SCIENCE CHINA
Information Sciences

• **Supplementary File** •

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, *United Kingdom;*
[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 Electronic Engineering, University of Essex, Colchester* CO4 3SQ, *United Kingdom*

Table S1 listed the main actions the organizations should prepare in order to defend against malwares. Table S2 provides the malware related security recommendations on how to act upon them. Table S3 listed the common sources where the malware precursors and indicators are collected from. Table S4 listed the detection and analysis recommendations in regards to malware incidents.

Table S1 Malware IR Lifecycle - Preparation [1, 2]

Preparation	Action
Communication & Facilities	Contact information; on and off hour contact information; on-call contact information; incident reporting mechanism; issue tracking system; encryption software; war room; and secure storage facility
Hardware & Software	Digital workstation; laptops; packet sniffers and protocol analysers; digital forensic software; additional workstations, servers, and networking equipment (or virtualised equivalents)
Resources	Port listings; network diagrams and listings of critical assets; current baselines
Incident Mitigation	Clean images of operating systems and application installations
Security Plans	Risk assessment; host security; network security; malware prevention; user awareness and training

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

Table S2 Malware IR Lifecycle - Preparation - Recommendation

Security Plans	Recommended Practices
Risk Assessment	Risk assessment determines the risks associated with each asset (e.g., system, network, application etc.) through assessing both the threats and vulnerabilities within the organization [3,4]. Each-specific threat should be prioritised based on its risk levels, which is to be mitigated, transferred, or accepted until the level of risk is acceptable.
Host Security	Host security includes standard configuration should be used when hardening hosts. This includes patches of hosts to be maintained and updated appropriately. organizations should configure hosts by following the principle of least privileged, granting users with the privileges that are only relevant to their operation [5, 6]. This can prevent the malware from spreading internally through the users [7]. Auditing [5] should be enabled, and security related events logged, for which organization should continuously monitor the hosts security and configuration. Some malwares are developed to alter security and configuration to avoid authentication and escalate privileges.
Network Security	Network security within network parameters should be configured to deny activities that are not expressively permitted [5,6], for example Virtual Private networks (VPN) and dedicated connections to other organizations [8].
Malware Prevention	Malware detection software should be implemented at every level within the organization [9, 10]. Malware protection should be deployed at application client level (e.g., instant messaging, email clients), the applications server level (e.g., web proxies, email server) and host level (e.g., workstation operating systems and server) [1,11].
User Awareness and Training	User training and awareness should be implemented to ensure that users are aware of policies and procedures regarding appropriate use of networks, systems, and applications. Individuals should apply lessons learns from previous malware incidents, and share it with other users to show how their action can affect the organization. The number of malware related incidents can be reduced by improving awareness across the whole organization. Specifically, IT staff should be trained in maintaining networks, systems, and applications in accordance with the organizations security standards [1, 2].

