BGP Blackholing PL
v2.0 re(boot|reload)

Łukasz Bromirski
bgp@null0.pl

Polish Network Operators' Group

Agenda

- Z jakim zagrożeniem walczymy?
- Jak działa BGP blackholing?
- Jak się przyłączyć?
- Q&A

Z jakim zagrożeniem walczymy?

Zagrożenia dla naszych sieci

Ataki DoS/DDoS

- Statystyki nadal pokazują, że ataki DoS/DDoS są **aktualnym** zagrożeniem dla sieci

Largest Single DDoS Attack Observed per Survey Year in Gbps

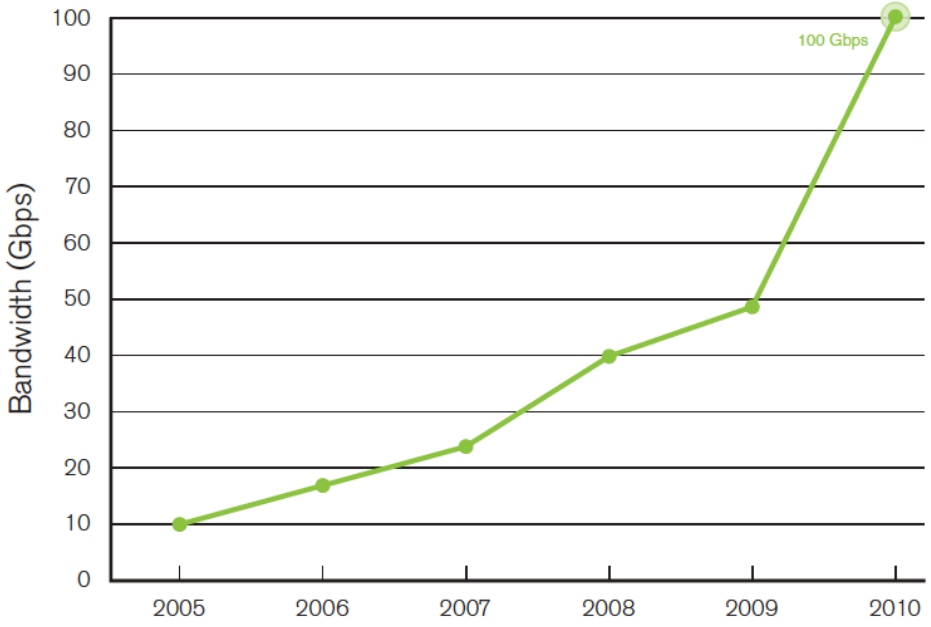
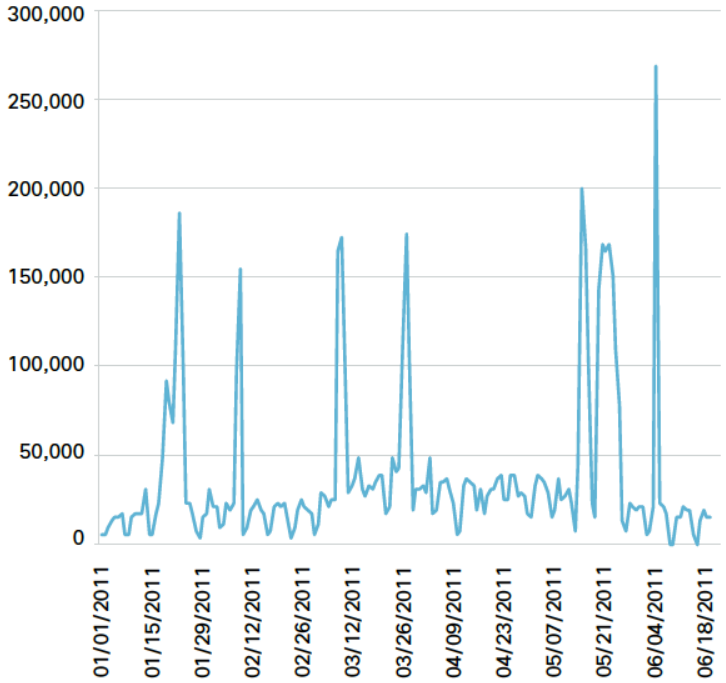


Figure 1

Source: Arbor Networks, Inc.

