

A detailed illustration of a black hole in space. It features a bright, glowing accretion disk with concentric rings of orange and yellow light. A powerful jet of white light emanates from the center of the black hole, extending upwards. Three small, dark, spherical objects are shown in orbit around the black hole, positioned at different points along the accretion disk. The background is a dark, starry space.

Projekt

BGP BLACKHOLING PL

Łukasz Bromirski

lukasz@bromirski.net

bgp@networkers.pl

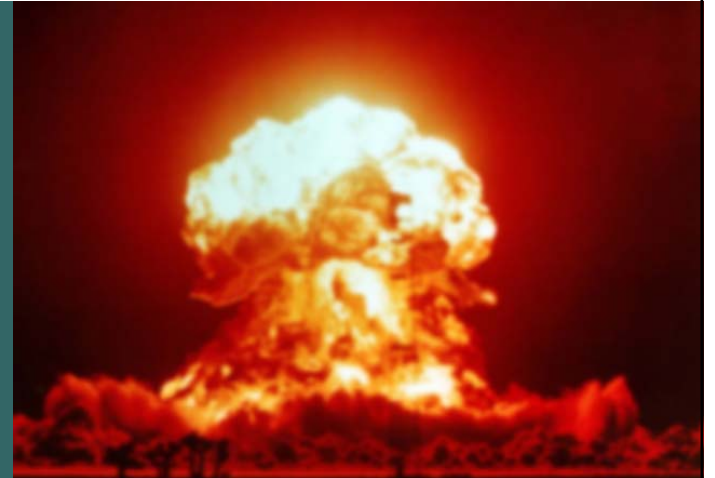


Projekt BGP Blackholing PL

<http://networkers.pl/bgp-blackholing>

- **Problem ataków DoS/DDoS**
- **Projekt BGP Blackholing PL**
co zrobić żeby się dołączyć?
- **Zastosowania BGP Blackholing w Twojej sieci**
- **Materiały**
- **Q&A**

PROBLEM DDoS



Typowy DDoS

„Mnie to nie dotyczy”

<http://networkers.pl/bgp-blackholing>

CNN.com sci-tech > computing > story page

From... **COMPUTERWORLD**
AN IDG.net SITE

'Immense' network assault takes down Yahoo

CNN.com technology > computing

CNN Sites | myCNN | Video | Audio | Headline News Brief | Free E-mail | Feedback

INSURGENCY on the internet

in-depthreports

[Main Page](#) | [Bracing for Cyberwar](#) | [Hacking Primer](#) | [Scenes from the 'Hacker Underground'](#) | [Hacking: Two Viewpoints](#) | [Timeline](#) | [Gallery](#) | [News Archive](#)

<http://www.eweek.com/article2/0,1759,1763273,00.asp>

By Ryan Naraine
February 9, 2005

Harvard researcher Ben Edelman, one of the most vocal critics of spyware purveyors, fell victim to a massive DDoS (distributed denial-of-service) attack over the past 24 hours.

Edelman's Web site, which publishes detailed research reports on spyware, was knocked offline for much of Monday and Tuesday by a DDoS attack that crippled the server capacity.

"My prior Web host tells me I was the target of the biggest DDoS attack they've ever suffered—some 600MB per second," Edelman said.

YAHOO!

amazon.com

CNN.com

ebay

EXTRADE

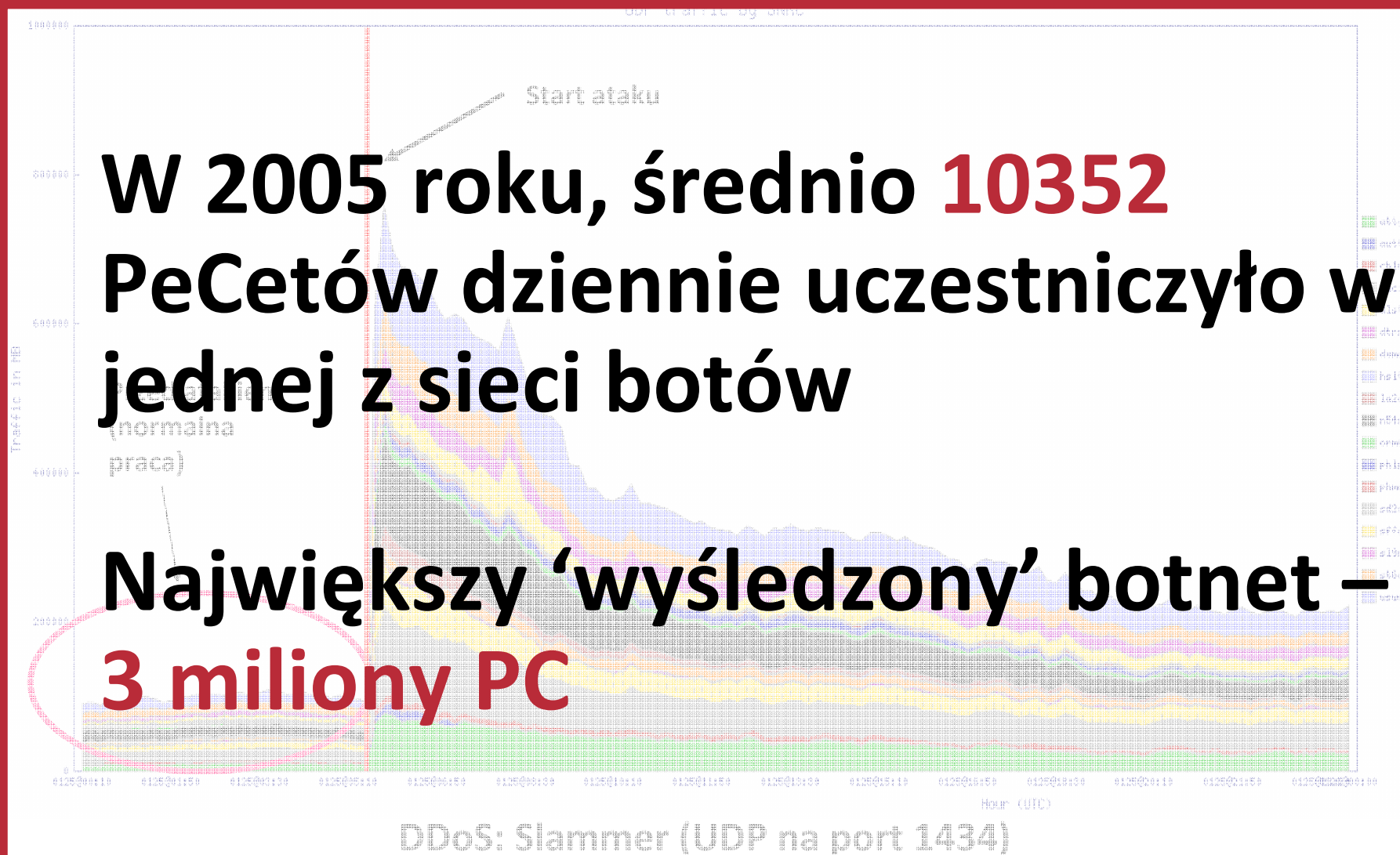
Typowy DDoS

<http://networkers.pl/bgp-blackholing>

- **Setki/tysiące** trojanów-zombie (**BOTNET***)
- **Setki tysięcy** pakietów na sekundę
- **Wielusetmegabitowy/gigabitowy** strumień śmieci
- Zatyka sukcesywnie kolejne wąskie gardła:
 - styk(i) z Internetem źródła
 - styk(i) z Internetem atakowanego
 - sieć ISP
 - styki ISP z innymi ISP
 - „kto popsuł Internet?”

