Remotely Triggered Black Holes

RIPE65 Routing Working Group
Amsterdam 2012

Nick Hilliard
CTO
nick@inex.ie
typical isp topology
RTBH Tutorial - Defining the Problem

what type of problem
- smart attacks

too much traffic
- dos
- ddos

single / multiple sources

traffic profile

single / multiple destinations
resolution tools
RTBH Tutorial - Dropping Packets in a Hurry

- Drop packets based on:
  - Source address?
  - Destination address?

Diagram:
- Attacker sends bad packets to victim.
- Victim is connected to ISP network.
ip route 192.168.12.34 255.255.255.255 Null0

routing-options {
    route 192.168.12.34/32 {
        discard;
        install;
    }
}

traffic to 192.168.12.34 is dropped

but only on a single router
need mechanism to propagate a null route throughout an entire network

cannot be done with an IGP

distribute a prefix with next-hop to a pre-defined address

null-route the pre-defined address on all routers

bgp
RTBH Tutorial - Smart Destination Drops

traffic to 192.0.2.1 is dropped on entire network

```
ip route 192.0.2.1 255.255.255.255 Null0

routing-options {
    static {
        route 192.0.2.1/32 {
            discard;
            install;
        }
    }
}
```
ipv6 route 194.88.241.237 192.0.2.1

routing-options {
    static {
        route 194.88.241.237 {
            next-hop 192.0.2.1;
            install;
        }
    }
}

RTBH Tutorial - Distribution via iBGP

traffic to 194.88.241.237 dropped network-wide
RTBH Tutorial - Works on IPv6 Too

- `ipv6 route 100::1/128 Null0`
- `routing-options {
  rib inet6.0 {
    static {
      route 100::1/128 {
        discard;
        install;
      }
    }
  }
}

- Traffic to 100::1/128 is dropped
shameless plug

RFC 6666
100::/64
drop packets based on:

source address?

urpf: unicast reverse path forwarding

RTBH Tutorial - Source Filtering

ISP network

null / discard prefix

ISP network
RTBH Tutorial - Methodology

traffic filtering

- destination address
  - prefix-based null routing

- source address
  - unicast rpf with null routing

ibgp

remotely triggered black hole
RTBH Tutorial - Methodology

Service Provider Network

bgp rtbh server

transit #1

customer #1

customer #2

transit #2
RTBH Tutorial - It’s Good Stuff

fully standards compliant

defined in rfc5635

fast, efficient means of black-holing

also rfc6666, w00t!

supported by most transit providers
RTBH Tutorial - Client Configuration

- bgp routers on network
- null-route discard prefixes
- ip route 192.0.2.1 255.255.255.255 Null0
  ipv6 route 100::1/128 Null0
- ! Link with BGP
  interface GigabitEthernet1/1
  ip verify unicast source reachable-via any
  ipv6 verify unicast source reachable-via any

- urpf on edge interfaces
- set routing-options rip met6.0 static route 100::1/128 discard install
  set routing-options static route 192.0.2.1/32 discard install
  set interfaces ge-0/0/0 unit 0 family inet rpf-check
  set interfaces ge-0/0/0 unit 0 family inet6 rpf-check
  set interfaces ge-0/0/0 unit 0 family inet6 rpf-check

- ip verify unicast source reachable-via rx
  ipv6 verify unicast source reachable-via rx
be careful that your hardware supports unicast rpf properly

if you use next-hop-self in your ibgp policy, best to have separate rtbh box

don’t run ipv6 unicast rpf on a sup720

separate rtbh works well with route reflector config

asr9k requires IOS XR >= 4.1.1

can also run rtbh server on quagga, bird, etc
RTBH Tutorial - Server Configuration

- mechanism to inject prefixes
- tags to control injection policy
- policy of accepting host prefixes only
- ipv4 and ipv6 configuration examples
- uplink configuration to transits
- downlink configuration to isp customers
- juniper and cisco configuration
- includes trigger configuration