

## Cybersecurity Advisory



Defense  
Security  
Agency

## #StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

### Summary

Note: This Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and various ransomware threat actors. These #StopRansomware advisories detail historically and recently observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit [stopransomware.gov](https://stopransomware.gov) to see all #StopRansomware advisories and to learn about other ransomware threats and no-cost resources.

The United States National Security Agency (NSA), the U.S. Federal Bureau of Investigation (FBI), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Department of Health and Human Services (HHS), the Republic of Korea (ROK) National Intelligence Service (NIS), and the ROK Defense Security Agency (DSA) (hereafter referred to as the “authoring agencies”) are issuing this joint Cybersecurity Advisory (CSA) to highlight ongoing ransomware activity against [Healthcare and Public Health Sector](#) organizations and other [critical infrastructure sector](#) entities.

This CSA provides an overview of Democratic People’s Republic of Korea (DPRK) state-sponsored ransomware and updates the July 6, 2022, joint CSA [North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector](#). This advisory highlights TTPs and IOCs DPRK cyber actors used to gain access to and conduct ransomware attacks against Healthcare and Public Health (HPH) Sector organizations and other critical infrastructure sector entities, as well as DPRK cyber actors’ use of cryptocurrency to demand ransoms.

# Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

The authoring agencies assess that an unspecified amount of revenue from these cryptocurrency operations supports DPRK national-level priorities and objectives, including cyber operations targeting the United States and South Korea governments—specific targets include Department of Defense Information Networks and Defense Industrial Base member networks. The IOCs in this product should be useful to sectors previously targeted by DPRK cyber operations (e.g., U.S. government, Department of Defense, and Defense Industrial Base). The authoring agencies highly discourage paying ransoms as doing so does not guarantee files and records will be recovered and may pose sanctions risks.

For additional information on state-sponsored DPRK malicious cyber activity, see CISA's [North Korea Cyber Threat Overview and Advisories](#) webpage.

## Technical Details

Note: This advisory uses the MITRE ATT&CK for Enterprise framework, version 12. See [MITRE ATT&CK for Enterprise](#) for all referenced tactics and techniques.

This CSA is supplementary to previous reports on malicious cyber actor activities involving DPRK ransomware campaigns—namely [Maui](#) and [H0lyGh0st](#) ransomware. The authoring agencies are issuing this advisory to highlight additional observed TTPs DPRK cyber actors are using to conduct ransomware attacks targeting South Korean and U.S. healthcare systems.

## Observable TTPs

The TTPs associated with DPRK ransomware attacks include those traditionally observed in ransomware operations. Additionally, these TTPs span phases from acquiring and purchasing infrastructure to concealing DPRK affiliation:

- **Acquire Infrastructure [T1583].** DPRK actors generate domains, personas, and accounts; and identify cryptocurrency services to conduct their ransomware operations. Actors procure infrastructure, IP addresses, and domains with cryptocurrency generated through illicit cybercrime, such as ransomware and cryptocurrency theft.
- **Obfuscate Identity.** DPRK actors purposely obfuscate their involvement by operating with or under third-party foreign affiliate identities and use third-party foreign intermediaries to receive ransom payments.

## Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

- **Purchase VPNs and VPSs [T1583.003]**. DPRK cyber actors will also use virtual private networks (VPNs) and virtual private servers (VPSs) or third-country IP addresses to appear to be from innocuous locations instead of from DPRK.
- **Gain Access [TA0001]**. Actors use various exploits of common vulnerabilities and exposures (CVE) to gain access and escalate privileges on networks. Recently observed CVEs that actors used to gain access include remote code execution in the Apache Log4j software library (known as [Log4Shell](#)) and [remote code execution in various SonicWall appliances](#) [T1190 and T1133]. Observed CVEs used include:
  - CVE 2021-44228
  - CVE-2021-20038
  - CVE-2022-24990

Actors also likely spread malicious code through Trojanized files for “X-Popup,” an open source messenger commonly used by employees of small and medium hospitals in South Korea [T1195].

The actors spread malware by leveraging two domains: `xpopup.pe[.]kr` and `xpopup.com`. `xpopup.pe[.]kr` is registered to IP address `115.68.95[.]128` and `xpopup[.]com` is registered to IP address `119.205.197[.]111`. Related file names and hashes are listed in table 1.