* <http://swatit.org/bots/index.html>

Typowy DDoS – na żywo



Jeśli jeszcze się nie boicie, po prostu **nie rozumiecie** powagi sytuacji.

Mike O'Dell, IETF

„Mnie nie zatkacie”

Rzeź routerów...

<http://networkers.pl/bgp-blackholing>

- Większość routerów nieoperatorskich jest czuła na ilość pakietów/sekundę a nie ich długość (każdy pakiet = konkretny zestaw operacji, realizowanych w większości sprzętowo)
- Nawet mając wolny upstream, możemy wygenerować dużo 40 bajtowych pakietów IP

2Mbit/s = 6400 pakietów/s

10Mbit/s = 31,250 pakietów/s

34Mbit/s = 106,250 pakietów/s

155Mbit/s = 484,375 pakietów/s

622Mbit/s = 1,943,750 pakietów/s

2,4Gbit/s = 7,500,000 pakietów/s

- Stacja z pasmem upstream 256kbit/s może wygenerować tylko 800 40-bajtowych pakietów IP/sekundę

..ale wystarczy zebrać **8** i zatykamy łącze **2Mbit/s**, **600** i zatykamy łącze **155Mbit/s**...

*Nie bierzemy pod uwagę narzutu protokołów

„Mnie nie zatkacie”

Kradzież pasma...

<http://networkers.pl/bgp-blackholing>

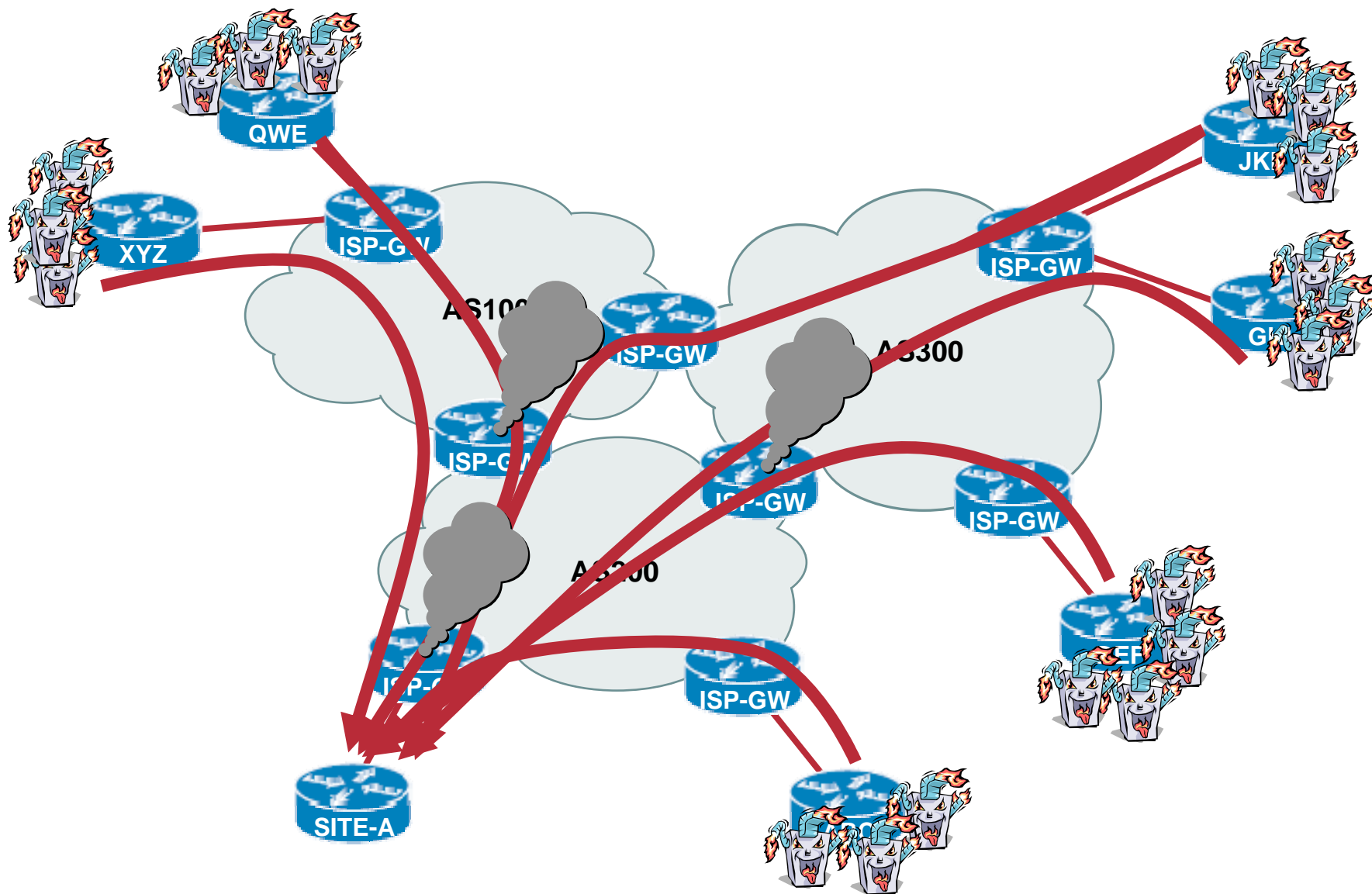
- Pasma jest ograniczone...
- Generujemy 1500 bajtowe pakiety IP
 - 2Mbit/s = 167 pakietów/s
 - 10Mbit/s = 834 pakiety/s
 - 34Mbit/s = 2834 pakiety/s
 - 155Mbit/s = 12917 pakietów/s
 - 622Mbit/s = 51814 pakietów/s
 - 2,4Gbit/s = 200000 pakietów/s
- Stacja z pasmem upstream 256kbit/s może wygenerować tylko 21 1500-bajtowych pakietów/sekundę
 - ..ale wystarczy zebrać **8** i zatykamy łącze **2Mbit/s**, **600** i zatykamy łącze **155Mbit/s**...

*Pakiet IP = 40 bajtów, najgorszy scenariusz - często stosowany dla DDoS
Nie bierzemy pod uwagę narzutu protokołów

Typowy DDoS

Jak to się dzieje?

