BGP Blackholing Project

Łukasz Bromirski
lukasz.bromirski@gmail.com
lbromirski@cisco.com

http://portal.null0.pl
BGP blackholing project

From 10000 meters

- Started in 2004, during last two years completely rebuilt & restarted during last PLNOG
- Using RTBH and/or uRPF and/or QPPB with a “twist”
- (currently) four redundant clusters of
  - Cisco IOS/IOS XE based routers (Cisco 7201/CSR 1000v)
  - FreeBSD "feed" VMs
    - Geographically dispersed in Poland, covering direct access to biggest core networks in the country (TelecityGroup, Thinx & SPs)
- Each of the Cisco boxes serves as a route reflector for customers – project members
- FreeBSD boxes digest and serve the prefixes with properly assigned communities
BGP blackholing project

From 3500 meters…

- Route servers announce prefixes for IPv4 and IPv6 AFs
- The “twist” – it can also pass (with verification) prefixes announced by member routes!
- Prefixes can be of a different kind, distinguished using known communities:
  - **bogons** – not assigned, reserved, special
    64999:666
  - **evil** – known C&C networks, spam sources, scanning, etc.
    64999:25, 64999:80, 64999:135 and others
  - **members prefixes** – to enable self-defense
    $MY_ASN:667, my_own_ipv4/ipv6_prefix
  - **other members prefixes** – to enable remote self-defense
    $ATTACKING_ASN:667, remote_ipv4/ipv6_prefix
- BGP gives us a powerful policy tool, even for members with limited trust to other/smaller entities
BGP blackholing project

Other details

- We're experimenting with the QoS policy propagation with BGP
  
  ...and with BGP FlowSpec thanks to IOS-XR implementation (experimental RS you can connect to and pass/receive FlowSpec data)

- …and with SIDR

  unfortunately, ROAs cover usual announced prefix length, not the ones we’re using (/28-/32 for IPv4 & /96-/128 for IPv6)

  ...alternative cache?
It’s a wider idea, not one project

- We’re mainly about educating how to securely connect your network to the internet.. and internet to your network 😊
  - IPv4 and IPv6 typical edge scenarios
  - basic hardening, more advanced tweaks
  - establishing RR, going from iBGP full-mesh to RR for IPv4/IPv6
  - IPv4 and IPv6 SP scenarios, involving 6PE, 6VPE and other VRF/MPLS scenarios (many different deployment types)
  - uRPF and the value of it (spoofing!)
  - NetFlow v5, v9
  - value of trust between parties
  - SIDR – RPKI (yeah!)

- If you want to donate rack space/IP connectivity in secure & safe location – please contact me!
BGP Blackholing Project

Thank You!

Łukasz Bromirski
lukasz.bromirski@gmail.com
lbromirski@cisco.com

http://portal.null0.pl