Table S3 Malware IR Lifecycle - Sources of Precursors and Indicators

Source	Description
Antivirus and Antispam Software	Antivirus software generates alerts when detecting and preventing malware from infecting hosts [1, 5, 6]. Keeping signatures within the anti-virus software up to date can help prevent malware. Antispam software will create an alert if any spam is detected, preventing it from reaching the user' mailboxes. Spam is renowned for containing malware and other malicious content. Therefore, organizations should take any alerts from anti-spam software seriously as it could indicate potential attack attempts.
Intrusion Detection Prevention System (IDPS)	An IDPS [12] can be used to identify any suspicious events and record data in relation to them. These include the date and time in which the attack was detected, the form on attack, the source and destination IP address as well as the user name [5, 6]. The majority of IDPS tools work by identifying malicious activity through attack signatures. It it important to keep the signatures up to date so that the newest attacks can be detected. IDPS will produce a high volume of alerts daily, often producing false positives that indicate malicious activity. IDPS alerts need to be validated through crosschecking alters from other sources such as SIEM, SOC [13] internally and US/UK CERT [5, 6] externally.
File Integrity Checking Software	File integrity checking software should be used to detect any changes made to file names [5,6]. It will obtain a cryptographic checksum for each assigned file via the use of hashing algorithms. If the file is altered, the checksum will be recalculated to a new checksum and will signify a change. There is a chance that the recalculated checksum will remain the same and therefore cannot be identified, however probability of this is extremely low. The changes within files can be detected by regularly recalculating checksums and comparing them with previous values.
Operating Systems, Services and Application logs	An organization should check logs from the operating system, services and applications [1]. These logs may be of great value as they record which accounts were accessed and what actions where performed. All systems within the organization should have a required base line for logging, with an increased baseline level for more critical systems. These logs can then be analyses by correlating all event information. An alert can be generated depending on the event information issued and can be used as an indicator for an incident [5, 6].
Network Device Logs	Network device logs such as routers and firewalls are useful for the detecting precursors and indicators [5,6], though they are not typically used as a primary source. organizations should configure these devices to log any blocked connection attempts. However, these logs provide limited information regarding the nature of the activity. These network devices are able to identify network trends as well as be being used in event correlation with other devices [1].
Network Flows	When hosts commutate, they create numerous sessions, one in particular being a network flow [1, 5, 6]. This information can be provided by routers and other networking devices. It can be used to identify indicators cause from malware by finding anomalous network activities. There are standards for data flow formats including, NetFlow, sFlow, and APFIX.
New Vulnerabilities and Exploits	Keeping up to date with information on new vulnerabilities and exploits could prevent some incidents form occurring as well as assisting the detection and analysis of new attacks [5, 6]. The National Vulnerability Database (NVD) [14] contain information on vulnerabilities. organization such as US CERT and UK CERT periodically provide threat update information through briefings, web posting and emailing lists.
People Inside the organization	People from within the organization are to report any signs of an incident. They range from users, system administrators, network administrators, security staff, and any other people from within the organization who can report signs of an incident [1, 2]. organization should consider asking the staff who provide the incident related information how confident they are in regards to the information accuracy. The addition of this estimation alongside the information provided can help incident analysis, partially when conflicting data in discovered.
People Outside the organizations	An organization should take external malware incidents by people from other organizations seriously [1, 2]. For example, additional information about indicators may be known by these external parties such unavailable services and defaced web pages. organizations should implement a mechanism so that external parties can report incidents that trained member of staff can monitor. This could be done by setting an email address or phone number, configuring it to send messaged to the help desk.

Table S4 Malware IR Lifecycle - Detection and Analysis Recommendations

Recommendations	Description
Profile Systems	Profile systems can help to identify changes in a system, by measuring the characteristics of excepted activity. On a host, file integrity software could be used to derive checksums for critical files [1, 2]. Profiling should be used in conjunction with other detection techniques. Most profiling techniques have proven difficult when accurately detecting incidents.
Understand System Normal Behaviours	The IR team should be familiar with their networks, systems and applications. Understanding normal behaviours, makes it easier to recognise abnormalities that could be a result of a malware activities [5, 6]. The team can get a baseline knowledge of normal behaviours through reviewing log entries and security alerts. Filtering should be applied to condense the log to a reasonable size. To upstand the knowledge regarding their logs, conducting frequent reviews is a must, and should allow the analysts to notice trends and changes over time. Through these reviews, the analyst should get an indicator of the sources that are more reliable.
Create a Log Retention Policy	Malware incident are recorded in the IDPS, firewalls and application logs. The creation of a log retention policy should define the duration in which data will be maintained. These log entries can be helpful during the analysis of current attack as they provide previous reconnaissance activity or previous incidents of a similar attack. The organization's data retention policies and volume of data are some of the factors that determine the length of time that these logs will be maintained [1, 2].
Perform Event Correlation	There are numerous logs that can be used to capture incidents relating to malware, each of which containing different types of data [5, 6]. The malwares source IP could be contained within a firewall log; and users involved could be contained within an application log. Network IDPS could help identify the targeted host. The hosts logs can tell whether the attack has been successfull. Performing event correlation from multiple sources [15, 16] can help determine whether particular incidents occurred.
Keep All Clocks Synchronised	To keep all clocks synchronised among hosts, protocols such as Network Time Protocol (NTP) can be used. The synchronisation of clocks settings among devices will make event correlation much easier. Having consistent timestamps within logs is preferable when being used as evidence. For example, having numerous logs that show an attack happened at the exact same time, rather than minutes or hours apart [1, 2].
Maintain Knowledge Base	organizations should maintain a knowledge base so the incident handlers can reference quickly while analysing an incident. The knowledge base can be in the form of a simple databases, spreadsheets and text documents, all providing effective, flexible and researchable mechanisms for when a team member needs to share data [5, 6]. The content should include precursor and indicator significance and validity with an explanation of IDPS alerts, applications error codes and operating system entries.
Internet Search Engines	There are numerous sources on internet search engines [1, 2]that provide information regarding unusual activity as a result of malware. An analyst can identify the most common ports that attackers use when attempting to infect systems with malware.
Seek Assistance from Other Sources	The IR team may be unable to fully determine the cause and nature of a piece of malware. They should seek assistance by consulting internal resources (e.g. information security staff) and external sources (e.g., US-CERT [5, 6], other CSIRTs, contractors with IR expertise).

