Why do Internet Devices Remain Vulnerable? A Survey with System Administrators

T. Bondar , H. Assal, **A. Abdou**
Carleton University, Canada

Introduction

- Long tail of vulnerable systems remain after a patch is issued.
- **A compromised system affects many, beyond owner!**
  - a compromise leaks a new data dimension --> user profiling.
  - attackers learn and improve as they compromise more devices
    - e.g., password reuse, and/or password-choosing habits.
  - For web, libraries means a vulnerability in any would have a ripple effect.
  - Compromised device can be used to damage other systems.

Related Work

- **Vulnerability notification effectiveness.**
  - Durumeric et al. [2] (2014): Heartbleed.
    - 13% remediation rate.
  - Li et al. [1] (2016): who to contact, email language, format.
    - 18% remediation rate (within 2 weeks).
  - Stock et al. [3] (2016): XSS vulnerabilities.
    - 10% remediation rate.
  - Zeng et al. [4] (2019): outdated ciphersuites/TLS.
    - 2-3% remediation rate (within 2 weeks).

Related Work

- **Factors affecting notification success.**
  - Ensuring delivery to the proper person/team:
    - not enough [2,5] (2014 and 2018).
  - Sender's reputation:
    - Cetin et al. [6] – unimportant (2016).
    - Stock et al. [5] – important (2018).
  - Notification method:
    - Stock et al. [5] -- social-media and phones not better than emails (2016).
    - Maass et al. [7] -- snail mail increased remediation by 42% (2021).
  - Providing a proof-of-concept of the vulnerability:
    - no significant improvement to remediation rates [8] (2017).

Related Work

- **Notification of compromised (vs. vulnerable) systems.**
  - Li et al. [9] (2016): notified *already hijacked* sites.
    - 50% remediation rate.
  - Vasek and Moore [10] (2012): malware-distributing websites.
    - 17% remediation rate.
  - Quarantining infected machines (e.g., ISP support).
    - 92% remediation rates for infected ISP machines [13].
    - 87% for end systems [14].

Related Work

- **Notification++: active engagement.**
  - Kührer et al. [15] (2014): active engagement with involved parties:
    - collaboration with security organizations.
    - creating technical advisories explaining how to remediate.
    - engaging with industry players (e.g., Cisco).
    - 90% remediation rate.

Next Step

- Why aren't notifications working?
  - We directly solicit the admins' input on the matter.

- Some of the previous literature surveyed [2], [1], [8], [5], [4] (or interviewed [13]) admins.
  - Surveys solicit input/feedback on research methodology
    - not designed to answer the main question.

Research Questions

RQ1. *what admins think are the main factors that prevent them from remediating a vulnerability?*

RQ2. *how such factors change with variables such as, severity, company size, administrator's team size?*

Study Design and Methodology

- Participant Recruitment.
  - Surveyed admins who have a known vulnerability in their systems
    - their input is more relevant to us at this stage.
  - Focused specifically on software vulnerabilities.

Study Design and Methodology

- Randomly chose 9 vulnerabilities from past 8 years.
  - Various severity levels.
  - Patches were available between 4 days (POODLE) and 47 days (Exim) from when the vuln. was made public.

Vulnerability	AKA	Severity
CVE-2019-6111	OpenSSH	5.9 (M)
CVE-2014-3566	POODLE	3.4 (L)
CVE-2018-3110	Java VM	9.9 (C)
CVE-2014-0160	Heartbleed	7.5 (H)
CVE-2019-15846	Exim vuln	9.8 (C)
CVE-2020-6287	SAP NetWeaver	10 (C)
CVE-2018-16845	Nginx	6.1 (M)
CVE-2017-3169	Apache vuln	9.8 (C)
CVE-2018-15599	Dropbear	5.3 (M)

Severity levels: C – Critical, H – High, M – Medium, L – Low.

Study Design and Methodology

- For each vulnerability:
  - used Censys to find devices running the specific vulnerable software version.

