CERT Polska

Raport 2006

Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2006

1 Wstęp

1.1 Informacje dotyczące zespołu 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. Działa od 1996 roku, a od 1997 jest członkiem FIRST (Forum of Incidents Response and Security Teams - http://www.first.org/) - największej organizacji zrzeszającej zespoły reagujące i zespoły bezpieczeństwa z całego świata. Od roku 2000 jest także członkiem inicjatywy europejskich zespołów reagujących – 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 w zakresie 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 przygotowywanie 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.

2 Statystyki CERT Polska

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 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.

Jednym z ważniejszych celów tych działań jest wypracowanie i stałe korzystanie z tego samego sposobu klasyfikowania incydentów, co umożliwi porównywanie danych w kolejnych latach, jak również różnic pomiędzy własnymi obserwacjami i obserwacjami innych zespołów reagujących. W tym roku po raz czwarty z kolei przygotowane zostały statystyki zgodnie z klasyfikacją wypracowaną w ramach projektu eCSIRT.net (http://www.ecsirt.net/cec/service/documents/wp4-pub-userguide-v10.html#HEAD7).

3 Statystyka incydentów

3.1 Słownik

W celu lepszego zrozumienia raportu zamieszczamy poniżej słownik, zawierający opis niektórych pojęć:

Abuse (Zespół abuse) – zepsół zajmujący się zgłoszeniami naruszenia bezpieczeństwa w sieci dostawcy usług

Blackholing – po angielsku „black hole" to czarna dziura, a sformułowanie „blackholing" opisuje wrzucanie do niej różnego rodzaju zawartości - w naszym przypadku, chodzi o niepotrzebny lub szkodliwy ruch sieciowy. (źródło http://networkers.pl)

Dialer – to wyspecjalizowany rodzaj programu komputerowego służący do łączenia się z Internetem za pomocą modemu. Niekiedy program tego rodzaju, instalowany w komputerze bez wiedzy i zgody użytkownika, jest wykorzystywany do nawiązywania połączenia z siecią. (źródło: http://pl.wikipedia.org)

Koń trojański – złośliwe oprogramowanie stwarzające pozory programu użytkowego, często o zastosowaniu rozrywkowym (np. odtwarzacz multimedialny) lub wątpliwym prawnie (np. łamacz zabezpieczeń czy haseł), wykonujące zamiast lub oprócz spodziewanych funkcji także dodatkowe zadania prowadzące do przejęcia kontroli nad komputerem przez atakującego.

---

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

Oprogramowanie szpiegowskie (Spyware) - oprogramowanie, którego zadaniem jest zbieranie i wykradanie informacji o użytkowniku, jego zachowaniu, począwszy od odwiedzanych stron a kończąc na danych wpisywanych do formularzy (np. hasła).

Phishing – oszustwo polegające na wprowadzeniu w błąd i najczęściej wyłudzeniu pieniędzy lub zdobyciu haseł, numerów kart kredytowych, kont bankowych itp. Odbywa się to poprzez podanie danych na specjalnie spreparowanej stronie internetowej, która najczęściej wygląda identycznie jak właściwa. Oszust robi kopię strony np. banku, udostępnia ją w Internecie pod łudząco podobnym adresem jak oryginał i pozwala na logowanie się. (źródło: http://www.digipedia.pl)

Robak sieciowy – złośliwe oprogramowanie rozprzestrzeniające się w sposób automatyczny przez wykorzystanie do infekcji luk pozwalających na zdalne przejęcie kontroli nad systemem. W klasyfikacji jako „robak sieciowy" pojawiają się przypadki, w których potwierdzono obecność robaka w systemie lub charakterystyka objawów pozwalała na stwierdzenie, że właśnie robak był przyczyną incydentu.

Skanowanie portów to działanie polegające na wysyłaniu do określonego komputera w sieci pakietów TCP i UDP, a następnie badaniu nadchodzących odpowiedzi. Jako „skanowanie" zostały sklasyfikowane te incydenty, w których przyczyną zgłoszenia było zaobserwowane skanowanie i nie istniały przesłanki pozwalające na ustalenie szczegółowej przyczyny (np. robak).

Spam – masowa niezamawiana korespondencja; jako Spam w statystykach CERT Polska zostały sklasyfikowane zarówno zgłoszone zdarzenia rozsyłania spamu przez zainfekowane komputery jak i otrzymania takiej korespondencji przez polskich użytkowników.

SpamCop – międzynarodowy projekt, mający na celu walkę ze spamem. Internauci mogą przesyłać nagłówki wraz z treścią otrzymanego spamu do serwisu SpamCop, który prześle odpowiednie skargi do abuse. (źródło: http://pl.wikipedia.org)

Wirus komputerowy – złośliwe oprogramowanie, które nie potrafi rozprzestrzeniać się automatycznie, lecz do zainstalowania w systemie wymaga dodatkowego mechanizmu np. emaila, zarażonego programu wykonywalnego itp.

3.2 Liczba przypadków naruszających bezpieczeństwo teleinformatyczne

W roku 2006 odnotowaliśmy 2427 incydenty. W następnych rozdziałach znajduje się szczegółowa klasyfikacja zgłoszonych do nas incydentów.

3.3 Typy odnotowanych incydentów

Poniższa tabela przedstawia zbiorcze zestawienie statystyk odnotowanych incydentów. Klasyfikacja zawiera osiem głównych typów incydentów oraz kategorię „inne". Każdy z głównych typów zawiera podtypy, które najczęściej stanowią precyzyjny opis incydentu, z jakim mieliśmy do czynienia.

Typ/Podtyp incydentu	Liczba	Suma-typ	Procent-typ
Obraźliwe i nielegalne treści	2[3]	888	36,6
Spam	857[4]		
Dyskredytacja, obrażanie	21		
Pornografia dziecięca, przemoc[5]	8		
Złośliwe oprogramowanie	63	340	14
Wirus	28		
Robak sieciowy	55		
Koń trojański	191		
Oprogramowanie szpiegowskie	3		
Dialer	0		
Gromadzenie informacji	0	665	27,4
Skanowanie	658		
Podsłuch	2		
Inżynieria społeczna	5		
Próby włamań	1	91	3,7
Wykorzystanie znanych luk systemowych	28		
Próby nieuprawnionego logowania	62		
Wykorzystanie nieznanych luk systemowych	0		
Włamania	3	15	0,6
Włamanie na konto uprzywilejowane	3		
Włamanie na konto zwykłe	8		
Włamanie do aplikacji	1		
Atak na dostępność zasobów	2	42	1,7
Atak blokujący serwis (DoS)	20		
Rozproszony atak blokujący serwis (DDoS)	19		
Sabotaż komputerowy	1		
Atak na bezpieczeństwo informacji	0	5	0,2
Nieuprawniony dostęp do informacji	3		
Nieuprawniona zmiana informacji	2		
Oszustwa komputerowe	9	360	14,8

