ABUSE-Forum

Przemysław Jaroszewski
CERT Polska

- **Agenda**
  - Koncepcja ABUSE-Forum
  - Repozytorium danych
  - BGP Blackholing

- **Czym jest ABUSE Forum?**
  - Pomysł zespołu CERT Polska na integrację członków zespołów abuse różnych operatorów
  - Pierwszy cel – poznać się nawzajem: od kogo przychodzą te maile? do kogo zadzwonić?
  - Wymiana doświadczeń, pomysłów, działających rozwiązań
  - Współpraca operacyjna, wymiana danych, wspólne projekty
  - Poszerzenie forum o dostawców treści i usług


Gadu-Gadu
polski komunikator internetowy


era
MOŻESZ WIĘCEJ


CROWLEY


EXATEL


GTS
Energis


ASTER


CERT
POLSKA


Gazeta.pl


orange™


tp


WBBLiI


nasza-klasa.pl
PORTAL DLA LUDZI Z KLASĄ


netia


o2.pl


INTERIA.PL


onet.pl


POLSKI INTERNET OPTYCZNY


PKP Informatyka
spółka z o.o.


VECTRA


upc


WP.PL


NASK


Plus

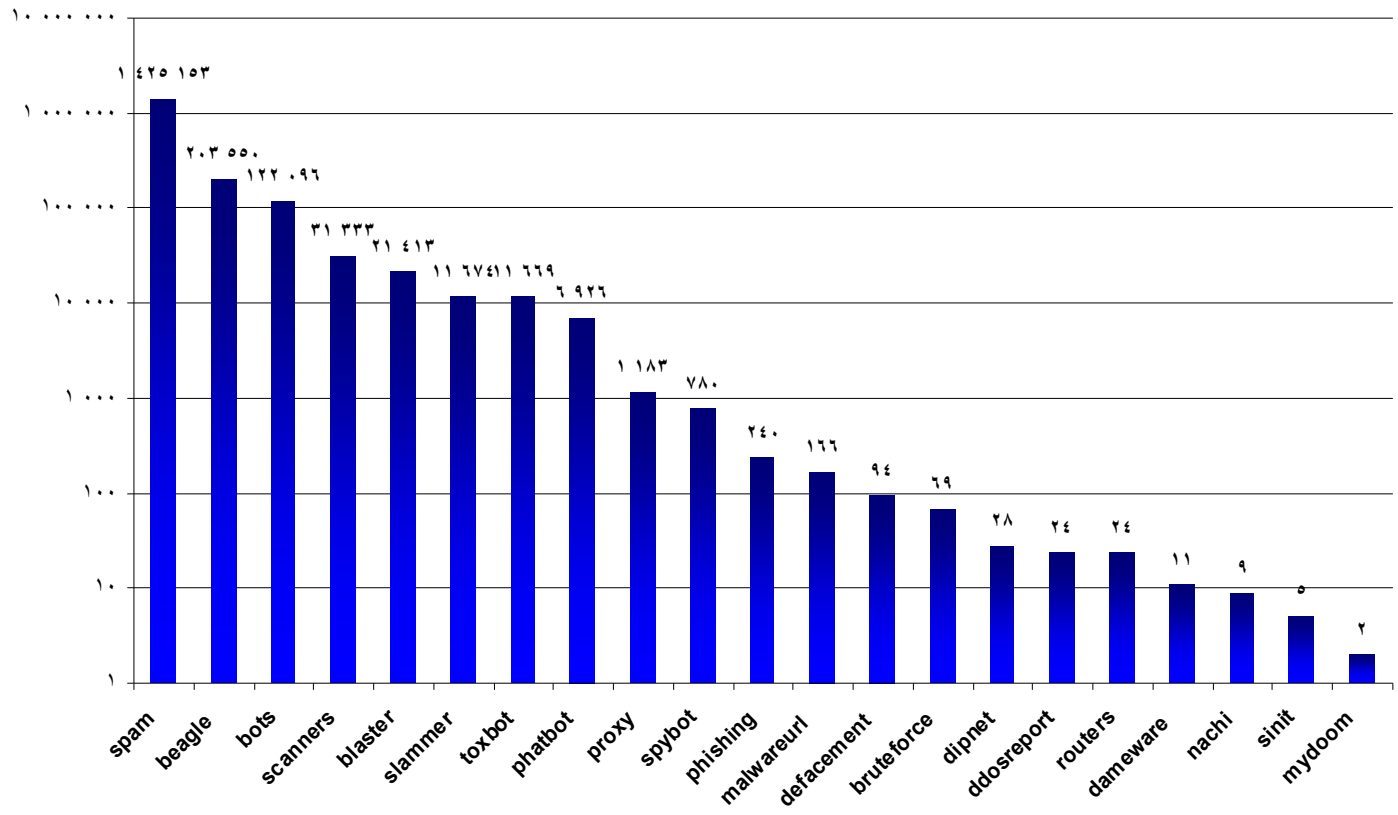

CERT GOV PL

- **Formuła**
  - Spotkania co cztery miesiące
  - Pierwsze spotkanie na jesieni 2005, 10. spotkanie planowane na październik 2008
  - Lista mailingowa
  - Wymiana bezpośrednich kontaktów
  - Stawianie na aktywność – weryfikacja aktywności poszczególnych zespołów