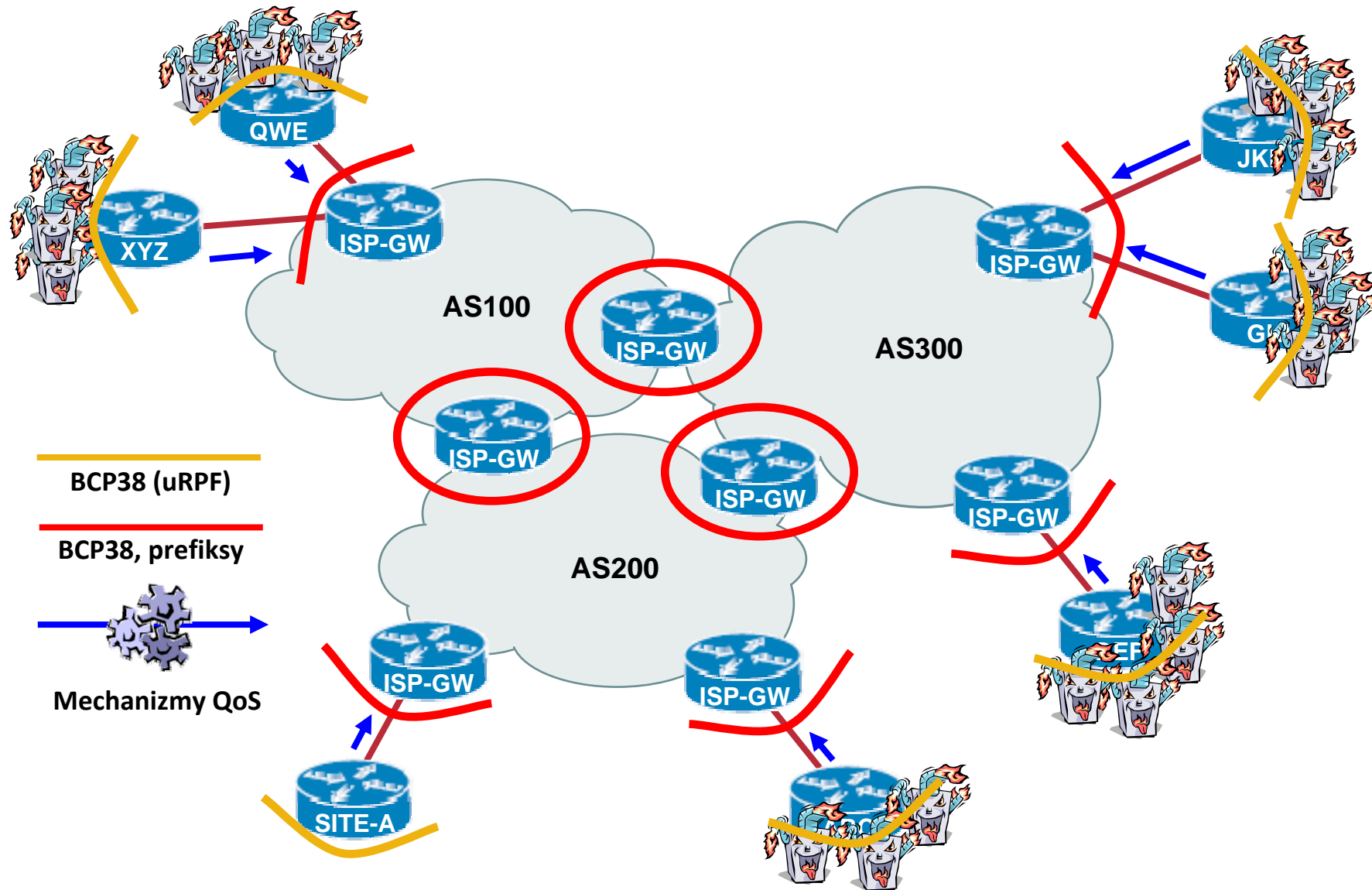
<http://networkers.pl/bgp-blackholing>



Typowy DDoS

Co ja mogę zrobić dla zwiększenia bezpieczeństwa?

<http://networkers.pl/bgp-blackholing>



Czego brakuje do skutecznej walki z DoS/DDoS?

<http://networkers.pl/bgp-blackholing>

- **Wszelkiego rodzaju filtry wymagają interwencji ręcznej przy dowolnej zmianie ich zawartości**
 - bogon list – casus **83/8**
 - spoofed source – realnie brak możliwości
 - atakowany host/podsieć – filtry zakładane lokalnie (efektywnie nic to nie zmienia)
- **Rozwiązania dedykowane zwykle wymagają osobnej infrastruktury, którą trzeba utrzymywać**
 - ...i która oczywiście może stać się celem ataku
- **Wykorzystanie mechanizmów routingu daje możliwość wyjścia z filtrowaniem poza swoją sieć...**

PROJEKT BGP BLACKHOLING PL



BGP blackholing PL

O czym mówimy?

<http://networkers.pl/bgp-blackholing>

- Grupa entuzjastów różnego rodzaju zagadnień sieciowych
- Grupa route-serwerów
 - prefiksy bogon (nieprzydzielone przez IANA* i zarezerwowane)
 - opcja akceptowania prefiksów rozgłaszanych przez członków projektu
- Regulamin dostępny na WWW projektu
- Projekt oparty o dobrą wolę i wolny czas
 - brak jakichkolwiek gwarancji
- Analogia do projektu grupy Cymru
 - <http://www.cymru.com/BGP/bogon-rs.html>
 - my dodatkowo umożliwiamy rozgłaszanie własnych prefiksów

<http://www.iana.org/assignments/ipv4-address-space>

BGP blackholing PL

Czego będę potrzebował?

<http://networkers.pl/bgp-blackholing>

- **Cisco IOS**

oprogramowanie z BGP – IP Plus, ew. SP Services

<http://www.cisco.com/go/fn>

- **BSD/Linux**

Quagga (na BSD z patchem dla Null0*)

Dla OpenBSD/FreeBSD: OpenBGPd

- **Pozostałe platformy/systemy**

...zapytaj dostawcę – zwykle osobna licencja

* <http://lukasz.bromirski.net/projekty/quagga-null0.diff>

BGP blackholing PL

Czego będę potrzebował?

<http://networkers.pl/bgp-blackholing>

- Quagga/Zebra – patch do poprawnej obsługi **Null0**

```
--- quagga-0.99.1/zebra/zebra_rib.c
+++ quagga-0.99.1-blackhole/zebra/zebra_rib.c
@@ -405,6 +405,8 @@
     {
         SET_FLAG (nexthop->flags, NEXTHOP_FLAG_RECURSIVE);
         nexthop->rtype = newhop->type;
+        if (newhop->type == NEXTHOP_TYPE_BLACKHOLE)
+            nexthop_blackhole_add (rib);
         if (newhop->type == NEXTHOP_TYPE_IPV4 ||
             newhop->type == NEXTHOP_TYPE_IPV4_IFINDEX)
             nexthop->rgate.ipv4 = newhop->gate.ipv4;
```

* <http://lukasz.bromirski.net/projekty/quagga-null0.diff>

JAK DOŁĄCZYĆ DO BGP BLACKHOLING PL



BGP blackholing

BGP refresher

<http://networkers.pl/bgp-blackholing>

- **BGP rozgłasza osiągalność prefiksów – pul adresów IP**
Funkcjonalność realizowana dynamicznie
- **Każdy z prefiksów ma pewien zestaw atrybutów – m.in. community**

Zwykle używane do sygnalizacji co i gdzie rozgłaszać/jak preferować

- **Każdy z prefiksów w trakcie akceptowania przez proces BGP może mieć również zmienione pole next-hop**

...routing do interfejsu Null0 powoduje, że pakiety ‘znikają’ bez potrzeby stosowania ACL

Czasami routing bezpośrednio do Null0 jest niedostępny lub z innych powodów niewygodny – routujemy zatem do statycznej trasy (192.0.2.1/32 jest dobrym przykładem) która z kolei wskazuje na Null0

BGP blackholing

Konfiguracja – z lotu ptaka

<http://networkers.pl/bgp-blackholing>

- **Zestawiamy sesje eBGP z naszymi route-serwerami**
zwykle dwie na każdy AS (członka projektu)
- **Sesje rozgłaszają prefiksy:**
typowe bogon oznaczone community **64999:666**
prefiksy członków oznaczone community **64999:999**
- **Prefiksy należy zaakceptować a następnie:**
za pomocą route-map skierować ruch do tych prefiksów do Null0 lub jego odpowiednika
można wykorzystać iBGP żeby rozgłosić prefiksy głębiej do swojej sieci, jeśli składa się z większej ilości routerów

