SCIENCE CHINA
Information Sciences

• LETTER •

July 2022, Vol. 65 179105:1–179105:3
https://doi.org/10.1007/s11432-019-2774-4

Malware incident response (IR) informed by cyber threat intelligence (CTI)

Ying HE[1], Ellis INGLUT[1] & Cunjin LUO[2,3,4*]

[1]*School of Computer Science and Informatics, De Montfort University, Leicester* LE1 9BH, *UK;*
[2]*Key Lab of Medical Electrophysiology, Ministry of Education, Luzhou* 646000, *China;*
[3]*The Health Informatics Group, Institute of Cardiovascular Research, Southwest Medical University, Luzhou* 646000, *China;*
[4]*School of Computer Science and Engineering, Northeastern University, Shenyang* 110004, *China*

Received 10 June 2019/Revised 25 December 2019/Accepted 20 January 2020/Published online 5 August 2021

Citation He Y, Inglut E, Luo C J. Malware incident response (IR) informed by cyber threat intelligence (CTI). Sci China Inf Sci, 2022, 65(7): 179105, https://doi.org/10.1007/s11432-019-2774-4

Dear editor,

Security experts have been fighting against cybercriminals for many years and existing research shows that this battle will continue. Malicious software has no remorse when it targets different organizations, regardless of its forms [1]. Ransomware [2] has caused serious issues in different industries, especially in healthcare. The existing report shows that 34% of ransomware is targeting healthcare organizations. Nowadays, criminals prefer crypto-jacking over ransomware (which also relies on cryptocurrency for anonymous ransom payments). Healthcare organizations are favoured by the crypto-jackers, because they have critical systems to provide medical services within their medical infrastructure. Healthcare organizations infected with crypto-jacking malware will suffer the impact of system performance degradation. Lives will be jeopardised if healthcare systems fail to perform as expected. It is imperative to counteract the crypto-jacking attack, especially in healthcare.

Cyber threat intelligence (CTI) such as security advisories from the US/UK computer emergency response team (CERT) contains knowledge including roots causes, affected assets, and course of actions and should be ideally applied to inform security incident response (IR). The UK government sets up the National Cyber Security Strategy 2016–2021, investing £1.9 billion to develop security solutions to defend against emerging threats. It focuses on "proactive defense", which requires proactive threat response. A proactive security defense approach relies on the CTI as a consultative practice, is dedicated to achieving continuous improvement of cyber security through the construction of processes, people, and technology [3].

However, current studies show that the IR has not been effectively informed by CTI, especially in the area of Malware IR. This study fills in this gap by proposing a Malware IR methodology based on the National Institute of Standards and Technology (NIST) IR methodology [4]. Through embedding CTI into the Malware IR lifecycle, organizations can benefit from an informed IR with the CTI advisories from US/UK CERT. This study then presents a crypto-jacking case study to demonstrate the use of the proposed Malware IR lifecycle.

Our solution. We propose the novel IR methodology for malware incident response, by mapping the NIST IR methodology [4] to the extracted CTI best practices from US CERT [5, 6]. Organizations should be able to adopt this methodology and apply it to their IR processes in order to enhance the security of their systems against malware. Figure 1 shows an overview of our proposed Malware IR lifecycle with actions in different stages of IR.

Preparation. The organizations should prepare the main actions to defend against malware [4]. These include communication facilities, hardware and software, resources, incident mitigation, security plans for securing networks, systems and applications (see Table S1). An extension of the security plan includes risk assessment, host -based security, network-based security, malware prevention, as well as user awareness training (see Table S2).

Detection and analysis. The organizations identify the common sources from which the malware precursors and indicators are collected. Those include the antivirus and antispam software, intrusion detection prevention system (IDPS), file integrity checking software, operating system, services and network logs, network flows, application logs, information on emerging vulnerabilities and exploits, people inside and outside of the organization (see Table S3). The main security recommendations include profiling systems, understanding system normal behaviours, performing event correlation, creating a log retention policy, keeping all clocks synchronised, maintaining a knowledge base, applying internet search engines, and seeking assistance from both internal and external sources (see Table S4).

Containment, eradication and recovery. Most incidents need to be contained before eradication and recovery as containment can reduce the damage caused to the main business processes. However, containment may also cause issues [4].

* Corresponding author (email: cunjin.luo@yahoo.co.uk)

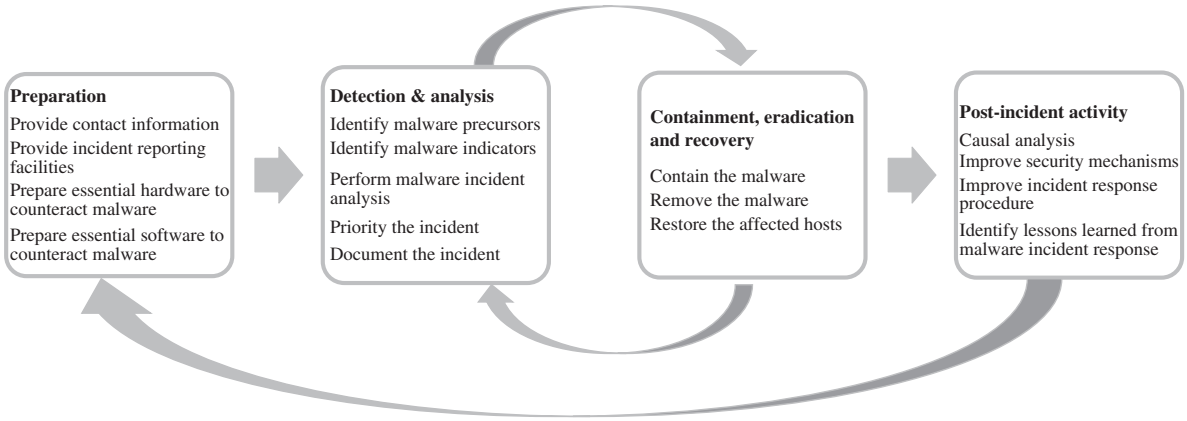

Figure 1 Malware incident response lifecycle.

