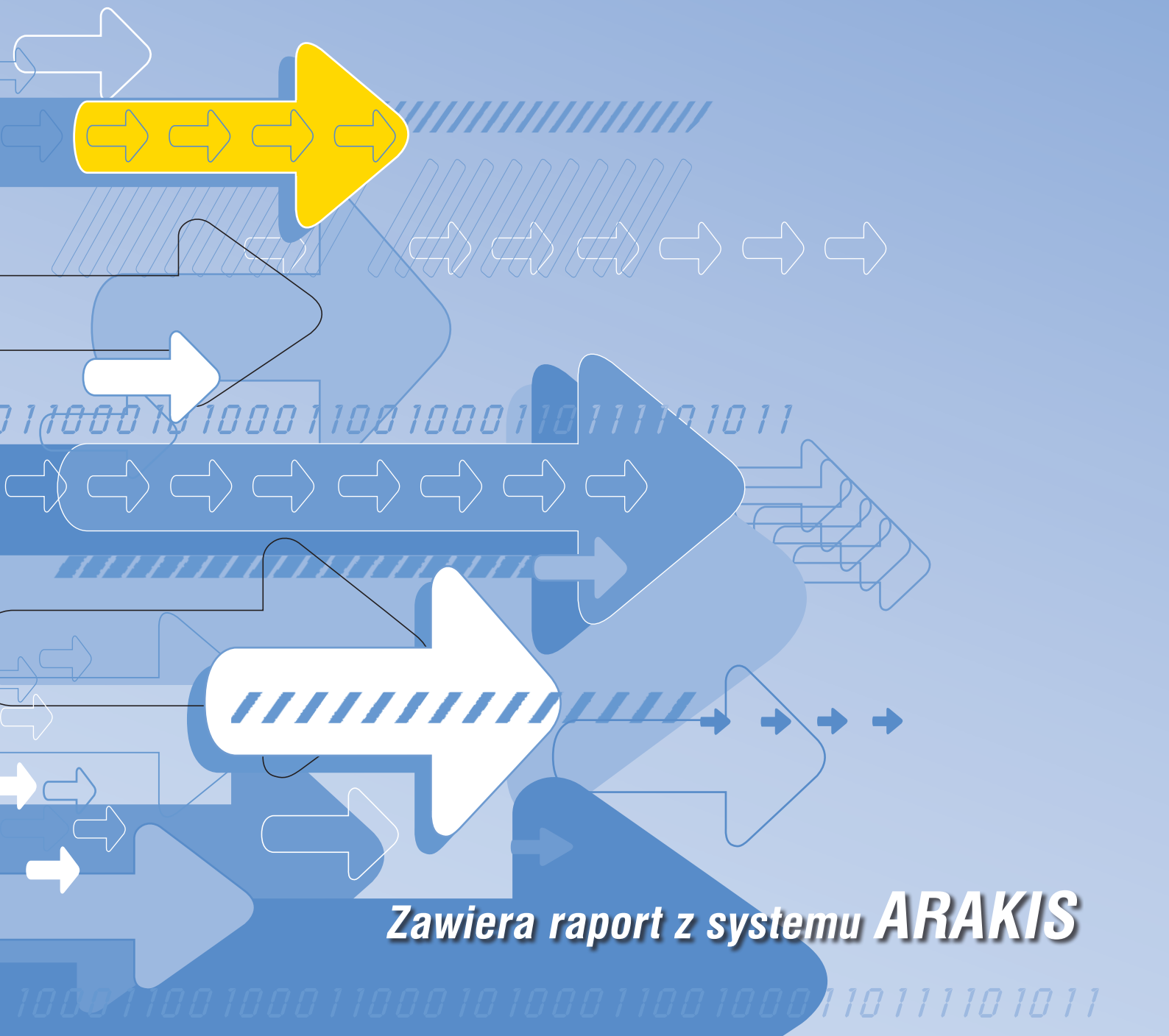
RAPORT 2008

NASK

CERT POLSKA

Analiza incydentów naruszających
bezpieczeństwo teleinformatyczne
zgłaszanych do zespołu CERT Polska w roku 2008



Zawiera raport z systemu **ARAKIS**

SPIS TREŚCI

RAPORT CERT POLSKA Z OBSŁUGI INCYDENTÓW W ROKU 2008

RAPORT Z SYSTEMU ARAKIS

RAPORT CERT POLSKA Z OBSŁUGI INCYDENTÓW W ROKU 2008

1. DZIAŁALNOŚĆ ZESPOŁU

CERT Polska działa od 1996 roku, a od 1997 jest członkiem FIRST (Forum of Incidents Response and Security Teams – *www.first.org*) – największej na świecie organizacji zrzeszającej zespoły reagujące i zespoły bezpieczeństwa z całego świata. Od 2000 roku jest także członkiem inicjatywy zrzeszającej europejskie zespoły reagujące – TERENA TF-CSIRT (*www.terena.org/activities/tf-csirt*) i działającej przy tej inicjatywie organizacji Trusted Introducer[1] (*www.trusted-introducer.org*). W ramach tych stowarzyszeń współpracuje z podobnymi zespołami na całym świecie, zarówno w działalności operacyjnej, jak też badawczo-wdrożeniowej.

CERT Polska (Computer Emergency Response Team Polska – *www.cert.pl*) jest zespołem działającym w ramach Naukowej i Akademickiej Sieci Komputerowej (*www.nask.pl*), zajmującym się reagowaniem na zdarzenia naruszające bezpieczeństwo w Internecie.

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

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 *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, rejestracji, klasyfikacji i statystyk incydentów,
- udział w krajowych i międzynarodowych projektach związanych z tematyką bezpieczeństwa teleinformatycznego.

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. CERT Polska 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, zarówno w kolejnych latach, jak i różnic pomiędzy raportami CERT Polska i raportami innych zespołów reagujących. W tym roku po raz szósty z kolei przygotowaliśmy statystyki zgodnie z klasyfikacją wypracowaną w ramach projektu eCSIRT.net (*http://www.ecsirt.net/cec/service/documents/wp4-pub-userguide-v10.html#HEAD7*).

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

STATYSTYKI INCYDENTÓW 3.

3.1 Liczba przypadków naruszających bezpieczeństwo teleinformatyczne

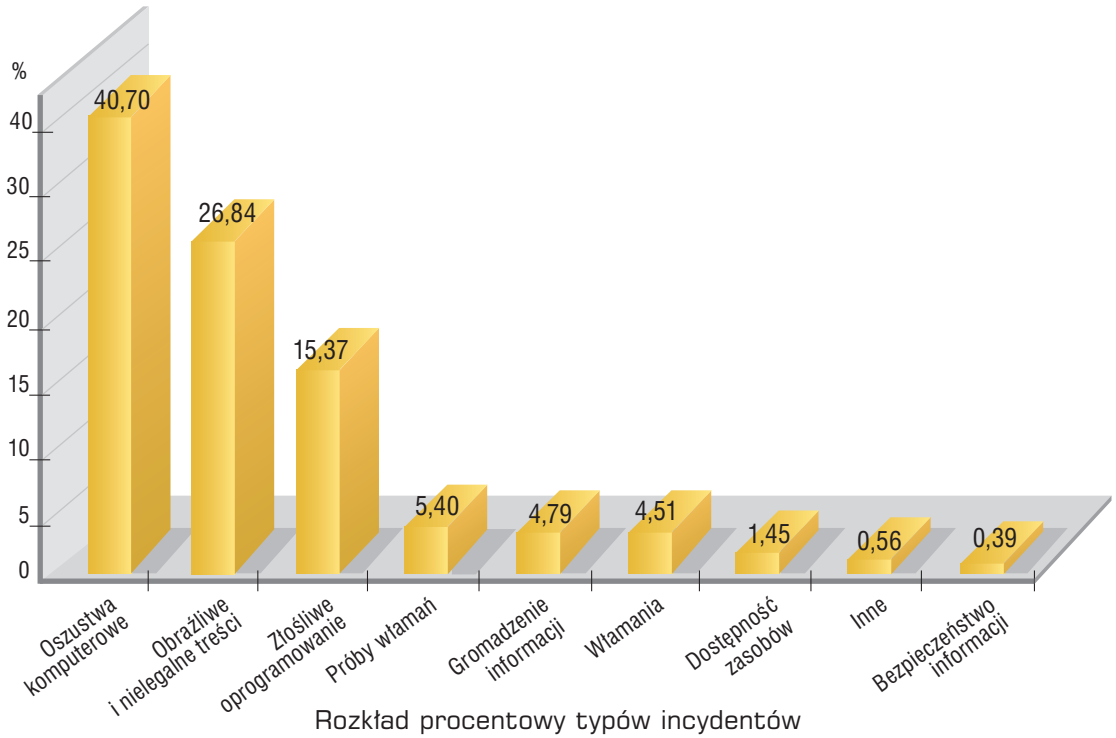
W roku 2008 odnotowaliśmy 1796 incydentów. W następnych rozdziałach znajduje się szczegółowa klasyfikacja przypadków zgłoszonych do CERT Polska w minionym roku.

