Collaborative Attack Mitigation and Response: A survey

Jessica Steinberger*†, Anna Sperotto†, Harald Baier* and Aiko Pras†

*da/sec - Biometrics and Internet Security
Research Group University of Applied Sciences
Darmstadt, Darmstadt, Germany
Email:{Jessica.Steinberger, Harald.Baier}@h-da.de

†Design and Analysis of Communication Systems
(DACS) University of Twente,
Enschede, The Netherlands
Email:{J.Steinberger, A.Sperotto, A.Pras}@utwente.nl

***Abstract*—Over recent years, network-based attacks have become one of the top causes of network infrastructure and service outages. To counteract such attacks, an approach is to move mitigation from the target network to the networks of Internet Service Providers (ISP). However, it remains unclear to what extent countermeasures are set up and which mitigation approaches are adopted by ISPs. The goal of this paper is to present the results of a survey that aims to gain insight into processes, structures and capabilities of ISPs to mitigate and respond to network-based attacks.**

I. Introduction

Nowadays most business processes depend on the Internet. Disruption of Internet-based services causes financial loss, brand and reputation damage as well as incurring penalties [1]. These disruptions are often caused by network-based attacks. In the last years network-based attacks, such as Distributed Denial of Service (DDoS), evolve to one of the top concerns responsible for network infrastructure and service outages [1], [2]. The reason is that attacks are getting larger, more sophisticated (e.g. multi-vector attacks) and more frequent. At the same time it has never been easier to execute DDoS attacks [3], e.g., Booter services offer paying customers, without any technical knowledge, the possibility to perform DDoS attacks as a service [4].

Traditional security solutions such as firewall and Intrusion Prevention System devices are often not able to handle the large amount of traffic reaching the target network. One reason is that the monitoring equipment located at the victim side might exhaust its own resources as a side-effect of the attack [5]. Further, if a DDoS attack already reached the perimeter of the target network, it is often too late to start mitigation procedures, since the network link is already saturated. Therefore detection and mitigation need to be located closer to the source of these kinds of attacks.

The study in [6] shows that ISP networks are considered to be key points for network-based attack detection and mitigation. Additionally, ISPs should collaborate to share and exchange information in the context of network security [7] to support proactive detection, real-time and automatic mitigation of current types of attacks. But will such an approach be adopted by ISPs? Do ISPs currently collaborate? In this paper, we investigate how network operators detect, mitigate and respond to network-based attacks in practice. To achieve insight into real-world processes, structures and capabilities of IT companies and their computer networks, we conducted a survey that was sent to the most important network operators mailing lists. The questionnaire was answered by 42 respondents from ISPs and other network operators.

TABLE I. Overview of the survey

#	Category	# of questions	# of answers
1	Organization and personal info	8	42
2	Process and involved third-parties	9	38
3	Automatic mitigation and response systems	11	35
4	Data	18	31
5	Exchange and Collaboration	6	28

The remainder of this paper is organized as follows: Section II describes the setup of our survey. The results are analyzed and evaluated in Section III. In Section IV, the paper is concluded and directions for future research are suggested.

II. Survey methodology

The survey[1] targeted ISPs and consisted of 52 questions related to 5 categories. These categories include a number of questions that are summarized in Table I. Category 1 allows us to create a demographic of the respondents, their organizations and their network. Category 2 gathers information about internal and external parties involved in the mitigation and reaction process. Category 3 collects information about the tools our respondents use to mitigate and respond to network-based attacks, the quantity of security events and incidents, and the attack mitigation on average. Further, we ask questions regarding the accuracy of the automatic detection and mitigation systems. Category 4 gathers information about the use of publicly available security event data and their inclusion into the mitigation and response process. This category also covers DDoS protection networks, the use of BCP 38 and the use of network configuration protocols. Within category 5, we asked questions regarding collaboration between third parties and the exchange of security related information.