BGP blackholing

Konfiguracja – z lotu ptaka dla wzrokowców

<http://networkers.pl/bgp-blackholing>

AS 64999



BGP BH PL routeserver



Zupełnie Zwyczajna sesja BGP
(z TCP>1024 na TCP=179)



Zupełnie Zwyczajny Router

AS X

BGP blackholing

Konfiguracja – z lotu ptaka dla wzrokowców

<http://networkers.pl/bgp-blackholing>

AS 64999



BGP BH PL



Zupełnie z

AS X

Rozgłaszam:

1/8, community 64999:666

2/8, community 64999:666

3/8, community 64999:666

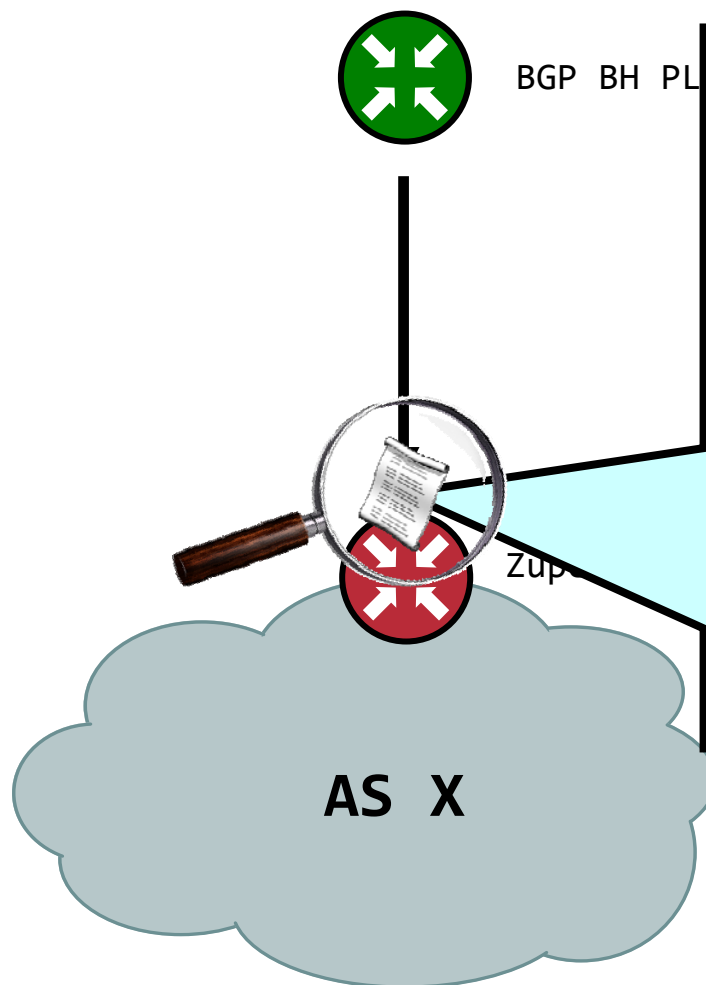
[...]

BGP blackholing

Konfiguracja – z lotu ptaka dla wzrokowców

<http://networkers.pl/bgp-blackholing>

AS 64999



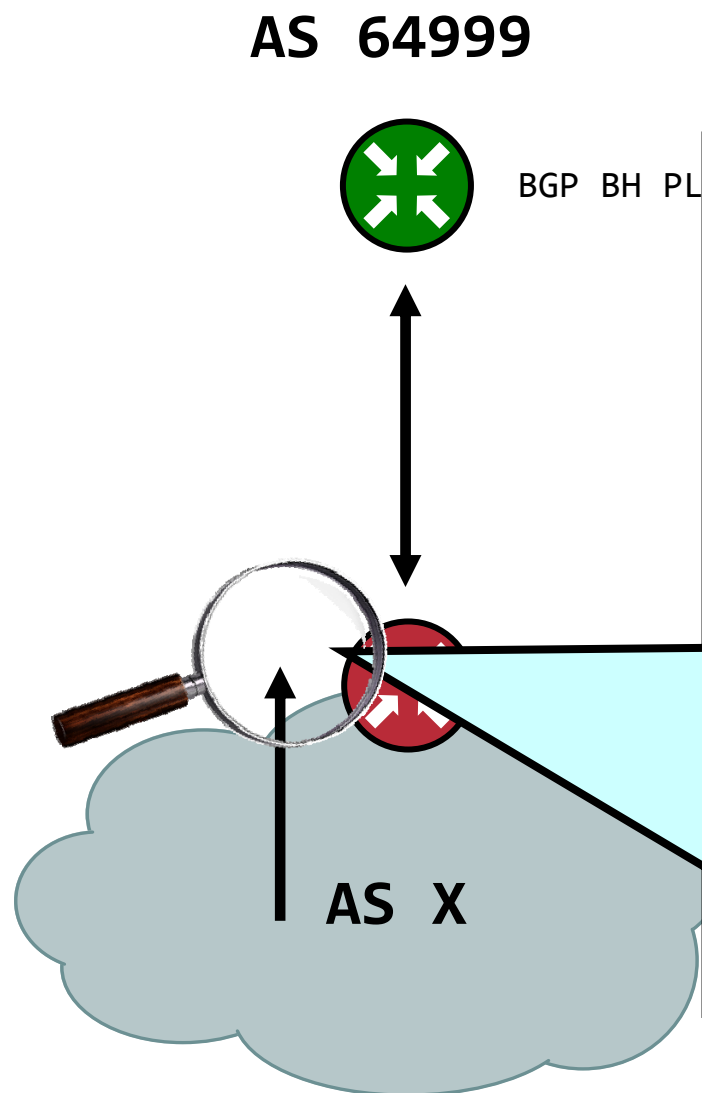
Całkiem Zwykła route-mapa:

- a) Jeśli prefiks ma **community 64999:666** to zainstaluj go w FIB ale z **next-hop** wskazującym na **Null0**
- b) Jeśli ma community...

BGP blackholing

Konfiguracja – z lotu ptaka dla wzrokowców

<http://networkers.pl/bgp-blackholing>



Po otrzymaniu pakietu:

- Czy IP docelowe jest w tablicy routingu?
- Jeśli **tak**, jaki ma next-hop?
 - **Null0**? To /dev/null...
- Jeśli **nie**, wykonaj normalne czynności...