3.2 Typy odnotowanych incydentów

Tabela na str. 6 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.

3.3 Typy odnotowanych ataków

Poniższy wykres przedstawia rozkład procentowy typów incydentów; na str. 7 prezentujemy rozkład procentowy podtypów incydentów.



Rozkład procentowy typów incydentów

Typ/Podtyp incydentu	Liczba	Suma-typ	Procent-typ
Obraźliwe i nielegalne treści	0	482	26,84
Spam	466		
Dyskredytacja, obrażanie	8		
Pornografia dziecięca, przemoc[3]	8		
Złośliwe oprogramowanie	143	276	15,37
Wirus	3		
Robak sieciowy	24		
Koń trojański	104		
Oprogramowanie szpiegowskie	2		
Dialer	0		
Gromadzenie informacji	0	86	4,79
Skanowanie	84		
Podsłuch	0		
Inżynieria społeczna	2		
Próby włamań	11	97	5,40
Wykorzystanie znanych luk systemowych	24		
Próby nieuprawnionego logowania	62		
Wykorzystanie nieznanych luk systemowych	0		
Włamania	2	81	4,51
Włamanie na konto uprzywilejowane	6		
Włamanie na konto zwykłe	16		
Włamanie do aplikacji	57		
Atak na dostępność zasobów	0	26	1.45
Atak blokujący serwis (DoS)	4		
Rozproszony atak blokujący serwis (DDoS)	22		
Sabotaż komputerowy	0		
Atak na bezpieczeństwo informacji	1	7	0,39
Nieuprawniony dostęp do informacji	5		
Nieuprawniona zmiana informacji	1		
Oszustwa komputerowe	10	731	40,70
Nieuprawnione wykorzystanie zasobów	5		
Naruszenie praw autorskich	316		
Kradzież tożsamości, podszycie się (w tym phishing)	400		
Inne	10	10	0,56
SUMA	1796	1796	100

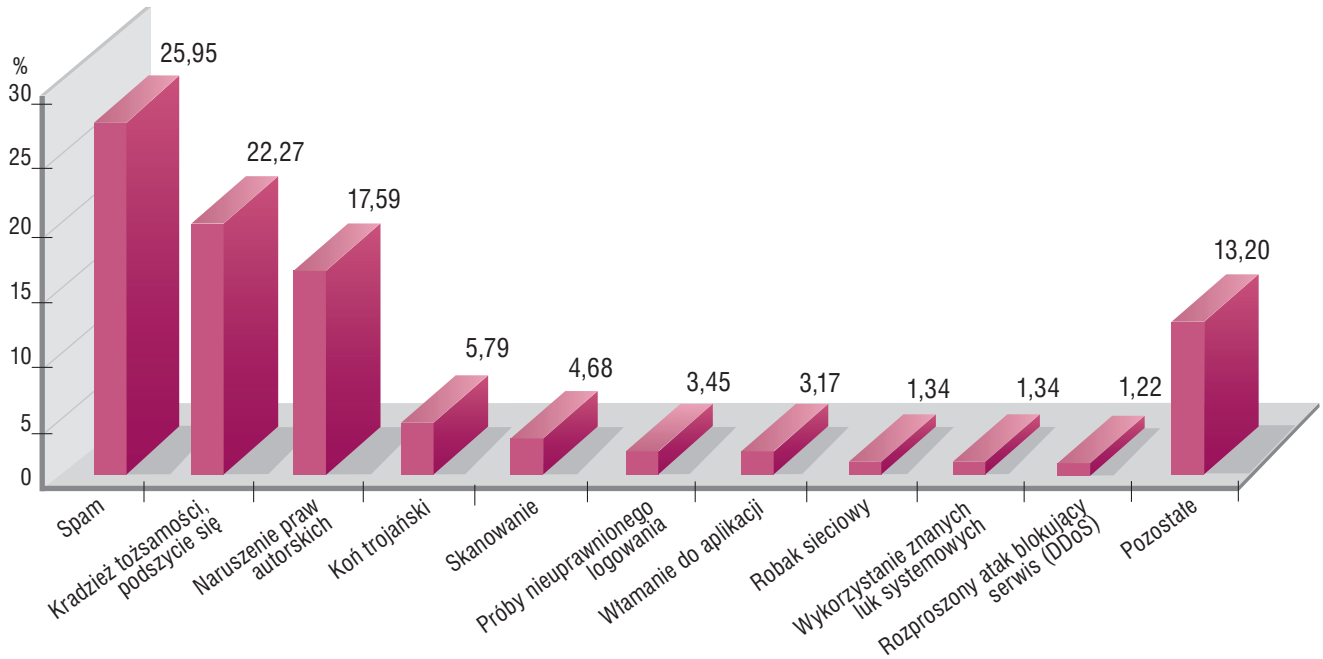
[3] Wszelkie zgłoszenia dotyczące nielegalnych treści, w rozumieniu polskiego prawa, kierowane są do zespołu Dyżurnet.pl, również działającego w ramach NASK (www.dyzurnet.pl).

W 2008 roku znacząco uwydatniła się przewaga kategorii *Oszustwa komputerowe*, stanowiącej przeszło 40% wszystkich obsłużonych przez nas incydentów. Na typ ten składa się przede wszystkim *phishing* – średnio co piąty incydent dotyczył tego przestępstwa (podtyp *Kradzież tożsamości*, *podszycie się* na wykresie poniżej). Niemały udział miały także zgłoszone przypadki *Naruszenia praw autorskich*, stanowiące 17,59% incydentów. W praktyce część zgłoszeń z tej ostatniej podkategorii nie jest obsługiwana, ponieważ nie spełnia wymogów dostatecznej wartości operacyjnej (np. brak możliwości identyfikacji urządzenia w sieci z NAT).

Drugim najsilniej reprezentowanym typem incydentów były *Obraźliwe i nielegalne treści*. Podobnie jak w 2007 roku mniej więcej co czwarty incydent kwalifikował się do tej kategorii. Zaliczają się tu prawie wyłącznie przypadki dotyczące *Spamu*, najliczniej reprezentowanego podtypu incydentów. Warto podkreślić, że chodzi tu przede wszystkim o przypadki rozsyłania niechcianej korespondencji, a nie zgłoszenia przypadków jej otrzymania, ponieważ tymi ostatnimi zajmujemy się w bardzo ograniczonym zakresie, podyktowanym polskim prawem.

Kolejną kategorią jest *Złośliwe oprogramowanie* – 15,37% wszystkich incydentów. Były to często przypadki stron zawierających złośliwe oprogramowanie, automatycznie infekujące komputer osoby odwiedzającej (*drive by download*) lub inne przypadki o skomplikowanych metodach dystrybucji – nie ujęte w związku z tym w szczegółowej klasyfikacji podtypów. Najliczniejszy podtyp *Koń trojański* stanowił połowę przypadków złośliwego oprogramowania.

Warto zauważyć, że zdecydowanie poza czołówką – dopiero na 5. miejscu z udziałem nieprzekraczającym 5% znalazło się *Gromadzenie informacji*, a więc głównie *Skanowanie*. Przez



Rozkład procentowy podtypów incydentów

wiele lat jeden z najpowszechniej zgłaszanych typów incydentów, w tej chwili uważany jest za normalny szum internetowy. Zresztą jego skala również uległa znacznemu zmniejszeniu w wyniku obniżenia się skuteczności automatycznych masowych ataków na zdalne usługi – najczęściej przeprowadzanych przez robaki internetowe. Wraz z całkowitym niemal zniknięciem ze statystyk tego podtypu incydentów (zaledwie 1,34%) jest to jeden z wyznaczników trendów w zagrożeniach na przestrzeni ostatnich dwóch lat.

3.4 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.

Tabela na str. 9 przedstawia zbiorcze zestawienie danych dotyczących podmiotów incydentu.

