20 May 2015

Reference/Subject:

DDoS Mitigation in the NREN Environment Report

GÉANT
Networks • Services • People

DDoS Mitigation in the NREN Environment Workshop

10th – 11th October 2015

Vienna, Austria hosted by ACOnet

Table of Contents

1. Overview

On 10th and 11th November 2015, ACOnet hosted a workshop on DDoS Mitigation in the NREN Environment. The workshop was formed as part of the GÉANT Community Programme work in response to requirements identified by two GÉANT Task Forces and two SIGs.

TF-CSIRT, TF-MSP, SIG-ISM and SIG-NOC invited everybody interested in DDoS mitigation to attend this workshop and bring his/her own experience to discussing how DDoS mitigation is currently managed within the NREN environment and what future joint steps could be taken to better support requirements.

The workshop aimed to:

- provide a general overview of current DDoS mitigation solutions;
- collect available solution know-how and experience from and for NRENs and GÉANT;
- identify "federated mechanisms" and solutions particularly well suited for and within the NREN / GÉANT community.

A mailing list has been set-up for further discussion from this workshop: https://lists.geant.org/sympa/info/ddos.

2. Participating NRENS / Organisations

A total of 52 participants attended the workshop (8 remotely) representing 24 different NREN and supporting organisations:

BELNET, ACOnet, SURFnet bv, AARNet, CSUC, DeiC, GIP RENATER, RESTENA, Jisc, GÉANT, DFN, NORDUnet A/S, Consortium GARR, SWITCH, Research and Educational Networking Association of Moldova, HEAnet, CERT ZSIS, CERN, EENet/HITSA, BelWü, RedIRIS, CANARIE, SRCE, RNP.

The attendees noted the following reasons for their interest in the workshop:

- Many NRENs have not seen a real need to address DDoS as yet but envisage a greater need for the service in the near future.
- NRENS that have deployed commercial solutions are using one specific company and have concerns about the ability to negotiate a cost-effective procurement in the future from the options available.
- All participants were interested in information sharing and a general desire to work together on future solutions.

- Attendees wished to discuss how mitigation could be effectively rolled out beyond NREN CSIRT / NOC parameters and engage with customers for DDoS mitigation.

3. Presentations

All presentations from the workshop are available at: https://wiki.geant.org/display/SIGISM/DDoS+Mitigation+Workshop+Agenda.

4. Why is DDoS Mitigation Important Now?

NREN service provision as shown in the NREN Service Matrix was discussed at the meeting: https://compendium.geant.org/reports/nrens_services. The service matrix shows a total of 77 services provided by NRENS, but only six of these are areas where the NRENs have a monopoly position in terms of it being difficult for institutions to buy the service elsewhere, even though cloud-based solutions are becoming more common. DDoS mitigation is one of these strategic services, so it is essential the NRENs find an effective way to provide this support to their customers.

Other factors are influencing the need for action. NRENs cannot ignore the growing number and volume of attacks being seen in their environments and for GÉANT itself the increase in peering arrangements makes mitigation an important factor in risk management.

NRENs need to develop specialised tools to deal with this problem and to provide online real-time reporting from and for users.

5. Business Case Approaches

DDoS mitigation is known to be an expensive service and it is often difficult to make an effective business case for the expenditure. Security is typically seen as something that should “just happen” as part of typical network operations; more work is needed to make the case for further investment that demonstrates value for money. The value for mitigation is often not appreciated until after an attack occurs.

Jisc described how its renewed focus on security was driven by government initiatives with new requirements for online safety, combined with a demonstrable increase in security incidents in recent years. This has allowed them to develop a comprehensive security strategy covering ISO 27001, DDoS mitigation, malware analysis and vulnerability assessment.

6. Cross-team Ownership

The combination of interest groups at the workshop from a wide variety of task forces and SIGs within the GÉANT community demonstrates clearly that a coordinated approach to mitigation is needed. Attendees all described various different approaches to mitigation with workflows for mitigation starting at different points of the organisation and being owned by different teams within an organisation. Typical parties involved include central service desk, CSIRT teams, NOC teams and (where existing) SOC teams. All NRENS highlighted the importance of communication both internally and with the customer.

For this structure to be effective, the DDoS mitigation approach needs to be well documented, well understood by all the teams, and well supported by management.

7. Typical Attacks

There are various use cases for DDoS attacks in R&E, including research on DDoS itself. Lots of attacks generate from students for a variety of reasons: from the simple "game" of being able to cause disruption to the intention to disrupt classes or exams - it is simple and cheap to buy a DDoS attack online. There is also evidence that DDoS attacks are targeting specific research projects.

