North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector

cisa.gov/uscert/ncas/alerts/aa22-187a

Summary

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and the Department of the Treasury (Treasury) are releasing this joint Cybersecurity Advisory (CSA) to provide information on Maui ransomware, which has been used by North Korean state-sponsored cyber actors since at least May 2021 to target Healthcare and Public Health (HPH) Sector organizations.

This joint CSA provides information—including tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs)—on Maui ransomware obtained from FBI incident response activities and industry analysis of a Maui sample. The FBI, CISA, and Treasury urge HPH Sector organizations as well as other critical infrastructure organizations to apply the recommendations in the Mitigations section of this CSA to reduce the likelihood of compromise from ransomware operations. Victims of Maui ransomware should report the incident to their local FBI field office or CISA.

The FBI, CISA, and Treasury highly discourage paying ransoms as doing so does not guarantee files and records will be recovered and may pose sanctions risks. **Note:** in September 2021, Treasury issued an updated advisory highlighting the sanctions risks associated with ransomware payments and the proactive steps companies can take to mitigate such risks. Specifically, the updated advisory encourages U.S. entities to adopt and improve cybersecurity practices and report ransomware attacks to, and fully cooperate with, law enforcement. The updated advisory states that when affected parties take these proactive steps, Treasury's Office of Foreign Assets Control (OFAC) would be more likely to resolve apparent sanctions violations involving ransomware attacks with a non-public enforcement response.

For more information on state-sponsored North Korean malicious cyber activity, see CISA's North Korea Cyber Threat Overview and Advisories webpage.

Download the PDF version of this report: pdf, 553 kb.

Click here for STIX.

Technical Details

Since May 2021, the FBI has observed and responded to multiple Maui ransomware incidents at HPH Sector organizations. North Korean state-sponsored cyber actors used Maui ransomware in these incidents to encrypt servers responsible for healthcare services—including electronic health records services, diagnostics services, imaging services, and intranet services. In some cases, these incidents disrupted the services provided by the targeted HPH Sector organizations for prolonged periods. The initial access vector(s) for these incidents is unknown.

Maui Ransomware

Maui ransomware (`maui.exe`) is an encryption binary. According to industry analysis of a sample of Maui (SHA256: 5b7ecf7e9d0715f1122baf4ce745c5fcd769dee48150616753fec4d6da16e99e) provided in Stairwell Threat Report: Maui Ransomware—the ransomware appears to be designed for manual execution [TA0002] by a remote actor. The remote actor uses command-line interface [T1059.008] to interact with the malware and to identify files to encrypt.

Maui uses a combination of Advanced Encryption Standard (AES), RSA, and XOR encryption to encrypt [T1486] target files:

1. Maui encrypts target files with AES 128-bit encryption. Each encrypted file has a unique AES key, and each file contains a custom header with the file's original path, allowing Maui to identify previously encrypted files. The header also contains encrypted copies of the AES key.
2. Maui encrypts each AES key with RSA encryption.
   Maui loads the RSA public (`maui.key`) and private (`maui.evd`) keys in the same directory as itself.
3. Maui encodes the RSA public key (`maui.key`) using XOR encryption. The XOR key is generated from hard drive information (`\\.\PhysicalDrive0`).

During encryption, Maui creates a temporary file for each file it encrypts using `GetTempFileNameW()` . Maui uses the temporary to stage output from encryption. After encrypting files, Maui creates `maui.log` , which contains output from Maui execution. Actors likely exfiltrate [TA0010] `maui.log` and decrypt the file using associated decryption tools.

See Stairwell Threat Report: Maui Ransomware for additional information on Maui ransomware, including YARA rules and a key extractor.

Indicators of Compromise

See table 1 for Maui ransomware IOCs obtained from FBI incident response activities since May 2021.