BGP blackholing

Przykład konfiguracji – Quagga/Zebra/Cisco

<http://networkers.pl/bgp-blackholing>

- Definiujemy trasę wskazującą na Null0:

```
ip route 192.0.2.1 255.255.255.255 Null0
```

- Definiujemy community-list pasującą do **64999:666** i osobną, pasującą do **64999:999**:

```
ip community-list 10 permit 64999:666
```

```
ip community-list 20 permit 64999:999
```

- Definiujemy prefix-listę, która odrzuci wszystkie prefiksy (potrzebne, jeśli nie chcesz rozgłaszać swoich prefiksów do route-serwerów projektu):

```
ip prefix-list 10 deny any
```

BGP blackholing

Przykład konfiguracji – Quagga/Zebra/Cisco

<http://networkers.pl/bgp-blackholing>

- Definiujemy route-mapę, która prefiksy oznaczone pasującymi community skieruje do Null0:

```
route-map BGP-BH-PL permit 10  
  match community 10 ! (permit 64999:666)  
  set ip next-hop address 192.0.2.1
```

! jeśli chcesz odrzucać również prefiksy rozgłaszane
! przez innych członków projektu:

```
route-map BGP-BH-PL permit 20  
  match community 20 ! (permit 64999:999)  
  set ip next-hop address 192.0.2.1
```

BGP blackholing

Przykład konfiguracji – Quagga/Zebra/Cisco

<http://networkers.pl/bgp-blackholing>

- Konfigurujemy sesje z route-serwerami projektu BGP Blackholing PL:

```
router bgp <Twój_numer_AS>
  neighbor <IP_rs_1> remote-as 64999
  neighbor <IP_rs_1> description BGP BH 01
  neighbor <IP_rs_1> ebgp-multihop 255
  neighbor <IP_rs_1> route-map BGP-BH-PL in
  neighbor <IP_rs_1> prefix-list 10 out
  neighbor <IP_rs_1> password <tutaj_otrzymane_hasło>
```

Więcej pod: <http://networkers.pl/bgp-blackholing/configs.html>

BGP blackholing

Przykład konfiguracji – Quagga/Zebra/Cisco

<http://networkers.pl/bgp-blackholing>

- Każdy prefiks otrzymany od danego sąsiada, sprawdzany jest przez route-mapę BGP-BH-PL:

```
route-map BGP-BH-PL permit 10
  match community 10
  set ip next-hop 192.0.2.1
```

jeżeli prefiks oznaczony będzie pasującym community (w tym przypadku **64999:666**), zostaje umieszczony w tablicy routingu z adresem next-hop ustawionym na 192.0.2.1

trasa do 192.0.2.1 skierowana jest na interfejs Null0

efektywnie, cały ruch pod rozgłoszony prefiks zostaje odrzucony

BGP blackholing

Jak mogę się przyłączyć?

<http://networkers.pl/bgp-blackholing>

- Napisz maila na adres bgp@networkers.pl
- Podaj:
 - typ swojego routera (np. Cisco 7206 albo Juniper M10i)
 - rodzaj i ilość styków z operatorami (adresacja IP!)
 - z jakich IP chcesz zestawiać sesje z route-serwerami
 - czy posiadasz i jeśli tak to jaki publiczny ASN?
 - czy chcesz korzystać z możliwości wstrzykiwania prefiksów ze swojego ASa?
jeśli tak, jakie to prefiksy? **(oczywiście musimy to zweryfikować w RIPE)**
 - czy możemy podać informacje o Twoim uczestnictwie na stronie projektu?
(tylko AS i nazwa firmy/ew. imię i nazwisko osoby prywatnej)
 - działający telefon kontaktowy
- Postaramy się jak najszybciej skontaktować, podając potrzebne do zestawienia sesji informacje

BGP blackholing

Jak mogę się przyłączyć? Przykładowy e-mail

<http://networkers.pl/bgp-blackholing>

Cześć !

Chciałbym przyłączyć się do projektu BGP BH PL.

Posiadam dwa routery Cisco 7200.

Sesje będę zestawiał z IP 10.10.10.254 i 10.10.10.250.

Nie posiadam swojego numeru AS.

Chciałbym mieć możliwość wstrzykiwania prefiksów: 10.11.11.0/24

Mój numer telefonu to 0(22)202122

BGP blackholing

Jak mogę się przyłączyć? Przykładowa odpowiedź.

<http://networkers.pl/bgp-blackholing>

Witamy!

Skonfigurowaliśmy dwie sesje, po jednej do każdego Twojego routera.

Router A:

Nasz IP : A.B.C.D

Twój IP : 10.10.10.250

Hasło MD5 : tajne_hasło_1

Nasz AS : 64999

Twój AS : 65500

Router B:

Z.X.C.V

10.10.10.254

tajne_hasło_2

64999

65500

BGP blackholing

Więcej informacji o konfiguracjach?

<http://networkers.pl/bgp-blackholing>

- **Inne konfiguracje, porady praktyczne oraz regulamin znajduje się na stronie projektu:**

<http://networkers.pl/bgp-blackholing>

- **Dostępne są również dwie listy: dyskusyjna projektu oraz administracyjna – informacje o nowych podsieciach, incydentach itp.:**

bh-pl-discuss@lists.networkers.pl

bh-pl-announce@lists.networkers.pl

- **Strona z listami na networkers.pl:**

<http://lists.networkers.pl/mailman/listinfo>

ZASTOSOWANIA BGP BLACKHOLING



Zastosownania BGP Blackholing

<http://networkers.pl/bgp-blackholing>

- **Profilaktyka**
- **Jak wykryć DoS/DDoS?**
- **Wysyłanie informacji o ataku na własną sieć**
- **Wykorzystanie mechanizmu uRPF w filtrowaniu ruchu**
- **BGP Blackholing wewnątrz Twojej sieci**

Profilaktyka

<http://networkers.pl/bgp-blackholing>

- **Dobra obrona jest jak ogr (ogier? ☺):**
ma warstwy
- 1. hardening
- 2. ochrona antyspoofingowa
- 3. ACL/stateful firewall
- 4. uwierzytelnianie sesji routingu
- 5. IDS/IPS
- 6. mechanizmy QoS
- 7. mechanizmy specyficzne dla sieci
- ...inne...



Jak wykryć DoS/DDoS?

<http://networkers.pl/bgp-blackholing>

- **Rozwiązania oparte o rozproszone sondy IDS/IPS**
zwykle z opóźnieniem
- **Rozwiązania oparte o modyfikacje/pluginy aplikacji atrakcyjnych jako cele**
zwykle mało skalowalne
- **Rozwiązania oparte o NetFlow**
powszechnie przyjęty standard
dostępne rozwiązania GPL/BSD/etc. oraz komercyjne
relatywna łatwość w implementacji
dokładne dane – o miejscu, rodzaju i sile ataku

Jak wykryć DoS/DDoS?

Czyli co NetFlow może zrobić dla Ciebie

<http://networkers.pl/bgp-blackholing>

- **NetFlow to mechanizm zbierania informacji o potokach (ang. flow) w sieci**

w zależności od wersji, ilość informacji o potoku różni się – wersje 5 i 9 są najpowszechniejsze

w potoku dostajemy między innymi źródłowy i docelowy: adres IP, porty TCP/UDP, typ/kod ICMP, numer AS, oraz zwykle również: ilość bajtów, ilość pakietów, czas trwania itp. itd.