Table 1: Malicious file names and hashes spread by xpopup domains

| File Name   | MD5 Hash                         |
|-------------|----------------------------------|
| xpopup.rar  | 1f239db751ce9a374eb9f908c74a31c9 |
| X-PopUp.exe | 6fb13b1b4b42bac05a2ba629f04e3d03 |
| X-PopUp.exe | cf8ba073db7f4023af2b13dd75565f3d |
| xpopup.exe  | 4e71d52fc39f89204a734b19db1330d3 |
| x-PopUp.exe | 43d4994635f72852f719abb604c4a8a1 |
| xpopup.exe  | 5ae71e8440bf33b46554ce7a7f3de666 |

- **Move Laterally and Discovery [TA0007, TA0008]**. After initial access, DPRK cyber actors use staged payloads with customized malware to perform reconnaissance activities, upload and download additional files and executables,

## Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

and execute shell commands [T1083, T1021]. The staged malware is also responsible for collecting victim information and sending it to the remote host controlled by the actors [TA0010].

- **Employ Various Ransomware Tools [TA0040].** Actors have used privately developed ransomware, such as Maui and H0lyGh0st [T1486]. Actors have also been observed using or possessing publically available tools for encryption, such as BitLocker, Deadbolt, ech0raix, GonnaCry, Hidden Tear, Jigsaw, LockBit 2.0, My Little Ransomware, NxRansomware, Ryuk, and YourRansom [T1486]. In some cases, DPRK actors have portrayed themselves as other ransomware groups, such as the REvil ransomware group. For IOCs associated with Maui and H0lyGh0st ransomware usage, please see Appendix B.
- **Demand Ransom in Cryptocurrency.** DPRK cyber actors have been observed setting ransoms in bitcoin [T1486]. Actors are known to communicate with victims via Proton Mail email accounts. For private companies in the healthcare sector, actors may threaten to expose a company's proprietary data to competitors if ransoms are not paid. Bitcoin wallet addresses possibly used by DPRK cyber actors include:
  - 1MTHBCrBKYEthfa16zo9kabt4f9jMJz8Rm
  - bc1q80vc4yjgg6umedkut3e9mhehxl4q4dcjjyzh59
  - 1J8spy62o7z2AjQxoUpiCGnBh5cRWKVVJC
  - 16ENLdHbnmDcEV8iqN4vuyZHa7sSdYRh76
  - bc1q3wzxvu8yhs8h7mlkmf7277wyklkah9k4sm9anu
  - bc1q8xyt4jxhw7mgqpwd6qfdjyxgvjeuz57jxrv9k9
  - 1NqihEqYaQaWiZkPVdSMiTbt7dTy1LMxgX
  - bc1qxrpevck3pq1yzrx2pq2rkvkvy0jnm56nzjv6pw
  - 14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
  - 1KCwfCUgnSy3pzNX7U1i5NwFzRtth4bRBc
  - 16sYqXancDDiijcuruZecCkdBDwDf4vSEC
  - 1N6JphHFaYmYaokS5xH31Z67bvk4ykd9CP
  - LZ1VNJfn6mWjPzkCyoBvqWaBZYXAwN135
  - 1KmWW6LgdgykBBR5XrFu9kdoHz95Fe9kQF
  - 1FX4W9rrG4F3Uc7gJ18GCwGab8XuW8Agy2
  - bc1qlqgu2l2kms5338zuc95kxavctzyy0v705tpvyc
  - bc1qy6su7vrh7ts5ng2628escmhr98msmzg62ez2sp
  - bc1q8t69gpxsezdc8w6tfzp3jeptq4tcp2g9d0mwy

# Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

- bc1q9h7yj79sqm4t536q0fdn7n4y2atsvvl22m28ep
- bc1qj6y72rk039mqpgtcy7mwjd3eum6cx6027ndgmd
- bc1qcp557vltuu3qc6pk3ld0ayagrxf2thp3pjzpe
- bc1ql8wsflrf9zlsruauynzjm83mupq6c9jz9vnqyg
- bc1qx60ec3nfd5yhsyyxkzkpts54w970yxj84zrdck
- bc1qunqnjdlvqkjuhtclfp8kzkjpvdz9qnk898xczp
- bc1q6024d73h48fnhwswhwt3hqz2lzw6x99q0nulm4
- bc1qwdvexlyvg3mqvqw7g6l09qup0qew80wj9jh7x
- bc1qavrtge4p7dmcnrvhlvuhaarx8rek76wxyk7dgg
- bc1qagaayd57vr25dlqgk7f00nhz9qepqgnlnt4upu
- bc1quvnaxnpqlzq3mdhfddh35j7e7ufxh3gpc56hca
- bc1qu0pvfmtxawm8s99lcjvxapungtsmkvwyvak6cs
- bc1qg3zlxxhhcvt6hkuhmqml8y9pas76cajcu9ltdl
- bc1qn7a3g23nzpuytchyyteyhkcse84cnylznl3j32
- bc1qhfmqstxp3yp9muvuz29wk77vjtdyrkff4nrpxu
- bc1qnh8scrvuqvlzmzg7eesyrmtes9c5m78duetf3
- bc1q7qry3lsrphmnw3exs7tkwzpvzjcx942aq8n0y
- bc1qcmlcxfsy0zlqhh72jvvc4rh7hvwhx6scp27na0
- bc1q498fn0gauj2kkjsg35mlwk2cnxhaqlj7hkh8xy
- bc1qnz4udqkumjghnm2a3zt0w3ep8fwdcyv3krr3jq
- bc1qk0saaw7p0wrwla6u7tfjlxrutlgrwnudzx9tyw
- bc1qyue2pgjk09ps7qvfs559k8kee3jkcw4p4vdp57
- bc1q6qfkt06xmrpclht3acmq00p7zyy0ejydu89zwv
- bc1qmge6a7sp659exnx78zhm9zgrw88n6un0rl9trs
- bc1qcywkd7zqlwmjy36c46dpf8cq6ts6wgkx0u7cn