W roku 2008 najwięcej zgłoszeń otrzymaliśmy od *Firm komercyjnych* (39,37%). Były to głównie przypadki *Naruszeń praw autorskich* oraz zgłaszany przez banki *Phishing*. 24,89% zgłoszeń pochodziło z *Innych instytucji ds. bezpieczeństwa*. Większościowy udział ma tutaj SpamCop, który bardzo aktywnie raportował urządzenia wykorzystywane do rozsyłania spamu. Trzecim co do liczebności źródłem zgłaszania incydentów były zespoły CERT (14,2%). W większości były to zgłoszenia wygenerowane automatycznie przez system ARAKIS (*www.arakis.pl*). Na poziomie powyżej 10% utrzymała się liczba zgłoszeń pochodzących od *Osób prywatnych*.

Wśród *Poszkodowanych* najczęściej występowały *Firmy komercyjne* (49,11%). Sytuacja taka ma miejsce od kilku lat, a dodatkowo zauważalny jest trend wzrostowy w udziale procentowym. Wynika to po pierwsze ze wzrostu incydentów związanych z *Phishingiem*, gdzie jako *Poszkodowanego* przyjmuje się bank (w większości przypadków nie posiadamy danych klientów banku), po drugie z aktywności podmiotów dochodzących praw z tytułu *Naruszeń praw autorskich*. Aż w 35,7% przypadków nie można było ustalić poszkodowanego, ponieważ były to w głównej mierze zgłoszenia przesyłane przez SpamCopa oraz zespoły reagujące w imieniu osób trzecich.

Wśród *Atakujących*, tak jak w poprzednich kategoriach, największy udział mają *Firmy komercyjne* (56,46%). W 25,39% *Atakujący* pozostawał *Nieznany*. Tak jak w latach poprzednich, często nie jesteśmy w stanie zidentyfikować prawdziwego źródła ataku. *Atakujący* ukrywa się za serwerem Proxy, botnetem czy przejętą maszyną nieświadomej ofiary. Dodatkowo rozwijają się już istniejące oraz powstają nowe firmy działające na granicy prawa, udostępniające łącza, serwery fizyczne i wirtualne, na których umieszczane są nielegalne treści. Oczywiście firmy takie zapewniają pełną anonimowość swoim klientom.

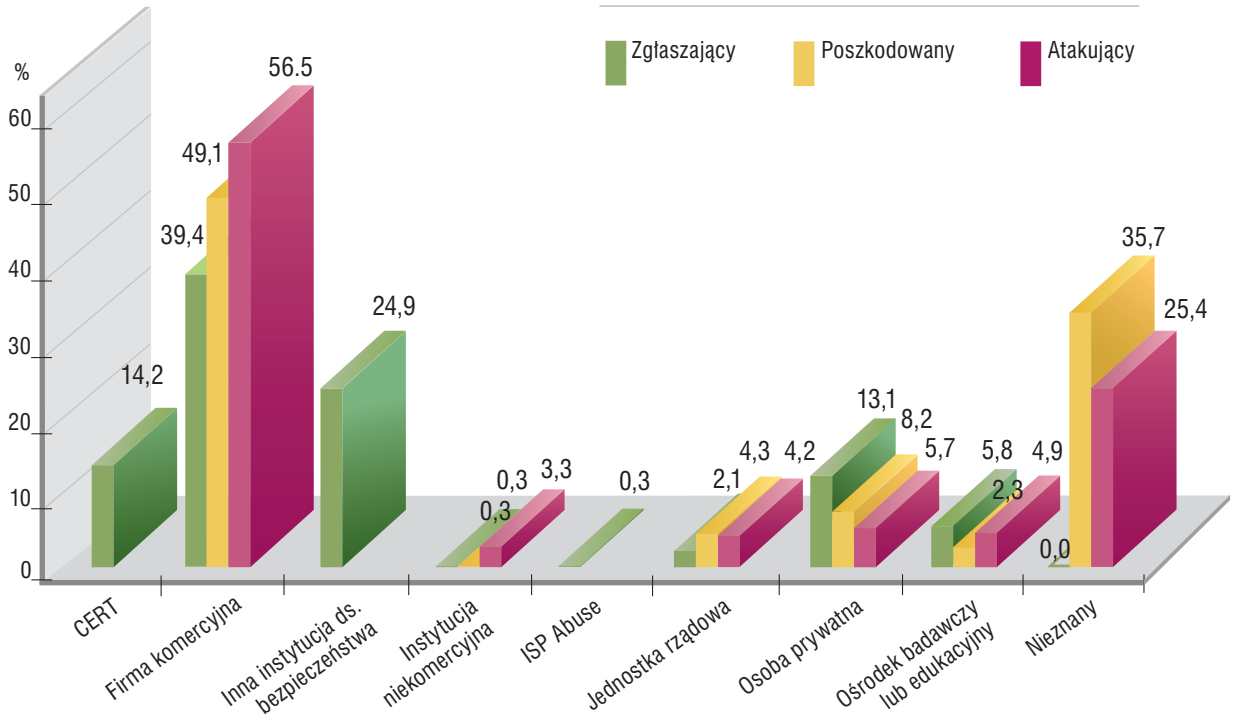
W kategorii źródło pochodzenia w rozumieniu geograficznym, jeszcze bardziej niż w roku poprzednim zarysowała się różnica wśród *Zgłaszających*. W 2008 roku mieliśmy ponad dwa razy więcej *Zgłaszających* z zagranicy, niż z Polski (68,88% oraz 31,07%). Duży wpływ ma tutaj

Podmiot	Zgłaszający	%	Poszkodowany	%	Atakujący	%
Osoba prywatna	236	13,14	148	8,24	103	5,73
CERT[4]	255	14,20	0	0,00	0	0,00
ISP Abuse	5	0,28	0	0,00	0	0,00
Inna instytucja ds. bezpieczeństwa	447	24,89	0	0,00	0	0,00
Firma komercyjna	707	39,37	882	49,11	1014	56,46
Ośrodek badawczy lub edukacyjny	104	5,79	42	2,34	88	4,90
Instytucja niekomercyjna	5	0,28	6	0,33	59	3,29
Jednostka rządowa	37	2,06	77	4,29	76	4,23
Nieznany	0	0,00	641	35,69	456	25,39
Kraj	558	31,07	415	23,11	1495	83,24
Zagranica	1237	68,88	761	42,37	152	8,46
Nieznany	1	0,06	620	34,52	149	8,3

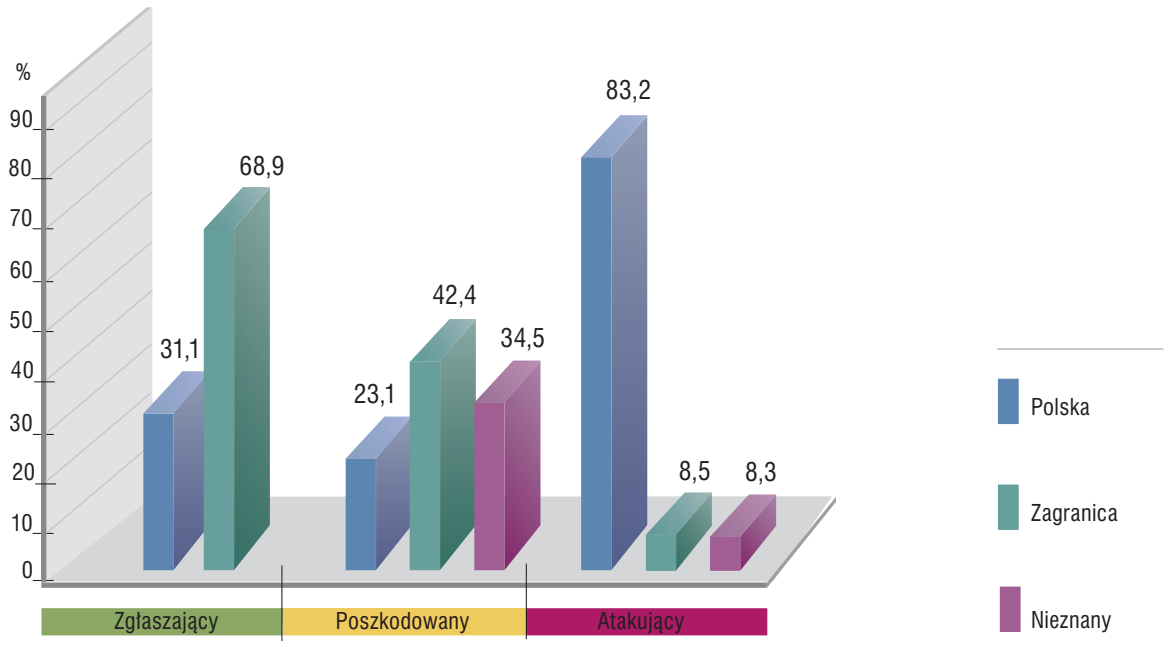
Dane dotyczące podmiotów incydentów

mniejsza liczba zgłoszeń dotyczących *Skanowań* generowanych przez system ARAKIS oraz zgłoszenia ze SpamCopa. *Poszkodowany* najczęściej pochodził z zagranicy (42,37%). W 34,52% był nieznany (zgłoszenia w imieniu osób trzecich ze SpamCopa). 23,11% *Poszkodowanych* pochodziło z Polski. Grupa *Atakujących* najczęściej pochodziła z Polski (aż 83,2%). Niebagatelny wpływ mają tu zgłoszenia dotyczące *Spamu* oraz *Naruszenia praw autorskich*. Udział *Atakujących* z zagranicy oraz tych, których pochodzenie jest nieznane jest stosunkowo niewielki i wynosi odpowiednio 8,46% i 8,3%.