- **Skorzystanie z NetFlow daje doskonałe narzędzie do monitoringu sieci i poznania jej specyfiki**

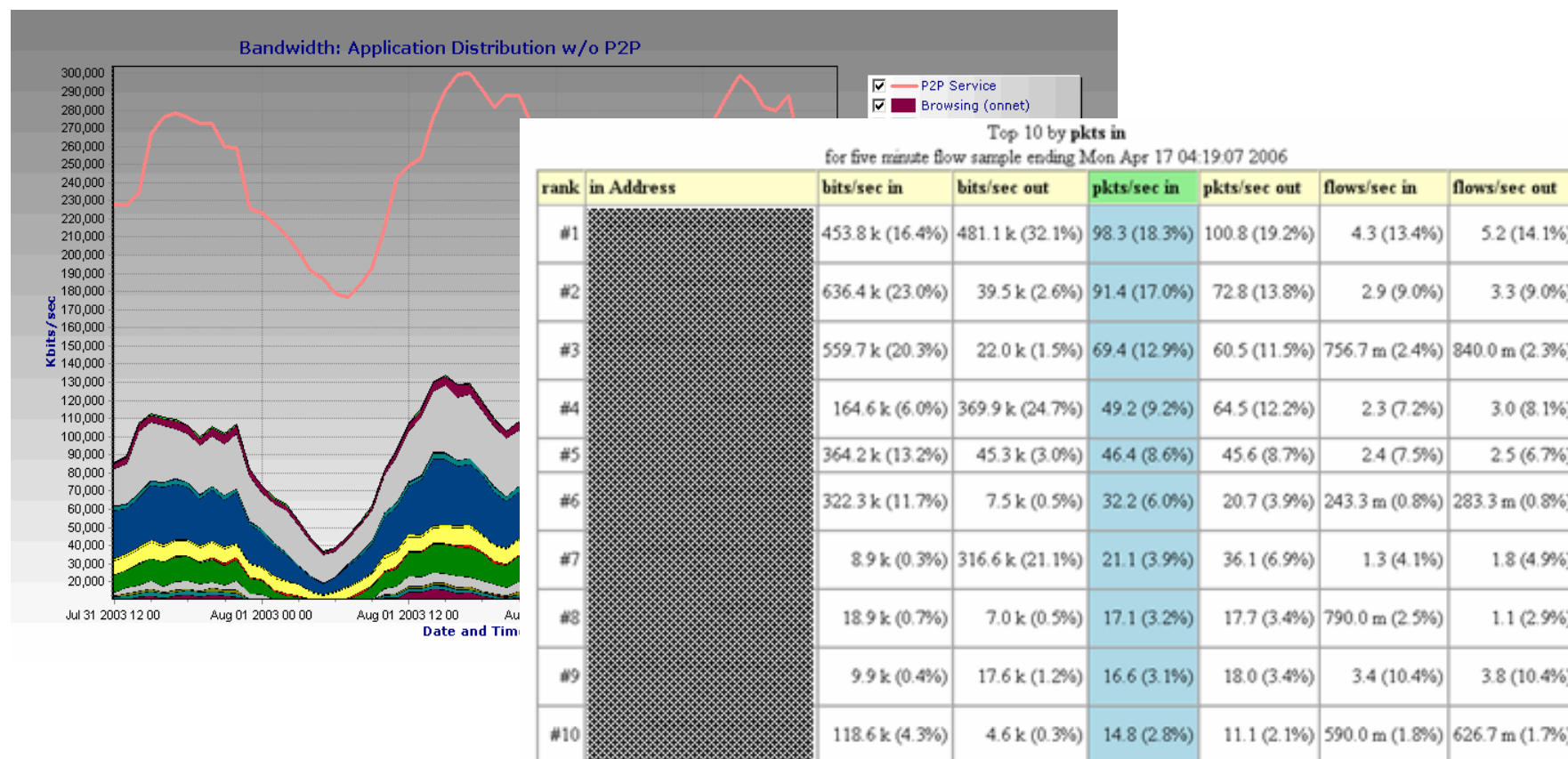
zanim DDoS zapuka w Twoje routery...

Jak wykryć DoS/DDoS?

Czyli co NetFlow może zrobić dla Ciebie

<http://networkers.pl/bgp-blackholing>

- Przykładowe dane z systemu monitoringu NetFlow:



Jak wykryć DoS/DDoS?

Chcę takie dwa!

<http://networkers.pl/bgp-blackholing>

- **Na systemy Linux/BSD:**

cflowd, flow-tools, ng_netflow (FreeBSD), pfflowd (OpenBSD)

fprobe, softflowd, ntop

- **W Cisco IOS:**

włączyć NetFlow na interfejsach

skonfigurować eksport informacji do serwerów

...plus ewentualnie inne opcje (sampling, agregacja itp)

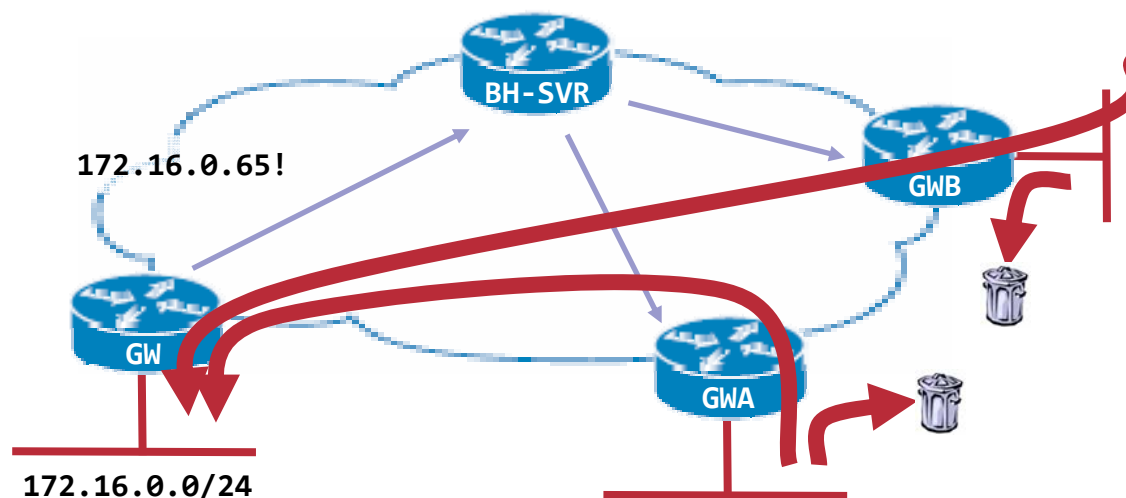
<http://freshmeat.net/search/?q=netflow§ion=projects>

Jak wysłać informacje o ataku na własną sieć?

- Można rozgłaszać IP i podsieci z **własnego AS'a** jeśli wykryjemy na nie atak do wszystkich uczestników projektu tak, by:

pomóc walczyć operatorom z DDoSem

zatrzymać zombie w innych sieciach przed generowaniem śmieci upstream



BGP blackholing

Jak wysłać informacje o ataku na własną sieć?