## Mitigations

Note: These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the U.S. National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. For more information on the CPGs, including additional recommended baseline protections, see [cisa.gov/cpg](https://cisa.gov/cpg).

The authoring agencies urge HPH organizations to:

## Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

- Limit access to data by authenticating and encrypting connections (e.g., using public key infrastructure certificates in virtual private network (VPN) and transport layer security (TLS) connections) with network services, Internet of Things (IoT) medical devices, and the electronic health record system [\[CPG 3.3\]](#).
- Implement the principle of least privilege by using standard user accounts on internal systems instead of administrative accounts [\[CPG 1.5\]](#), which grant excessive system administration privileges.
- Turn off weak or unnecessary 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.
- Protect stored data by masking the permanent account number (PAN) when displayed and rendering it unreadable when stored—through cryptography, for example.
- Secure the collection, storage, and processing practices for personally identifiable information (PII)/protected health information (PHI), per regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Implementing HIPAA security measures could prevent the introduction of malware to the system [\[CPG 3.4\]](#).
  - Secure PII/ PHI at collection points and encrypt the data at rest and in transit using technologies, such as TLS. Only store personal patient data on internal systems that are protected by firewalls, and ensure extensive backups are available.
  - Create and regularly review internal policies that regulate the collection, storage, access, and monitoring of PII/PHI.
- Implement and enforce multi-layer network segmentation with the most critical communications and data resting on the most secure and reliable layer [\[CPG 8.1\]](#).
- Use monitoring tools to observe whether IoT devices are behaving erratically due to a compromise [\[CPG 3.1\]](#).

In addition, the authoring agencies urge all organizations, including HPH Sector organizations, to apply the following recommendations to prepare for and mitigate ransomware incidents:

- **Maintain isolated backups of data, and regularly test backup and restoration** [\[CPG 7.3\]](#). These practices safeguard an organization's continuity of

# Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

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 [[CPG 7.1, 7.2](#)].
  - Organizations should also ensure their incident response and communications plans include data breach incidents response and notification procedures. Ensure the notification procedures adhere to applicable laws.
  - See the [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.
- **Install updates for operating systems, software, and firmware as soon as they are released** [[CPG 5.1](#)]. 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** [[CPG 5.4](#)].
  - 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 [phishing-resistant multifactor authentication \(MFA\)](#) to mitigate credential theft and reuse [[CPG 1.3](#)]. If RDP must be available externally, use a 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 [[CPG 1.1, 3.1](#)].

## Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

- Ensure devices are properly configured and that security features are enabled. Disable ports and protocols not in use for a business purpose (e.g., RDP Transmission Control Protocol port 3389).
- Restrict the Server Message Block (SMB) protocol within the network to only access necessary servers 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 [\[CPG 5.6, 6.2\]](#).
- Implement application control policies that only allow systems to execute known and permitted programs [\[CPG 2.1\]](#).
- Open document readers in protected viewing modes to help prevent active content from running.
- **Implement a user training program and phishing exercises** [\[CPG 4.3\]](#) to raise awareness among users about the risks of visiting websites, clicking on links, and opening attachments. Reinforce the appropriate user response to phishing and spearphishing emails.
- **Require phishing-resistant MFA for as many services as possible** [\[CPG 1.3\]](#)—particularly for webmail, VPNs, accounts that access critical systems, and privileged accounts that manage backups.
- **Use strong passwords** [\[CPG 1.4\]](#) 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** [\[CPG 1.5\]](#).
- **Audit user accounts with administrative or elevated privileges** [\[CPG 1.5\]](#) and configure access controls with least privilege in mind.
- **Install and regularly update antivirus and antimalware software on all hosts.**
- **Only use secure networks.** Consider installing and using a VPN.
- **Consider adding an email banner to messages coming from outside your organizations** [\[CPG 8.3\]](#) indicating that they are higher risk messages.

# Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

- **Consider participating in CISA's no-cost [Automated Indicator Sharing \(AIS\)](#)** program to receive real-time exchange of machine-readable cyber threat indicators and defensive measures.

If a ransomware incident occurs at your organization:

- Follow your organization's ransomware response checklist.
- 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.
- **U.S. organizations:** Follow the notification requirements as outlined in your cyber incident response plan. Report incidents to appropriate authorities; in the U.S., this would include the FBI at a [local FBI Field Office](#), CISA at [cisa.gov/report](#), or the U.S. Secret Service (USSS) at a [USSS Field Office](#).
- **South Korean organizations:** Please report incidents to NIS, KISA (Korea Internet & Security Agency), and KNPA (Korean National Police Agency).
  - NIS (National Intelligence Service)
    - Telephone : 111
    - <https://www.nis.go.kr>
  - KISA (Korea Internet & Security Agency)
    - Telephone : 118 (Consult Service)
    - <https://www.boho.or.kr/consult/ransomware.do>
  - KNPA (Korean National Police Agency)
    - Electronic Cybercrime Report & Management System: <https://ecrm.police.go.kr/minwon/main>
- 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.

## Resources

Stairwell provided a YARA rule to identify Maui ransomware, and a Proof of Concept public RSA key extractor at the following link:

<https://www.stairwell.com/news/threat-research-report-maui-ransomware/>

## 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

# Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

decryptor file, and/or benign samples of encrypted files. As stated above, the authoring agencies discourage 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 agencies understand 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 decide to pay a ransom, the authoring agencies urge you to promptly report ransomware incidents using the [contact information](#) above.

## Acknowledgements

NSA, FBI, CISA, and HHS would like to thank ROK NIS and DSA for their contributions to this CSA.

### *Disclaimer of endorsement*

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

### *Trademark recognition*

Microsoft Threat Intelligence Center is a registered trademark of Microsoft Corporation. Apache®, Sonicwall, and Apache Log4j are trademarks of Apache Software Foundation. TerraMaster Operating System is a registered trademark of Octagon Systems.

### *Purpose*

This document was developed in furtherance of the authors' cybersecurity missions, including their responsibilities to identify and disseminate threats, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

### *Contact*

NSA Client Requirements / General Cybersecurity Inquiries: [CybersecurityReports@nsa.gov](mailto:CybersecurityReports@nsa.gov)

Defense Industrial Base Inquiries and Cybersecurity Services: [DIB\\_Defense@cyber.nsa.gov](mailto:DIB_Defense@cyber.nsa.gov)

To report incidents and anomalous activity related to information found in this Joint Cybersecurity Advisory, contact CISA's 24/7 Operations Center at [Report@cisa.gov](mailto:Report@cisa.gov) or (888) 282-0870 or your local FBI field office at [www.fbi.gov/contact-us/field](http://www.fbi.gov/contact-us/field). 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.

Media Inquiries / Press Desk:

- NSA Media Relations, 443-634-0721, [MediaRelations@nsa.gov](mailto:MediaRelations@nsa.gov)
- CISA Media Relations, 703-235-2010, [CISAMedia@cisa.dhs.gov](mailto:CISAMedia@cisa.dhs.gov)

## Appendix A: CVE Details

| CVE-2021-44228                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | CVSS 3.0: 10 (Critical) |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <b><u>Vulnerability Description</u></b><br><p>Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.</p> |                         |
| <b><u>Recommended Mitigations</u></b><br><p>Apply patches provided by vendor and perform required system updates.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                         |
| <b><u>Detection Methods</u></b><br><p>See vendors' <a href="#">Guidance For Preventing, Detecting, and Hunting for Exploitation of the Log4j 2 Vulnerability</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                         |
| <b><u>Vulnerable Technologies and Versions</u></b><br><p>There are numerous vulnerable technologies and versions associated with CVE-2021-44228. For a full list, please check <a href="https://nvd.nist.gov/vuln/detail/CVE-2021-44228">https://nvd.nist.gov/vuln/detail/CVE-2021-44228</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                         |
| <p>See <a href="https://nvd.nist.gov/vuln/detail/CVE-2021-44228">https://nvd.nist.gov/vuln/detail/CVE-2021-44228</a> for more information.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                         |

## Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

| CVE-2021-20038                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | CVSS 3.0: 9.8 (Critical) |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <b><u>Vulnerability Description</u></b><br><p>A Stack-based buffer overflow vulnerability in SMA100 Apache httpd server's mod_cgi module environment variables allows a remote unauthenticated attacker to potentially execute code as a 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances firmware 10.2.0.8-37sv, 10.2.1.1-19sv, 10.2.1.2-24sv and earlier versions.</p>                                                                                                                                                                                                                                                                                                                                               |                          |
| <b><u>Recommended Mitigations</u></b><br><p>Apply all appropriate vendor updates<br/> Upgrade to:</p> <ul style="list-style-type: none"> <li>• SMA 100 Series - (SMA 200, 210, 400, 410, 500v (ESX, Hyper-V, KVM, AWS, Azure):</li> <li>• SonicWall SMA100 build versions 10.2.0.9-41sv or later</li> <li>• SonicWall SMA100 build versions 10.2.1.3-27sv or later</li> </ul> <p>System administrators should refer to the SonicWall Security Advisories in the reference section to determine affected applications/systems and appropriate fix actions.</p> <p>Support for 9.0.0 firmware ended on 10/31/2021. Customers still using that firmware are requested to upgrade to the latest 10.2.x versions.</p>                                                             |                          |
| <b><u>Vulnerable Technologies and Versions</u></b><br><p>Sonicwall Sma 200 Firmware 10.2.0.8-37Sv<br/> Sonicwall Sma 200 Firmware 10.2.1.1-19Sv<br/> Sonicwall Sma 200 Firmware 10.2.1.2-24Sv<br/> Sonicwall Sma 210 Firmware 10.2.0.8-37Sv<br/> Sonicwall Sma 210 Firmware 10.2.1.1-19Sv<br/> Sonicwall Sma 210 Firmware 10.2.1.2-24Sv<br/> Sonicwall Sma 410 Firmware 10.2.0.8-37Sv<br/> Sonicwall Sma 410 Firmware 10.2.1.1-19Sv<br/> Sonicwall Sma 410 Firmware 10.2.1.2-24Sv<br/> Sonicwall Sma 400 Firmware 10.2.0.8-37Sv<br/> Sonicwall Sma 400 Firmware 10.2.1.1-19Sv<br/> Sonicwall Sma 400 Firmware 10.2.1.2-24Sv<br/> Sonicwall Sma 500V Firmware 10.2.0.8-37Sv<br/> Sonicwall Sma 500V Firmware 10.2.1.1-19Sv<br/> Sonicwall Sma 500V Firmware 10.2.1.2-24Sv</p> |                          |
| <p>See <a href="https://nvd.nist.gov/vuln/detail/CVE-2021-20038">https://nvd.nist.gov/vuln/detail/CVE-2021-20038</a> for more information.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                          |

## Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

CVE-2022-24990

CVSS 3.x: N/A

**Vulnerability Description**

The TerraMaster OS Unauthenticated Remote Command Execution via PHP Object Instantiation Vulnerability is characterized by scanning activity targeting a flaw in the script enabling a remote adversary to execute commands on the target endpoint. The vulnerability is created by improper input validation of the webNasIPS component in the api.php script and resides on the TNAS device appliances' operating system where users manage storage, backup data, and configure applications. By exploiting the script flaw a remote unauthenticated attacker can pass specially crafted data to the application and execute arbitrary commands on the target system. This may result in complete compromise of the target system, including the exfiltration of information. TNAS devices can be chained to acquire unauthenticated remote code execution with highest privileges.

**Recommended Mitigations**

Install relevant vendor patches. This vulnerability was patched in TOS version 4.2.30

**Vulnerable Technologies and Versions**

TOS v 4.2.29

See <https://octagon.net/blog/2022/03/07/cve-2022-24990-termaster-tos-unauthenticated-remote-command-execution-via-php-object-instantiation/> and <https://forum.terra-master.com/en/viewtopic.php?t=3030> for more information.

## Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

## Appendix B: Indicators of Compromise (IOCs)

The IOC section includes hashes and IP addresses for the Maui and H0lyGh0st ransomware variants—as well as custom malware implants assumedly developed by DPRK cyber actors, such as remote access trojans (RATs), loaders, and other tools—that enable subsequent deployment of ransomware. For additional Maui IOCs, see joint CSA [North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector](#).

Table 2 lists MD5 and SHA256 hashes associated with malware implants, RATs, and other tools used by DPRK cyber actors, including tools that drop Maui ransomware files.