NRENS generally experience two types of attacks:

- Volumetric attacks: these target infrastructure or access, can be detected by NRENs (mostly) and are often brute force.
- Application layer attacks: these target specific services, seem/are legitimate traffic to NRENs and are more sophisticated, making use of vulnerabilities in app.

The majority of attacks in the research and education environment are largely simple OSI/ISO Layer 2-4 attacks, mostly initiated by students. Simple black-holing, ACL filtering or rate-limiting are the easiest solutions to mitigate these attacks, however, black-holing cuts customers off the network completely.

More sophisticated traffic-washing can be used also against complex Layer 4-7 attacks, but this technique is not that significant currently. The biggest impact of a DDoS attack would be if an NRENs' upstream connectivity would go down. As GÉANT provides ever more peering services, more and more NRENs are looking at GÉANT to serve as their upstream provider. Firewall-on-demand and a three-step filtering architecture helps GÉANT to mitigate attacks in the pan-European backbone.

8. Current Mitigation Solutions

- Blackholing.

Black-holing - the act of silently dropping traffic without informing the source - is one of the simplest solutions to DDoS mitigation, however it results in cutting of traffic from the network; effectively playing into the hands of the attackers.

- ACL filtering or rate-limiting.

Can reduce the effects of a DDoS attack but also has the potential to impact targets which are not currently under attack (collateral damage).

- Commercial Mitigation ("scrubbing") solutions.

There are many commercial tools offering DDoS mitigation solutions but many are too expensive or unsuitable for the NREN environment. Arbor (http://www.arbornetworks.com/) is by far the most common commercial anomaly detection and/or scrubbing solution used inside NRENs.

Also ISPs (e.g. Level 3) and CDN or cloud providers (e.g. Akamai) are offering DDoS mitigation on demand, often based on cloud based scrubbing centers distributed over the globe.

- Firewall on Demand and BGP Flowspec.

Firewall-on-demand (FoD) is a service being piloted by GÉANT based on work developed by GRnet. This provides a web GUI that allows users to instantly set up filtering. The project is still in its early stages and needs to go through full pen testing and piloting but offers a useful tool to be added to the portfolio of available approaches. FoD is built on the BGP Flowspec approach scaled up to a multidomain NREN environment.

- DFN Solution.

DFN presented and described a homegrown solution created by DFN to address requirements for their own service portfolio based on X-WIN. This project is due to complete in 2016 and may be suitable for use-cases outside of DFN (https://wiki.geant.org/download/attachments/49120066/Groeper-DDoS-WS_Wien.pdf).

- UTRS.

UTRS (Unwanted Traffic Removal Service) is provided by Team Cymru: http://www.team-cymru.org/UTRS/. It works across existing networks of cooperating BGP speakers such as ISPs, hosting providers and educational institutions that automatically distribute verified BGP-based filter rules from victim to cooperating networks. The service is has no fee associated with it, but information on current usage is restricted to those involved. The main drawback of the approach is the need to effectively allow third parties into your network. The success of the trust framework that Team Cymru is able to build will impact on the quality of the service.

9. Community / Project Approaches

As well as solutions designed directly for the NREN customer, several presenters at the workshop gave an overview of DDoS projects with wider participation and goals.

CESNET and NIX.CZ (Czech IXP) introduced the FENIX project to national participants. In 2013, organisations in the Czech Republic experienced sustained attacks across a single week which started with portals and online tools and then escalated to banks and mobile carriers. In response to this, various CSIRT teams within the Czech Republic agreed to work together on a safe VLAN peering project for trusted partners, through which users could access services. For being allowed into the FENIX trust group ISPs need to have implemented BCP38 (IP anti-spoofing measures), protected sessions BGP, IPv6 and DNSSEC. FENIX is self-governed and independent of cz.nic (the national CSIRT team) but cz.nic acts as an arbitrator for participants. The project is managed as a trust-circle approach, and members must be recommended by other participants,vetted and go through a trial process.

RNP described the SeVen project: A Selective Defense for Low-Rate Application Layer DDoS Attacks. The project was a collaboration between local universities and RNP in Brazil to specifically address application layer DDoS attacks. RNP highlighted the fact that in 2013 37.2% of DDoS attacks exploited the http protocol and application layer attacks were both simple to run, difficult to spot (traffic is similar to legitimate clients) and there are few defenses available (beyond IP filtering and denying service to slow clients). SeVen provides a generic strategy for application layer defense through a simple mechanism of selective verification of connections. When the maximum number of connections is reached, SeVeN decides on which of the existing connections to drop to accommodate the new request. Through its design and monitoring approach, it is able to predict and drop attacker traffic rather than legitimate sources. This allows for legitimate traffic to operate normally even throughout the period of attack, and provides appropriate defense until mitigation can be carried out.

