Unwanted Traffic Removal Service

https://www.team-cymru.org/UTRS/

John Kristoff
jtk@cymru.com
RTBH Illustrated

ATTACK 192.0.2.1!!

Send us traffic towards 192.0.2.0/24 BUT do NOT send any traffic towards 192.0.2.1/32

Customer ISP
DDoS. What is Missing?

A coordinated, automated, rapid community response.
UTRS Illustrated

ATTACK 192.0.2.1 !!

UTRS Peer A

ATTACK 192.0.2.1 !!

UTRS Peer B

ATTACK 192.0.2.1 !!

UTRS Peer C

ATTACK 192.0.2.1 !!

UTRS Peer D

RTBH Distribution!

UTRS community

Send us traffic towards 192.0.2.0/24 BUT do NOT send any traffic towards 192.0.2.1/32
UTRS

• Nothing more than a community run multi hop RTBH
• Purpose: severe infrastructure attack mitigation project
• Victims inject /32's (IPv4)
• We validate and pass on to participant peers
• Next-hop is an address that points to null interface
• Flow-specification capable
• Authoritative announcement and verification very critical
UTRS Configuration Example

neighbor 198.51.100.2 {
  description "gw.example.net";
  router-id 198.51.100.1;
  local-address 198.51.100.1;
  local-as 64496;
  peer-as 64497;
  hold-time 180;
  md5 abcdef0123456789;

  # normally no announcements, no attacks
  static {
  }
}

UTRS Peering Properties

- Local ASN: 64496 (private by default, can customize)
- Local IPaddr: 154.35.32.141 (what we have to work with)
  - This is really the only thing we can't customize
- TCP MD5 password is required
  - Arguably important for this multi-hop critical peering
- Static routes are the list of black holes, usually empty
- Each separate peer configuration built from an m4 template
What is announced and by who?

- Prefixes limited to IPv4 /32's
  - IPv4 prefixes could be larger given community input
  - We will IPv6 if demand warrants it
- Prefix admin or origin AS initiates the announcement
  - i.e. if you are under attack, submit a prefix to UTRS
- Manual process today, to be controlled by BGP soon
  - i.e. if you “own” the prefix, you can announce for it and we will pass it along after best effort verification
How will prefixes be validated?

• We will evaluate BGP origination history
• Anomalies and emergencies can be sent to the NOC
• New announcements are shared with community
  • Out of band updates (e.g. mailing list)
  • Community should provide oversight
Won't UTRS “Finish” an Attack

• An address in UTRS is sacrificed for the greater good
• This will not work in certain cases
• This will work where RTBH works
• Note: we can support flow-spec (IETF RFC 5575)
  • but it remains to be seen if many peers will too
Who can use it, who is using it?

• Internet BGP routing speakers can use it
• Various networks are currently peered or in the process
  • Participants not publicly disclosed, talk to me offline
• Long term prospects... still open. Discuss.
• NOTE: if we do not attract sufficient interest and use, we may terminate this project
Todo

• Automated validation (ExaBGP customization required)
• Web portal
  • Web form to start the setup process
  • Security contacts can enable/disable on our end
• Consolidate BGP feeds into a single feed
  • e.g. bogons, IXP
• RTSH (Sink Hole)?
• Take the keys away from jtk, and let the NOC run it