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



Źródła zgłoszeń, ataków i poszkodowani



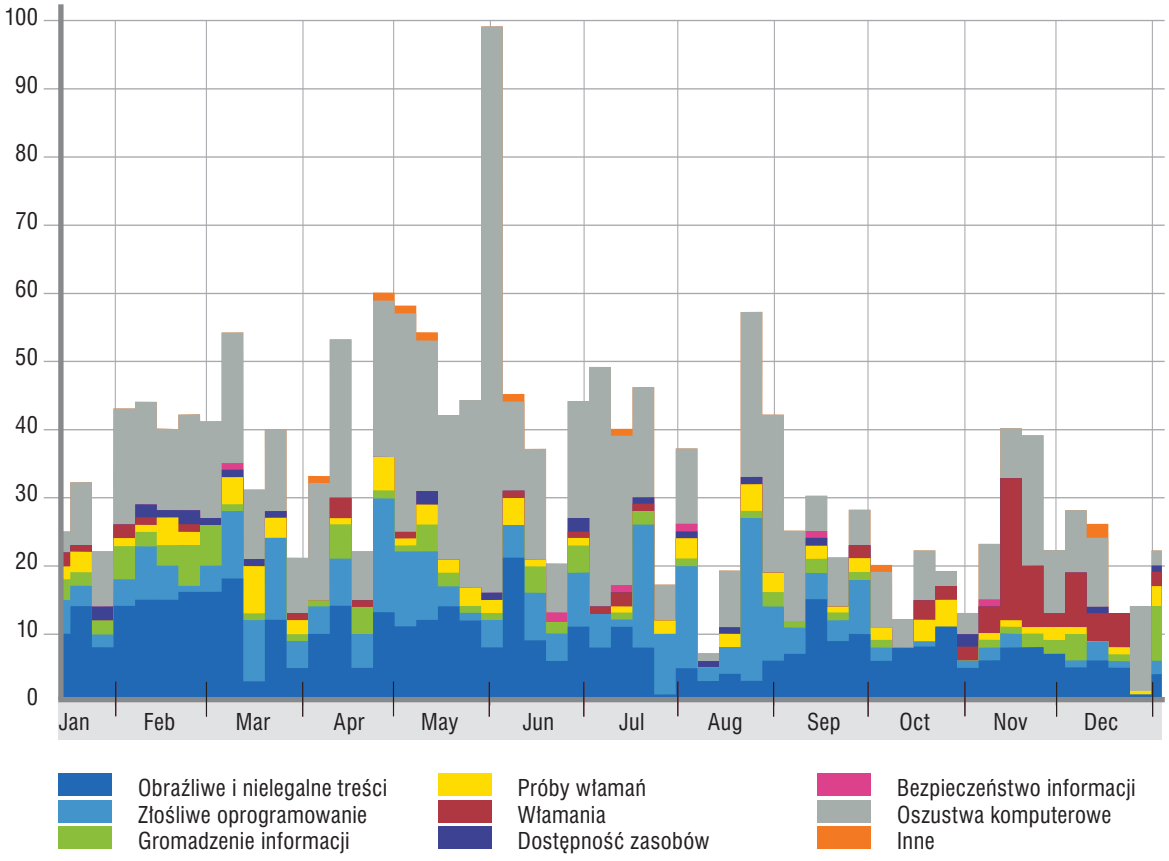
Pochodzenie zgłaszającego, poszkodowanego i atakującego

STATYSTYKI DODATKOWE 4.

4.1 Liczba incydentów zgłaszanych tygodniowo z podziałem na główne kategorie

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

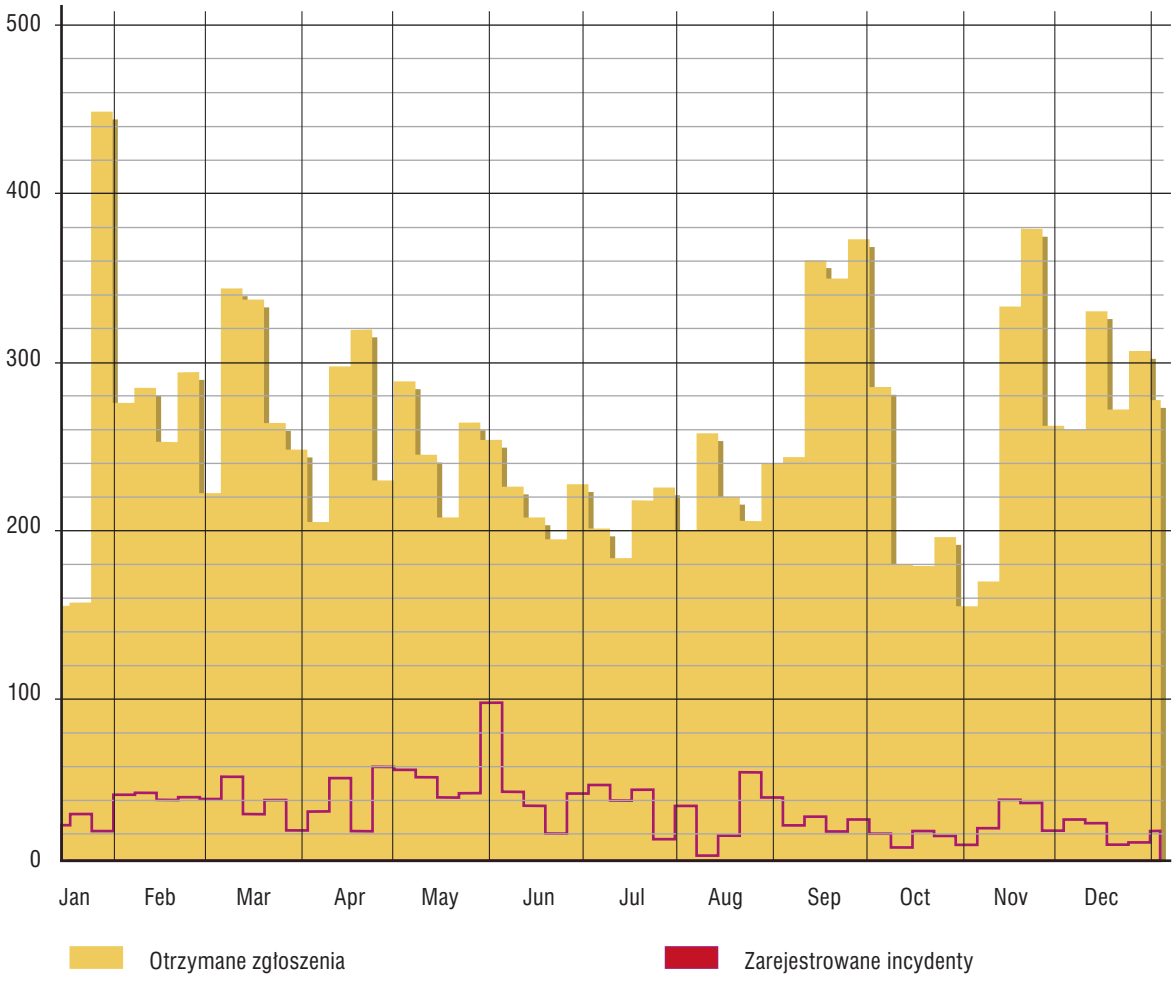
Średnio rejestrowaliśmy od 25 do 60 incydentów tygodniowo. Na przełomie maja i czerwca otrzymaliśmy bardzo dużo zgłoszeń dotyczących *Phishingu* zagranicznych banków. Zgłoszenia pochodziły z polskiego *Ośrodka badawczego lub edukacyjnego* i dotyczyły polskich maszyn. W ostatnim kwartale 2008 roku zanotowaliśmy zwiększona liczbę zgłoszeń dotyczących *Włamań*, a dokładniej *Włamań do aplikacji*. Jest to wynik raportowania przez *Osoby prywatne* luk w serwisach www. Jak do tej pory tego typu odstępstwa od normy są czysto przypadkowe. Dany miesiąc, tydzień, bądź też jakiś szczególny okres w roku nie mają wpływu na ilość i jakość zgłaszanych incydentów.