These collaborative style projects are in line with proposals put forward by ISOC for collaborative security in a recent whitepaper: http://www.internetsociety.org/sites/default/files/CollaborativeSecurity-v1-0.pdf.

10.Customer Support

Attendees at the workshop discussed whether it was possible to fully automate DDoS mitigation or whether some manual intervention by the NREN was necessary to support customers. NRENs operate very differently from typical ISPs in their relationship with customers and it is important that the approach to mitigation is driven by the needs of the customer. It would be highly unusual for an NREN to make decisions on traffic without explicit approval from the organisation in question. Automated approaches, whilst cost effective, do not necessarily produce the desired outcome. Attendees with experience in mitigation highlighted many factors that impact on providing a fully automated approach, including issues caused by the roll-out of IPv6.

Mostly simple attacks are easily mitigated on a per customer basis, although the level of knowledge and ability at each organisational site varies depending on the customer and its size - NRENs serve everything from large, complex research universities to small schools with fully managed services in place.

Another factor for discussion was the length of time that mitigation should be carried out in scenarios where the site is not able to resolve issues. Examples were given of scenarios where mitigation had to be carried out that lasted longer than desirable, which has a cost implication for the NREN that might have to be passed on to the customer where commercial solutions are being utilised due to cost factors being applied to the size of traffic being managed.

11.What are the Alternatives to Procurement?

Attendees at the workshop agreed that exploring options for a joint procurement for commercial mitigation solutions was one part of the solution process, however it was felt that NRENs should explore a range of tools to meet the complex needs of the NREN environment and to ensure that a dependency lock-in to proprietary approaches did not cause risks for the community further down the road. The Firewall on Demand project has already taken steps to support an alternative approach and is an important part of the strategic approach.

Two further approaches to the mitigation tool-set were discussed at the workshop. Work on open source solutions to DDoS mitigation was discussed, which could build on the DFN tool (if appropriate resources and developers could be found) or work with external companies like Radically Open Security (https://radicallyopensecurity.com/) on an open source DDoS mitigation tool. Other external solutions were discussed, such as the Team Cymru UTRS - or Unwanted Traffic Removal Service (http://www.team-cymru.org/UTRS/) as described above.

12.Proposed Actions and Recommendations

At the end of the workshop, attendees agreed the following actions and recommendations:

a. GÉANT should set up a mailing list (ddos@lists.geant.org), initially with just the attendees from the workshop. This should be a closed list and intended as just a general discussion list for cross-group discussions. It is not necessary to establish another SIG or TF for this activity, but it would be good to identify a general home for the work and a small amount of GÉANT coordination support.

b. NRENs should explore the interest in joint procurement of commercial DDoS mitigation solutions.

c. The SGA2 white paper on security should be reviewed to see if it is possible to fund some of the activity discussed in the workshop within GN4-2.

d. NRENs should explore the options for further developing home-grown solutions such as the work done by DFN. Funding would be required to support this work.

e. NRENs should explore opportunities to jointly work with organisations undertaking alternative approaches to mitigation. Team Cymru, Radically Open Security and Flowspec production trials were proposed as initial organisations to approach.

f. SIG-NOC should consider putting some questions on DDoS into their survey and feeding this information back into the compendium.

13.Resources and References

- Akamai: https://www.akamai.com/.

- Arbor: http://www.arbornetworks.com/.

- CERT.be Whitepaper DDoS: Proactive and reactive measures: https://www.cert.be/docs/whitepaper-ddos-proactive-and-reactive-measures.

- DDoS Mitigation Workshop Slides and Agenda: https://wiki.geant.org/display/SIGISM/DDoS+Mitigation+Workshop+Agenda.

- ISOC Collaborative Security White Paper: http://www.internetsociety.org/sites/default/files/CollaborativeSecurity-v1-0.pdf.

Jisc security products and services strategic plan: https://community.jisc.ac.uk/system/files/288/Plan%20for%20Jisc%20security%20products%20and%20services%20-%20March%202015_0.pdf.

- Radically Open Security: https://radicallyopensecurity.com/index.htm.

- RFC 5575 - Dissemination of Flow Specification Rules: https://tools.ietf.org/html/rfc5575.

- Team Cymru UTRS (Unwanted Traffic Removal Service): http://www.team-cymru.org/UTRS/.

- WISE workshop presentations: https://www.terena.org/activities/ism/wise-ws/agenda.html.