Figure 8 DoS Event Firings, 1H11

Source: Cisco IPS



Zagrożenia dla naszych sieci

Wyłudzenia / IP o podejrzanym zachowaniu

- Serwery działające jako węzły C&C botnetów
- Źródła malware'u
- Źródła spamu
- Dowolne adresy IP i podsieci, które jesteśmy w stanie zidentyfikować jako "wrogie"
- Zapytania DNS – DNS aplification attack

  czy spoofing IP w Polsce jest możliwy?*

* pierwszy raz to pytanie zadałem 6 lat temu, sam sobie odpowiedziałem, potem sam się poprawiłem, a od tamtego czasu nauczyłem się, że warto jest zadawać pytania ☺

Dużo półśrodków

- Zabezpieczenie wszystkich stacji końcowych w Internecie jest nierealne
  - ...choć wielu próbuje
- Usługi „cloud” wydają się być krokiem w dobrym kierunku
  - zintegrowanie „pranie” ruchu od i do hosta
  - nadal jednak ich obecność na rynku jest niewielka, choć rośnie
- Parę wyspecjalizowanych firm realizujących pomoc/ usługi w ochronie przed DDoS
  - „pomoc” w wielu wypadkach nie wystarcza, ale pozwala określić atakujących i zbadać narędzia których używali

Jak działa BGP Blackholing?

Jak działa BGP blackholing?

Z 10000 metrów

- Utrzymujemy grupę serwerów tras oraz infrastruktury pomocniczej
  - routery Cisco
  - serwery FreeBSD
- Każdy z serwerów tras serwuje komplet tras "nieprzydzielonych" oraz przekazuje po kontroli na poziomie protokołu BGP prefiksy od jednego członka projektu do pozostałych
- Serwery tras rozlokowane są "strategicznie" w Polsce

Jak działa BGP blackholing?

…co to jest BGP? Co to jest community?

- BGP jest "klejem" utrzymującym światowy Internet w ruchu
- Community – to umowna wartość przekazywana wraz z prefiksem
  - rozgłaszamy osiągalność danej sieci
  - …oraz jej "atrybuty" – community jest jednym z atrybutów prefiksu
  - część wartości community jest ustandaryzowana
  - używamy community uzgodnionych przez regulamin projektu BGP blackholing PL

Jak działa BGP blackholing?

Z 3500 metrów

- Dla prefiksów oznaczonych konkretną wartością BGP community, modyfikujemy sposób przetwarzania ruchu do/z nich

  na podstawie umownej wartości BGP community dla prefiksu rozgłoszonego przez serwer tras uznajemy, że ruch do/z tego prefiksu należy traktować w konkretny, specyficzny sposób