We distributed our survey using several relevant mailing lists as described in [8]. The most important ones are listed in Table II. The answers were collected with the aid of an online system over a time period from May to July in the year 2014. A total of 42 respondents submitted valuable data. The respondents originate from Europe (93%), North America (2%) and Asia (5%). Table III lists the market segments, the abbreviation and the number of times a market segment was selected by a respondent in relation to the total number of

[1] https://www.dasec.h-da.de/wp-content/uploads/2014/10/SurveyOnMitigationAndResponseOfNetworkAttacks.pdf

TABLE II. OVERVIEW OF MAILING LISTS

Name, URL
European IP Networks forum RIPE, http://labs.ripe.net
German Network Operators Group DENOG , http://www.denog.de
DE-CIX competence group security, http://www.de-cix.net
Swiss Network Operators Group SwiNOG, http://www.swinog.ch
North American Network Operators Group NANOG, http://www.nanog.org
Competence Center for Applied Security Technology, http://www.cast-forum.de
Advanced Cyber Defence Centre for Europe, http://www.acdc-project.eu
Trans-European Research and Education Networking Association http://www.terena.org

TABLE III. OVERVIEW OF THE MARKET SEGMENT AND FREQUENCY

Organization	Abbr.	Frequency
CDN/Content Delivery	CDN	2%
Cloud Service Provider	Cloud SP	2%
Educational/Research Institution	ERI	31%
Hosting/Data Center/Co-Location Services	Hosting	7%
Managed Service Provider	Managed SP	2%
National Research and Education Network provider	NREN	31%
Other	–	6%
Tier 1 Service Provider	Tier 1 SP	7%
Tier 2/3 Service Provider	Tier2/3 SP	12%

responses. The majority of the participants are headquartered in Europe and classified their company as NREN provider. The average traffic rate transported over the respondents' routers vary between $1-5$ and $11-50$ Gbits per second. As the majority of our participants are based in Europe, our results are expected to be valid for at least the European context. Besides these four characteristics, our respondents have been working in the field of IT or security with an average of 16 years. Further, they hold their current position with an average of 9 years. All of our respondents have the capability to reconfigure access or border routers.

III. RESULT SET ANALYSIS AND EVALUATION

In this section, we present and discuss the main results of our survey. Section III-A provides information about the mitigation and response process and other involved third-parties. Section III-B describes which automatic mitigation and response are in place and what kind of automatic mitigation and response methods are used. Section III-C shows which external available data ISPs and network operators consider important and include into their mitigation and response process. Finally, we discuss collaboration among Internet Service Providers and network operators in Section III-D.

A. Processes and involved third-parties

Although mitigation approaches using collaboration have been reported [9] and national CERTs/CSIRTs are established to assist organizations in mitigating and responding to a security event/incident, 50% of the respondents disclosed having a cooperation with an external third party (e.g., ISP or network protection service). However, 17 of 19 replying participants (89%) cooperate with an ISP. Significantly fewer, namely 5% respondents cooperate with a forensic firm or a packet cleaning house (e.g., Cloudflare). In the first place, collaboration is done to aid the respondents' Network Operations Center (NOC) (63% of the respondents). Further, 31% of the respondents use cooperation to augment the skill set and capacity of the organization's CSIRT (36% of the respondents) in daily business and during crisis situations.

Fig. 1. Average number of attacks in relation to average traffic rate

In our next question, we asked the participants about their communication with national CSIRTs. 65% of the participants report communicating with national CSIRTs, of which 85% uses email and 35% the telephone. Only 10% make use of an automatic mitigation and response system to communicate with national CSIRTs.

B. Automatic mitigation and response systems

Arbor Networks [1] reported that the most significant operational threats are DDoS attacks. The majority (58%) faces $1-2$ DDoS attacks targeting their organization's infrastructure per month on average. Surprisingly, most of the DDoS attacks are detected in mid-size networks where the average traffic rate transported over network border router varies between 1-50 Gbits per second as shown in Figure 1[2]. In contrast to mid-size networks, transport networks (such as Tier 1/2/3 Service Provider, Cloud Service Providers) only report a small amount of DDoS attacks per month on average. One reason might be that attackers predominantly target end users [1]. Another reason might be that these service providers are not able to detect DDoS attacks as their effect within a high-speed network might be too small.