Table 1: Maui Ransomware IOCs

Indicator Type	Value
Filename	maui.exe
maui.log	
maui.key	
maui.evd	
aui.exe	
MD5 Hash	4118d9adce7350c3eedeb056a3335346
9b0e7c460a80f740d455a7521f0eada1	
fda3a19afa85912f6dc8452675245d6b	
2d02f5499d35a8dffb4c8bc0b7fec5c2	
c50b839f2fc3ce5a385b9ae1c05def3a	
a452a5f693036320b580d28ee55ae2a3	
a6e1efd70a077be032f052bb75544358	
802e7d6e80d7a60e17f9ffbd62fcbbeb	
SHA256 Hash	5b7ecf7e9d0715f1122baf4ce745c5fcd769dee48150616753fec
45d8ac1ac692d6bb0fe776620371fca02b60cac8db23c4cc7ab5df262da42b78	
56925a1f7d853d814f80e98a1c4890b0a6a84c83a8eded34c585c98b2df6ab19	
830207029d83fd46a4a89cd623103ba2321b866428aa04360376e6a390063570	
458d258005f39d72ce47c111a7d17e8c52fe5fc7dd98575771640d9009385456	
99b0056b7cc2e305d4ccb0ac0a8a270d3fceb21ef6fc2eb13521a930cea8bd9f	
3b9fe1713f638f85f20ea56fd09d20a96cd6d288732b04b073248b56cdaef878	
87bdb1de1dd6b0b75879d8b8aef80b562ec4fad365d7abbc629bcfc1d386afa6	

Attribution to North Korean State-Sponsored Cyber Actors

The FBI assesses North Korean state-sponsored cyber actors have deployed Maui ransomware against Healthcare and Public Health Sector organizations. The North Korean state-sponsored cyber actors likely assume healthcare organizations are willing to pay ransoms because these organizations provide services that are critical to human life and health. Because of this assumption, the FBI, CISA, and Treasury assess North Korean state-sponsored actors are likely to continue targeting HPH Sector organizations.

Mitigations

The FBI, CISA, and Treasury urge HPH Sector organizations to:

- Limit access to data by deploying public key infrastructure and digital certificates to authenticate connections with the network, Internet of Things (IoT) medical devices, and the electronic health record system, as well as to ensure data packages are not manipulated while in transit from man-in-the-middle attacks.
- Use standard user accounts on internal systems instead of administrative accounts, which allow for overarching administrative system privileges and do not ensure least privilege.
- Turn off network device management interfaces such as Telnet, SSH, Winbox, and HTTP for wide area networks (WANs) and secure with strong passwords and encryption when enabled.
- Secure personal identifiable information (PII)/patient health information (PHI) at collection points and encrypt the data at rest and in transit by using technologies such as Transport Layer Security (TPS). Only store personal patient data on internal systems that are protected by firewalls, and ensure extensive backups are available if data is ever compromised.
- Protect stored data by masking the permanent account number (PAN) when it is displayed and rendering it unreadable when it is stored—through cryptography, for example.
- Secure the collection, storage, and processing practices for PII and PHI, per regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Implementing HIPAA security measures can prevent the introduction of malware on the system.
- Implement and enforce multi-layer network segmentation with the most critical communications and data resting on the most secure and reliable layer.
- Use monitoring tools to observe whether IoT devices are behaving erratically due to a compromise.
- Create and regularly review internal policies that regulate the collection, storage, access, and monitoring of PII/PHI.

In addition, the FBI, CISA, and Treasury urge all organizations, including HPH Sector organizations, to apply the following recommendations to prepare for, mitigate/prevent, and respond to ransomware incidents.

Preparing for Ransomware

- **Maintain offline (i.e., physically disconnected) backups of data, and regularly test backup and restoration.** These practices safeguard an organization's continuity of operations or at least minimize potential downtime from a ransomware incident and protect against data losses.
  Ensure all backup data is encrypted, immutable (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure.
- **Create, maintain, and exercise a basic cyber incident response plan and associated communications plan** that includes response procedures for a ransomware incident.
  - Organizations should also ensure their incident response and communications plans include response and notification procedures for data breach incidents. Ensure the notification procedures adhere to applicable state laws.
    - Refer to the National Conference of State Legislatures: Security Breach Notification Laws for information on each state's data breach laws.
    - For breaches involving electronic health information, you may need to notify the Federal Trade Commission (FTC) or the Department of Health and Human Services, and, in some cases, the media. Refer to the FTC's Health Breach Notification Rule and U.S. Department of Health and Human Services' Breach Notification Rule for more information.
  - See CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide and CISA Fact Sheet Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches for information on creating a ransomware response checklist and planning and responding to ransomware-caused data breaches.

