An Internet-wide BGP RTBH Service

John Kristoff <jtk@cymru.com>

April 17, 2015

Abstract

For over a decade Internet operators have used techniques described in IETF RFC 3882, Configuring BGP to Block Denial-of-Service Attacks, to mitigate packet flooding attacks aimed at specific target networks and hosts. Deployment of these BGP-based remotely triggered black hole (RTBH) mechanisms have largely been limited to the customer-ISP peering relationships, where the customer signals its upstream ISP that it wishes to cease receiving traffic for a given target. While this use of IETF RFC 3882 has been effective in many cases, it has not been able to effectively squelch the largest and most widely distributed attacks that have arisen in recent years. We propose equipping the Internet operator community with a shared RTBH system we have built and deployed called the Unwanted Traffic Removal Service or UTRS (pronounced "utters"). We argue that this community-based approach can not only help significantly reduce the most severe attacks beyond what has been possible before, but UTRS can stop the attack traffic nearer its origination, which helps limit the impact on transit networks as well as the target.

1 Introduction

Team Cymru has recently deployed the Unwanted Traffic Removal Service (UTRS), which relays black hole route announcements between otherwise unconnected BGP network operators. In this sense, UTRS is essentially a multihop route server. However, rather than coordinating packet forwarding between peering participants, UTRS effectively coordinates packet dropping rules. Since UTRS only announces black hole routes, each participant will associate these routes with a specially configured next-hop address pointing to a discard or null interface. Therefore any packets towards destinations matching UTRS announcements will be dropped by all UTRS participant networks.

It is important to realize that UTRS participants cannot announce any prefix they wish. They are limited to announcing host-specific IPv4 routes today (/32 prefixes) for addresses they have a history of being the sole route originator for. This is part of the route verification process that is unique to the UTRS service and enables participants to safely exchange route announcements through the system.

2 Technical Details

At the heart of the UTRS system is route verification methodology. Currently we only accept IPv4 /32 route announcements from participants and each participant is limited to 25 active routes at a time. Most importantly, we must ensure that these announcements are for addresses the participant is justifiably allowed to announce. In lieu of BGPSEC and a RPKI infrastructure, which is not yet widely available, we had to come up with a way to associate a valid route to a peer. We decided that an acceptable approach was to base this decision on Internet routing table history. We stipulate that if the address has been solely originated by the peer within the last 30 days, the announcement is credible and we will relay it. To examine route history we use RIPE NCC's RIPEstat API, a JSON-based framework that leverages their extensive route measurement and monitoring infrastructure.

This verification system exists within a larger router OS framework and we have chosen to implement ExaBGP as the core routing process, because it provides the flexibility we need to perform tasks such as validation before relaying announcements.

When route announcements are verified and relayed to participants we also generate routing update messages which go out to an UTRS mailing list as well as a local database. If and when a withdrawal is received, we will of course withdraw the route. We will also automatically withdraw any route that has been active for more than seven days, which helps limit stale routes and keeps the active routes to a minimum.

3 Current Status

As of this writing there are over 65 networks of varying sizes participating in UTRS. All major regions of the world are represented and if we were to just count the number of IPv4 addresses originated by these UTRS peer ASNs it would account for approximately 3% of the entire IPv4 address space. At any one time there are typically a handful of announcements active while throughout the day there are many transitory announcements that last for just a few minutes or hours. The overall volume of route update traffic has been relatively modest, certainly well below the limits of even the smallest BGP environments. While operators are certainly taking advantage of UTRS what we cannot directly see is the effect UTRS has. We are working with the participants to try to measure any effect UTRS might be having.

4 Future Plans

The automated route verification and relay function in UTRS just went live in March of 2015. When that capability went live we begun to attract a regular stream of new UTRS participants. We are also working to promote UTRS to network operators since participation will only increase its value to UTRS. We

are also considering partnering with internet exchange (IX) operators, providing them with a read-only feed to help extent the reach of UTRS.

We have also been soliciting interest in additional features or behavior. For instance, a few participants or potential participants have expressed interest in IETF RFC 5575, Dissemination of Flow Specification Rules (aka flow-spec). We may considering providing this capability in the future since the underlying router software we use already supports it. We have also been asked about IPv6, larger prefix sizes and announcements for other types of unwanted traffic.

References

[1] Unwanted Traffic Removal Service (UTRS) landing page
`https://www.team-cymru.org/UTRS`

[2] UTRS technical information and FAQ page
`https://www.cymru.com/jtk/misc/utrs.html`

[3] IETF RFC 3882, Configuring BGP to Block Denial-of-Service Attacks, September 2004

[4] IETF RFC 5575, Dissemination of Flow Specification Rules, August 2009

[5] ExaBGP, `https://github.com/Exa-Networks/exabgp/`

[6] RIPEstat, `https://stat.ripe.net/`