Vulnerability	AKA	Severity	#vuln devices
CVE-2019-6111	OpenSSH	5.9 (M)	671
CVE-2014-3566	POODLE	3.4 (L)	91,413
CVE-2018-3110	Java VM	9.9 (C)	1,382
CVE-2014-0160	Heartbleed	7.5 (H)	64,187
CVE-2019-15846	Exim vuln	9.8 (C)	618,866
CVE-2020-6287	SAP NetWeaver	10 (C)	9,684
CVE-2018-16845	Nginx	6.1 (M)	24,045
CVE-2017-3169	Apache vuln	9.8 (C)	1,048,405
CVE-2018-15599	Dropbear	5.3 (M)	2,040,824

Severity levels: C – Critical, H – High, M – Medium, L – Low.

Study Design and Methodology

- For each IP address:
  - queried the RIRs WHOIS databases for contact information
    - prioritizing abuse contact if found, and falling back to regular email contact otherwise.

Vulnerability	AKA	Severity	#vuln devices	#emails found in WHOIS
CVE-2019-6111	OpenSSH	5.9 (M)	671	587
CVE-2014-3566	POODLE	3.4 (L)	91,413	38,900
CVE-2018-3110	Java VM	9.9 (C)	1,382	1,047
CVE-2014-0160	Heartbleed	7.5 (H)	64,187	37,824
CVE-2019-15846	Exim vuln	9.8 (C)	618,866	401,722
CVE-2020-6287	SAP NetWeaver	10 (C)	9,684	2,574
CVE-2018-16845	Nginx	6.1 (M)	24,045	7,509
CVE-2017-3169	Apache vuln	9.8 (C)	1,048,405	440,305
CVE-2018-15599	Dropbear	5.3 (M)	2,040,824	668,513

Severity levels: C – Critical, H – High, M – Medium, L – Low.

Study Design and Methodology

- For each email address:
  - Remove redundant ones (keep unique).

Vulnerability	AKA	Severity	#vuln devices	#emails found in WHOIS	#unique emails
CVE-2019-6111	OpenSSH	5.9 (M)	671	587	117
CVE-2014-3566	POODLE	3.4 (L)	91,413	38,900	2,739
CVE-2018-3110	Java VM	9.9 (C)	1,382	1,047	89
CVE-2014-0160	Heartbleed	7.5 (H)	64,187	37,824	1,802
CVE-2019-15846	Exim vuln	9.8 (C)	618,866	401,722	1,835
CVE-2020-6287	SAP NetWeaver	10 (C)	9,684	2,574	262
CVE-2018-16845	Nginx	6.1 (M)	24,045	7,509	147
CVE-2017-3169	Apache vuln	9.8 (C)	1,048,405	440,305	4,143
CVE-2018-15599	Dropbear	5.3 (M)	2,040,824	668,513	1,464

Severity levels: C – Critical, H – High, M – Medium, L – Low.

Study Design and Methodology

- We do not test whether vulnerable systems were remediated after emailing admins.

Ethical Considerations

- Emphasize that participation is voluntary.
- Transparency about our activities.
  - web page explaining who we are, what we do, how we can be contacted.
    - on the same domain from which emails were sent.
- Opt-out option, e.g., from future studies, both in our email and in the web page.
- Limited the emails sent to each email address to one to avoid spamming.

Data Set

- Sent 13,191 emails. Received 92 responses.
- Discarded responses from 3 participants who selected *"I prefer not to answer"* for more than 90% of the questions.

Vulnerability	AKA	Severity	#vuln devices	#emails found in WHOIS	#unique emails	#participants (%)
CVE-2019-6111	OpenSSH	5.9 (M)	671	587	117	-
CVE-2014-3566	POODLE	3.4 (L)	91,413	38,900	2,739	4.5 ($n = 4$)
CVE-2018-3110	Java VM	9.9 (C)	1,382	1,047	89	-
CVE-2014-0160	Heartbleed	7.5 (H)	64,187	37,824	1,802	2.2 ($n = 2$)
CVE-2019-15846	Exim vuln	9.8 (C)	618,866	401,722	1,835	30.3 ($n = 27$)
CVE-2020-6287	SAP NetWeaver	10 (C)	9,684	2,574	262	2.2 ($n = 2$)
CVE-2018-16845	Nginx	6.1 (M)	24,045	7,509	147	2.2 ($n = 2$)
CVE-2017-3169	Apache vuln	9.8 (C)	1,048,405	440,305	4,143	50.6 ($n = 45$)
CVE-2018-15599	Dropbear	5.3 (M)	2,040,824	668,513	1,464	4.5 ($n = 4$)
	n/a					3.4 ($n = 3$)

Severity levels: C - Critical, H - High, M - Medium, L - Low.