Nowadays, automatic systems (such as Intrusion Detection Systems, Security information and event management systems) are in place to detect network-based attacks. Therefore we asked our respondents how many security events/incidents are reported by automated detection mechanism per month on average. The majority (49%) report less than 10 security events/incidents raised by automated detection mechanisms per month on average. Automatic detection mechanisms that cause more than 500 security events/incidents per month are reported by 20% of our participants. The expectation, that the massive amount of events/incidents are reported from participants of high-speed network turned out to be false and is shown in Figure 2 (left side)[2]. More than 500 security events/incidents were found in ERIs. Subsequently, we asked our respondents how many security events/incidents raised by

[2] Both axes represent the answer options given by the multiple choice question and thus are discrete data scales. As a result, multiple points have exactly the same coordinates. To avoid overlapping data points, we make use of a jitter range. This jitter range is 0.2 on the x-axis and 0.1 on the y-axis.

automated detection mechanisms per month on average are real security events/incidents that need to be handled. The majority (74%) claim that a maximum of 10% of the reported security events/incidents on average are real security events as shown in Figure 2 (right side)[2].

Next, we asked our participants if their organization makes use of mitigation and response tools that perform automatic mitigation and reaction steps to defend the organization's network. Just over one third of our respondents reported to perform automatic mitigation and reaction steps. In case our respondents decline to use an automatic mitigation and response system, we asked if the use of those systems would speed up their organization's mitigation and response capabilities. 71% of the participants agree to this statement. Especially respondents who report a high number of security events/incidents caused by a detection mechanism and report a high false positive rate state that the use of an automatic mitigation and response tool would speed up mitigation and response capabilities. Subsequently, we asked the respondents who declined to use an automatic system if they plan to make use of it in the future. 62% of the participants plan or consider to use automatic mitigation and response tools and would like to perform the following mitigation and response actions: Change blocking or filter capabilities (71%), rerouting traffic (67%), rate limiting at ingress (62%), notification of involved function or departments within the organization (48%), exchange data with trusted partners (38%), quarantine machine (33%) and changing the target's IP address (14%).

Respondents who reported that their organization already uses automatic mitigation tools perform the following actions: Change blocking or filter capabilities (87%), notification of involved function or departments within the organization (54%), rerouting traffic (46%), rate limiting at ingress (46%), quarantine machine (31%), exchange data with trusted partners (15%) and changing the target's IP address (8%). The majority of these mitigation and response actions are performed using a self-built tool (77%). 54% of the respondents report to use open-source software to perform automatic mitigation and response and only 38% rely on commercial products. The reasons not to use commercial products are manifold. 57% of the respondents report that commercial products are too expensive. Followed by 43% of the participants that do not use automatic mitigation and response tools due to the high risk of false positives.

C. Data

One benefit of the inclusion of external information is that the external information might contain additional information relevant for the mitigation and response process. In addition, they provide the opportunity to enhance available security event/incident information. External data sources, such as the CVE database, Shadowserver and RIPE provide high-quality publicly available security related information. Thus, we asked our participants if they make use of these particular data sources. CVE is used by 52% of the participants. Information published on RIPE is used by 35%, on Shadowserver by 16%, and 29% do not make use of any external data source. Other external data sources are black, white and greylists. One defense mechanism described in the literature is IP filtering [10]. As IP filtering might filter out legitimate traffic, only 48% of the participants report making use of it.All respondents who claim to use IP filtering report using a blacklist filtering approach, whereas only 53% of the respondents also report using whitelists and only 33% report also using greylists.

Another approach mitigating and responding to network-based attacks is a cloud-based approach that are offered by several companies (e.g., Cloudflare, Incapsula). We asked our participants if they would make use of a cloud-based mitigation and response solution. The results reveal that only 26% of our respondents would make use of them. The reasons not to make use of cloud-based solutions are: the data should remain in the organization's own network (64%), customer's privacy (45%) and an unknown impact (54%).

