Internet2 Security Working Group DDoS Mitigation Recommendations

23-Oct-2015
ssw@iu.edu on behalf of the Internet2 Security Working Group

Background

During the October 2015 Technology Exchange, at the Network Members and Connectors BOF, Internet2 asked the Security Working Group to recommend Distributed Denial of Service (DDoS) mitigation capabilities that should be “fast-tracked” (i.e., expeditiously offered as Internet2 services). After receiving clarification concerning the request from I2 network services, an e-mail was sent to the Security WG list requesting input by Friday October 23rd. This document contains the Security WG’s recommendations.

The 17 e-mails[1] generated by the request represent a group discussion of various DDoS capabilities and their attributes. The following recommendations reflect the author’s interpretations, and their translation into specific recommendations. The recommendations fall into three categories; additional capabilities in the operation of the Internet2 network, vended services that can leverage the Internet2 Network and/or the collective influence of the Internet2 community, and activities that Internet2 can support and coordinate.

Recommendation for additional Internet2 Network capabilities

1. Following the advice of a small group of engineers experienced with Unwanted Traffic Removal Service[2] (UTRS), Remote Triggered Black Hole Filtering[3] (RTBH), and BGP FlowSpec[4], implement backbone support for all three mechanisms as-soon-as reasonable.
2. Where reasonable, establish layer 3 and/or layer 2 connectivity with all credible[5] DDoS mitigation providers. Such connectivity represents a fundamental value to Internet2 members, regardless of the provider's participation in Internet2’s Net+ program. To ensure success, the connectivity should be settlement free with reasonable interconnection terms.
3. Develop and share real-time detection of DDoS incidents with affected stakeholders.

---

[1] https://lists.internet2.edu/sympa/arc/security-wg/2015-10/msg00006.html
[2] http://www.team-cymru.org/UTRS/
[3] https://tools.ietf.org/html/rfc5635
[4] https://tools.ietf.org/html/rfc5575#section-5
[5] credible as determined by the advice of the Security WG

Recommendation for vended services that leverage the Internet2 network

1. Offer vended DDoS mitigation capabilities that are appropriate for the Internet2 community. Given the variety of capabilities and their implementation details, engage at least two network engineers from the community to vet potential vended capabilities. In addition, given the variety of pricing models, engage at least one campus and one RON volunteer to participate in the negotiations.
2. Where possible, with the consensus of stakeholders, use Internet2's influence with peers and transit providers to participate in UTRS and RTBH.

Recommended activities Internet2 support and coordinate

1. Make RON and Network participants universal adoption of UTRS a goal of Internet2's Network Services team.
2. Sponsor technically-focused workshops in coordination with select community members to aid in the implementation of tools such as RTBH, UTRS, exabgp[6], and FastNetMon[7].
3. Engage GEANT in the transfer of experience and expertise. Create a formal and structured relationship with GEANT concerning security and DDoS mitigation. Internet2 can learn from their progress.
4. Work with funding agencies, such as the National Science Foundation, to establish a Best Common Practice (BCP) required of awardees to prevent a campus from contributing to DDoS attacks.
5. Report progress on these recommendations quarterly to the Internet2 NTAC and Security WG.

[6] https://labs.ripe.net/Members/thomas_mangin/content-exabgp-new-tool-interact-bgp
[7] https://github.com/FastVPSEestiOu/fastnetmon