[3] Jeśli w głównym typie została podana liczba, to znaczy że dane przypadki nie zostały zaklasyfikowane do żadnej z podkategorii

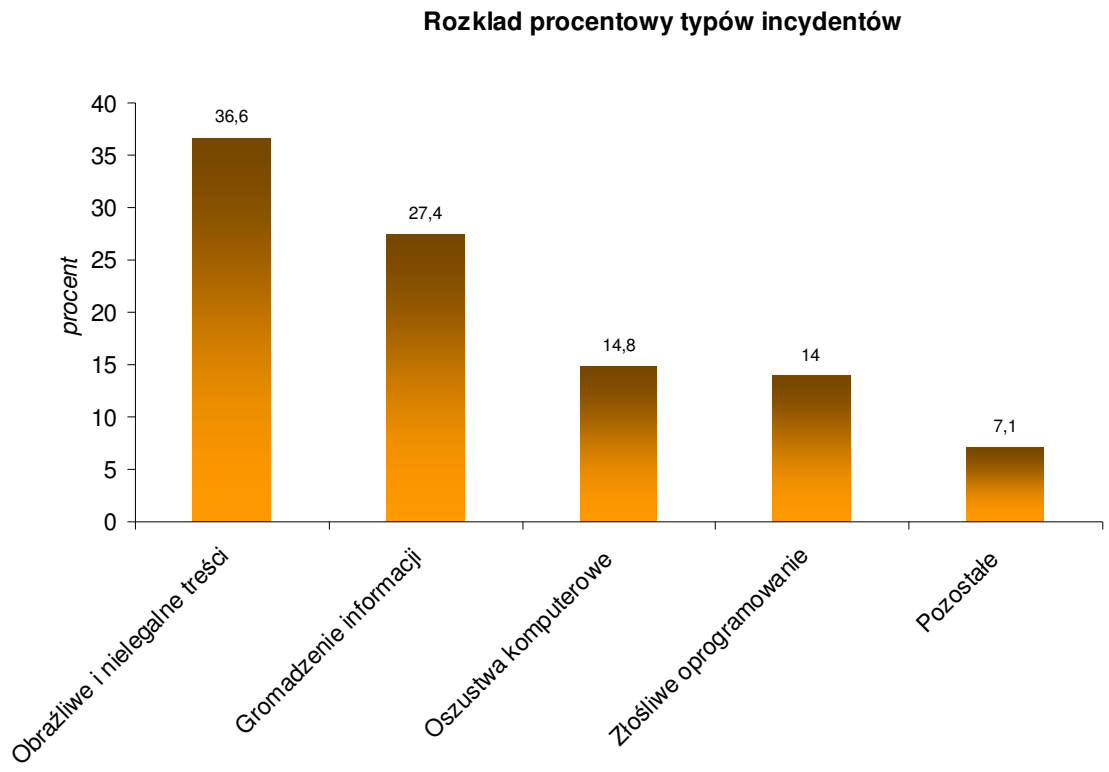
[4] Incydenty dotyczą serwerów rozsyłających spam, przy czym są to zazwyczaj maszyny „przejęte" przez hakera i wykorzystane bez wiedzy właściciela

[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/)

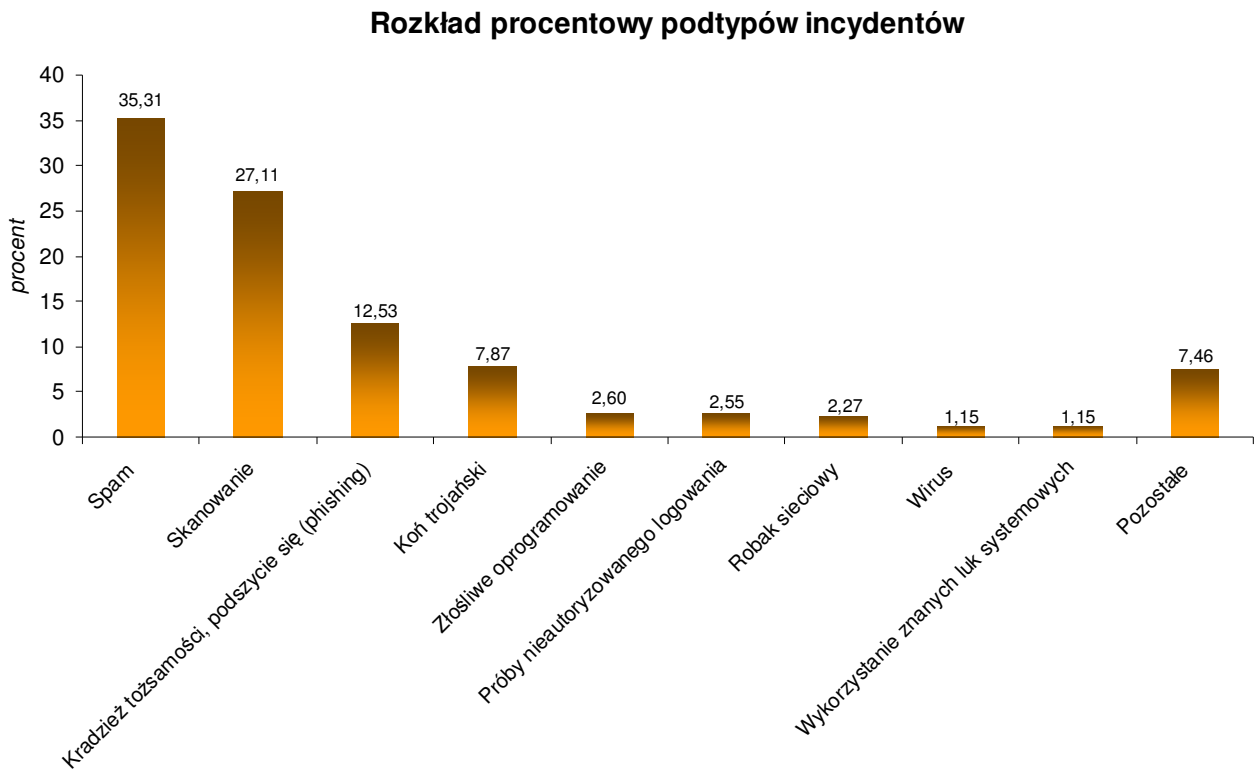
Nieuprawnione wykorzystanie zasobów	23		
Naruszenie praw autorskich	24		
Kradzież tożsamości, podszycie się (w tym Phishing)	304		
Inne	21	21	0,9
SUMA	2427	2427	100,0

3.4 Typy odnotowanych ataków

Poniższe wykresy przedstawiają rozkład procentowy typów i podtypów incydentów.