Table S5 listed the Preparation actions when defending against crypto-jacking. Table S6 listed the common sources where the malware precursors and indicators are collected from in regards to Crypto-jacking. Table S7 listed the detection and analysis recommendations in regards to Crypto-jacking.

Table S5 Crypto-jacking: Preparation [5, 6, 11]

Preparation List	Rationale
Contact Information	Unlike other malware incidents, the help desk team play an important role in the detection of crypto-jacking. Crypto-jacking causes lack in computing power, which means, if service-providing organization such as the NHS are infected, they will receive complaints from customers about the lack of performance. Help desk team will be trained to understand this could be an indicator of crypto-jacking and will therefore need all the necessary contact information.
On and Off Hour Contact	Crypto-jacking malware can be developed to only be active during off-hour time. Therefore, off hour communication is also required.
Ticket Tracking Systems	To log the malware investigation information, especially the lack in computing power to be further investigated
Additional Workstations	Unlike other malwares, crypto-jacking has the ability to physically damage devices due to the excessive computing power [11]. Therefore, organizations should consider purchasing additional workstations in case of a crypto-jacking attack.
Digital Forensic Tools	The organization will need forensic softwares and hardwares to analyse networks and systems for excessive resource use.
Port Listings	organizations should look into common attack vectors use by crypto-jackers that require the use of ports. The security of these ports should then be strengthened to prevent the attack vector.
Network Diagrams and Critical Assets List	This will allow the organization to identify the key assets that may be affected by crypto-jacking malware. With this information they can strengthen the system in a way that targets crypto-jacking [11] .
Current Baselines	The organization should understand the current baselines of their system and network in order to acknowledge an increase in resource usage. This is essential for critical systems as they are targeted by crypto-jacking malware more often.
Clean OS and Application Installations	As crypto-jacking malware can physically damage machines, organizations should have clean copies of operating systems and application installation in the case damaged machines need to be replaced and restored back to its current state.

Table S6 Crypto-jacking: Sources of Precursors and Indicators

Source	Description
Antivirus and Antispam Software	Anti-virus and anti-spam software allows the operator to detect and remove a potentially unwanted program before it can do any damage. For example, it can detect and prevent the malicious email from arriving at the victim's inbox in the first place.
Blacklist for Websites	organizations should incorporate publicly available blacklists for websites that include malicious JavaScript from CTI sources, so that they remain safer when browsing the internet.
Network Monitoring	An easy way of detecting crypto-jacking malware indicators is through network monitoring. Liliberete identified that networking perimeter monitoring that reviews all web traffic has a better chance of detecting crypto-miners [17]. The majority of network monitoring tools are able to specific exactly which machine has been infected through the use of abnormal spikes within the web traffic.
Web Server Monitoring	organization should also check for indicators within their frequently visited websites, monitoring for signs of crypto-jacking code and visual changes to the content [11]. organizations should not only check for indicators within their websites, but also the web-servers [17]. The analysts should look for the indicators within webserver and pages that can be identified by monitoring the content for abnormalities.
Help Desk Monitoring	For crypto-jacking malware, a spike in complaints about slow computer performance could be the first indicator that an infection has occurred [11]. The overheating of machines is common during crypto-jacking, and should therefore be used as an indicator of attack.
Performance Management System	Crypto-jacking developers have discovered a sophisticated way to bypass the detection by employees. This is by designing the malware to remain inactive during peak times (office hours), and to start crypto-mining as soon as business hours were over. The performance management system can raise the alarm by highlighting the fact that computer resources were being used during non-business hours [17].