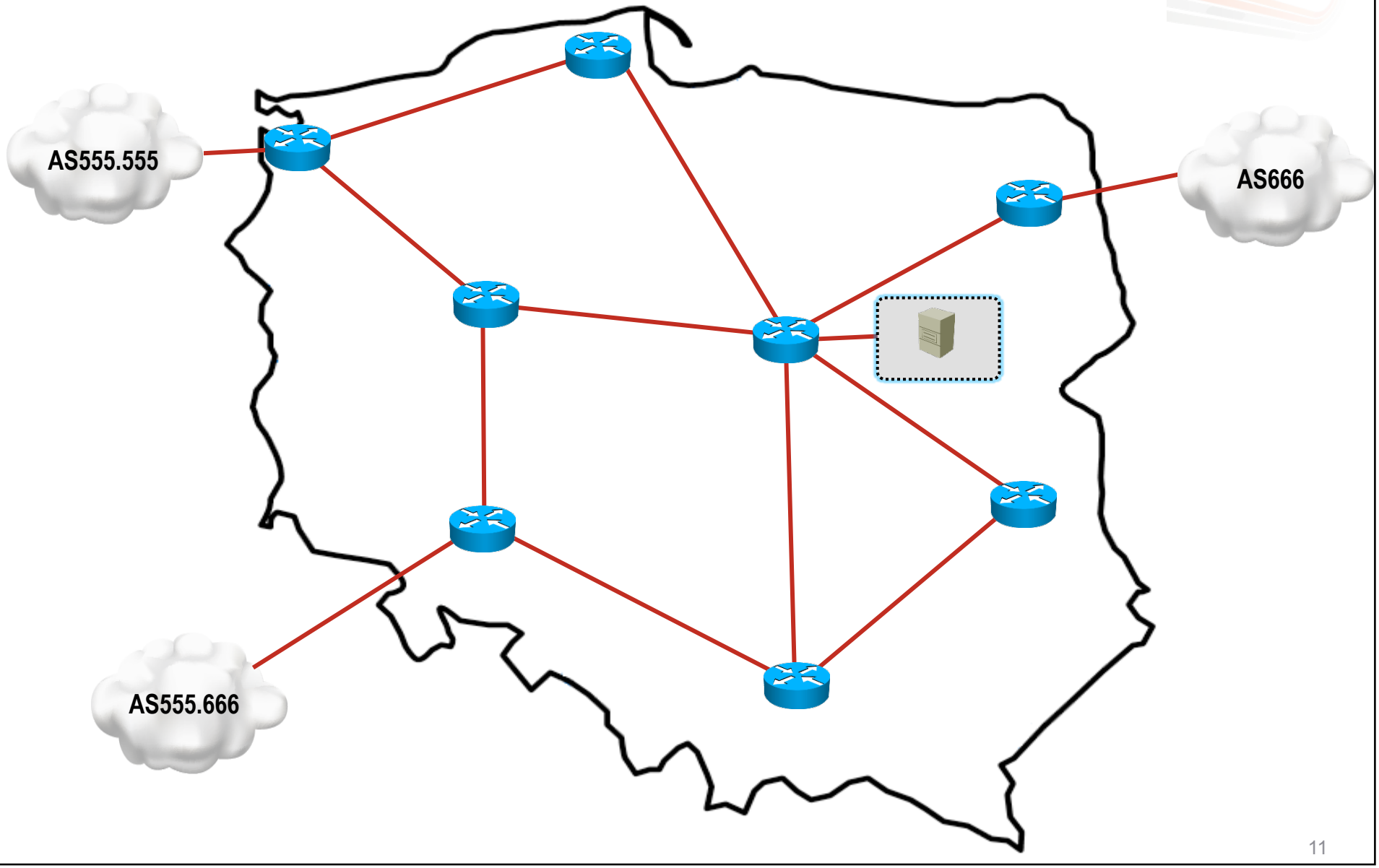
  np:

  64999:666 – odrzucamy (zmieniamy normalnie ustawiony interfejs next-hop na inny)

  64999:667 – kopiujemy do "śmietnika" – specjalny host w sieci, zbierający ruch do późniejszej analizy

