49	80	XXX.XX.XX.66	29508	TCP
2010-08-25 09:40:56	69.63.189.31	80	XXX.XX.XX.90	2701	TCP
2010-08-25 14:01:42	69.63.181.12	80	XXX.XX.XX.90	4899	TCP
2010-08-25 15:29:28	69.63.180.48	80	XXX.XX.XX.5	8843	TCP
2010-08-26 08:20:19	69.63.180.44	80	XXX.XX.XX.5	24142	TCP
2010-08-26 08:26:00	69.63.190.14	80	XXX.XX.XX.66	37812	TCP
2010-08-26 09:15:32	69.63.181.50	80	XXX.XX.XX.66	8563	TCP
2010-08-26 09:50:52	69.63.181.51	80	XXX.XX.XX.106	1974	TCP

Połączenia świadczące o atakach na serwery Facebook

2.2 HuaweiSymantecSpider – co to za pająk i dlaczego szuka phpMy Admin?

Na początku października donosiliśmy o aktywności pająka HuaweiSymantecSpider (protokół HTTP), widzianej w honeypotach systemu ARAKIS. Poprzez żądania GET próbowano pobrać z naszych honeypotów pliki konfiguracyjne (setup.php) znanego narzędzia do zarządzania bazami danych MySQL – phpMyAdmin. Na pierwszy rzut oka wyglądało to jak połączenia generowane przez typowy skaner luk próbujący na ślepo znaleźć podatne lub źle skonfigurowane narzędzie na sprawdzanym serwerze:

```
Hypertext Transfer Protocol
  GET /phpMyAdmin-2.6.1-pl1/scripts/setup.php HTTP/1.0\r\n
    [Expert Info (Chat/Sequence): GET /phpMyAdmin-2.6.1-pl1/scripts/setup.php HTTP/1.0\r\n]
      [Message: GET /phpMyAdmin-2.6.1-pl1/scripts/setup.php HTTP/1.0\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /phpMyAdmin-2.6.1-pl1/scripts/setup.php
    Request Version: HTTP/1.0
  Host: 1[redacted]45\r\n
  Accept: */*\r\n
  User-Agent: Huaweisymantecspider (compatible; MSIE 8.0; DSE-support@huaweisymantec.com)\r\n
  Connection: Close\r\n
  Referer: http://1[redacted]45/phpMyAdmin-2.6.1-pl1/scripts/setup.php\r\n
  \r\n
```

Przykładowy pakiet wygenrowany przez pająka

Do każdego z przeskanowanych adresów honeynetowych było nawiązanych po sześć połączeń różniących się ścieżką dostępu do pliku konfiguracyjnego uzależnioną od wersji phpMyAdmin. To upewniło nas, że połączenia były nawiązywane “na ślepo”:

```
GET /phpMyAdmin-2.6.0-pl2/scripts/setup.php HTTP/1.0\r\n
GET /phpMyAdmin-2.6.1-pl1/scripts/setup.php HTTP/1.0\r\n
GET /phpMyAdmin-2.6.4-rc1/scripts/setup.php HTTP/1.0\r\n
GET /phpMyAdmin-2.6.4/scripts/setup.php HTTP/1.0\r\n
GET /typo3/phpmyadmin/scripts/setup.php HTTP/1.0\r\n
```

Ślepe próby połączeń HTTP

Nie znaliśmy narzędzia, które w polu “User-Agent” przedstawiało się jako “Huaweisymantecspider (compatible; MSIE 8.0; DSE-support@huaweisymantec.com)“, dlatego postanowiliśmy przypatrzeć się mu bliżej. Poza samym narzędziem zaciekawiło nas skąd wziął adresy IP skanowanych hostów? Czy zostały wytypowane losowo, czy sukcesywnie sprawdzana była większa podsieć należąca do polskich providerów? Ciekawostką jest to, że firma HuaweiSymantec ma główną siedzibę w Chinach a ich domeną są produkty bezpieczeństwa sieciowego… Na stronie producenta można przeczytać, że – wbrew naszym początkowym założeniom – crawler HuaweiSymantecSpider nie jest wykorzystywany przez skanery podatności, lecz używa go narzędzie do sprawdzania stron WWW pod kątem zawartości złośliwego kodu (czyżby konkurencja dla tworzonego przez nas systemu klienckich honeypotów HoneySpider Network?). W takim razie skąd wzięto adresy URL prowadzące do naszych honeypotów?