Table 2: File names and hashes of malicious implants, RATs, and tools

| MD5Hash                           | SHA256Hash                                                           |
|-----------------------------------|----------------------------------------------------------------------|
| 079b4588eaa99a1e802adf5e0b26d8aa  | f67ee77d6129bd1bcd5d856c0fc5314169<br>b946d32b8abaa4e680bb98130b38e7 |
| 0e9e256d8173854a7bc26982b1dde783  | --                                                                   |
| 12c15a477e1a96120c09a860c9d479b3  | 6263e421e397db821669420489d2d3084<br>f408671524fd4e1e23165a16dda2225 |
| 131fc4375971af391b459de33f81c253  | --                                                                   |
| 17c46ed7b80c2e4dbea6d0e88ea0827c  | b9af4660da00c7fa975910d0a19fda0720<br>31c15fad1eef935a609842c51b7f7d |
| 1875f6a68f70bee316c8a6eda9ebf8de  | 672ec8899b8ee513dbfc4590440a61023<br>846ddc2ca94c88ae637144305c497e7 |
| 1a74c8d8b74ca2411c1d3d22373a6769  | ba8f9e7afe5f78494c111971c39a89111ef<br>9262bf23e8a764c6f65c818837a44 |
| 1f6d9f8fbdbbd4e6ed8cd73b9e95a928  | 4f089afa51fd0c1b2a39cc11cedb3a4a32<br>6111837a5408379384be6fe846e016 |
| 2d02f5499d35a8dfffb4c8bc0b7fec5c2 | 830207029d83fd46a4a89cd623103ba23<br>21b866428aa04360376e6a390063570 |
| 2e18350194e59bc6a2a3f6d59da11bd8  | 655aa64860f1655081489cf85b77f72a49<br>de846a99dd122093db4018434b83ae |
| 3bd22e0ac965ebb6a18bb71ba39e96dc  | 6b7f566889b80d1dba4f92d5e2fb2f5ef24<br>f57fcfd56bb594978dffe9edbb9eb |
| 40f21743f9cb927b2c84ecdb7dfb14a6  | 5081f54761947bc9ce4aa2a259a0bd60b<br>4ec03d32605f8e3635c4d4edaf48894 |
| 4118d9adce7350c3eedeb056a3335346  | 5b7ecf7e9d0715f1122baf4ce745c5fcd76<br>9dee48150616753fec4d6da16e99e |

## Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

|                                  |                                                                   |
|----------------------------------|-------------------------------------------------------------------|
| 43e756d80225bdf1200bc34eef5adca8 | afb2d4d88f59e528f0e388705113ae54b7b97db4f03a35ae43cc386a48f263a0  |
| 47791bf9e017e3001ddc68a7351ca2d6 | 863b707873f7d653911e46885e261380b410bb3bf6b158daefb47562e93cb657  |
| 505262547f8879249794fc31eea41fc6 | f32f6b229913d68daad937cc72a57aa45291a9d623109ed48938815aa7b6005c  |
| 5130888a0ad3d64ad33c65de696d3fa2 | c92c1f3e77a1876086ce530e87aa9c1f9c bc5e93c5e755b29cad10a2f3991435 |
| 58ad3103295afcc22bde8d81e77c282f | 18b75949e03f8dcad513426f1f9f3ca209d779c24cd4e941d935633b1bec00cb  |
| 5be1e382cd9730fbe386b69bd8045ee7 | 5ad106e333de056eac78403b033b89c58b4c4bdda12e2f774625d47ccfd3d3ae  |
| 5c6f9c83426c6d33ff2d4e72c039b747 | a3b7e88d998078cfd8cdf37fa5454c45f6c bd65f4595fb94b2e9c85fe767ad47 |
| 640e70b0230dc026eff922fb1e44c2ea | 6319102bac226dfc117c3c9e620cd99c7e afbf3874832f2ce085850aa042f19c |
| 67f4dad1a94ed8a47283c2c0c05a7594 | 3fe624c33790b409421f4fa2bb8abfd701d f2231a959493c33187ed34bec0ae7 |
| 70652edadedbacfd30d33a826853467d | 196fb1b6eff4e7a049cea323459cfd6c0e3900d8d69e1d80bffaabd24c06eba   |
| 739812e2ae1327a94e441719b885bd19 | 6122c94cbfa11311bea7129ecd5aea6fae6c51d23228f7378b5f6b2398728f67  |
| 76c3d2092737d964dfd627f1ced0af80 | bffe910904efd1f69544daa9b72f2a70fb29f73c51070bde4ea563de862ce4b1  |
| 802e7d6e80d7a60e17f9ffbd62fcbbeb | 87bdb1de1dd6b0b75879d8b8aef80b562ec4fad365d7abbc629bcfc1d386afa6  |
| 827103a6b6185191fd5618b7e82da292 | --                                                                |
| 830bc975a04ab0f62bfedf27f7aca673 | --                                                                |
| 85995257ac07ae5a6b4a86758a2283d7 | --                                                                |
| 85f6e3e3f0bdd0c1b3084fc86ee59d19 | f1576627e8130e6d5fde0dbe3dffcc8bc9e ef1203d15fcf09cd877ced1ccc72a |
| 87a6bda486554ab16c82bdfb12452e8b | 980bb08ef3e8afcb8c0c1a879ec11c41b29fd30ac65436495e69de79c555b2be  |
| 891db50188a90ddacfaf7567d2d0355d | 0837dd54268c373069fc5c1628c6e3d75e b99c3b3efc94c45b73e2cf9a6f3207 |
| 894de380a249e677be2acb8fbdfba2ef | --                                                                |
| 8b395cc6ecdec0900facf6e93ec48fbb | --                                                                |

## Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

|                                   |                                                                  |
|-----------------------------------|------------------------------------------------------------------|
| 92a6c017830cda80133bf97eb77d3292  | d1aba3f95f11fc6e5fec7694d18891955b7ff097500e811ff4a5319f8f230be  |
| 9b0e7c460a80f740d455a7521f0eada1  | 45d8ac1ac692d6bb0fe776620371fca02b60cac8db23c4cc7ab5df262da42b78 |
| 9b9d4cb1f681f19417e541178d8c75d7  | f5f6e538001803b0aa008422caf2c3c2a79b2eeee9ddc7feda710e4aba96fea4 |
| a1f9e9f5061313325a275d448d4ddd59  | dfdd72c9ce1212f9d9455e2bca5a327c88d2d424ea5c086725897c83afc3d42d |
| a452a5f693036320b580d28ee55ae2a3  | 99b0056b7cc2e305d4ccb0ac0a8a270d3fceb21ef6fc2eb13521a930cea8bd9f |
| a6e1efd70a077be032f052bb75544358  | 3b9fe1713f638f85f20ea56fd09d20a96cd6d288732b04b073248b56cdaef878 |
| ad4eababfe125110299e5a24be84472e  | a557a0c67b5baa7cf64bd4d42103d3b2852f67acf96b4c5f14992c1289b55eaa |
| b1c1d28dc7da1d58abab73fa98f60a83  | 38491f48d0cbaab7305b5ddca64ba41a2beb89d81d5fb920e67d0c7334c89131 |
| b6f91a965b8404d1a276e43e61319931  | --                                                               |
| bdece9758bf34fcad9cba1394519019b  | 9d6de05f9a3e62044ad9ae66111308ccb9ed2ee46a3ea37d85afa92e314e7127 |
| c3850f4cc12717c2b54753f8ca5d5e0e  | 99b448e91669b92c2cc3417a4d9711209509274dab5d7582baacfab5028a818c |
| c50b839f2fc3ce5a385b9ae1c05def3a  | 458d258005f39d72ce47c111a7d17e8c52fe5fc7dd98575771640d9009385456 |
| cf236bf5b41d26967b1ce04ebbdbb4041 | 60425a4d5ee04c8ae09bfe28ca33bf9e76a43f69548b2704956d0875a0f25145 |
| d0e203e8845bf282475a8f816340f2e8  | f6375c5276d1178a2a0fe1a16c5668ce523e2f846c073bf75bb2558fdec06531 |
| ddb1f970371fa32faae61fc5b8423d4b  | dda53eee2c5cb0abdbf5242f5e82f4de83898b6a9dd8aa935c2be29bafc9a469 |
| f2f787868a3064407d79173ac5fc0864  | 92adc5ea29491d9245876ba0b2957393633c9998eb47b3ae1344c13a44cd59ae |
| fda3a19afa85912f6dc8452675245d6b  | 56925a1f7d853d814f80e98a1c4890b0a6a84c83a8eded34c585c98b2df6ab19 |
| --                                | 0054147db54544d77a9efd9baf5ec96a80b430e170d6e7c22fcf75261e9a3a71 |
| --                                | 151ab3e05a23e9ccd03a6c49830dabb9e9281faf279c31ae40b13e6971dd2fb8 |
| --                                | 1c926fb3bd99f4a586ed476e4683163892f3958581bf8c24235cd2a415513b7f |

## Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

|    |                                                                  |
|----|------------------------------------------------------------------|
| -- | 1f8dcfaebbcd7e71c2872e0ba2fc6db81d651cf654a21d33c78eae6662e62392 |
| -- | f226086b5959eb96bd30dec0ffcbf0f09186cd11721507f416f1c39901addafb |
| -- | 23eff00dde0ee27dabad28c1f4ffb8b09e876f1e1a77c1e6fb735ab517d79b76 |
| -- | 586f30907c3849c363145bfdcdabe3e2e4688cbd5688ff968e984b201b474730 |
| -- | 8ce219552e235dcaf1c694be122d6339ed4ff8df70bf358cd165e6eb487ccfc5 |
| -- | 90fb0cd574155fd8667d20f97ac464eca67bdb6a8ee64184159362d45d79b6a4 |
| -- | c2904dc8bbb569536c742fca0c51a766e836d0da8fac1c1abd99744e9b50164f |
| -- | ca932ccaa30955f2fffb1122234fb1524f7de3a8e0044de1ed4fe05cab8702a5 |
| -- | f6827dc5af661fbb4bf64bc625c78283ef836c6985bb2bfb836bd0c8d5397332 |
| -- | f78cabf7a0e7ed3ef2d1c976c1486281f56a6503354b87219b466f2f7a0b65c4 |