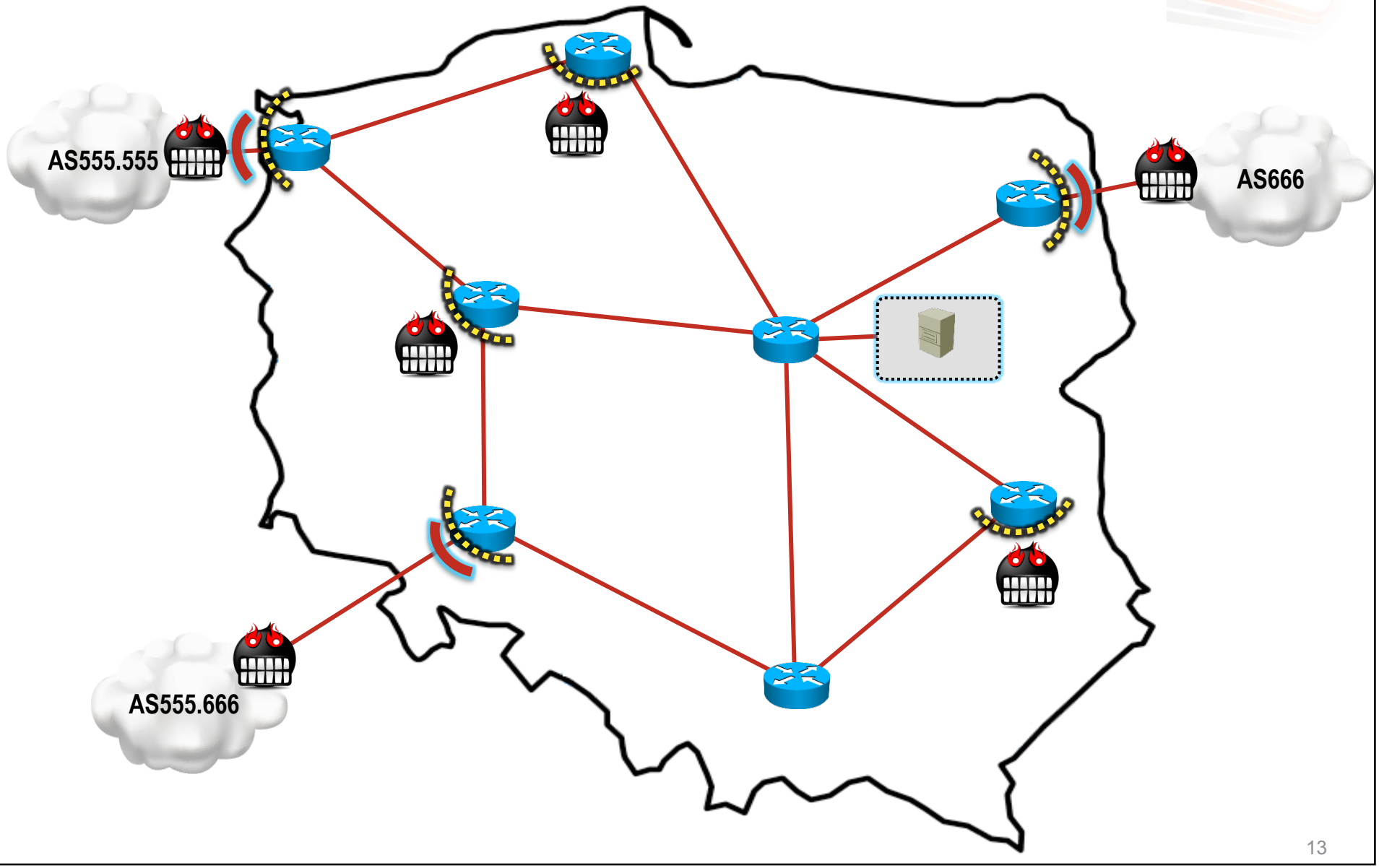
  64999:999 – warunkowo przekazujemy dalej, ale nakładając ograniczenie pasma/pps – np. do 2Mbit/s

BGP blackholing w akcji



BGP blackholin mp-up"

"Najlepsze praktyki"



Destination-based BGP blackholing

"Zgrubne" działanie mechanizmu

- Wszyscy uczestnicy projektu odrzucają ruch z/do konkretnego prefiksu oznaczonego uzgodnionym community
- Np.:

  192.0.2.44 z community 64999:666 > Null0/disc0

- Cały ruch od wszystkich uczestników projektu do danego prefiksu (tu – 192.0.2..44/32) jest odrzucany

  rezultat: blackholing (DDoS się powiódł)

  próba ominięcia problemu: zmiana rekordów DNS usługi na inny IP i kontynuowanie usług (potencjalnie – również ataku)

Source-based BGP blackholing

Trochę dokładniejsza wersja

- Jako właściciel atakowanego prefiksu po zidentyfikowaniu atakującego AS mogę go "zablokować"
- Np.:

  posiadam prefiks 192.0.2.0/24

  atakuje mnie prefiks 10.6.72.0/24 z ASN 65007

  rozgłaszam prefiks 192.0.2.0/24 (mój) z community 65007:666

- Jeśli ASN 65007 jest uczestnikiem projektu powinien jako "dobry obywatel" zablokować ruch do wskazanego prefiksu – 192.0.2.0/24

Source-based BGP blackholing

Trochę dokładniejsza wersja – czemu ma sens?