<http://networkers.pl/bgp-blackholing>

```
route-map BH-SEND permit 10
  match tag 666 ! trasy oznaczone tym tagiem wysyłamy przez BGP
  set community 64999:999
!
router bgp 100
  redistribute static route-map BH-SEND
  neighbor 10.0.0.8 remote-as 64999
  neighbor 10.0.0.8 send-community
  [...]
! atak na 172.16.10.15?
ip route 172.16.10.15 255.255.255.255 Null0 tag 666
...

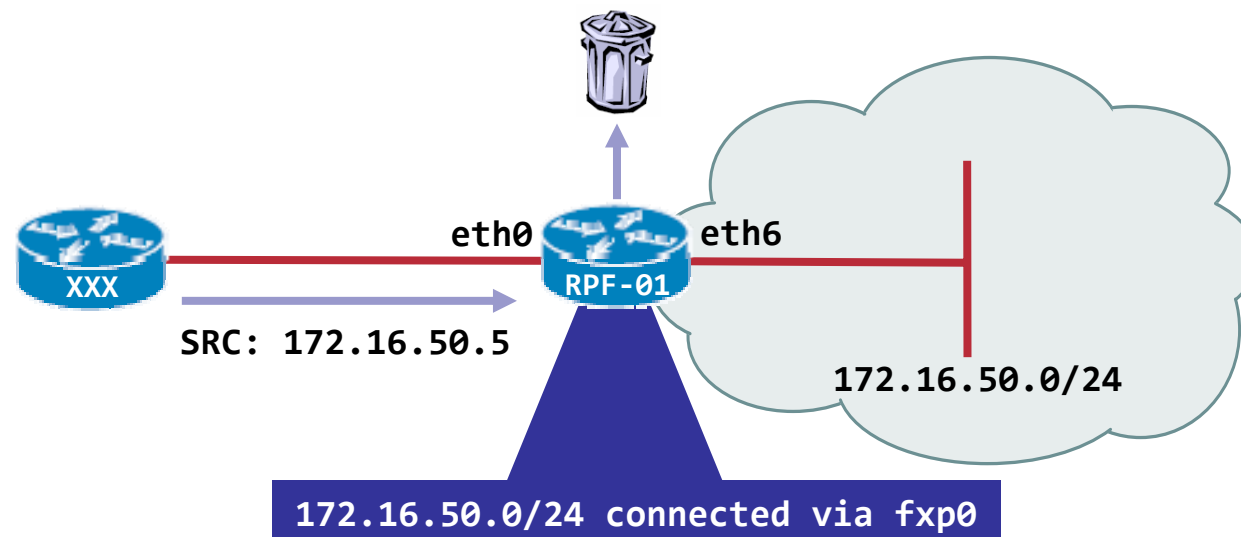
! koniec ataku na 172.16.10.15?
no ip route 172.16.10.15 255.255.255.255 Null0 tag 666
```

BGP blackholing

RPF - Jak to działa?

<http://networkers.pl/bgp-blackholing>

- RPF = **R**everse **P**ath **F**iltering
- Źródłowy adres każdego pakietu jest porównywany z zawartością tablicy routingu
- Adres źródłowy pakietu i interfejs którym dotarł on do routera, musi zgadzać się z tablicą routingu



BGP blackholing

Konfiguracja - RPF

<http://networkers.pl/bgp-blackholing>

- Dzięki mechanizmowi RPF, ruch również **z** odebranych z route-servera prefiksów, kierujemy na interfejs Null0:

FreeBSD, tryb „strict”:

```
deny log ip from any to any not verrevpath in via em0
```

FreeBSD, tryb „loose”:

```
deny log ip from any to any not versrcpath in via em0
```

Cisco, tryb „strict”:

```
ip verify unicast source reachable via rx [allow-default]
```

Cisco, tryb „loose”:

```
ip verify unicast source reachable via any
```

Linux:

```
echo 1 > /proc/sys/net/ipv4/conf/(all|ethX)/rp_filter
```

uRPF dla FreeBSD niezależny od filtra pakietów:

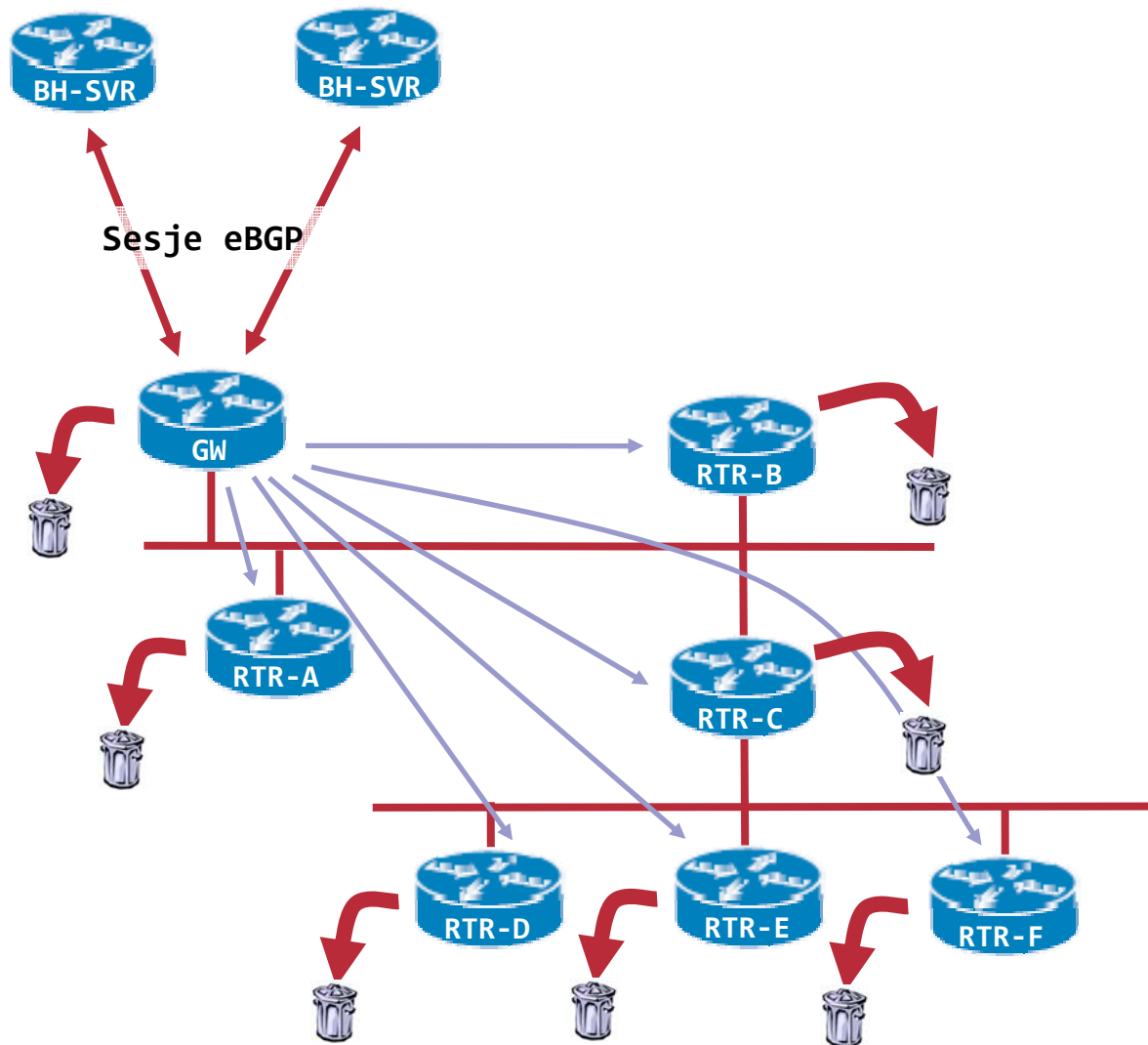
<http://lukasz.bromirski.net/projekty/patches.html>

BGP blackholing

Jak wykorzystać peering z BGP BH PL w środku sieci?

<http://networkers.pl/bgp-blackholing>

- Mimo uruchomienia BGP BH na GW, nadal reszta sieci może być przeciążana przez ataki inicjowane z jej środka
- Rozwiązaniem jest konfiguracja iBGP



BGP blackholing

Jak wykorzystać peering z BGP BH PL w środku sieci?

<http://networkers.pl/bgp-blackholing>

- **GW – eBGP do BGP BH PL i iBGP do routerów w środku sieci:**

```
router bgp 100
  neighbor 10.0.0.8 remote-as 64999
  neighbor 10.0.0.8 description BGP BH 01
  neighbor 10.0.0.8 route-map BH in
  neighbor 10.0.0.8 ebgp-multihop 255
  neighbor 172.16.0.10 remote-as 100
  neighbor 172.16.0.10 description iBGP-RTR-A
  neighbor 172.16.0.10 send-communities ! w nowszych Quaggach zbędne
  [...]
```


BGP blackholing

Jak wykorzystać peering z BGP BH PL w środku sieci?