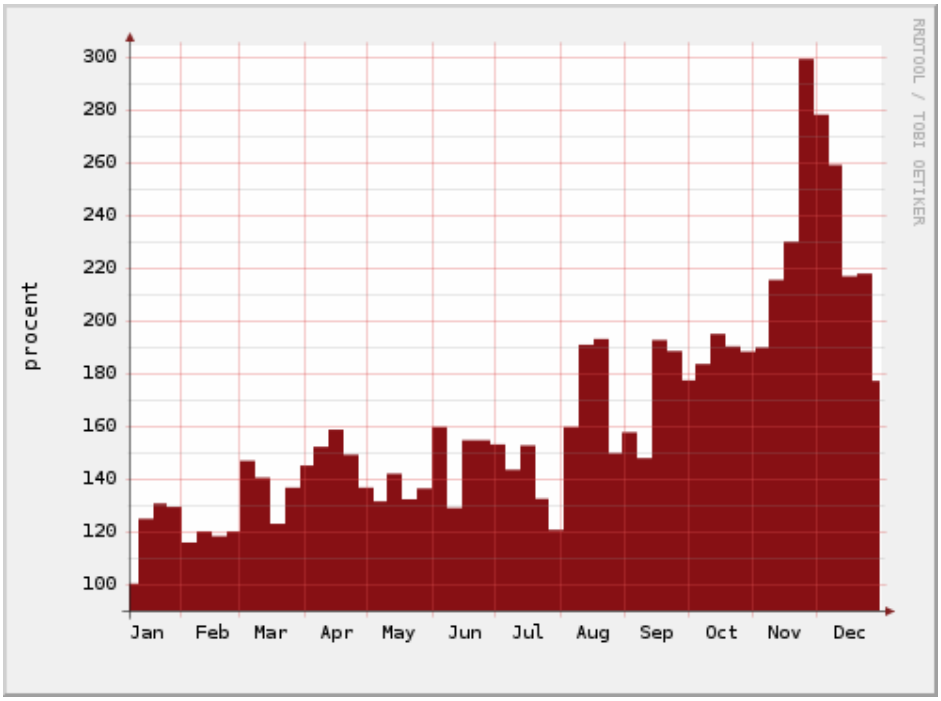


.



W roku 2006 najczęściej występujący typ incydentu stanowiły O*brażliwe i nielegalne treści* (36,6%), a w szczególności *Spam* (aż 35,3%). Większość zgłoszeń dotyczących spamu pochodziła z organizacji SpamCop oraz od użytkowników indywidualnych. W tym roku nastąpił znaczny wzrost niezamówionych ofert handlowych, szczególnie w ostatnim kwartale 2006 roku. Zjawisko to było na tyle silne, że zostało zauważone na poziomie operatorskim.

Poniżej zamieszczamy wykres ilościowy spamu otrzymywanego na konta pocztowe CERT Polska (I.2006 = 100%), na którym widać wyraźny wzrost w ostatnim kwartale oraz potwierdzenie rosnącego trendu dla tego zjawiska.



Drugim, co do liczebności typem incydentów były *Przypadki gromadzenia informacji* (27,4%), przy czym najczęściej mieliśmy do czynienia ze *Skanowaniami* (27,11%). W większości przypadków są to zdarzenia generowane przez botnety poszukujące nowych ofiar. Na przestrzeni roku 2006 zauważyliśmy działalność kilku bardzo dużych botnetów. Pod koniec roku bardzo aktywny był botnet, skanujący rzadko spotykaną do tej pory kombinację portów 139,1433/TCP. Z dużym prawdopodobieństwem można powiązać go ze wspomnianym wzrostem liczby rozsyłanego spamu. Duży odsetek zgłoszeń pochodził z systemu Arakis.

14,8 % incydentów zostało zaliczonych do typu *Oszustwa komputerowe.* W obrębie tego typu najliczniejszą grypę stanowią *Kradzieże tożsamości, podszycie się* (12,53%). Są to incydenty związane z phishingiem. Rok 2006 przyniósł wzrost tego zjawiska. Coraz częściej komputery polskich internautów są wykorzystywane do instalacji pułapek, które mają „złowić" dane autoryzacyjne klientów serwisów internetowych – przede wszystkim instytucji finansowych. W większości spraw atakujący podszywał się pod zagraniczne instytucje. Zgłaszane do nas były również próby podszywania się pod serwisy internetowe polskich banków. Były to jednak przypadki incydentalne. Większość tego typu zgłoszeń otrzymywaliśmy ze źródeł zagranicznych.

3.5 Zgłaszający, poszkodowani, atakujący

Na potrzeby prowadzenia statystyk odnotowywane są trzy kategorie podmiotów związanych z incydentami: zgłaszający incydent, poszkodowany w incydencie i odpowiedzialny za przeprowadzenie ataku, czyli atakujący. Dodatkowo, kategorie te uwzględniane są w rozbiciu na podmiot krajowy i podmiot zagraniczny.

Poniższa tabela przedstawia zbiorcze zestawienie danych dotyczących podmiotów incydentu.

Podmiot	Zgłaszający	%	Poszkodowany	%	Atakujący	%
Osoba prywatna	597	**24,6**	530	**21,8**	128	**5,3**
CERT[6]	926	**38,2**	0	**0**	0	**0**
ISP Abuse	8	**0,3**	0	**0**	0	**0**
Inna instytucja ds. Bezpieczeństwa	437	**18**	0	**0**	0	**0**
Firma komercyjna	371	**15,3**	1048	**43,2**	972	**40**
Ośrodek badawczy lub edukacyjny	23	**0,9**	141	**5,8**	411	**16,9**
Instytucja niekomercyjna	9	**0,4**	17	**0,7**	58	**2,4**
Jednostka rządowa	36	**1,5**	34	**1,4**	37	**1,5**
Nieznany	20	**0,8**	657	**27,1**	821	**33,8**
Kraj	1546	**63,7**	1488	**61,3**	1678	**69,1**
Zagranica	877	**36,1**	432	**17,8**	386	**15,9**
Nieznany	4	**0,2**	507	**20,9**	363	**15**

Najwięcej incydentów, podobnie jak w zeszłym roku, zgłosiły *zespoły reagujące* (38,2%). Część tych zgłoszeń pochodzi z systemu Arakis i była wygenerowana automatycznie, dzięki metodom identyfikacji ataków zaimplementowanych w system. Istotnymi źródłami zgłaszania incydentów były również O*soby Prywatne* (14,6%). Większość tego typu zgłoszeń była wysłana do nas za pośrednictwem formularza znajdującego się na stronie <https://www.cert.pl/formularz/formularz.php>. 18% zgłoszeń otrzymaliśmy od *Innych Instytucji ds. Bezpieczeństwa*. Niebagatelny wpływ miały tu incydenty dotyczące rozsyłania spamu