IP Geolocation Lookup

Country	N	Country	N
United States	34	Japan	1
Canada	16	Netherlands	1
Australia	12	Norway	1
Austria	3	Philippines	1
France	2	Romania	1
United Kingdom	2	Switzerland	1
Belgium	1	Thailand	1
Germany	1	Turkey	1
India	1	Uzbekistan	1

Analysis Methodology

- Quantitative analysis
- Qualitative analysis
  - Within survey responses.
  - From email replies.
  - Thematic analysis.
    - Open coding
      - e.g., looked at participants' reasoning to remediate or forgo remediation, additional remediation barriers, remediation plans.

The Survey

- [..]
- What is the size of your organization?
- How many people are involved in addressing issues related to the Host's security/privacy vulnerabilities?
- [..]

Participant Demographics

Criteria	Percentage (%)
Size of organization	
At most 500 employees	61.8
501 to 5000 employees	20.2
5001+ employees	6.7
Prefer not to answer	11.2
Size of The Remediation Team	
Just me	23.6
2 to 10 people	64.0
11 to 20 people	4.5
21+	3.4
Prefer not to answer	4.5

The Survey

- [..]
- Were you previously aware of the vulnerability we detected?
- Have you already remediated, or previously attempted to remediate, the vulnerability we detected?
- If you have not, do you plan to remediate the vulnerability we detected?
- [..]

Results

Criteria	Percentage (%)
Aware $(n = 89)$	
Yes	46% $(n = 41)$
No	51% $(n = 45)$
Prefer not to answer	3% $(n = 3)$
Remediated $(n = 89)$	
Yes	45% $(n = 40)$
No	51% $(n = 45)$
Prefer not to answer	4% $(n = 4)$
Plan to remediate $(n = 45)$	
Yes	67% $(n = 30)$
No	27% $(n = 12)$
Prefer not to answer	6% $(n = 3)$