Table 3 lists MD5 and SHA256 hashes are associated with Maui Ransomware files.

Table 3: File names and hashes of Maui ransomware files

| MD5 Hash                          | SHA256 Hash                                                      |
|-----------------------------------|------------------------------------------------------------------|
| 4118d9adce7350c3eedeb056a3335346  | 5b7ecf7e9d0715f1122baf4ce745c5fcd769dee48150616753fec4d6da16e99e |
| 9b0e7c460a80f740d455a7521f0eada1  | 45d8ac1ac692d6bb0fe776620371fca02b60cac8db23c4cc7ab5df262da42b78 |
| fda3a19afa85912f6dc8452675245d6b  | 56925a1f7d853d814f80e98a1c4890b0a6a84c83a8eded34c585c98b2df6ab19 |
| 2d02f5499d35a8dfffb4c8bc0b7fec5c2 | 830207029d83fd46a4a89cd623103ba2321b866428aa04360376e6a390063570 |
| c50b839f2fc3ce5a385b9ae1c05def3a  | 458d258005f39d72ce47c111a7d17e8c52fe5fc7dd98575771640d9009385456 |
| a452a5f693036320b580d28ee55ae2a3  | 99b0056b7cc2e305d4ccb0ac0a8a270d3fceb21ef6fc2eb13521a930cea8bd9f |

## Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

|                                   |                                                                  |
|-----------------------------------|------------------------------------------------------------------|
| a6e1efd70a077be032f052bb75544358  | 3b9fe1713f638f85f20ea56fd09d20a96cd6d288732b04b073248b56cdaef878 |
| 802e7d6e80d7a60e17f9ffbd62fcbbbeb | 87bdb1de1dd6b0b75879d8b8aef80b562ec4fad365d7abbc629bcfc1d386afa6 |
| --                                | 0054147db54544d77a9efd9baf5ec96a80b430e170d6e7c22fcf75261e9a3a71 |

Table 4 lists MD5 and SHA256 hashes associated with H0lyGh0st Ransomware files.

Table 4: File names and hashes of H0lyGh0st ransomware files

| SHA256 Hash                                                       |
|-------------------------------------------------------------------|
| 99fc54786a72f32fd44c7391c2171ca31e72ca52725c68e2dde94d04c286fccd* |
| F8fc2445a9814ca8cf48a979bff7f182d6538f4d1ff438cf259268e8b4b76f86* |
| Bea866b327a2dc2aa104b7ad7307008919c06620771ec3715a059e675d9f40af* |
| 6e20b73a6057f8ff75c49e1b7aef08abfcfe4e418e2c1307791036f081335c2d  |
| f4d10b08d7dacd8fe33a6b54a0416eecdad92c69c933c4a5d3700b8f5100fad   |
| 541825cb652606c2ea12fd25a842a8b3456d025841c3a7f563655ef77bb67219  |
| 2d978df8df0cf33830aba16c6322198e5889c67d49b40b1cb1eb236bd366826d  |
| 414ed95d14964477bebf86dced0306714c497cde14dede67b0c1425ce451d3d7  |
| Df0c7bb88e3c67d849d78d13cee30671b39b300e0cda5550280350775d5762d8  |
| MD5 Hash                                                          |
| a2c2099d503fcc29478205f5aef0283b                                  |
| 9c516e5b95a7e4169ecbd133ed4d205f                                  |
| d6a7b5db62bf7815a10a17cdf7ddb4b                                   |
| c6949a99c60ef29d20ac8a9a3fb58ce5                                  |
| 4b20641c759ed563757cdd95c651ee53                                  |
| 25ee4001eb4e91f7ea0bc5d07f2a9744                                  |
| 29b6b54e10a96e6c40e1f0236b01b2e8                                  |
| 18126be163eb7df2194bb902c359ba8e                                  |
| eaf6896b361121b2c315a35be837576d                                  |
| e4ee611533a28648a350f2dab85bb72a                                  |
| e268cb7ab778564e88d757db4152b9fa                                  |

\* from [Microsoft blog post on h0lygh0st](#)