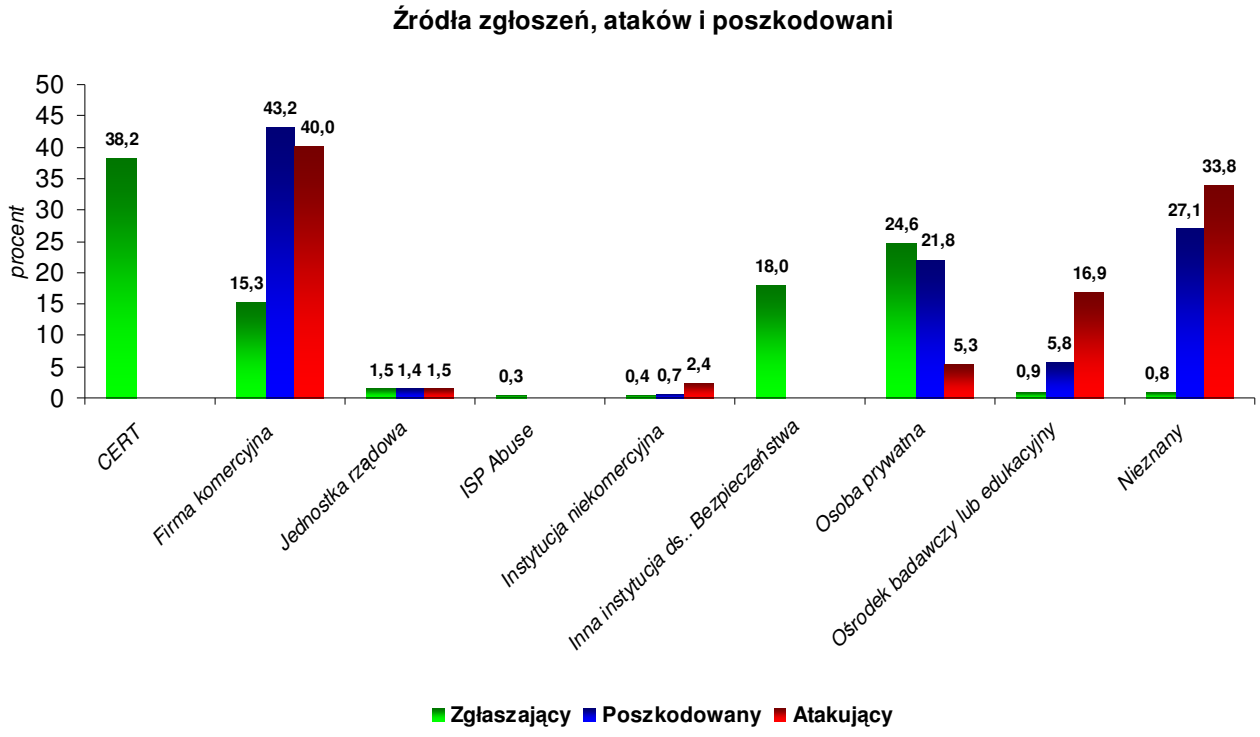
[6] Zawiera zgłoszenia pochodzące z systemów automatycznych obsługiwanych przez zespoły typu CERT, w tym także z systemu ARAKIS należącego do CERT Polska.

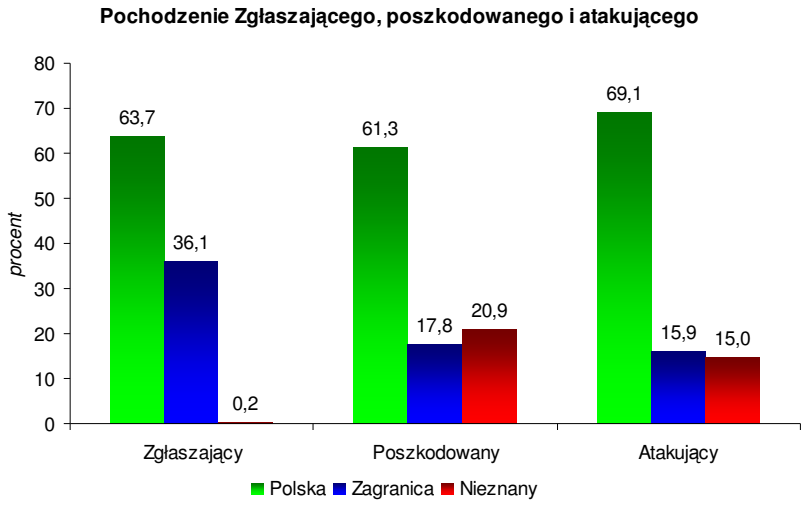
raportowane przez SpamCopa. Znaczący odsetek stanowiły zgłoszenia przesłane przez *Firmy Komercyjne* (15.3%).

Wśród *Poszkodowanych* najczęściej występowały *Firmy komercyjne* (43,2%). Aż w 27,1% przypadków nie znaliśmy poszkodowanego. Jest to wynik wzrostu zgłoszeń, które są przesyłane przez operatorów czy zespoły reagujące w czyimś imieniu (bez wskazania poszkodowanego). Dodatkowo, trudno jednoznacznie określić poszkodowanego, jeśli incydent dotyczy wielu podmiotów. Tradycyjnie duży odsetek poszkodowanych stanowią *Osoby prywatne* (21,8 %).

Spośród *Atakujących* najliczniejszą grupę stanowią *Firmy komercyjne* (40%). Jest to duży wzrost w porównaniu do roku poprzedniego. Wiele *Firm komercyjnych* posiada słabo zabezpieczone sieci. Często są one wykorzystywane do rozsyłania spamu czy skanowania sieci. Zmalała liczba incydentów, w których *Atakujący* pozostał nierozpoznany (33,1%). Pomimo tego, jest to nadal dość duży odsetek wszystkich incydentów. Przyczyny są identyczne jak w latach poprzednich. *Atakujący* zazwyczaj korzysta z „pośrednika", jakim jest np. serwer proxy, botnet czy skompromitowany host nieświadomego użytkownika. Trzecim w kolejności najczęściej atakującym okazały się *Ośrodki Badawcze lub Edukacyjne* (16,9%). W praktyce oznacza to, przede wszystkim, wyższe uczelnie i szkoły średnie. Niebagatelny wpływ na ten wynik mają sieci akademickie, które bardzo często są „wylęgarnią" wszelakiego rodzaju robaków .

Jeśli chodzi o klasyfikację dotyczącą źródła pochodzenia w rozumieniu geograficznym, to nadal na dość wysokim poziomie utrzymuje się odsetek incydentów „polskich". W większości przypadków zarówno *zgłaszający, poszkodowany i atakujący* pochodził z Polski (odpowiednio: 63,7%, 61,3%, 69,1%). Dla zagranicy te odsetki są znacznie mniejsze (odpowiednio: 36,1%, 17,8%, 15,9%). Niestety dość duży procent stanowią incydenty, w których pochodzenie *poszkodowanego* i *atakującego* pozostają nieznane (20,9% i 15%).