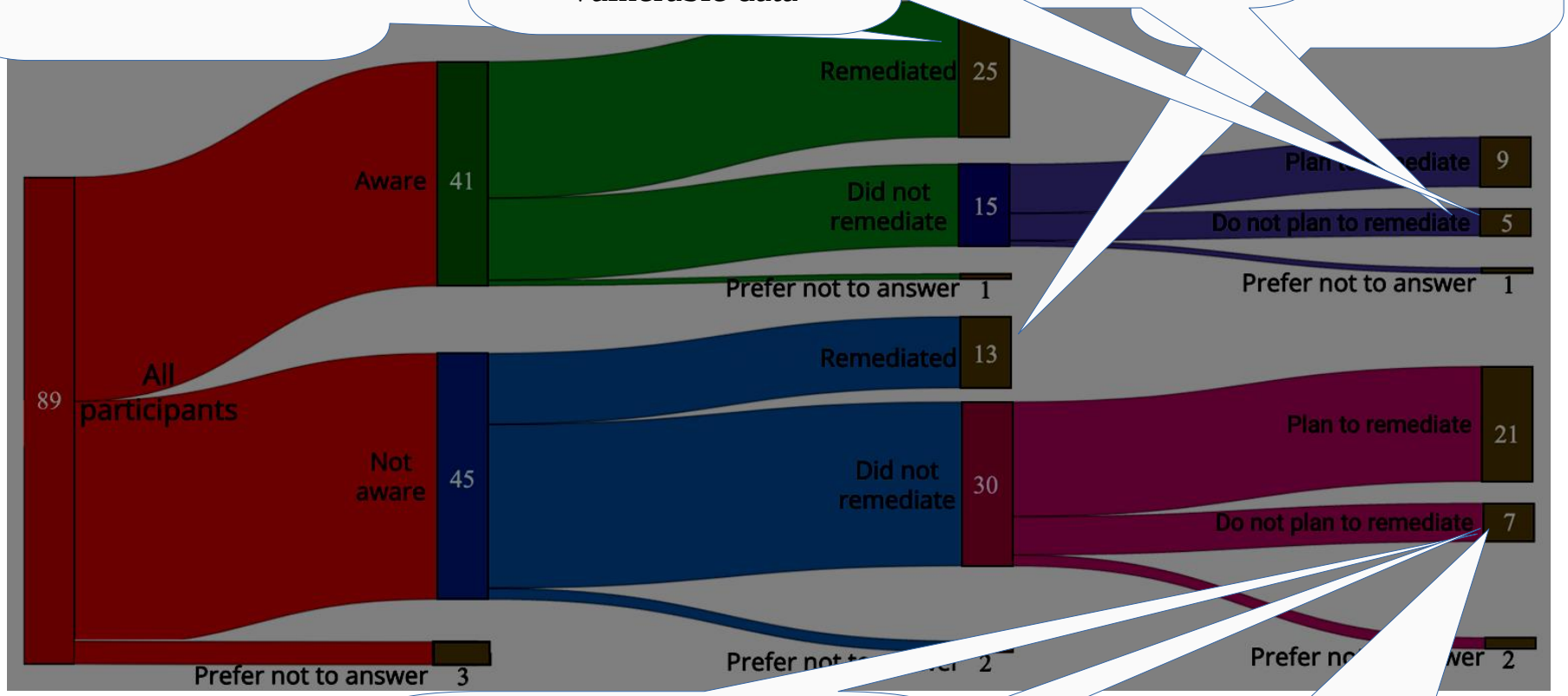
Results: Quantitative Analysis

Some are FPs

the server acts as a honeypot and does not include vulnerable data

Some other FPs

ed by the time
d the survey



the vulnerable server is old

its shutdown is planned

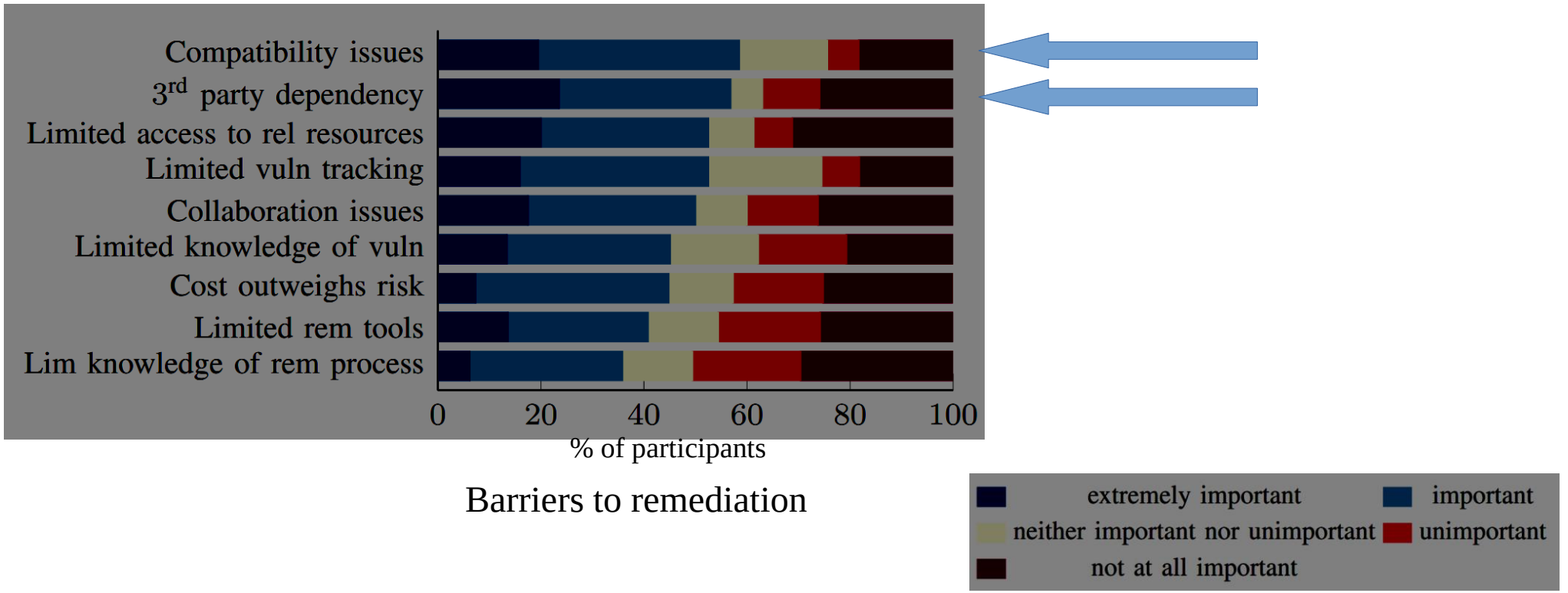
"no one is interested in fixing unused systems on that server"