- Przygotowanie własnych routerów brzegowych do współpracy jest bardzo proste i stałe
- Akceptujemy tylko dwa community:

  64999:666 – prefiksy nie przypisane przez IANA

  $MOJ_ASN:666 – prefiksy które atakuje mój własny ASN
- Proste i efektywne
- Wymaga zaufania dla filtrów wejściowych route serwerów BGP Blackholing PL ☺
- **ZAWSZE** możecie nie akceptować konkretnych prefiksów – piękno selektywnego filtrowania w BGP

BGP blackholing?

Zalety

- BGP i tak zwykle jest obecne na routerach brzegowych
- Technika jest **dynamiczna** i **skalowalna** – pojedyncze prefiksy i całe pule można usuwać/ dodawać bez żadnych modyfikacji po stronie routerów brzegowych
  - potrzebny jest jedynie jeden lub dwa (redundancja) routery "wrzucające" – ustawiające community na prefiksie
  - nasze serwery tras
  - równie dobrze – Wasze własne serwery tras "na użytek wewnętrzny"

BGP blackholing?

Wady

- Wymaga konfiguracji ☺
- Działa/nie działa

  dla "wątpliwego" ruchu zastosować można QoS

  QoS Policy Propagation with BGP – dodatkowa technika

- Dokładność to adres IP

  BGP FlowSpec rozszerza zastosowanie na informacje o L4, nie jest jednak uniwersalnie dostępny, a jego implementacje mają swoją specyfikę

Jak działa BGP blackholing PL?

Co właściwie rozgłaszamy?

- Przestrzeń nie przydzielona przez IANA

  IPv4 – 13 prefiksów, realistycznie ponad 5k prefiksów

  IPv6 – ponad 47k prefiksów!

  Każdy członek projektu może rozgłosić do pozostałych uczestników swoje prefiksy jeśli zostanie zaatakowany i woli je odciąć, niż zupełnie umrzeć

  "Administracyjnie" – w przypadku **dużych** problemów, zespół BGP BH PL – dowolny prefiks

- **ZAWSZE** możecie nie akceptować konkretnych prefiksów – piękno selektywnego filtrowania w BGP

  np. "nie akceptuje w ogóle od Was prefiksów do infrastruktury krytycznej w internecie (serwery DNS root/ etc) oraz do portali które lubię"

Jak się przyłączyć?

Napisać list

bgp+join@null0.pl

- Pula IPv4/IPv6 – musi być widoczna w bazie RIPE jako rekord route/route6
- Numer ASN
- Jak zestawiamy sesję – IPv4, IPv6 lub dwie sesje dla obu protokołów osobno
- Mail i telefon kontaktowy
- Czy uwierzytelniamy sesję za pomocą hashy MD5
- Z jakim sprzętem zestawiamy sesję
- Czy zgadzacie się na publikowanie informacji o uczestnictwie

Dodatkowe źródła informacji

Listy dyskusyjne

- bgp-bh-announce@null0.pl

  zmiany w rozgłaszanych prefiksach

- bgp-bh-discuss@null0.pl

  ogólna, do dyskusji

BGP Blackholing PL

Zestawienie sesji to nie wszystko

- Szkolenia 2x do roku przy okazji PLNOG – utrzymanie i zaawansowanego bezpieczeństwa dla operatorów
  - 2-3 dni ćwiczeń praktycznych z podstawowymi mechanizmami żeby rozgrzać palce i poznać nowe mechanizmy
  - 2 dni ćwiczeń praktycznych w dużej drużynie wirtualnych operatorów
    - przekierowywanie ruchu do dalszego badania
    - sinkholing / ip anycasting / traceback
    - wykorzystanie NetFlow do analizy ruchu i wykrywania anomalii
    - architektury sprzętowe z punktu widzenia w/w mechanizmów
- 5 dni, z daleka od pracy, sieć składająca się z 4-5 ASów (i grup), po 20-30 routerów każdy

Q&A

Łukasz Bromirski
bgp@null0.pl
lukasz@bromirski.net