Table S7 Crypto-jacking: Detection and Analysis Recommendations

Recommendations	Description
Keep Software and Operating Systems Up to Date	Make sure the software and operating systems are up to date. This can prevent the potential attackers from exploiting the known system weaknesses or vulnerabilities.
Enforce Appropriate Privilege Policies	Stop using default usernames and passwords and enforce strong password policy. Regularly review user accounts and verify that users have the right need for those privileges. Restrict general user accounts from performing administrative functions [18].
Whitelist Applications	Use application whitelisting to prevent nonauthorized applications from been executed automatically [19].
Avoid Downloading Files from Untrusted Websites	Avoid downloading files from untrusted websites [19]. An authentic website certificate needs to be verified when downloading files from a unfamiliar website.
Understand Normal CPU Behaviours	The IR team should continuously monitor systems and train their staff to recognise any abnormal CPU behaviours on computer systems, mobile devices, and network servers [18]. The team should be able to investigate noticeable degradation in computer performance.
Disable Unnecessary Services	The IR team should review all running services and disable those that are unnecessary for businesses. Disabling or blocking some services may create problems by obstructing access to files, data, or devices.
Uninstall Unused Software	Review installed software applications and remove those that are not needed for businesses. These unnecessary applications can provide opportunities for potential attackers to exploit a system.
Validate Inputs	Perform input validation on internet-facing web server and web applications to mitigate injection (e.g. Crypto-jacking) attacks. Disable JavaScript execution on web browsers. For Microsoft Internet Explorer, enable the cross-site scripting filter [11,17].
Install Firewalls	Firewall can be used to prevent certain types of attacks by blocking malicious traffic researching computer systems. It can also restrict unnecessary outbound communications. Also make sure the firewall is properly configured as specified in the manual.

References

1 Souppaya M, Scarfone K. Guide to malware incident prevention and handling for desktops and laptops. NIST Special Publication. 2013;800:83.
2 Cichonski P, Millar T, Grance T, Scarfone K. Computer security incident handling guide. NIST Special Publication. 2012;800(61):1–147.
3 Shameli-Sendi A, Aghababaei-Barzegar R, Cheriet M. Taxonomy of information security risk assessment (ISRA). Computers & Security. 2016;57:14–30.
4 Lopez D, Pastor O, Villalba LJG. Data model extension for security event notification with dynamic risk assessment purpose. Science China Information Sciences. 2013;56(11):1–9.
5 CERT US. Best Practices for Continuity of Operations (Handling Destructive Malware); 2015. Available from: https://ics-cert.us-cert.gov/tips/ICS-TIP-15-022-01.
6 CERT US. Security Tip (ST13-003) Handling Destructive Malware; 2016. Available from: https://www.us-cert.gov/ncas/tips/ST13-003.
7 Yeh A. Early malware detection by cross-referencing host data; 2015.
8 Aravindakshan V, Kumar K, Kummur A. Systems and methods for network filtering in VPN. Google Patents; 2015.
9 Porat R, Bayora A, Farage O, Blayer-gat A. Detection and prevention for malicious threats. Google Patents; 2016.
10 Zhang P, Wang W, Tan Y. A malware detection model based on a negative selection algorithm with penalty factor. Science China Information Sciences. 2010;53(12):2461–2471.
11 CERT US. Security Tip (ST18-002) Defending Against Illicit Cryptocurrency Mining Activity; 2018. Available from: https://www.us-cert.gov/ncas/tips/ST13-003.
12 Liao HJ, Lin CHR, Lin YC, Tung KY. Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications. 2013;36(1):16–24.
13 Demertzis K, Kikiras P, Tziritas N, Sanchez S, Iliadis L. The Next Generation Cognitive Security Operations Center: Network Flow Forensics Using Cybersecurity Intelligence. Big Data and Cognitive Computing. 2018;2(4):35.
14 NIST. National Vulnerability Database; 2019. Available from: http://nvd.nist.gov.
15 Stickle TC, Moses CJ, HOLLAND RC. Computer security threat correlation. Google Patents; 2019.
16 Lotem A, Cohen G, Naon LB. Method for simulation aided security event management. Google Patents; 2016.
17 Nadeau M. What is cryptojacking? How to prevent, detect, and recover from it; 2018. Available from: https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html.
18 Gov UC. Security Tip (ST18-002) Defending Against Illicit Cryptocurrency Mining Activity; 2018. Available from: https://www.us-cert.gov/ncas/tips/ST18-002.
19 Marchetto V, et al. An Investigation of Cryptojacking: Malware Analysis and Defense Strategies. Journal of Strategic Innovation and Sustainability. 2019;14(1):66–80.