W tej kwestii wiele wyjaśniła nam odpowiedź przesłana mailem od firmy HuaweiSymantec, którą zapytaliśmy skąd mogły pojawić się połączenia ich crawlera do nie istniejących stron. Okazało się, że URL-e zasilające ich system są pozyskiwane z pakietów z ruchu, który przechodzi przez ich inne produkty. Czyli ktoś kiedyś wcześniej z wewnątrz sieci, którą chronią ich produkty, próbował przeskanować nasze honeypoty szukając podatnych

Szczegóły klastra	[SCAN] huawei symantec spider bot (80/TCP)
Nazwa:	[SCAN] huawei symantec spider bot (80/TCP)
Data utworzenia:	2010-10-10 05:30:28
Data aktualizacji:	2010-10-10 05:30:28
Poziom klasyfikacji:	Attack
Rdzeń:	[SCAN] huawei symantec spider bot (80/TCP)
Porty:	80/TCP
Unikalnych źródeł:	3
Rozmiar sygnatury:	199
Sygnatura klastra:	

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"[SCAN] huawei symantec spider bot (80/TCP)"; flow:\
to_server,established; content:"/scripts/setup.php HTTP/1.0|0d 0a|Host\: "; pcre:"/\b\d{1,3}\.\d{1,3}\.\d{1,3}
\.\d{1,3}\b/"; content:"|0d 0a|Accept\:\
*/*|0d 0a|User-Agent\: Huaweisymantecspider (compatible\; MSIE 8.0\; DSE-support@huaweisymantec.com\
)|0d 0a|Connection\: Close|0d 0a|Referer\: http\://"; pcre:"/\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b/"; content:"/";)
```

Klaster stworzony przez system ARAKIS

lub źle skonfigurowanych aplikacji phpMyAdmin. Mógł to być atakujący bezpośredni, lub (co bardziej prawdopodobne) nieświadomy, być może zarażony jakimś złośliwym oprogramowaniem i wcielony do botnetu (tzw. komputer-zombie).

Mamy nadzieję, że powyższy opis pomoże administratorom, którzy zauważą w logach swoich serwerów WWW takiego "User-Agent'a". Warto dodać, że według opisu na stronie producenta crawler obsługuje mechanizm Robots Exclusion Protocol. Aby całkowicie zabronić temu pająkowi przeszukiwania stron WWW, należy do pliku "robots.txt" dodać wpis:

```
User-agent: HuaweiSymantecSpider
Disallow: /
```

Potwierdzają to obserwacje ARAKIS-a, który wykrył próby pobrania tego pliku dla każdego adresu IP. Jednakże to nie uchroni przed skanowaniem wykonanym przez prawdziwego "atakującego" (tego, od którego HuaweiSymantecSpider pozyskał adres URL).

2.3 Luka w aplikacji ProFTPd oraz jej wykorzystanie

Piątego listopada pisaliśmy o błędzie przepełnienia bufora w aplikacji ProFTPd (szczegóły: http://www.cert.pl/news/2812). Dwa tygodnie później system ARAKIS zarejestrował próby włamania z wykorzystaniem exploitów na tę lukę. Jako źródło ataku określiliśmy sieć znajdującą się na terenie Stanów Zjednoczonych, a zastosowany do ataku exploit to prawdopodobnie skrypt Perl opublikowany na liście full-disclosure kilka dni po ujawnieniu luki. Poniżej fragment przechwyconego przez honeypoty pakietu, w którym znajdował się exploit:

```
        0x03d0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x03e0:  0000 0000 0000 0000 00ff 4b43 4f50 4552  ..........KCOPER
        0x03f0:  554c 455a 4b43 4f50 4552 554c 455a 4b43  ULEZKCOPERULEZKC
        0x0400:  90c2 0408 cccc cccc 0100 0000 90c2 0408  ................
        0x0410:  ffff 0000 0a                             .....
09:37:19.478824 IP [redacted].189.21 > [redacted].129.58484: . ack 498760291
```

Fragment pakietu zawierającego exploit na ProFTPd

Podsumowanie

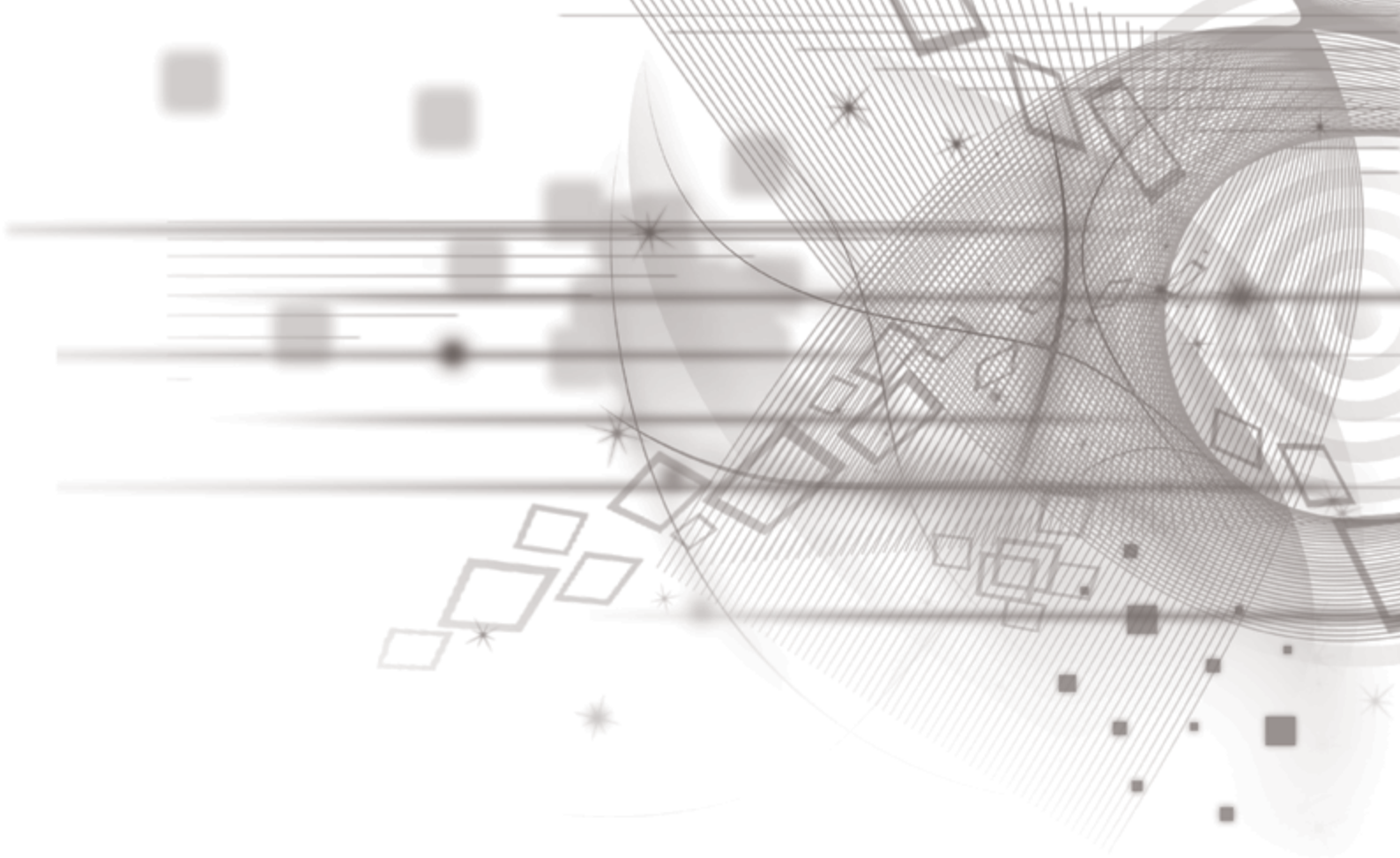
W 2010 r. operatorzy systemu ARAKIS obsłużyli łącznie 27 500 alarmów (średnio ok. 75 alarmów na dzień). Jest to ponad 12 000 (ok. 80 proc.) więcej niż przed rokiem, lecz nie wszystkie dotyczyły incydentów bezpieczeństwa. Najwyższy priorytet oznaczający realne zagrożenie dla któregoś z podmiotów biorących udział w systemie miało 2 proc. z nich (w roku 2009 było to 4 proc.). Jednakże porównując ich liczbę a nie procentowy udział we wszystkich alarmach, okazuje się, że ich liczba zmalała o ok. 25 proc. Należy dodatkowo pamiętać, że stało się tak pomimo faktu, że liczba sond zwiększyła się – obecnie wynosi ona 70 (o 10 więcej niż w 2009 r.). Są one umiejscowione w różnych instytucjach państwowych (w ramach implementacji dla administracji rządowej – ARAKIS-GOV, więcej informacji na stronie polskiego CERTu rządowego – www.cert.gov.pl) oraz w sieci NASK. Ponadto zaimplementowano 2 nowe typy alarmów oraz dodano nową funkcjonalność polegającą na pozyskiwaniu informacji z systemu HoneySpider Network (więcej informacji o projekcie HSN: http://www.cert.pl/projekty#hsn).

Jednym z podstawowych zadań stawianych systemowi była dodatkowa ochrona lokalnych sieci, w których instalowane były sondy ARAKIS-owe. W przypadku prawdziwych alarmów wykrywane były przede wszystkim wewnętrzne infekcje robakami i wirusami, ewentualnie próby ataków ze źródeł zewnętrznych lub poprzez