Next, we asked our respondents if their network devices are configured according to BCP 38, because it is a well-known standard to mitigate spoofing and thus DDoS attacks. Although the attack target cannot enforce the origin ISP to implement BCP 38 and thus its intention of mitigation DDoS is questionable, 77% of our participants have already implemented BCP 38.

In our next question, we ask if the respondents use network configuration protocols to configure network devices. The majority (74%) of our respondents makes use of network configuration protocols. 68% of our participants report to use the Simple Network Management Protocol, 19% use Netconf, and only 6% use OpenFlow and Command-Line interface (CLI) based configuration protocols.

Moving Target Defense (MTD) [11] is a use case of Software Defined Networking and describes a constantly adapting environment to mitigate DDoS attacks. We asked our respondents about their technical ability to use OpenFlow. Currently, 71% of the respondents do not have the technical ability to use OpenFlow to configure network devices, but 69% plan or consider to have the technical ability to use it in 3 years.

Besides BCP 38 and MTD, BGP FlowSpec [12] introduces traffic filtering rules to mitigate DoS and DDoS attacks. To be able to use BGP FlowSpec, the routers must use BGP's Capability Advertisement facility to exchange the Multiprotocol Extension Capability Code [13]. Therefore, we asked our participants about their technical ability to use BGP FlowSpec. Currently, 52% of the respondents do not have the technical ability to use BGP FlowSpec and 69% do not even plan to use it in 3 years.

D. Exchange and Collaboration

We asked our respondents to rate the statement, that collaboration between trusted parties would improve mitigation and response capabilities. Even though 96% of our participants strongly agreed or agreed with the statement, Table IV shows that 50% of the participants do not share threat indicators. In contrast, 69% of our participants share security events or incidents. The majority of the participants report sharing threat indicators (46%) or security events/incidents (61%) with various CERTS or CSIRTs. Significantly fewer respondents, report sharing threat indicators (21%) or security events/incidents (25%) with law enforcement or other governmental entities. In the absence of widespread collaboration between trusted partners to mitigate and respond to network-based attacks, a

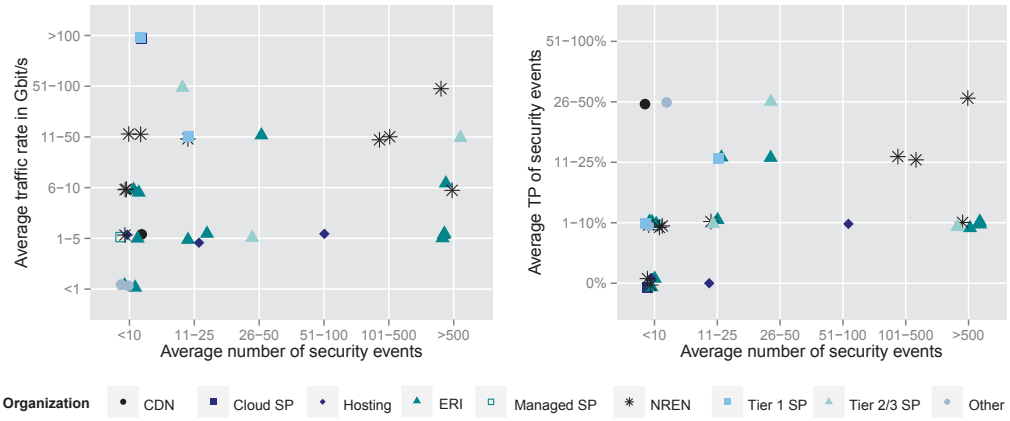

Fig. 2. Average security events in relation to average traffic rate and average true positives of reported security events

TABLE IV. SHARING THREAT INDICATORS OR SECURITY EVENTS/INCIDENTS WITH SEVERAL ENTITIES

	Threat indicators		Security events/incidents	
	Yes	No	Yes	No
None	7	21	4	24
CERTs/CSIRTs	13	15	17	11
Law/governmental entities	6	22	7	21
Industry peers	0	23	7	21
Receiving information	4	24	3	25
Sharing information	3	25	2	26

non-trusted approach to exchange security events/incidents is used by 54%.