Results: Quantitative Analysis

- No statistically significant association between awareness and vulnerability remediation response.

The Survey

- Cost of remediation outweighs risk
- Limited knowledge of vulnerability
- Limited knowledge of remediation process
- Issues impending the collaboration between The Remediation Team and other stakeholders
- Limited remediation tools
- Limited vulnerability tracking tools
- Third-party dependencies (e.g. hosting provider, certificate authority)
- Compatibility issues (e.g. backwards compatibility, legacy code, new libraries)
- Limited access to relevant resources that are not controlled by the Remediation Team (e.g. data, tools)



Barriers to remediation

Results: Quantitative Analysis

- We found:
  - statistically significant difference in the importance of different factors for participants.

  - ***Limited knowledge of remediation*** *process* was significantly less important than ***Compatibility issues.***

Results: Quantitative Analysis

- Dividing participants into two groups:
  - those who remediated
  - those who did not
- ... we found a significant difference between factors in both groups
- More data is needed to identify the most important factors for each group.
  - From post-hoc analysis.

Results: Quantitative Analysis

- Influential parameters for: awareness, remediation, remediation barriers
  - Organization size.
    - LEs more likely **aware** of vulnerability vs SMEs.
  - Vuln. Severity.
    - vulnerabilities with L-M severity levels more likely to have negative **remediation** response.
    - For the H-C group, Compatibility issues significantly more important than Limited knowledge of **remediation** process.
  - Size of admin team.
    - *"Issues impeding the collaboration within the remediation team or with other stakeholders"* was more important for bigger teams.

Results: Qualitative Analysis

- We identified 6 themes from open-ended responses
  - Lack of control over the vulnerable system.
  - Politics.
  - Benefit does not outweigh the cost.
  - Limited resources.
  - Complex remediation processes.
  - Legacy systems.

Results: Qualitative Analysis

- We identified 6 themes from open-ended responses
  - Lack of control over the vulnerable system.
    - *"[..] once we notify the responsible party of the vulnerability we allow 24 hours to remediate before traffic to the affected IP address will be blocked until remediation is completed."*
  - Politics.
  - Benefit does not outweigh the cost.
  - Limited resources.
  - Complex remediation processes.
  - Legacy systems.

Results: Qualitative Analysis

- We identified 6 themes from open-ended responses
  - Lack of control over the vulnerable system.
  - Politics.
    - having to go through bureaucratic processes with other departments
    - having to convince management and other stakeholders of the importance of remediating vulnerabilities.
    - *"Political/Business Infrastructure supportive of time and personnel [is an] extremely important [factor]"*.
  - Benefit does not outweigh the cost.
  - Limited resources.
  - Complex remediation processes.
  - Legacy systems.

Results: Qualitative Analysis

- We identified 6 themes from open-ended responses
  - Lack of control over the vulnerable system.
  - Politics.
  - Benefit does not outweigh the cost.
    - the impact of the remediation process on existing services (e.g., downtime).
    - the perceived risk and expected losses from a vulnerability exploitation.
    - their plans to decommission old vulnerable servers.
  - Limited resources.
  - Complex remediation processes.
  - Legacy systems.

Results: Qualitative Analysis

- We identified 6 themes from open-ended responses
  - Lack of control over the vulnerable system.
  - Politics.
  - Benefit does not outweigh the cost.
  - Limited resources.
    - lack of time to keep servers updated. lack of personnel. unavailability of vendor patches. lack of documentation from previous admins
      - *“I am the network administrator. The administrator of this system recently died. I was not completely aware that this server had a public network exposure [...]”.*
  - Complex remediation processes.
  - Legacy systems.