wiadomości email. Szybka detekcja infekcji wewnątrz sieci uczestników systemu zapobiegała dalszemu rozprzestrzenianiu się zagrożenia. W przypadku zarażonych stacji roboczych instytucji rządowych reakcją zajmował się CERT. GOV. PL. działający w ramach Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego (DBTI ABW), natomiast w przypadku infekcji w sieci NASK interweniował działający w NASK Zespół Integracji i Bezpieczeństwa Systemów.

ARAKIS był także bardzo pomocny przy poznawaniu i badaniu nowych oraz aktualnych zagrożeń w sieci Internet, a także w korelacjach obserwacji poczynionych przez inne systemy wczesnego wykrywania zagrożeń sieciowych. Do najciekawszych incydentów zaobserwowanych przez system w 2010 r. należy m.in. wykrycie ataków DDoS na serwery portalu Facebook, obserwacja działania pająka sieciowego HuaweiSymantecSpider, wykrycie ataków na telefonię internetową VoIP, obserwacja ataków na aplikację serwerową ProFTPd.

Dane pozyskane przez system ARAKIS są wykorzystywane przez inne zespoły reagujące należące do FIRST (Forum for Incident Response and Security Teams). System i jego obserwacje prezentowane były na wielu krajowych i zagranicznych konferencjach. Opisywany był również w serwisach internetowych, prasie traktującej o bezpieczeństwie IT oraz publikacjach naukowych. Dane zbierane przez system wykorzystane zostały do opublikowania wiadomości na blogu www.cert.pl oraz mikroblogu Twitter (http://twitter.com/cert_polska oraz w wersji anglojęzycznej http://twitter.com/cert_polska_en)

W roku 2011 system ARAKIS zostanie wzbogacony o nowe typy alarmów oraz nowe funkcjonalności usprawniające pracę operatorów. Zwiększy się również liczba rozproszonych sond zbierających ruch sieciowy.



Kontakt

Zgłaszanie incydentów:	cert@cert.pl
Zgłaszanie spamu:	spam@cert.pl
Informacja:	info@cert.pl
Klucz PGP:	http://www.trusted-introducer.nl/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