Delayed eradication and recovery are risky as the malware can infect other parts of the healthcare system. It may also escalate its privileges during this period. In the eradication stage, organizations need to identify all the victim hosts so that these hosts can be remedied. To counteract malware, the eradication step cannot be skipped [6]. In the recovery stage, the security analyst will take actions to restore systems and verify that these system functions properly. Clean versions of disks are needed to restore and rebuild the system. Other actions include the replacement of comprised files with clean versions, patch installation, change of passwords, as well as switching to high level logging and monitoring [6].

Post-incident activity. In this stage, the organizations learned lessons from the IR process. Questions should be asked around, what has happened, and when it has happened; how well the staff and management team react to the incident; whether the procedures have been followed, and whether they were adequately followed; whether there were any tasks carried out that could affect the recovery; what could the team perform better next time to counteract similar incidents; how could information and lessons be shared effectively with other organizations; what actions need to be taken to prevent similar incidents; what indicators or precursors should be collected and monitored in the long term; what other resources are required in order to identify and mitigate malware attacks in the future [5].

Case study. We used a crypto-jacking case study to demonstrate the use of the Malware IR lifecycle. We collate cyber security best practices to protect healthcare systems from being compromised by crypto-jacking malware. The best practices are extracted from the crypto-jacking CTI advisories [6, 7] taken from US CERT.

Crypto-jacking preparation. The organizations need to prepare main actions to defend against Crypto-jacking. These include the contact information, issue tracking systems, additional workstations, digital forensic software, port listings, IT infrastructure diagrams and profiling of critical assets, lean copies of operating systems and application installations as well as current baselines (see Table S5).

Crypto-jacking detection and prevention. The organizations need to identify the attack vectors and precursors for crypto-jacking. The common sources where the malware precursors and indicators are collected include the antivirus and anti-spam software, blacklist for websites that include malicious JavaScript, network monitoring, web server monitoring, and help desk monitoring and performance management system (see Table S6). The main security recommendations in this stage are keeping the software and operating systems up to date, enforcing appropriate privilege policies, applying application whitelisting, avoiding downloading files from untrusted websites, understanding normal CPU behaviours and looking for abnormal activity, disabling unnecessary services, uninstalling unused software, validating input and installing a firewall (see Table S7).

Crypto-jacking containment, eradication and recovery. There are limited containment solutions for crypto-jacking malware. This is owing to the aggressive nature of the crypto-jacking that can affect organizations' systems in a very short time. When the organizations identify a crypto-jacking malware, the best way of containment would be to cut off its communication with the hosts in the organization. Crypt-jacking malware can propagate very fast within an organization through its network paths [7]. In the eradication stage, the organizations usually adopt the same techniques applied to all the other types of malware [6, 7]. The affected hosts, systems and networks should be identified and isolated. The crypto-jacking malware should be removed. The organizations should also temporarily disable all the users connected to the infected hosts. In the recovery stage, it is also necessary to carry out generic malware recovery solutions. The infected devices and hosts are required to be recovered back to normal.

Crypto-jacking post-incident activity. The organization should spend time to follow up the malware attack. This is to learn from this incident [6, 8]. They should reflect on how the attack happened, and whether the detection mechanisms used were adequate. They need to feed these lessons learned back to the preparation stage and implement additional detection mechanisms if needed.

Conclusion. This study proposed a Malware IR lifecycle that is embedded with CTI. We examined different stages of the IR lifecycle and identified the points where CTI can be fed into the IR processes. We then presented a crypto-jacking case study to demonstrate the use of the Malware IR lifecycle. We walked through different stages and collated cybersecurity best practices in order to protect healthcare systems from crypto-jacking malware. These best practices are the CTI advisories from US CERT. The practitioners can use the proposed Malware IR lifecycle to counteract malware in a systematic manner. Future work will focus on applying the proposed Malware IR lifecycle in real practice in healthcare organizations. Future work will also consider integrating the Malware IR lifecycle with existing CTI products such

as security information and event management (SIEM), orchestration automation and response (SOAR) [3], and security operations center (SOC).

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 61803318).

Supporting information Tables S1–S7. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Zhang H G, Han W B, Lai X J, et al. Survey on cyberspace security. Sci China Inf Sci, 2015, 58: 110101
2 Kharaz A, Arshad S, Mulliner C, et al. Unveil: a large-scale, automated approach to detecting ransomware. In: Proceedings of the 25th USENIX Security Symposium, 2016. 757–772
3 Islam C, Babar M A, Nepal S. A multi-vocal review of security orchestration. ACM Comput Surv, 2019, 52: 1–45
4 Cichonski P, Millar T, Grance T, et al. Computer security incident handling guide. NIST Special Publ, 2012, 800: 1–147
5 CERT US. Malware threats and mitigation strategies. 2012. https://us-cert.cisa.gov/sites/default/files/publications/malware-threats-mitigation.pdf
6 CERT US. Best practices for continuity of operations (handling destructive malware). 2015. https://ics-cert.us-cert.gov/tips/ICS-TIP-15-022-01
7 CERT US. Security tip (st18-002) defending against illicit cryptocurrency mining activity. 2018. https://www.us-cert.gov/ncas/tips/ST13-003
8 Souppaya M, Scarfone K. Guide to malware incident prevention and handling for desktops and laptops. NIST Special Publ, 2013, 800: 83