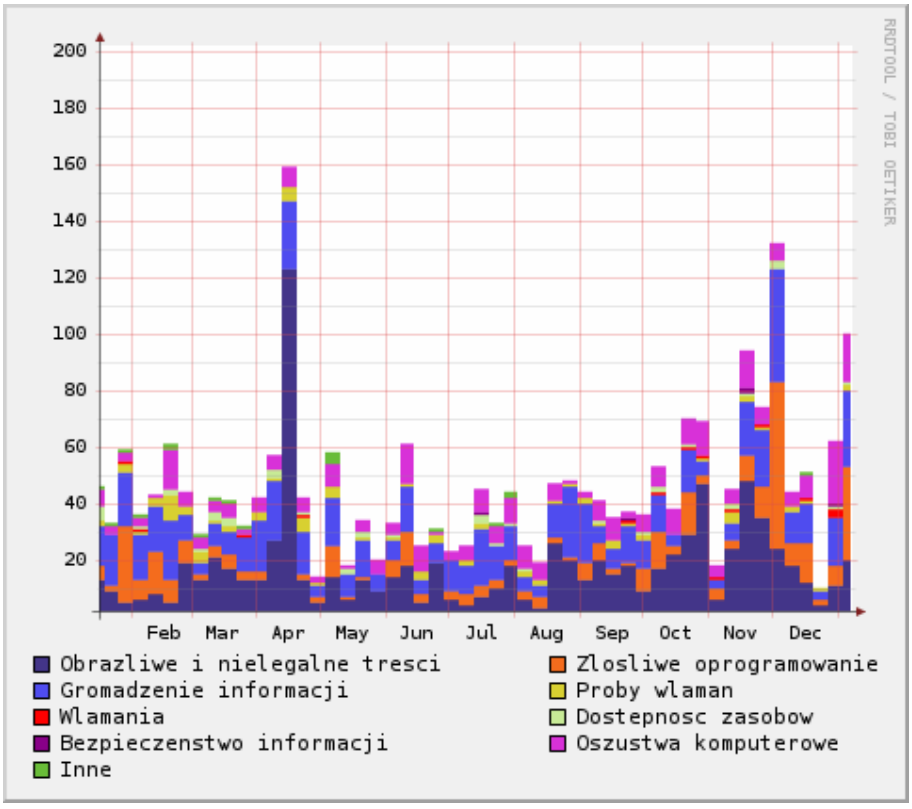




4 Statystyki dodatkowe

4.1 Liczba incydentów tygodniowo z podziałem na główne kategorie

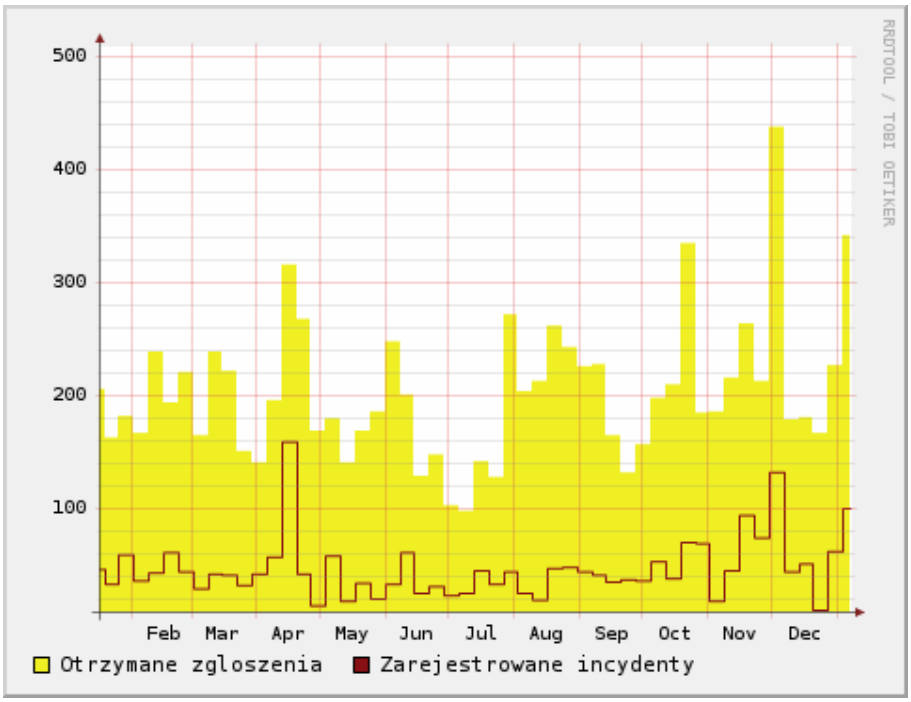
Poniższy wykres przedstawia liczbę incydentów zarejestrowanych w okresie tygodnia, z wyszczególnieniem głównych kategorii.



Średnio rejestrowaliśmy od 30 do 60 incydentów tygodniowo. Poszczególne przypadki wyraźnie większej liczby incydentów związane były z nagłym wzrostem ilości zgłaszanych przypadków spamu, które trafiały do systemu rejestracji oraz z działalnością bonetów. Można zauważyć, że pod koniec roku zwiększała się liczba rejestrowanych incydentów dotyczących *obraźliwych i nielegalnych treści* (w większości spamu) oraz *złośliwego oprogramowania* (najczęściej związane z końmi trojańskimi łączącymi komputery w botnet) i *oszustw komputerowych* (phishing).

4.2 Liczba zgłoszeń a liczba incydentów

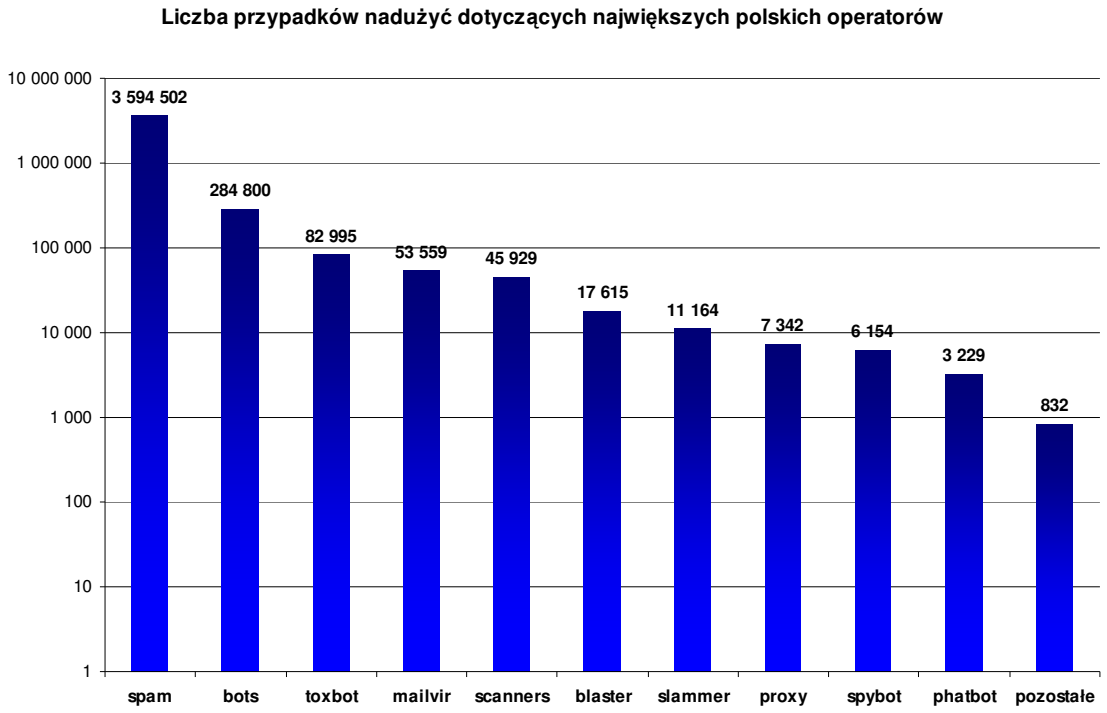
Poniższy wykres przedstawia liczbę zgłoszeń w stosunku do liczby incydentów.