Mitigating and Preventing Ransomware

- **Install updates for operating systems, software, and firmware as soon as they are released.** Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Regularly check for software updates and end-of-life notifications and prioritize patching known exploited vulnerabilities. Consider leveraging a centralized patch management system to automate and expedite the process.
- **If you use Remote Desktop Protocol (RDP), or other potentially risky services, secure and monitor them closely.**
  - Limit access to resources over internal networks, especially by restricting RDP and using virtual desktop infrastructure. After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources, and require multifactor authentication (MFA) to mitigate credential theft and reuse. If RDP must be available externally, use a virtual private network (VPN), virtual desktop infrastructure, or other means to authenticate and secure the connection before allowing RDP to connect to internal devices. Monitor remote access/RDP logs, enforce account lockouts after a specified number of attempts to block brute force campaigns, log RDP login attempts, and disable unused remote access/RDP ports.
  - Ensure devices are properly configured and that security features are enabled. Disable ports and protocols that are not being used for a business purpose (e.g., RDP Transmission Control Protocol Port `3389`).
  - Restrict Server Message Block (SMB) Protocol within the network to only access servers that are necessary and remove or disable outdated versions of SMB (i.e., SMB version 1). Threat actors use SMB to propagate malware across organizations.
  - Review the security posture of third-party vendors and those interconnected with your organization. Ensure all connections between third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity.
  - Implement listing policies for applications and remote access that only allow systems to execute known and permitted programs under an established.
  - Open document readers in protected viewing modes to help prevent active content from running.
- **Implement user training program and phishing exercises** to raise awareness among users about the risks of visiting suspicious websites, clicking on suspicious links, and opening suspicious attachments. Reinforce the appropriate user response to phishing and spearphishing emails.
- **Require MFA for as many services as possible**—particularly for webmail, VPNs, accounts that access critical systems, and privileged accounts that manage backups.
- Use strong passwords and avoid reusing passwords for multiple accounts. See CISA Tip Choosing and Protecting Passwords and National Institute of Standards and Technology (NIST) Special Publication 800-63B: Digital Identity Guidelines for more information.
- **Require administrator credentials to install software.**
- **Audit user accounts with administrative or elevated privileges** and configure access controls with least privilege in mind.
- **Install and regularly update antivirus and antimalware software on all hosts.**
- **Only use secure networks and avoid using public Wi-Fi networks.** Consider installing and using a VPN.
- **Consider adding an email banner to messages coming from outside your organizations.**
- **Disable hyperlinks in received emails.**

Responding to Ransomware Incidents

If a ransomware incident occurs at your organization:

- Follow your organization's Ransomware Response Checklist (see Preparing for Ransomware section).

- Scan backups. If possible, scan backup data with an antivirus program to check that it is free of malware. This should be performed using an isolated, trusted system to avoid exposing backups to potential compromise.
- Follow the notification requirements as outlined in your cyber incident response plan.
- Report incidents to the FBI at a local FBI Field Office, CISA at us-cert.cisa.gov/report, or the U.S. Secret Service (USSS) at a USSS Field Office.
- Apply incident response best practices found in the joint Cybersecurity Advisory, Technical Approaches to Uncovering and Remediating Malicious Activity, developed by CISA and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom.

Note: the FBI, CISA, and Treasury strongly discourage paying ransoms as doing so does not guarantee files and records will be recovered and may pose sanctions risks.

Request for Information

The FBI is seeking any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, bitcoin wallet information, the decryptor file, and/or benign samples of encrypted files. As stated above, the FBI discourages paying ransoms. Payment does not guarantee files will be recovered and may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. However, the FBI understands that when victims are faced with an inability to function, all options are evaluated to protect shareholders, employees, and customers. Regardless of whether you or your organization have decided to pay the ransom, the FBI, CISA, and Treasury urge you to promptly report ransomware incidents to the FBI at a local FBI Field Office, CISA at us-cert.cisa.gov/report, or the USSS at a USSS Field Office. Doing so provides the U.S. Government with critical information needed to prevent future attacks by identifying and tracking ransomware actors and holding them accountable under U.S. law.

Resources

- For more information and resources on protecting against and responding to ransomware, refer to StopRansomware.gov, a centralized, U.S. whole-of-government webpage providing ransomware resources and alerts.
- CISA's Ransomware Readiness Assessment is a no-cost self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident.
- A guide that helps organizations mitigate a ransomware attack and provides a Ransomware Response Checklists: CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide.
- The U.S. Department of State's Rewards for Justice (RFJ) program offers a reward of up to $10 million for reports of foreign government malicious activity against U.S. critical infrastructure. See the RFJ website for more information and how to report information securely.

Acknowledgements

The FBI, CISA, and Treasury would like to thank Stairwell for their contributions to this CSA.

Contact Information

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at report@cisa.gov.

Revisions

July 6, 2022: Initial Version

July 7, 2022: Added STIX

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.