4.2 Liczba zgłoszeń a liczba incydentów

Poniższy wykres 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.



WNIOSKI I TRENDY 5.

5.1 Najważniejsze zmiany w stosunku do ubiegłego roku

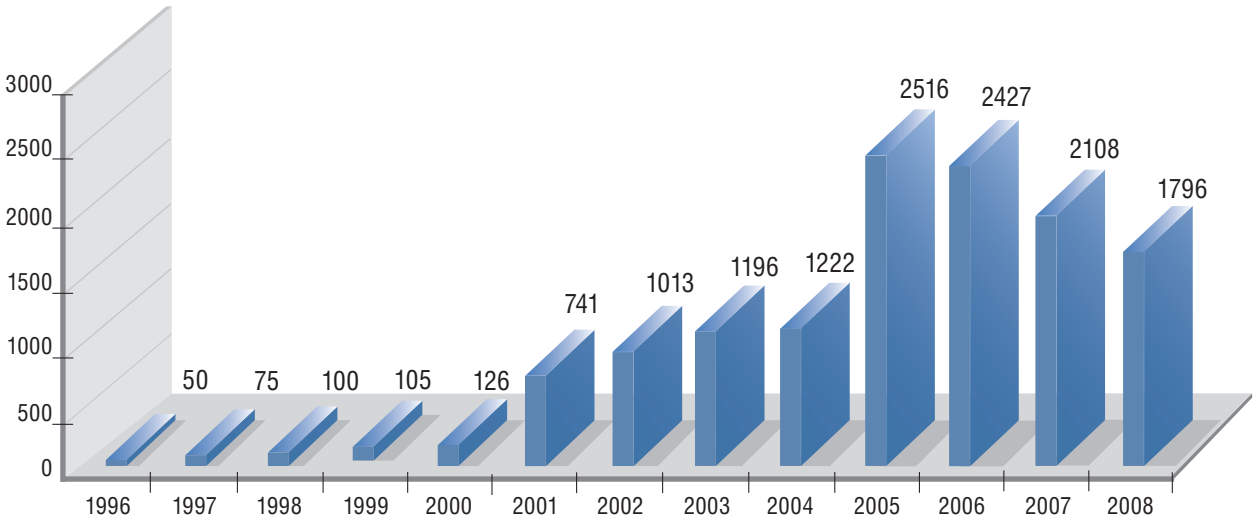
Oprócz najważniejszych trendów i zjawisk, które wyliczamy w rozdziale 5.4, warto zwrócić uwagę na kilka innych istotnych zmian w stosunku do roku 2007, ale także na utrzymanie się niektórych znaczących trendów. Poniżej przedstawiamy te, które są naszym zdaniem najważniejsze:

- Całkowicie zmarginalizowane zostało skanowanie. Udział w stosunku do roku ubiegłego spadł z 24,8% do 4,7%.
- Ustabilizowała się liczba przypadków rozsyłania spamu – 25,95% wobec 25,34% w roku ubiegłym przy nieco niższej liczbie incydentów w ogóle.
- Przez kolejny rok odnotowujemy zwiększenie udziału incydentów dotyczących *Phishingu* – 22,27% w 2008 roku wobec 18,93% i 12,5% odpowiednio w latach 2007 i 2006. Obecnie obsługujemy niemal wyłącznie przypadki dotyczące polskich banków oraz, w mniejszej liczbie, phishingi innych instytucji umieszczone w polskich sieciach.
- Po raz kolejny spadła wyraźnie ogólna liczba obsłużonych incydentów.

5.2 Liczba incydentów w latach 1996 – 2008

Poniższy wykres przedstawia liczbę incydentów w latach 1996 – 2008.

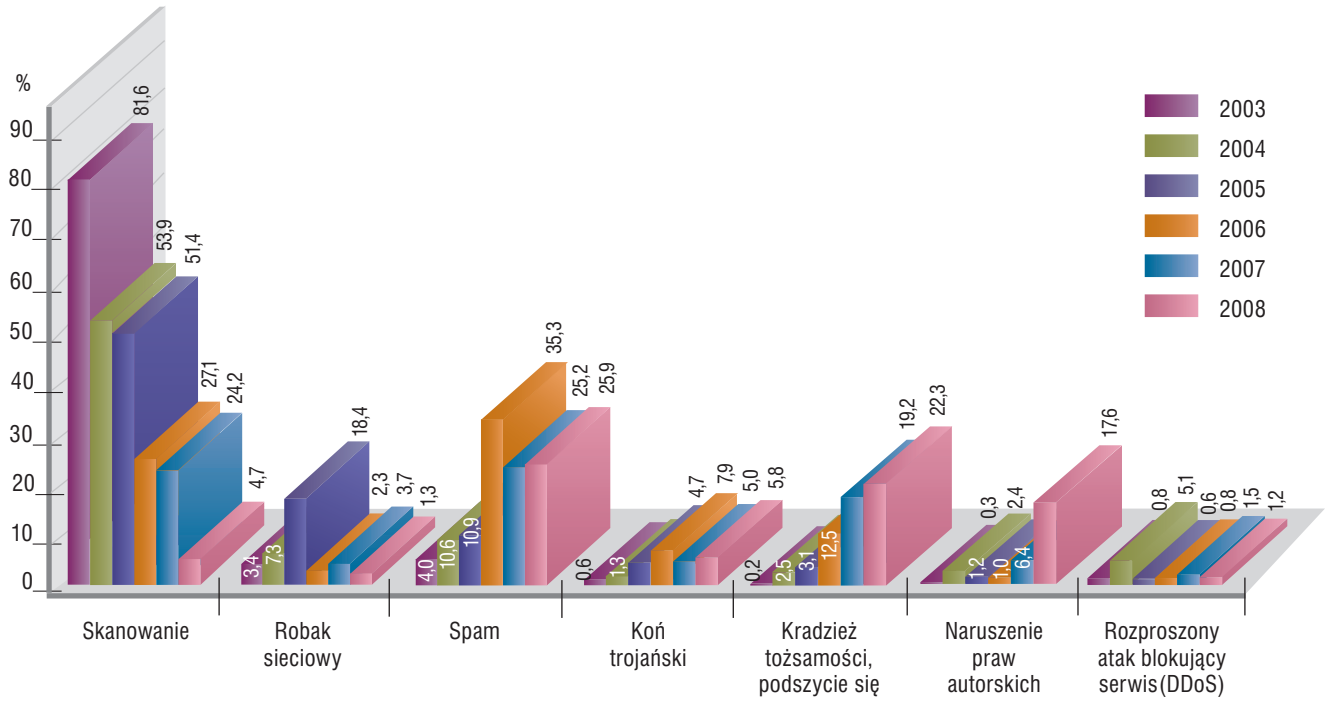
Tendencja zmniejszania się liczby incydentów utrzymuje się z roku na rok. Nie oznacza to jednak, że mamy coraz mniej pracy. Jak wspominaliśmy w poprzednich raportach i jak można wywnioskować z pozostałych rozdziałów raportu tegorocznego, znacząco zmienia się charakter



obsługiwanych spraw. Niemal w całkowite zapomnienie poszły przypadki zgłoszeń skanowania, często wysyłane z automatów instalowanych przez administratorów lub pochodzące z serwisów monitorujących. Nie oznacza to niestety, że zmalała znacząco liczba przejętych maszyn. Przyczyną jest natomiast zmiana wektorów infekcji czyli sposobów, w jaki dochodzi do zarażania komputerów. Jeszcze kilka lat temu każda zainfekowana maszyna szukała kolejnych ofiar. Efektem tego był łatwo zauważalny „hałas", pozwalający na zidentyfikowanie problematycznych końcówek sieci. Teraz do zarażeń dochodzi najczęściej przez konie trojańskie lub złośliwy kod na stronach www. Sam komputer po uruchomieniu takiego złośliwego programu nie wyróżnia się zwykle niczym szczególnym, a jeżeli już dojdzie do awarii systemu, użytkownik nie zgłasza takiego przypadku. W związku z tym rzeczywista liczba zainfekowanych komputerów nie ma przełożenia na liczbę incydentów.