- **Repozytorium danych**
  - Informacje o zainfekowanych hostach
  - Adresy kontrolerów botnetów wraz z użytymi protokołami itp.
  - Strony phishingowe
  - Miejsca dystrybucji złośliwego oprogramowania
  - Dane zbierane z wielu źródeł – własnych oraz zaufanych zewnętrznych
  - Dane obejmują systemy autonomiczne członków forum – adresy IP mapowane są automatycznie na kraje i ASy

- **Kontrola dostępu**
  - Część danych udostępniana wszystkim (np. adresy kontrolerów botnetów)
  - Większość danych zastrzeżona dla poszczególnych członków (np. zainfekowane hosty w sieci operatora)
  - Każdy członek forum korzystający z repozytorium otrzymuje własny certyfikat X.509 dedykowany dla dostępu do archiwum
  - Korzystanie z danych jest monitorowane a dostęp ograniczany w razie braku aktywności

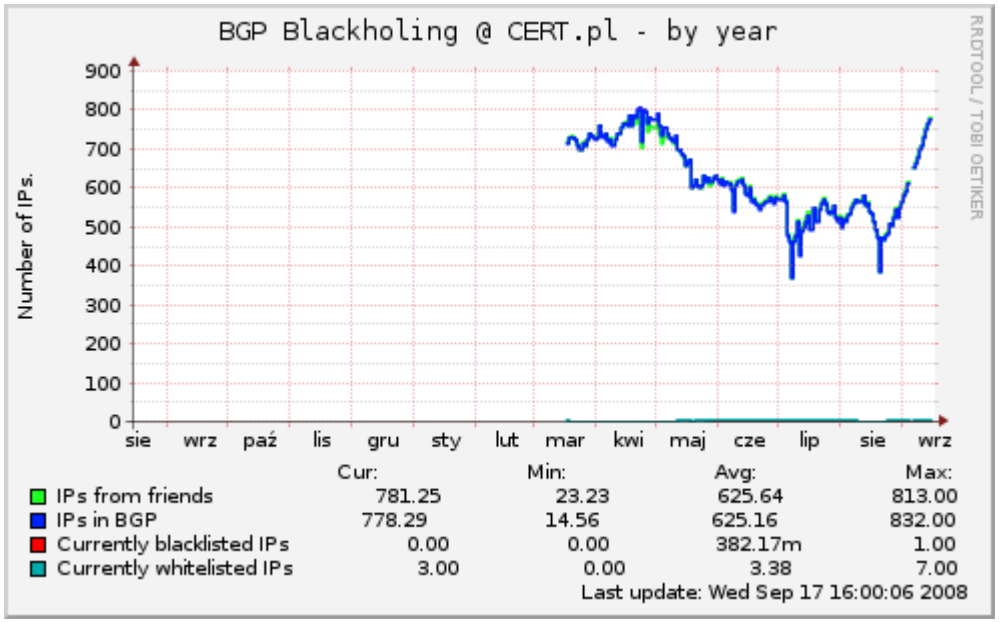
Liczba przypadków nadużyć przekazanych do największych polskich operatorów



Źródło: Raport roczny CERT Polska 2007

- **BGP Blackholing - ogólne zastosowanie**
  - Przekierowanie pakietów z wybranymi docelowymi adresami IP do „czarnych dziur” przez rozgłaszanie tras BGP do sieci /32, które mają być przekierowane na null interface
  - Dodatkowe informacje – takie jak powód filtrowania, źródło informacji – mogą być przekazywane poprzez BGP community
  - Służy do zmniejszania skutków ataków DDoS, może być także wykorzystywane do filtrowania ruchu wychodzącego do kontrolerów botnetów lub innych złośliwych adresów

- **BGP blackholing dla abuse-forum**
  - Projekt „firmowany” przez CERT Polska okazuje się wzbudzać dostateczne zaufanie dla akceptacji przez dostawców
  - Ograniczenia
    - każdy z dostawców może rozgłaszać w ramach BGP blackholing wyłącznie własne sieci
    - CERT Polska rozgłasza dodatkowo adresy złośliwych komputerów, np. kontrolerów botnetów


BGP Blackholing @ CERT.pl - by year
Number of IPs.
900
800
700
600
500
400
300
200
100
0
sie wrz paź lis gru sty lut mar kwi maj cze lip sie wrz
RRDTOOL / TOBI OETIKER
Cur: Min: Avg: Max:
IPs from friends 781.25 23.23 625.64 813.00
IPs in BGP 778.29 14.56 625.16 832.00
Currently blacklisted IPs 0.00 0.00 382.17m 1.00
Currently whitelisted IPs 3.00 0.00 3.38 7.00
Last update: Wed Sep 17 16:00:06 2008

CERT POLSKA

zgłaszanie incydentów: cert@cert.pl

strona internetowa: www.cert.pl

tel. +48 22 380 82 74

fax +48 22 380 83 99

adres pocztowy:

NASK - CERT Polska

ul. Wąwozowa 18

02-786 Warszawa

Polska

DZIĘKUJEMY ZA UWAGĘ