SURVEY ON MITIGATION AND RESPONSE OF NETWORK ATTACKS

CASED

da/sec
BIOMETRICS AND INTERNET-SECURITY
RESEARCH GROUP
http://www.dasec.h-da.de/

Welcome to the survey on mitigation and response of network attacks. Network-based attacks pose a strong threat to the Internet landscape. In my PhD I am investigating different approaches on attack mitigation and response. Yet, a clear understanding of how mitigation and response is performed in commercial networks is missing. Hence, this survey aims at gaining insight in real-world processes, structures and capabilities of IT companies and the computer networks they run. This survey is conducted in context of different publicly funded research projects.

Results of this survey shall frame future research and community activities in the area of Internet security.

This survey targets all organizations that manage their own network. Questions within this survey address some organizational aspects, as well as processes, techniques and tools you may have employed in order to perform automatic attack mitigation and response. Filling the survey should not last longer than 10 minutes. Hence, the survey can ideally be answered during a short and relaxing coffee break.

The survey is completely anonymous. We will not require you to enter any personally identifiable information, neither will log IP addresses with your responses.

Thank you very much for taking your time to support our work!

There are 52 questions in this survey

Company and personal information

The following questions will ask some general questions regarding your company and your role within your company. Answering these questions allows us to draw more fine-grained conclusions on the survey.

Questions marked with asterisk (*) are required.

1. **How familiar are you with your organization's mitigation and response activities? ***

   Please choose **only one** of the following:

   ○ Very familiar
   ○ Familiar
   ○ Somewhat familiar
   ○ Not familiar

2. **Are you involved in your organization's mitigation and response activities? ***

   Please choose **only one** of the following:

   ○ Significant involvement
   ○ Some involvement
   ○ No involvement

3. **How would you classify your organization? ***

   Please choose **only one** of the following:

   ○ Tier 2/3 Service Provider
   ○ Tier 1 Service Provider
   ○ Enterprise
   ○ Hosting/Data Center/Colocation Services Provider
   ○ Managed Service Provider
   ○ Educational/Research Institute
   ○ Government
   ○ Cloud Services Provider
   ○ DNS Registrar / DNS Service Provider
   ○ CDN/Content Delivery
   ○ National Research and Education Network Provider
   ○ Other

4. Where is your company headquartered? *

Please choose **only one** of the following:

○ Africa
○ Asia
○ Australia / Oceania
○ Europe
○ North America
○ South America

5. What organizational level best describes your current position? *

Please choose **only one** of the following:

○ Network operator or engineer
○ Security operator or engineer
○ Data protection officer / Information security officer
○ Other

6. How many years of relevant experience do you have? *

Please write your answer(s) here:

Total years of IT or security experience □

Total years in current position □

7. Please give an estimate of the average traffic rate transported over your organization’s network border routers. *

Please choose **only one** of the following:

○ < 1 Gbit/s
○ 1 - 5 Gbit/s
○ 6 - 10 Gbit/s
○ 11 - 50 Gbit/s
○ 51 - 100 Gbit/s
○ > 100 Gbit/s

8. Does your organization have the possibility to reconfigure access routers/border routers? *

Please choose **only one** of the following:

○ Yes
○ No

Processes and involved third parties

9. Is your organization target of DDoS attacks *

Please choose **only one** of the following:

○ Yes
○ No

10. Please estimate the number of attacks targeting your organization's infrastructure per month on average?*

Only answer this question if the following conditions are met: ((Q9 == YES))
Please choose **only one** of the following:

○ 1 - 2 attacks
○ 3 – 5 attacks
○ 6 – 10 attacks
○ 11 – 20 attacks
○ > 20 attacks

11. Please estimate the number of minutes it takes to initially mitigate an ongoing DDoS attack on average. *

Only answer this question if the following conditions are met: ((Q9 == YES))
Please choose **only one** of the following:

○ <15 minutes
○ 15 – 30 minutes
○ 31 – 60 minutes
○ 61 – 120 minutes
○ > 120 minutes

12. Please estimate the number of hours/days to completely resolve DDoS attacks on average. *

Only answer this question if the following conditions are met: ((Q9 == YES))
Please choose **only one** of the following:

○ <12 hours
○ 13 – 24 hours
○ 1 – 5 days
○ 6 – 10 days
○ 11 – 20 days
○ > 20 days

13. **Does your organization have a cooperation with a third party (e.g. ISP, network protection service) that can assist your organization in mitigating and responding to a security event/incident? ***

Please choose **only one** of the following:

○ Yes
○ No
○ Unsure

14. **What best describes this third party? ***

Only answer this question if the following conditions are met: ((Q13 == YES))
Please choose **all** that apply:

□ Consulting firm
□ Forensic firm
□ Risk management firm
□ Law firm
□ ISP
□ Packet cleaning house (e.g. Cloudflare)
□ Other:

15. **What best describes how this third party is utilized by your organization? ***

Only answer this question if the following conditions are met: ((Q13 == YES))
Please choose **all** that apply:

□ First responder to security events
□ To augment the skill set of your CSIRT
□ To augment the capacity of your CSIRT during crisis situations
□ To aid our NOC team
□ Other:

16. **What functions or departments are involved in the security response process? ***

Please choose **all** that apply:

□ IT management
□ Executive management
□ Board of directors
□ Risk management

□ Office of general counsel/legal
□ Human resource
□ Other:

17. Do your organization's incident investigations result in the production of threat indicators, which are then used to defend the organization from future attacks? *

Please choose **only one** of the following:

○ Yes
○ No
○ Unsure

Automatic mitigation and response systems

18. **Please estimate the number of security breaches experienced by your organization within the past 12 months. ***

Please choose **only one** of the following:

○ < 1 security breach
○ 2 – 5 security breaches
○ 6 – 10 security breaches
○ > 10 security breaches

19. **Please estimate the number of security events/incidents reported by automated detection mechanisms per month on average. ***

Please choose **only one** of the following:

○ < 10 security events/incidents
○ 11 - 25 security events/incidents
○ 26 - 50 security events/incidents
○ 51 - 100 security events/incidents
○ 101 - 500 security events/incidents
○ > 500 security events/incidents

20. **How many security events/incidents reported by automated detection mechanisms (e.g. Intrusion detection systems, SIEM etc) per month on average are real security events and need to be handled? ***

Please choose **only one** of the following:

○ None
○ 1 – 10 % of the reported security events/incidents
○ 11 – 25 % of the reported security events/incidents
○ 26 – 50 % of the reported security events/incidents
○ 51 – 100 % of the reported security events/incidents

21. **Does your organization make use of mitigation and response tools that perform automatic mitigation and reaction steps to defend the organization's network? ***

Please choose **only one** of the following:

○ Yes
○ No
○ Unsure

22. **Please rate the following statement: The usage of an automatic mitigation and response tool would speed up my organization's mitigation and response capabilities? ***

Only answer this question if the following conditions are met: ((Q21== No))
Please choose **only one** of the following:

○ Strongly agree
○ Agree
○ Disagree
○ Strongly disagree

23. **Does your organization plan to make use of mitigation and response tools, which perform automatic mitigation and reaction steps to defend the organization's network in the future? ***

Only answer this question if the following conditions are met: ((Q21== No))
Please choose **only one** of the following:

○ Yes, we are planning to do it
○ We are looking into it
○ No, we will not make use of it
○ I am not aware of it

24. What kind of actions would you and your organization like to use in an automatic mitigation and response tool? *

Only answer this question if the following conditions are met: ((Q21== No))
Please choose **all** that apply:

□ Rerouting traffic
□ Change blocking / filter capabilities (Blacklisting etc.)
□ Notification of involved functions or departments within the organization
□ Rate limiting at ingress
□ Exchange data with trusted partners
□ Quarantine machines
□ Changing the target's IP address
□ Other:

25. Which kind of automatic actions are performed with the aid of mitigation and response tools? *

Only answer this question if the following conditions are met: ((Q21== Yes))
Please choose **all** that apply:

□ Rerouting traffic
□ Change blocking / filter capabilities (Blacklisting etc.)
□ Notification of involved functions or departments within the organization
□ Rate limiting at ingress
□ Exchange data with trusted partners
□ Quarantine machines
□ Changing the target's IP address
□ Other:

26. Which type of mitigation and response tools does your organization use to perform automatic mitigation? *

Only answer this question if the following conditions are met: ((Q21== Yes))
Please choose **all** that apply:

□ Commercial product
□ Open source product
□ Self-built tools

27. Which commercial products/service does your organization employ to perform automatic mitigation? *

Only answer this question if the following conditions are met: ((Q26.Commercial Product == Yes))
Please choose **all** that apply:

□ Products from Arbor Networks
□ Products from Prolexic
□ Service from Cloudflare
□ Service from Incapsula
□ Other:

28. What best describes the reasons of your organization not to make use of an automatic mitigation and response tool? *

Only answer this question if the following conditions are met: ((Q21== No))
Please choose **all** that apply:

□ Commercial solutions are too expensive
□ Too high risks of false positives
□ No trust in open source solutions
□ No efficient support with open source solutions available
□ Other:

Data

29. Does your organization communicate with national CSIRTs ? *

Please choose **only one** of the following:

○ Yes
○ No

30. How does your organization communicate with national CSIRTs? *

Only answer this question if the following conditions are met: ((Q29== Yes))
Please choose **all** that apply:

□ Telephone
□ Email
□ Automated by mitigation and response systems
□ Other:

31. Does your organization make use of databases that provide vulnerability or threat information e.g. Common Vulnerabilities and Exposures (CVE), Shadowserver or RIPE.*

Please choose **all** that apply:

□ Yes, we ude CVE.
□ Yes, we use RIPE.
□ Yes, we use Shadowserver.
□ No, we do not make use of databases by external sources.
□ Other:

32. Does your organization perform traffic filtering based on IP blacklisting, whitelisting or greylisting? *

Please choose **only one** of the following:

○ Yes
○ No

33. What best describes the filtering approach your organization uses? *

Only answer this question if the following conditions are met: ((Q32== Yes))
Please choose **all** that apply:

□ Blacklists
□ Whitelists
□ Greylists
□ Other:

34. How frequently does your organization update black-, white- and greylists? *

Only answer this question if the following conditions are met: ((Q32== Yes))
Please choose **only one** of the following:

○ Once a day
○ More than once a day
○ 1 – 2 times a week
○ 3 – 5 times a week
○ Other:

35. Does your organization immediately include the changes at the black-, white- and greylist during an update process? *

Only answer this question if the following conditions are met: ((Q32== Yes))
Please choose **only one** of the following:

○ Yes
○ No, we review the modifications first and then include important changes
○ Other:

36. From which third party does your organization use black-, white- and greylists? *

Only answer this question if the following conditions are met: ((Q32== Yes))
Please choose **all** that apply:

□ Spamhaus
□ Sadowserver
□ Spamcop
□ DNSWL
□ Other:

37. **Does your organization configure networking devices according to BCP 38 (RFC 2827 or RFC2267)? ***

Please choose **only one** of the following:

○ Yes
○ No

38. **Does your organization use CyBex (Cybersecurity Information Exchange Framework (X.1500)) or parts of this framework? ***

Please choose **only one** of the following:

○ Yes
○ No
○ Unsure

39. **Would your organization make use of a cloud-based detection and mitigation solution to perform attack detection & mitigation? ***

Please choose **only one** of the following:

○ Yes
○ No
○ Unsure

40. **What best describes the filtering approach your organization uses? ***

Only answer this question if the following conditions are met: ((Q39== No))
Please choose **all** that apply:

□ Impact unknown
□ Customer's privacy
□ Data should remain within organization
□ Success rate unknown
□ Other:

41. Does your organization make use of network configuration protocols? *

Please choose **only one** of the following:

○ Yes
○ No

42. Which of the following network configuration protocols are used by your organization? *

Only answer this question if the following conditions are met: ((Q41== Yes))
Please choose **all** that apply:

□ Netconf
□ SNMP
□ OpenFlow
□ Open vSwitch DB Management Protocol
□ Other:

43. Does your organization's infrastructure currently offer the technical ability to make use of OpenFlow (SDN)? *

Please choose **only one** of the following:

○ Yes
○ No

44. Does your organization plan to have the technical ability to make use of OpenFlow (SDN) in 3 years? *

Only answer this question if the following conditions are met: ((Q43== No))
Please choose **only one** of the following:

○ Yes, we are planning to do it
○ We are looking into it
○ No, we will not make use of it
○ I am not aware of it

45. Does your organization’s infrastructure currently offer the technical ability to support BGP FlowSpec?*

Please choose **only one** of the following:

○ Yes
○ No

46. Does your organization plan to have the technical ability to make use of BGP FlowSpecin 3 years? *

Only answer this question if the following conditions are met: ((Q45== No))
Please choose **only one** of the following:

○ Yes, we are planning to do it
○ We are looking into it
○ No, we will not make use of it
○ I am not aware of it

Exchange and Collaboration

47. Does your organization share threat indicators with the following entities? *

Please choose **all** that apply:

□ None
□ Various CERTS or CSIRTs
□ Law enforcement or other governmental entities
□ We receive information from sharing partners, but we do not share our information with them
□ We neither receive nor share any information
□ Other:

48. Please rate the following statement: Collaboration between trusted parties would improve mitigation and response capabilities *

Please choose **only one** of the following:

○ Strongly agree
○ Agree
○ Disagree
○ Strongly disagree

49. Does your organization share security events/incidents with the following entities? *

Please choose **all** that apply:

□ None
□ Various CERTS or CSIRTs
□ Law enforcement or other governmental entities
□ Industry peers
□ We receive information from sharing partners, but we do not share our information with them
□ We neither receive nor share any information
□ Other:

50. Does your organization use a trusted exchange approach to transmit security events/incidents? *

Please choose **only one** of the following:

○ Yes
○ No
○ Unsure

51. How well do you know the following data exchange protcols and formats? *

Please choose the appropriate response for each item:

	Do or did use	Known	Heard of	Unknown
x.cybex-beep	○	○	○	○
x.bybex-tp	○	○	○	○
x.eaa	○	○	○	○
x.evcert	○	○	○	○
SCAP	○	○	○	○
IDXP	○	○	○	○
IDMEF	○	○	○	○
IODEF	○	○	○	○
x-ARF	○	○	○	○
PFOC	○	○	○	○

52. Please rate the following statement: Security events/incidents that are shared with third parties for collaboration must be signed and encrypted? **

Please choose **only one** of the following:

○ Strongly agree
○ Agree
○ Disagree
○ Strongly disagree

Thank you for participating in this survey, we really appreciate the time you spent!

If you have any questions regarding this survey or our research projects or if you'd like to further support our projects, please feel free to get in touch with jessica.steinberger@h-da.de.

Please submit by 31.07.2014 – 00:00 your survey.

Thank you for completing this survey.