5.3 Rozkład procentowy podtypów incydentów w latach 2003-2008

Od 2003 roku statystyki są tworzone w oparciu o tę samą klasyfikację. Umożliwia to nam porównanie rozkładu procentowego incydentów w ciągu ostatnich sześciu lat (patrz wykres poniżej).



Alarmy wygenerowane przez system ARAKIS

Najbardziej spektakularna zmiana związana jest ze *Skanowaniem* – od 81,6% w 2003 regularny, silny spadek do 4,7% w 2008 roku. Przyczyny tego zjawiska omawiane są już w innych rozdziałach tego raportu – przede wszystkim liczba przypadków skanowania jest zredukowana przez wyparcie ataków opartych o udostępnione usługi sieciowe, w szczególności robaków sieciowych, przez ataki po stronie klienta. Są to ataki ukierunkowane na aplikacje (przez spreparowane dokumenty lub strony www) albo samego użytkownika (głównie konie trojańskie). Potwierdzeniem tego zjawiska są również statystyki dotyczące zanikania *Robaka sieciowego* czy wzrostu udziału ogólnego typu *Złośliwego oprogramowania* (nie ujęte na powyższym wykresie).
Znaczny wzrost obserwujemy przede wszystkim w podtypie *Naruszenie praw autorskich*. Jest on spowodowany intensywną działalnością rozmaitych firm czerpiących zyski z praw autorskich. Mimo ich determinacji, zgłoszenia przypadków łamania praw autorskich są bardzo często słabo udokumentowane lub wręcz uniemożliwiają działania operacyjne przez brak istotnych z punktu widzenia administratora informacji. Z tego powodu duża część zgłoszeń *Naruszeń praw autorskich* jest przez nas odrzucana.
Utrzymuje się trend wzrostowy w udziale (także w liczbach bezwzględnych) przypadków *Kradzieży tożsamości*, *podszycia się*, oznaczających przede wszystkim phishing.
Jak widać, udział incydentów dotyczących spamu ustabilizował się na dość wysokim poziomie, w okolicach 25%. Są to przypadki rozsyłania spamu (zazwyczaj z przejętych maszyn), obejmują więc nierzadko całe kampanie spamerskie. Nie mówimy tu natomiast o poszczególnych przypadkach otrzymania niechcianego listu – tych jest naturalnie o wiele rzędów wielkości więcej.

5.4 Najważniejsze trendy i zjawiska obserwowane w 2008 roku

Poniżej przedstawiamy najbardziej znaczące trendy i zjawiska, występujące w roku 2008, wynikające zarówno z obsługi incydentów, jak i z innych obserwacji poczynionych przez CERT Polska:

- Zanikły niemal całkowicie zgłaszane przypadki *Skanowania*. Jest to kontynuacja trendu z ubiegłych lat, spowodowanego rzadkim występowaniem luk w otwartych usługach i przeniesieniem sposobów infekcji na stronę kliencką – przez błędy w aplikacjach lub wykorzystanie nieświadomości użytkownika.

- Stale zwiększa się liczba incydentów związanych z *Phishingiem*. W tym roku wśród obsługiwanych przypadków dominowały te związane z podszywaniem się pod polskie banki.

- Utrzymuje się trend dużej liczby zgłoszeń dotyczących *Naruszeń praw autorskich*, często pochodzących z automatów skanujących sieci P2P. Liczba zgłoszeń nie ma tu bezpośredniego przełożenia na liczbę obsłużonych incydentów, gdyż wiele z nich zawiera słabą dokumentację, nie pozwalającą na zweryfikowanie, czy rzeczywiście doszło do naruszenia prawa.

- Jednym z najpowszechniej używanych sposobów infekcji jest wykorzystanie techniki *drive-by download*, polegającej na umieszczeniu w kodzie skompromitowanej strony www odwołań do serwerów kontrolowanych przez przestępcę. Zazwyczaj jest to kod Javascript poddany zaciemnieniu (ang. *obfuscation*), czyli przekształceniu do postaci trudno czytelnej dla człowieka – tak aby utrudnić szybką analizę i zorientowanie się, jak zachowa się przeglądarka. Niestety, te same techniki wykorzystywane są czasem przez autorów legalnych stron, którzy w ten naiwny sposób starają się chronić swoje rozwiązania. Znacznie utrudnia to rozpoznawanie, które fragmenty kodu zostały umieszczone na stronie celowo, a które w wyniku włamania.

- Technika *fast flux*, polegająca na rozproszeniu serwisów kontrolowanych przez przestępców (np. stron phishingowych lub zarażających) wśród wielu przejętych komputerów wciąż nie jest powszechnie stosowana. Być może zjawisko jest relatywnie nowe i wymaga sprawowania kontroli nad odpowiednio dużym botnetem (siecią przejętych komputerów).

- Przejęcie komputera coraz częściej wiąże się z działaniami stricte przestępczymi. Bardzo często te same komputery, których dotyczą incydenty, są później przedmiotem dochodzeń policyjnych.

RAPORT Z SYSTEMU ARAKIS

1. ARAKIS – 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 Pionem 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 pięćdziesięciu instytucjach administracji publicznej szczebla centralnego we współpracy z polskim CERTem rządowym CERT GOV PL, działającym w strukturach Departamentu Bezpieczeństwa Teleinformatycznego ABW.

Niniejsze roczne podsumowanie jest pierwszą publikacją tego typu, ponieważ rok 2008 był pierwszym pełnym rokiem kalendarzowym, w którym ARAKIS był kompletnie obsługiwany przez dedykowanych operatorów. Od czasu uruchomienia system spełnił nie tylko swoje pierwotne założenia, ale dodatkowo dostarczył wielu innych cennych informacji dla specjalistów zajmujących się bezpieczeństwem IT. Dzięki pozyskanym informacjom możliwe było poznanie mechanizmów działania zarówno

nowych, jak i aktualnych ataków na aplikacje serwerowe. System sprawdził się bardzo dobrze również w ochronie zasobów sieciowych uczestników projektu, wykrywając źródła infekcji będącej we wczesnym stadium, dzięki czemu możliwe było szybkie zapobieganie jej rozprzestrzenianiu się. Projekt ARAKIS był wielokrotnie prezentowany na wielu krajowych i międzynarodowych konferencjach poświęconych bezpieczeństwu IT. 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.

2. ARAKIS – STRESZCZENIE

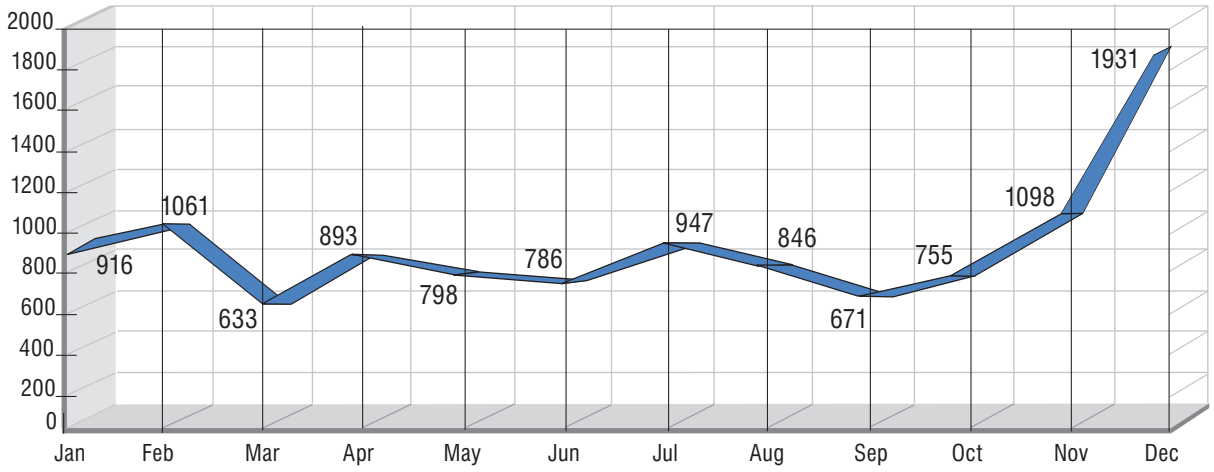
- W 2008 roku operatorzy systemu ARAKIS obsłużyli łącznie 11 335 alarmów (średnio ok. 31 alarmów na dzień), z czego 4% miało najwyższy priorytet, oznaczający realne zagrożenie dla któregoś z podmiotów biorących udział w systemie.
- Zainstalowanych zostało 6 nowych fizycznych sond, a łączna ich liczba wyniosła 54.
- Sondy są umiejscowione w różnych instytucjach państwowych szczebla centralnego (ARAKIS-GOV) oraz w sieci NASK.