W 2006 roku otrzymywaliśmy średnio 100-200 zgłoszeń tygodniowo – w sumie 6013. Oznacza to, że na jeden incydent przypadało średnio 2,48 zgłoszenia. Niemal identyczna proporcja zachodziła także w ubiegłym roku. W praktyce, w wielu przypadkach informacja o incydencie trafia do naszego zespołu z wielu źródeł. Często otrzymujemy niezależne zgłoszenia tego samego przypadku (np. zainfekowanego komputera będącego źródłem spamu) z automatycznych systemów detekcji oraz od użytkowników indywidualnych.

4.3 Liczba przypadków nadużyć dotyczących największych polskich operatorów

Poniższe dane prezentują liczbę przypadków nadużyć oszacowaną na podstawie wszelkich danych zgłaszanych do CERT Polska.



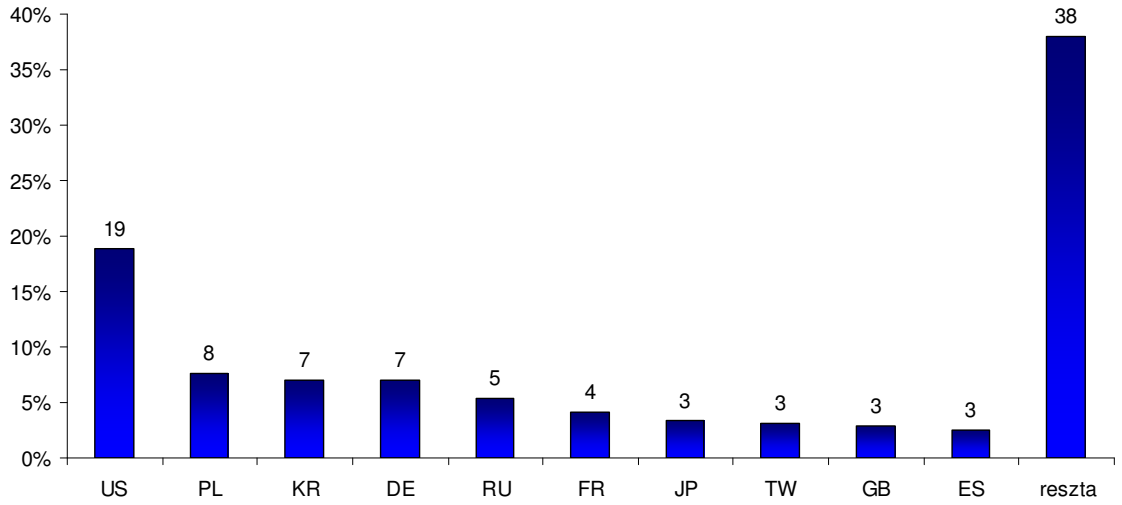
CERT Polska otrzymuje wiele informacji o poszczególnych wykrytych przypadkach infekcji, źródeł spamu, phishingu itp. znajdujących się w sieciach współpracujących z nami polskich operatorów internetowych. Dane te nie są uwzględniane w liczbie incydentów, ponieważ zgłoszenia takie nie są przez nas obsługiwane i monitorowane. Każdy z operatorów otrzymuje natomiast dane dotyczące swojej sieci. Wyjątkiem są przypadki phishingu oraz utrzymywania złośliwego oprogramowania (malware), które są przez CERT Polska monitorowane i zostały ujęte w statystykach incydentów.

Zwraca uwagę olbrzymia liczba przypadków wykorzystania zainfekowanych komputerów do rozsyłania spamu. Zidentyfikowano łącznie 3594502 takie przypadki, co stanowi 87,5% wszystkich nadużyć. Należy tu podkreślić, iż jest to liczba infekcji, a nie wysłanych w ich wyniku wiadomości. Ta ostatnia byłaby o kilka rzędów wielkości większa.

4.4 Rozkład procentowy zarejestrowanych adresów IP komputerów dystrybuujących złośliwe oprogramowanie.

CERT Polska zbiera także informacje dotyczące złośliwego oprogramowania atakującego polskie sieci. Poniższy wykres przedstawia rozkład procentowy zarejestrowanych adresów IP komputerów służących do dystrybucji takiego oprogramowania. Są to zazwyczaj przejęte maszyny, z których zainfekowane komputery pobierają aktualizacje robaka, dodatkowy złośliwy kod itp.

Rozkład procentowy zarejestrowanych adresów IP komputerów dystrybuujących złośliwe oprogramowanie.



Kraje, które znalazły się w czołówce można podzielić na:

- kraje o dużym nasyceniu szerokopasmowego dostępu do Internetu (np. Stany Zjednoczone, Korea, Japonia, Tajwan) – przejęte komputery w takich krajach są częstym narzędziem osób atakujących, ze względu na swoją dostępność i dobre parametry
- kraje bliskie nam geograficznie (np. Polska, Niemcy, Wielka Brytania) – tu wpływ ma rozsyłanie odnośników przez spam, komunikatory itp. a więc także więzi socjalne
- kraje będące „bezpiecznym portem" dla podziemia internetowego ze względu na prawodawstwo lecz także np. trudności organizacyjne u dużych dostawców internetowych oferujących dostęp dla znacznej liczby użytkowników końcowych – tutaj wymienić należy Rosję, Francję, Hiszpanię a także niestety Polskę