<http://networkers.pl/bgp-blackholing>

- **RTR-A – iBGP z GW**

```
router bgp 100
  neighbor 172.16.0.1 remote-as 100
  neighbor 172.16.0.1 description iBGP-GW
  neighbor 172.16.0.1 route-map BH in
!
ip route 192.0.2.1 255.255.255.255 Null0
ip community-list 99 permit 64999:666
!
route-map BH permit 10
  match community 99
  set ip next-hop 192.0.2.1
```

BGP blackholing

Czy to w ogóle działa?

<http://networkers.pl/bgp-blackholing>

```
busy-bsd ~$ netstat -nrf inet | grep B
```

1	127.0.0.1	UG1cB	0	31490	lo0
2	127.0.0.1	UG1cB	0	2853	lo0
5	127.0.0.1	UG1cB	0	11921	lo0
7	127.0.0.1	UG1cB	0	4321	lo0
10	127.0.0.1	UG1cB	0	184921	lo0
23	127.0.0.1	UG1cB	0	9392	lo0
169.254	127.0.0.1	UG1cB	0	94812	lo0
172.16/12	127.0.0.1	UG1cB	0	119486	lo0
173.0/8	127.0.0.1	UG1cB	0	11602	lo0
174.0/8	127.0.0.1	UG1cB	0	6731	lo0
175.0/8	127.0.0.1	UG1cB	0	996	lo0
192.168.0/16	127.0.0.1	UG1cB	0	89483	lo0

```
busy-cisco# sh ip traffic | incl RPF
```

7 no route, 4386198 unicast RPF, 0 forced drop

GDZIE WARTO RZUCIĆ OKIEM



Strona projektu

<http://networkers.pl/bgp-blackholing>

BGP Blackholing PL opis projektu

BGP blackholing PL team <bgp@networkers.pl>
v1.2 18-iii-2006

[OPIS PROJEKTU](#) | [KONFIGURACJE](#) | [REGULAMIN](#) | [FAQ](#) | [MATERIAŁY](#) | [UCZESTNICY](#)

O co chodzi?

Projekt **BGP Blackholing PL** narodził się jako pomysł na zwiększenie bezpieczeństwa naszej części internetu.

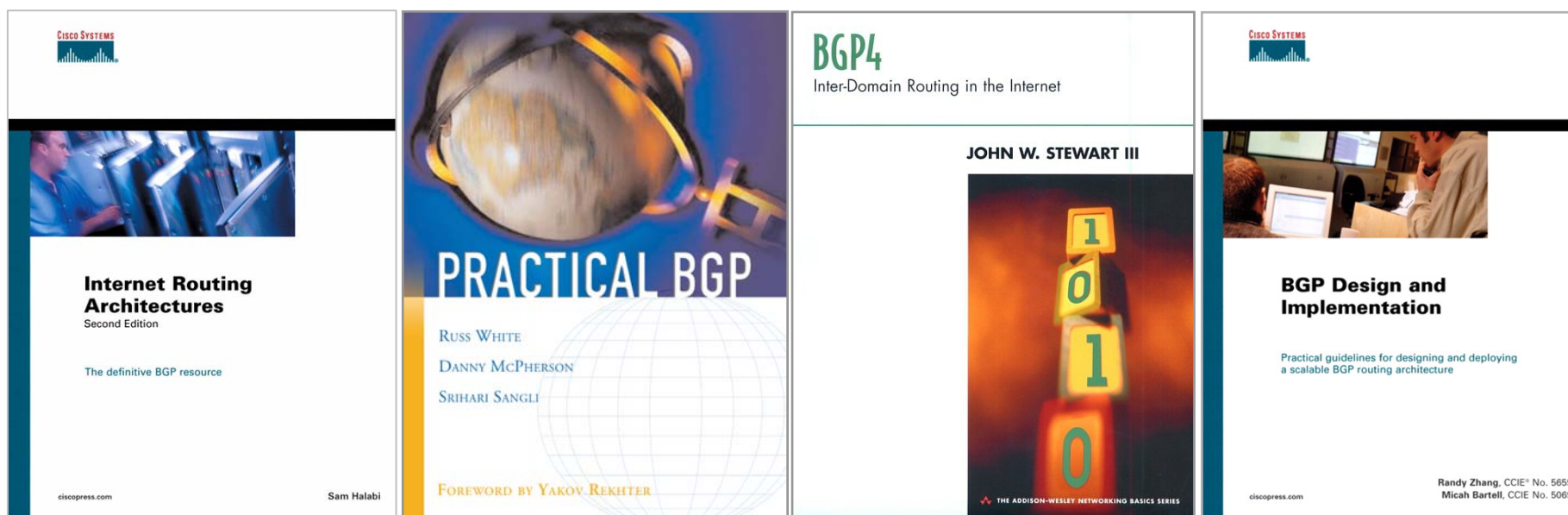
Nazwa projektu pochodzi od idei jego działania. Po angielsku **black hole** to czarna dziura, a sformułowanie **blackholing** opisuje wrzucania do niej różnego rodzaju rzeczy - w naszym przypadku, chodzi o niepotrzebny lub szkodliwy wręcz ruch sieciowy.

Projekt ma na celu zbudowanie i utrzymywanie infrastruktury, która każdej mniejszej lub większej sieci udostępni automatyczne informacje o:

- **pulach nieużywanych (nieprzydzielonych) adresów IP**
organizacja IANA zajmuje się przydzielaniem (lub delegacją praw do przydzielania) przestrzeni adresowej dla protokołów IPv4 i IPv6; adresy obecnie [zarezerwowane przez IANA](#) są nieużywane i jako takie, nie powinny pojawiać się w internecie; zadziwiająco jednak często widzimy taki ruch, generowany głównie przez rozmaite konie trojańskie i boty, które nie zważając na takie subtelności jak plan używanej przestrzeni adresowej, losowo generują adresy IP do dalszego rozmnażania
- **obecnie atakowanych adresach IP członka projektu**
mechanizm ataków DoS/DDoS polega na tym, że wiele hostów, świadomie bądź nie

Książki

<http://networkers.pl/bgp-blackholing>



Zasoby WWW

<http://networkers.pl/bgp-blackholing>

- **Strona projektu BGP Blackholing PL:**

<http://networkers.pl/bgp-blackholing>

- **BGP4.AS**

<http://www.bgp4.as>

- **ISP Essentials:**

<ftp://ftp-eng.cisco.com/cons/isp/essentials/>

- **ISP Security Essentials (NANOG):**

<http://www.nanog.org/ispsecurity.html>

- **Prezentacje Philipa Smitha**

<ftp://ftp-eng.cisco.com/pfs/seminars/>

Q&A



A detailed illustration of a black hole in space. It features a bright, glowing accretion disk with concentric rings of orange and yellow light. A powerful jet of white light emanates from the center of the black hole, extending upwards. Three small, dark, spherical objects are shown in orbit around the black hole, positioned at different points along the accretion disk. The background is a dark, starry space.

Projekt

BGP BLACKHOLING PL

Łukasz Bromirski

lukasz@bromirski.net

bgp@networkers.pl