Jednym z podstawowych zadań stawianych systemowi była dodatkowa ochrona lokalnych sieci, w których instalowane były sondy ARAKIS-owe. 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 DBTI ABW, natomiast w przypadku infekcji w sieci NASK interweniował Zespół Integracji i Bezpieczeństwa Systemów.
ARAKIS był także bardzo pomocny przy poznawaniu i badaniu nowych i 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 2008 roku należy m.in. propagacja groźnego robaka *Conficker* (zwanego także *Downadup* lub *Kido*), która miała początek w listopadzie i trwa nadal, cały czas zwiększając siłę oddziaływania (jest to największe zagrożenie tego typu na przestrzeni ostatnich lat). Innym ważnym zdarzeniem było wykrycie masowej propagacji (oraz poznanie mechanizmu działania)

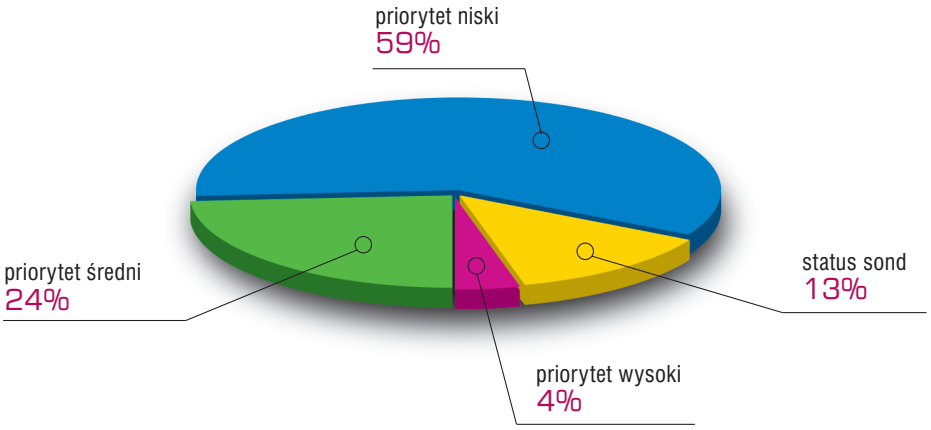
robaka PHP wykorzystującego luki w kilku aplikacjach webowych. Dzięki rozproszonej sieci sensorów system był także świadkiem ataków typu DDoS SYN Flood na zagraniczne serwery. Wykrycie nowego zagrożenia lub trendu w atakach przyczyniało się jednocześnie do poprawy bezpieczeństwa podmiotów biorących udział w systemie poprzez opublikowanie ostrzeżenia z analizą problemu wraz z opisem dostępnych rozwiązań.
Obserwacje ARAKIS-a były także dyskutowane z innymi zespołami reagującymi należącymi do FIRST (Forum for Incident Response and Security Teams). Na bieżąco są używane przez inne (również zagraniczne) zespoły typu CERT. Były też wykorzystane do opublikowania ośmiu wiadomości na portalu www.cert.pl. System opisany został także w wielu serwisach internetowych i publikacjach traktujących o bezpieczeństwie IT (także naukowych i prasowych).

STATYSTYKI DOTYCZĄCE ALARMÓW 3.

W roku 2008 w systemie ARAKIS zostało wygenerowanych 11 335 alarmów (średnio ok. 31 alarmów na dzień i ponad 994 na miesiąc).
Wykres poniżej przedstawia roczne zestawienie wszystkich alarmów bez podziału na typy.
Duży wzrost liczby alarmów pod koniec roku (w listopadzie i grudniu) spowodowany był przez echa ataków DDoS na zagraniczne serwery (głównie www) oraz skanowania dużego zakresu portów przy użyciu żądań *DCE RPC Bind*.
Większość wygenerowanych alarmów miała niski priorytet (59%). Następne w kolejności były alarmy o priorytecie średnim (24%) oraz te opisujące stan poszczególnych sond ARAKIS-owych (13%). Najmniej było alarmów opisujących wykrycie poważnych zagrożeń w sieci (4%).



Alarmy wygenerowane przez system Arakis



Rozkład procentowy alarmów ze względu na priorytety

4. INTERESUJĄCE PRZYPADKI

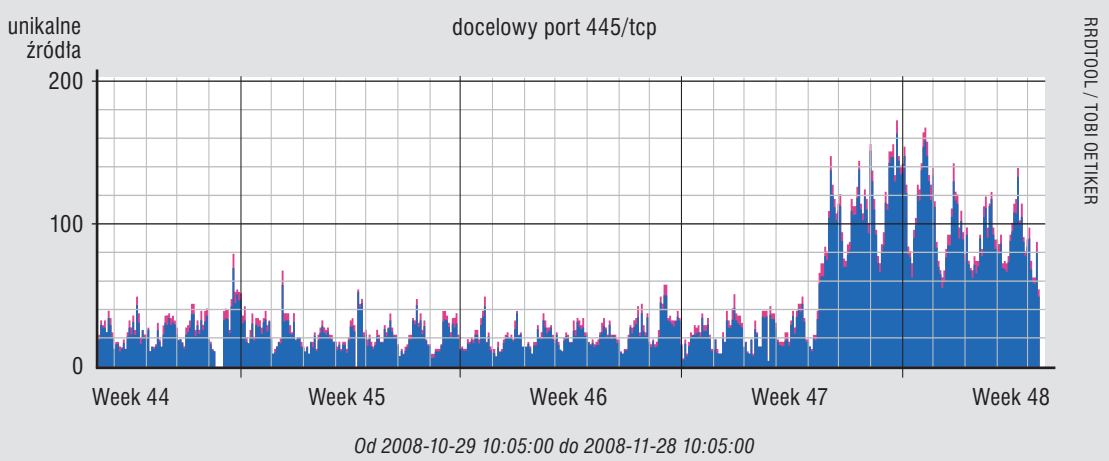
System ARAKIS, oprócz ochrony, jaką dostarczył sieciom z zainstalowanymi sondami, przyczynił się także do zrozumienia wielu rodzajów zagrożeń powszechnie występujących w Internecie. Poniżej skrótowo opisane zostały ciekawsze, naszym zdaniem, obserwacje dokonane przez ARAKIS-a w minionym roku.

4.1 Robak *Conficker*

ARAKIS obserwował propagację robaka *Conficker* od początku jego pojawienia się w sieci. Charakterystyczne dla niego początkowe fazy komunikacji (negocjacja protokołu SMB) wywołała szereg powiązanych ze sobą alarmów. Automatycznie wygenerowany został także nowy klaster opisujący pierwszy etap zarażania ofiary przez robaka, a także na jego podstawie reguła typu Snort. Od drugiej połowy listopada, kiedy to rozpoczęła się propagacja *Confickera* na masową skalę, robak widoczny był nie tylko w alarmach, ale także w statystykach (rankingi najczęściej występujących zagrożeń) i wykresach aktywności sieciowej zarówno w sieci honeynet, jak i darknet czy w logach pochodzących z systemów firewall.

Dzięki temu możliwe było ostrzeżenie najpierw uczestników systemu ARAKIS, a w następnej kolejności czytelników naszego bloga (*Masowy atak nowego robaka*, *www.cert.pl/news/1244*). Dane dostarczone przez ARAKIS-a były także omawiane na listach dyskusyjnych zespołów reagujących typu CERT.

Warto dodać, że od tego czasu widoczna w systemie ARAKIS propagacja *Confickera* wyraźnie przybrała na sile (szczególnie po nowym roku), co oznacza, że wzrosła (i dalej rośnie) liczba zarażonych nim komputerów.



Wykres ruchu (unikalne komputery) na porcie 445/TCP rejestrowany przez honeypoty

4.2 Phreaking w erze telefonii VoIP

W połowie września 2008 roku pojawiły się w Internecie skanowania w poszukiwaniu niezabezpieczonych bramek PSTN, które umożliwiają zestawienie połączenia pomiędzy siecią VoIP a publiczną siecią telefoniczną. Atakujący – po znalezieniu takiego urządzenia – mógł wykonywać rozmowy telefoniczne z abonentami sieci publicznych na koszt właściciela bramki. Poszukiwania polegały na wysyłaniu (najczęściej na port 5060/UDP) pakietów protokołu SIP zawierających sfałszowane żądanie INVITE.