5 Wnioski i trendy

5.1 Najważniejsze zmiany w stosunku do roku poprzedniego (2005)

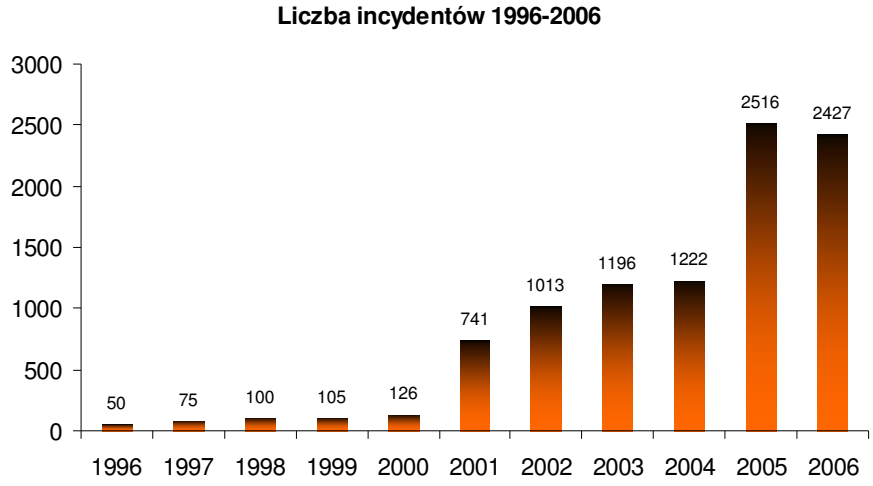
Odnotowaliśmy kilka istotnych zmian w stosunku do roku 2005, ale także utrzymanie się niektórych istotnych trendów. Poniżej przedstawiamy te, które są naszym zdaniem najważniejsze:

- Znacznie spadł udział skanowań - z 51,4% do 27,1%, częściowo jest to wynikiem lepszej identyfikacji rodzajów skanowań i ustalenia czy skanowanie powiązane jest z innym rodzajem ataku;
- Ośmiokrotnie zmalał odsetek incydentów dotyczących robaków sieciowych - z 18,4% do 2,3%;

- Ponad trzykrotnie wzrósł odsetek zgłoszonych serwerów rozsyłających spam – z 10,9% do 35,3%. Sama ilość spamu również znacząco wzrosła;
- Odnotowaliśmy czterokrotnie więcej incydentów dotyczących phishingu – wzrost z 3,1% do 12,5%, przy czym należy podkreślić, że wśród zgłoszeń były przypadki podszywania się pod polskie banki;
- Nadal najczęściej zgłaszającymi były zespoły typu CERT;
- Nadal zgłaszający, poszkodowany i atakujący pochodzili w większości z Polski;
- Zmniejszył się odsetek incydentów, w których nieznany był zgłaszający, poszkodowany i atakujący;
- Po raz pierwszy nie zanotowaliśmy większej liczby incydentów. Bezpośrednie przełożenie na taki stan rzeczy ma fakt, iż w zeszłym roku nie pojawił się żaden znaczący i „duży" robak sieciowy.

5.2 Liczba incydentów w latach 1996 – 2006

Poniższy wykres przedstawia liczbę incydentów w latach 1996 – 2006

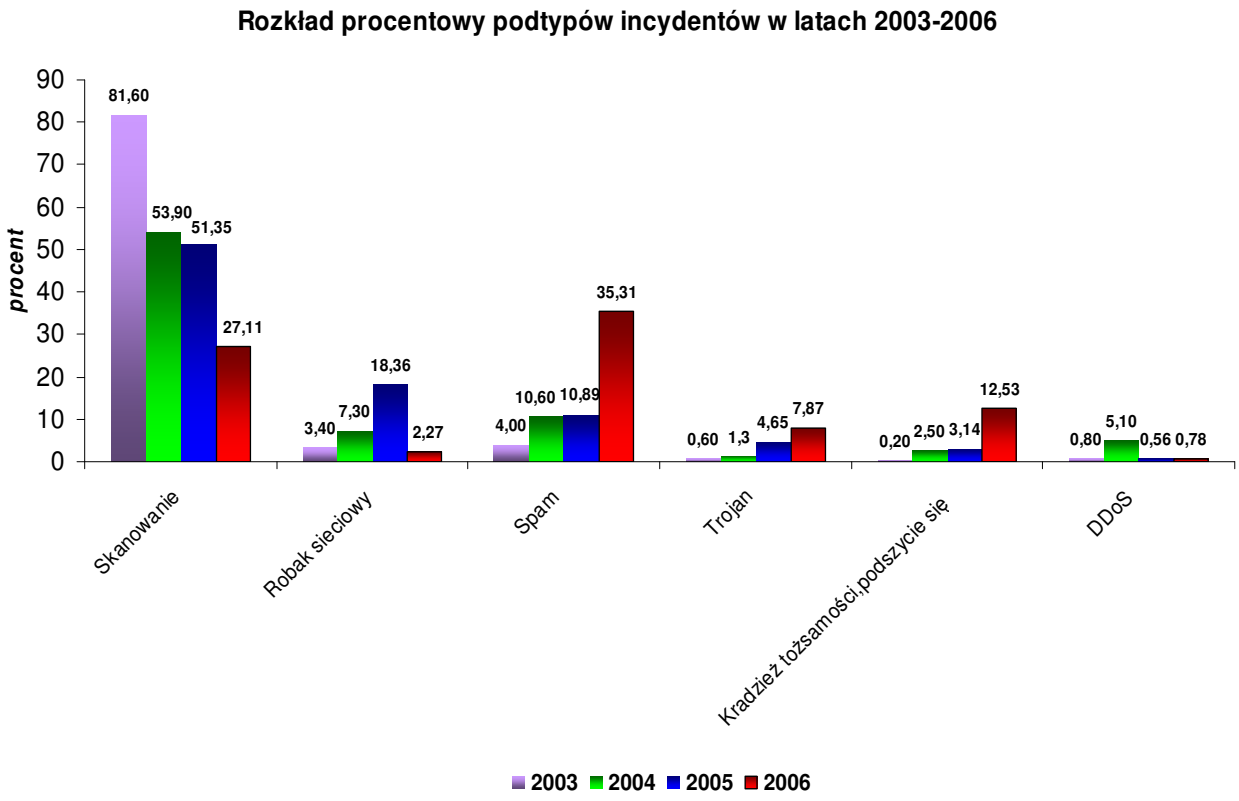


Liczba incydentów od kilku lat utrzymuje się na podobnym poziomie (z wyjątkiem gwałtownej zmiany w zeszłym roku spowodowanej uwzględnieniem nowych źródeł informacji, w szczególności systemu Arakis). W ubiegłym roku nie mieliśmy do czynienia z żadnymi nowymi epidemiami spowodowanymi lukami pozwalającymi na masowe, anonimowe przejęcia maszyn. Nastąpiła więc zmiana rozkładu udziałów poszczególnych rodzajów incydentów, co opisujemy w rozdziale 5.3.

W tym roku dysponujemy także dodatkowymi danymi, umożliwiającymi odniesienie liczby incydentów do rzeczywistej liczby zidentyfikowanych problemów w polskich sieciach. Dane te znajdują się w

punkcie 4.3. Jak łatwo zauważyć, liczby te różnią się o wiele rzędów wielkości. Oznacza to, że jedynie niewielki odsetek przypadków nadużyć dotyczących polskich sieci zostaje zgłoszony do zespołu CERT Polska i znajduje odbicie w statystykach. Pozostałe przypadki trafiają do zespołów *abuse* poszczególnych operatorów. Ze względu na ich liczbę, zajmowanie się nimi jedynie przez likwidację skutków jest bardzo nieefektywne.