IV. CONCLUSION

In this paper, we provide a first impression of how network operators and ISPs perform attack detection and mitigation. One key finding is that automatic attack detection systems are deployed but raise a massive amount of false positives. To handle the massive amount of security events, automatic mitigation and response systems could be established. We found that automatic mitigation and response systems to speed up mitigation and response capabilities are not widely deployed, but network operators would like to make use of them. Besides automatic detection and mitigation systems, collaboration of trusted partners to mitigate and respond to a network-based attack is regarded as valuable.

Furthermore, we gained knowledge about the use of external publicly available data to mitigate and respond to a network-based attack. An important finding is that traffic filtering based on IP blacklisting is not widely adopted. If our participants reported using traffic filtering, most of them make use of blacklists.

Based on the results of the survey, we indicate that future work should focus on automatic detection systems with low false positive rates that can be located in high-speed networks. Automatic mitigation and response system need to be deployed to efficiently and effectively handle the amount of security events/incidents raised by an automatic detection system. An important question for future studies is to determine the benefit of a collaborative mitigation and response approach.

ACKNOWLEDGMENT

The work has been funded by the German Federal Ministry of Education and Research (#16BY1201F), CASED and by EU FP7 Flamingo (ICT-318488).

REFERENCES

[1] D. Anstee, D. Bussiere, G. Sockrider, and C. Morales, "Worldwide Infrastructure Security Report," Arbor Networks Inc., Tech. Rep. IX, Jan. 2013.

[2] L. Marinos, "ENISA Threat Landscape 2013: Overview of current and emerging cyber-threats," 11.12.2013.

[3] J. Santanna, "DDoS as a Service," http://www.ietf.org/proceedings/interim/2013/10/14/nmrg/slides/slides-interim-2013-nmrg-1-11.pdf, nMRG workshop is co-located with Conference on Network and Service Management 2013.

[4] N. Hoque, M. H. Bhuyan, R. Baishya, D. Bhattacharyya, and J. Kalita, "Network attacks: Taxonomy, tools and systems," *Journal of Network and Computer Applications*, no. 0, 2013.

[5] R. Sadre, A. Sperotto, and A. Pras, "The effects of DDos attacks on flow monitoring applications," in *Network Operations and Management Symposium (NOMS), 2012 IEEE*, April 2012, pp. 269–277.

[6] M. van Eeten, J. Bauer, H. Asghari, and S. Tabatabaie, "The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data," in *OECD Science, Technology and Industry Working Papers*, 2013, vol. 2010/05.

[7] Internet Industry Association, "Internet Service Providers voluntary Code of Practice - For Industry Self-Regulation in the Area of Cyber Security," 08.09.2010, http://iia.net.au/userfiles/icode-v1.pdf.

[8] J. Steinberger, L. Schehlmann, S. Abt, and H. Baier, "Anomaly detection and mitigation at internet scale: A survey," in *Emerging Management Mechanisms for the Future Internet*. Springer Berlin Heidelberg, 2013.

[9] J. François, I. Aib, and R. Boutaba, "Firecol: A collaborative protection network for the detection of flooding DDoS attacks," *IEEE/ACM Transactions on Networking*, vol. 20, Dec 2012.

[10] M. Geva, A. Herzberg, and Y. Gev, "Bandwidth distributed denial of service: Attacks and defenses," *IEEE Security & Privacy*, vol. 12, no. 1, 2014.

[11] J. H. Jafarian, E. Al-Shaer, and Q. Duan, "Openflow random host mutation: Transparent moving target defense using software defined networking," in *Proceedings of the First Workshop on Hot Topics in Software Defined Networks*. New York, NY, USA: ACM, 2012.

[12] P. Marques, N. Sheth, R. Raszuk, B. Greene, J. Mauch, and D. McPherson, "Dissemination of Flow Specification Rules," RFC 5575 (Proposed Standard), Internet Engineering Task Force, Aug. 2009.

[13] T. Bates, R. Chandra, D. Katz, and Y. Rekhter, "Multiprotocol Extensions for BGP-4," RFC 4760 (Draft Standard), Internet Engineering Task Force, Jan. 2007.