Naszymi obserwacjami podzieliliśmy się na blogu (*Phreaking w erze telefonii VoIP, www.cert.pl/news/1135*).

4.3 Robaki PHP

W styczniu system ARAKIS zanotował wzrost aktywności robaka, który przez wykorzystanie luk w różnych skryptach PHP uzyskiwał dostęp do systemu (atak taki można nazwać *shell command injection*). Dzięki temu pobierał z zewnętrznego serwera plik binarny i uruchamiał go. Po przeanalizowaniu pozyskanego przez nasz system pliku okazało się, że był to linuksowy trojan/backdoor.

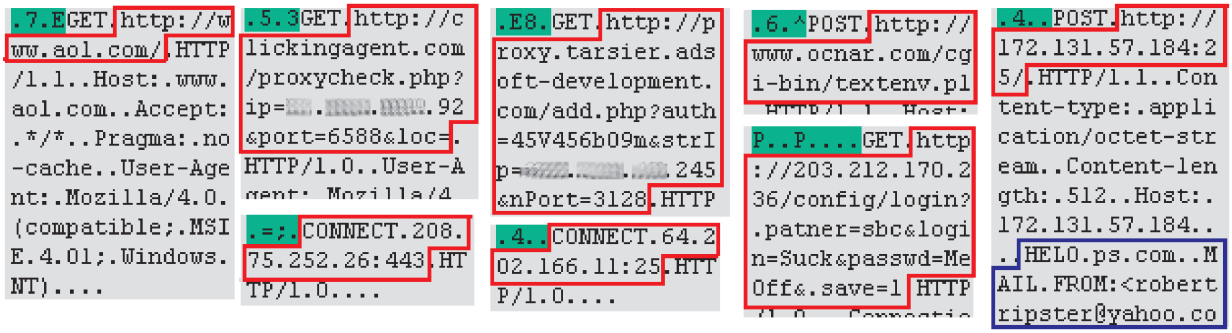
Robak atakował podatności w kilku aplikacjach webowych. Początek masowej propagacji zbiegł się w czasie z upublicznieniem informacji o lukach w MyBB – darmowym forum dyskusyjnym, które zaobserwowany robak także wykorzystywał. Informację o tym podaliśmy na stronie CERT Polska (*Robak wykorzystujący luki w skryptach PHP, www.cert.pl/news/843*).

Podobnie działające robaki były wielokrotnie wcześniej i później obserwowane przez honeypoty ARAKIS-a. Wgrywały one na serwery swoje skrypty PHP, które umożliwiały wykonywanie komend systemowych (tzw. *PHP WebShell*). Często atakowane były popularne systemy zarządzania treścią (CMS), takie jak *Joomla i Mambo*.

4.4 Poszukiwania i próby wykorzystania serwerów open proxy

Bardzo często obserwowanym przez ARAKIS-a ruchem były skanowania w poszukiwaniu serwerów typu *open web proxy*. Tego typu rekonesans przeprowadzają automaty, a zakres przeszukiwanych portów był bardzo szeroki (najmniejszy numer portu, na jakim widziano połączenia, to 1 i 12 TCP, a największy to 56770/TCP) i nie ogranicza się do powszechnie wykorzystywanych przez serwery proxy (jak 8000, 8080, 3128 TCP).

Wykorzystywane do tego były różne metody. Te najprostsze polegały na ślepej próbie połączenia się z jakąś popularną stroną www (np. yahoo.com, cnn.com) lub bezpośrednio na adresy IP (bez użycia nazw domenowych) jakichś serwerów www i ściągnięcia (przy użyciu metody GET) zawartości. Do poszukiwania proxy obsługujących połączenia szyfrowane (https) wykorzystane było polecenie CONNECT (dzięki czemu komunikacja jest tunelowana). Widoczne były także próby łączenia się do serwerów pocztowych – czy to po porcie 25/TCP (z użyciem metody CONNECT), czy przez serwery www (wykorzystanie tzw. *Web Mail Interface*). Innym ciekawym przypadkiem było przechwycenie przez ARAKIS-a całości komunikacji (komend) SMTP zawartego w jednym pakiecie, łącznie z wszystkimi nagłówkami pocztowymi i treścią maila. Do tego wykorzystana była metoda POST.



Metody wykorzystywane przy poszukiwaniu serwerów proxy

Nieco bardziej zaawansowane sposoby wykrywania proxy wymagały umieszczenia na serwerze, na który ma być przekierowanie połączenie, specjalnego skryptu (najczęściej napisanego w PHP), który notował adres serwera proxy i numer portu, ewentualnie czas (datę) połączenia

lub ciąg znaków będący dowodem na autentyczność połączenia (tak jak *token*). Na docelowych serwerach mogą także funkcjonować skrypty (najczęściej perlowe), które sprawdzają zmienne środowiskowe łączącego się z nimi serwera proxy (do tego typu skanowania wykorzystuje się metodę POST). Są to tzw. *Proxyjudge*.
Cele tego typu skanowań są dosyć jasne: służą poszukiwaniom ogólnodostępnego proxy, którego można użyć jako pośrednika (lub jednego z wielu) zapewniającego anonimowość. Intencje osób chcących wykorzystać taki serwer raczej nie są nieszkodliwe i z reguły służą jakiejś nielegalnej działalności (od przeglądania pornografii, wysyłania spamu, do atakowania dalszych serwerów, itp.).

4.5 Atak na routery Linksys

W lipcu 2008 roku widziane były w ARAKIS-ie masowe próby zalogowania się przy użyciu domyślnej pary „użytkownik-hasło" na routery firmy Linksys (do tzw. *Web-GUI*). Atak właściwy poprzedzony był za każdym razem skanowaniem portu 8080/TCP atakowanego IP. Jeżeli atakujący uzyskał połączenie, resetował je, a następnie otwierał kolejne, udając proces logowania się użytkownika do systemu. Używane było hasło stosowane domyślnie w pewnych starszych modelach routerów Linksys. Oczywiście atak ten miał szansę powodzenia tylko w przypadku pozostawienia przez administratora routera domyślnego hasła oraz przy zezwoleniu na zarządzanie nim przez interfejs www z komputera spoza sieci lokalnej. Jednakże w razie powodzenia ataku konsekwencje mogły być dosyć poważne – potencjalnym celem mogła być rekonfiguracja routingu lub adresów serwerów DNS, dzięki czemu cyberprzestępcy mogli w pełni kontrolować ruch i kierować nieświadomych użytkowników routera w zupełnie inne miejsce w Internecie.

4.6 Echa ataków DDoS

ARAKIS nie tylko wykrywa zagrożenia propagujące się w sposób aktywny, ale także obserwuje echa cyberprzestępczej działalności w innych rejonach świata i Internetu. Dzięki rozproszonej sieci sensorów, a przez to rozproszonej puli używanych adresów IP, system był wielokrotnie świadkiem ataku typu DDoS na serwery www. Ataki przeprowadzane były w sposób następujący: atakujący podszywając się pod różne adresy IP nawiązywali permanentnie wiele połączeń z atakowanymi serwerami (tzw. *TCP SYN flood*). Serwery jednak nie były w stanie obsłużyć tak dużej ich liczby, przez co strony internetowe znajdujące się na nich nie były dostępne. Zupełnie przypadkiem co najmniej część zakresu wykorzystywanych do podszywania adresów pokrywała się z adresami ARAKIS-owego honeynetu. Obserwując docierające do systemu odpowiedzi serwerów www, byliśmy w stanie wykryć atak DDoS skierowany na nie. Specyfika tego typu komunikacji (częste zmiany adresów IP oraz portów źródłowych) spowodowały w ARAKIS-ie nienaturalny wzrost liczby alarmów.
W podobny sposób obserwowane były ataki DDoS na serwery DNS – system ARAKIS rejestrował pochodzące z atakowanego serwera odpowiedzi na sfałszowane zapytania o adresy domen.

Kontakt do zespołu

CERT Polska

Zgłaszanie incydentów: ***cert@cert.pl***

spam: ***spam@cert.pl***

Informacja: ***info@cert.pl***

Klucz PGP: ***www.trusted-introducer.org/teams/0x553FEB09.asc***

Strona www: ***www.cert.pl***

Feed RSS: ***www.cert.pl/rss***

Adres: **NASK/CERT Polska, ul. Wąwozowa 18**

02-796 Warszawa

tel.: **+48 22 38 08 274**

fax: **+48 22 38 08 399**

Zespół CERT Polska działa w ramach Naukowej i Akademickiej Sieci Komputerowej – NASK.