5.3 Rozkład procentowy podtypów incydentów w latach 2003-2006.



Od roku 2003 statystyki są tworzone w oparciu o tę samą klasyfikację. Umożliwia to nam porównanie rozkładu procentowego incydentów na przestrzeni ostatnich czterech lat. Przez cały ten okres *skanowania* utrzymywały się na wysokim poziomie, przy czym można zauważyć tendencję spadkową. W ostatnim roku odnotowaliśmy prawie dwukrotny spadek udziału tego typu incydentów w stosunku do lat 2004 i 2005. W odniesieniu do roku 2003 spadek ten jest niemal trzykrotny. Odwrotna sytuacja dotyczy *spamu*. W ostatnim roku nastąpił znaczny wzrost odsetka tego typu incydentów, ponad trzykrotny względem dwóch poprzednich lat i prawie dziewięciokrotny względem roku 2003. Coraz większy problem zaczyna stanowić *phishing* (*kradzież tożsamości, podszycie się*). Kolejne lata przynoszą rozwój tego zjawiska. O ile w roku 2003 incydenty w tej kategorii stanowiły zaledwie 0,2% wszystkich spraw, to w roku 2006 już co ósmy incydent dotyczył tego zjawiska. Po trzyletnim okresie wzrostu incydentów dotyczących *robaka sieciowego*, nastąpił niespodziewany spadek (aż ośmiokrotny). Powoli, aczkolwiek regularnie rośnie liczba incydentów powodowanych przez *konie trojańskie*.

5.4 Najważniejsze trendy i zjawiska obserwowane w roku 2006

Poniżej przedstawiamy najbardziej istotne, naszym zdaniem, trendy i zjawiska występujące w roku 2006, wynikające zarówno z obsługi incydentów, jak i z innych obserwacji poczynionych przez CERT Polska:

- Zmalała liczba *skanowań*. Są dwie główne przyczyny takiego stanu rzeczy. Po pierwsze, nie pojawiły się w 2006 roku luki, dzięki którym możliwe było łatwe i masowe pozyskiwanie nowych członków botnetów. Po drugie, botnety„ustabilizowały" się i nie są nastawione tylko i wyłącznie na poszukiwanie nowych członków, a ich główna działalność polega na rozsyłaniu spamu, hostowaniu stron phishingowych itp. Podsumowując, skończyła się „rekrutacja", a zaczął się okres „czerpania korzyści".

- Zmniejszyła się liczba incydentów dotyczących *robaka sieciowego*. Przyczyny są podobne jak w przypadku *skanowań*, ze szczególnym uwzględnieniem braku „spektakularnych" luk.

- Częściej notowaliśmy incydenty związane z phishingiem. Większość spraw dotyczyła fałszywych stron zagranicznych banków, umieszczonych na polskich serwerach. Były to zazwyczaj maszyny przejęte przez hakera.

- Pojawił się *phishing* dotyczący polskich banków. Spodziewamy się wzrostu tego zjawiska, przy czym wprowadzane przez banki nowe zabezpieczenia (np.: kody sms) i stosowane dość wysokie standardy bezpieczeństwa praktycznie uniemożliwiają dokonanie jakiejkolwiek operacji, nawet przy przejęciu loginu i hasła do konta.

- Znacznie zwiększyła się liczba rozsyłanego *spamu*. Zgłoszenia odnotowane przez CERT dotyczą maszyn, za pośrednictwem których jest rozsyłany *spam*. Należy podkreślić, że większość z tych maszyn jest wykorzystywana przez osoby z zewnątrz, a ich właściciele nie zdają sobie spraw, że są narzędziem w ręku spamera.

- Nasiliło się używanie nowej techniki oszukiwania filtrów antyspamowych. W mailu treść zastąpiono obrazkiem, co utrudnia analizę zawartości takiej wiadomości. Metoda ta jednak wydaje się zbyt „nisko dochodowa", aby przetrwała dłuższy okres. Po pierwsze pojawiły się rozwiązania, dzięki którym można odczytać tekst zawarty w obrazku. Po drugie, spamer musi co pewien czas zmieniać „zawartość" obrazka, aby nie można było go rozpoznać np. po sumie kontrolnej pliku. Po trzecie i najważniejsze, brak w takim spamie bezpośredniego odsyłacza do reklamowanego produktu. Niewielki odsetek odbiorców decyduje się na ręczne przepisanie odsyłacza, który widoczny jest na obrazku.

- Szczególny wzrost *spamu* odnotowaliśmy w ostatnim kwartale 2006 roku. Był on tak duży, że został zauważony na poziomie operatorskim. Przewidujemy, że tendencja ta zostanie podtrzymana.

- Odsetek ataków *DDoS* był stosunkowo niewielki, przy czym odnotowaliśmy kilka „spektakularnych" ataków skierowanych na duże serwisy

- Sieci akademickie są nadal niezabezpieczone i zaniedbane. Poziom świadomości dotyczącej bezpieczeństwa wśród członków takich sieci jest zazwyczaj znikomy. Sieci akademickie są swoistym „inkubatorem" dla robaków internetowych.

- W roku 2006 CERT przekazywał największym operatorom dane z systemów automatycznych, dotyczące działalności *robaków, spamu, phishingu* itp. Skala zjawiska jest tak ogromna, że nie ma możliwości „ręcznego" obsłużenia takich zgłoszeń. Niezbędne wydaje się wypracowanie nowych mechanizmów i zmiana filozofii w podejściu do obsługi incydentu. Obsługa taka musi wykraczać poza usuwanie skutków już istniejącego incydentu i powinna się skupić na niedopuszczeniu do jego powstania. W ramach „Forum Polskich Zespołów Reagujących" powstał pomysł, aby stworzyć narzędzie, dzięki któremu będzie można zablokować dostęp do maszyn stanowiących szczególne zagrożenie w sieci (blackholing międzyoperatorski). Dzięki temu można by np. odciąć polskich użytkowników Internetu od znanych kontrolerów botnetów, co z pewnością przełożyłoby się na zmniejszenie liczby incydentów.

- Jak w zeszłych latach, działania hakerów są coraz bardziej zaawansowane, a wykorzystywane mechanizmy coraz bardziej skomplikowane.

6 Kontakt

Zgłaszanie incydentów:	cert@cert.pl, spam: spam@cert.pl
Informacja:	info@cert.pl
Klucz PGP:	ftp://ftp.nask.pl/pub/CERT_POLSKA/cert_polska_pgp_keys/CERT_POLSKA.pgp
Strona WWW:	http://www.cert.pl/
Feed RSS:	http:/www..cert.pl/rss
Adres:	NASK / CERT Polska
	ul. Wąwozowa 18
	02-796 Warszawa
tel.:	+48 22 3808 274
fax:	+48 22 3808 399