Conclusion: RQ1

- No one-size fits all solution.
  - no evidence that awareness of the existence of a vulnerability affects remediation plans
    - Demystifies results in previous literature.

Conclusion: RQ2

- Compatibility issues were more important than limited knowledge of remediation process.
- For L-M severity, we found that participants are more likely to have negative response to remediation.
- For company sizes
  - the importance of factors **does not** change with company size.
  - LEs are more likely to be aware than SMEs.
- Other factors that influence remediation decisions include politics, benefit vs cost, limited resources, and the maintenance of legacy systems.

Thank You!

References

1F. Li, Z. Durumeric, J. Czyz, M. Karami, M. Bailey, D. McCoy, S. Savage, and V. Paxson, “You’ve got vulnerability: Exploring effective vulnerability notifications,” in USENIX Security Symposium, 2016.

2Z. Durumeric, F. Li, J. Kasten, J. Amann, J. Beekman, M. Payer, N. Weaver, D. Adrian, V. Paxson, M. Bailey et al., “The matter of heartbleed,” in ACM Internet Measurement Conference (IMC), 2014.

3B. Stock, G. Pellegrino, C. Rossow, M. Johns, and M. Backes, “Hey, you have a problem: On the feasibility of large-scale web vulnerability notification,” in USENIX Security Symposium, 2016.

4E. Zeng, F. Li, E. Stark, A. P. Felt, and P. Tabriz, “Fixing HTTPS misconfigurations at scale: An experiment with security notifications,” in Workshop on the Economics of Information Security (WEIS), 2019.

5B. Stock, G. Pellegrino, F. Li, M. Backes, and C. Rossow, “Didn’t you hear me?–Towards more successful Web vulnerability notifications,” in Network and Distributed System Security (NDSS), 2018

6O. Cetin, M. Hanif Jhaveri, C. Gañán, M. van Eeten, and T. Moore, “Understanding the role of sender reputation in abuse reporting and cleanup,” Journal of Cybersecurity, vol. 2, no. 1, pp. 83–98, 2016.

7M. Maass, M.-P. Clement, and M. Hollick, “Snail Mail Beats Email Any Day: On Effective Operator Security Notifications in the Internet,” in Conference on Availability, Reliability and Security (ARES), 2021.

8O. Cetin, C. Ganan, M. Korczynski, and M. van Eeten, “Make notifications great again: learning how to notify in the age of large-scale vulnerability scanning,” in Workshop on the Economics of Information Security (WEIS), 2017.

References

9F. Li, G. Ho, E. Kuan, Y. Niu, L. Ballard, K. Thomas, E. Bursztein, and V. Paxson, “Remedying web hijacking: Notification effectiveness and webmaster comprehension,” in Conference on World Wide Web (WWW), 2016.

10M. Vasek and T. Moore, “Do Malware Reports Expedite Cleanup? An Experimental Study,” in USENIX Workshop on Cyber Security Experimentation and Test (CSET), 2012.

11D. W. Woods and R. Böhme, “SoK: Quantifying cyber risk,” in IEEE Symposium on Security and Privacy (S&P), 2021.

12M. Vasek, M. Weeden, and T. Moore, “Measuring the impact of sharing abuse data with web hosting providers,” in ACM Workshop on Information Sharing and Collaborative Security (WISCS), 2016.

13O. Cetin, C. Ganan, L. Altena, T. Kasama, D. Inoue, K. Tamiya, Y. Tie, K. Yoshioka, and M. van Eeten, “Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai,” in Network and Distributed System Security (NDSS), 2019.

14O. Cetin, C. Ganan, L. Altena, S. Tajalizadehkhoob, and M. Van Eeten, “Tell Me You Fixed It: Evaluating Vulnerability Notifications via Quarantine Networks,” in IEEE European Symposium on Security and Privacy (EuroS&P), 2019.

15M. Kührer, T. Hupperich, C. Rossow, and T. Holz, “Exit from hell? Reducing the impact of amplification DDoS attacks,” in USENIX Security Symposium, 2014.