JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA22-294A

October 21, 2022

#StopRansomware: Daixin Team

SUMMARY

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

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and Department of Health and Human Services (HHS) are releasing this joint CSA to provide information on the "Daixin Team," a cybercrime group that is actively targeting U.S. businesses, predominantly in the Healthcare and Public Health (HPH) Sector, with ransomware and data extortion operations.

This joint CSA provides TTPs and IOCs of Daixin actors obtained from FBI threat response activities and third-party reporting.

Actions to take today to mitigate cyber threats from ransomware:

- Install updates for operating systems, software, and firmware as soon as they are released.
- Require phishing-resistant MFA for as many services as possible.
- Train users to recognize and report phishing attempts.

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 11. See MITRE ATT&CK for Enterprise for all referenced tactics and techniques.

Cybercrime actors routinely target HPH Sector organizations with ransomware:

- As of October 2022, per FBI Internet Crime Complaint Center (IC3) data, specifically victim reports across all 16 critical infrastructure sectors, the HPH Sector accounts for 25 percent of ransomware complaints.

All organizations should report incidents and anomalous activity to CISA's 24/7 Operations Center at report@cisa.gov or (888) 282-0870 and/or to the FBI via your local FBI field office. 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.

- According to an IC3 annual report in 2021, 649 ransomware reports were made across 14 critical infrastructure sectors; the HPH Sector accounted for the most reports at 148.

The Daixin Team is a ransomware and data extortion group that has targeted the HPH Sector with ransomware and data extortion operations since at least June 2022. Since then, Daixin Team cybercrime actors have caused ransomware incidents at multiple HPH Sector organizations where they have:

- Deployed ransomware to encrypt servers responsible for healthcare services—including electronic health records services, diagnostics services, imaging services, and intranet services, and/or
- Exfiltrated personal identifiable information (PII) and patient health information (PHI) and threatened to release the information if a ransom is not paid.

Daixin actors gain initial access to victims through virtual private network (VPN) servers. In one confirmed compromise, the actors likely exploited an unpatched vulnerability in the organization's VPN server [T1190]. In another confirmed compromise, the actors used previously compromised credentials to access a legacy VPN server [T1078] that did not have multifactor authentication (MFA) enabled. The actors are believed to have acquired the VPN credentials through the use of a phishing email with a malicious attachment [T1598.002].

After obtaining access to the victim's VPN server, Daixin actors move laterally via Secure Shell (SSH) [T1563.001] and Remote Desktop Protocol (RDP) [T1563.002]. Daixin actors have sought to gain privileged account access through credential dumping [T1003] and pass the hash [T1550.002]. The actors have leveraged privileged accounts to gain access to VMware vCenter Server and reset account passwords [T1098] for ESXi servers in the environment. The actors have then used SSH to connect to accessible ESXi servers and deploy ransomware [T1486] on those servers.

According to third-party reporting, the Daixin Team's ransomware is based on leaked Babuk Locker source code. This third-party reporting as well as FBI analysis show that the ransomware targets ESXi servers and encrypts files located in `/vmfs/volumes/` with the following extensions: `.vmdk`, `.vmem`, `.vswp`, `.vmsd`, `.vmx`, and `.vmsn`. A ransom note is also written to `/vmfs/volumes/`. See Figure 1 for targeted file system path and Figure 2 for targeted file extensions list. Figure 3 and Figure 4 include examples of ransom notes. Note that in the Figure 3 ransom note, Daixin actors misspell "Daixin" as "Daxin."

```
mov     edi, 0Ah        ; c
call    _putchar
mov     edi, offset aVmfsVolumes ; "/vmfs/volumes"
call    __Files_and_encryption ; this sub does:
```

Figure 1: Daixin Team – Ransomware Targeted File Path

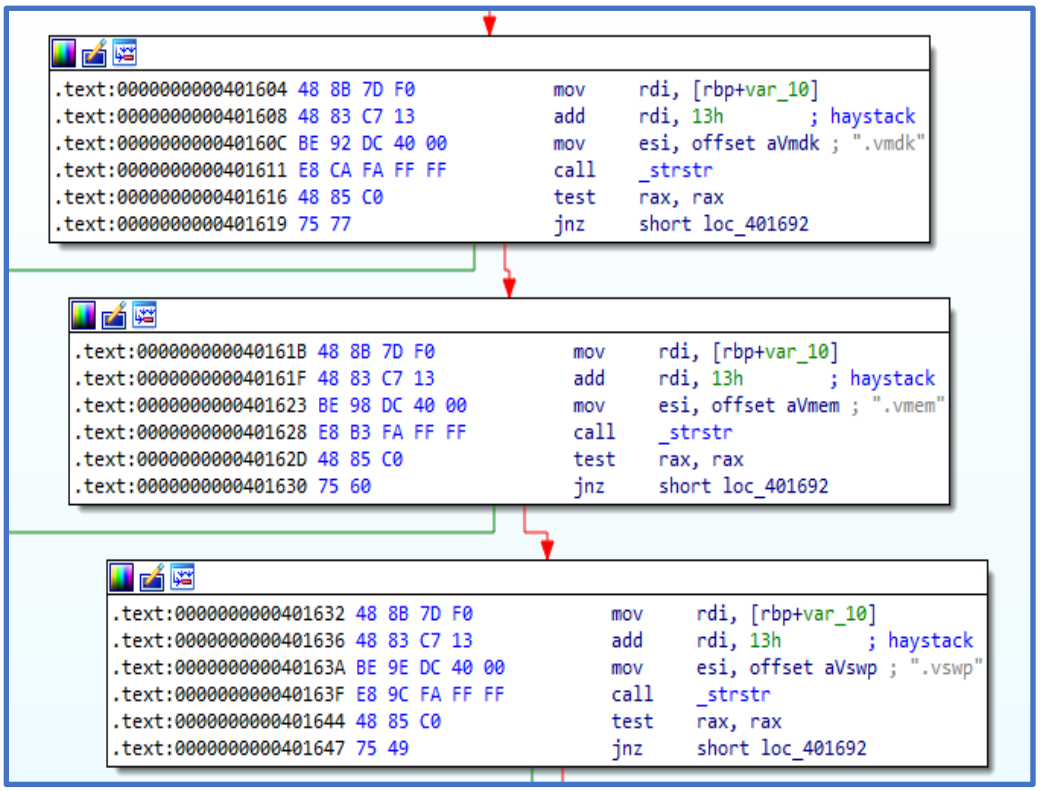

Figure 2: Daixin Team – Ransomware Targeted File Extensions

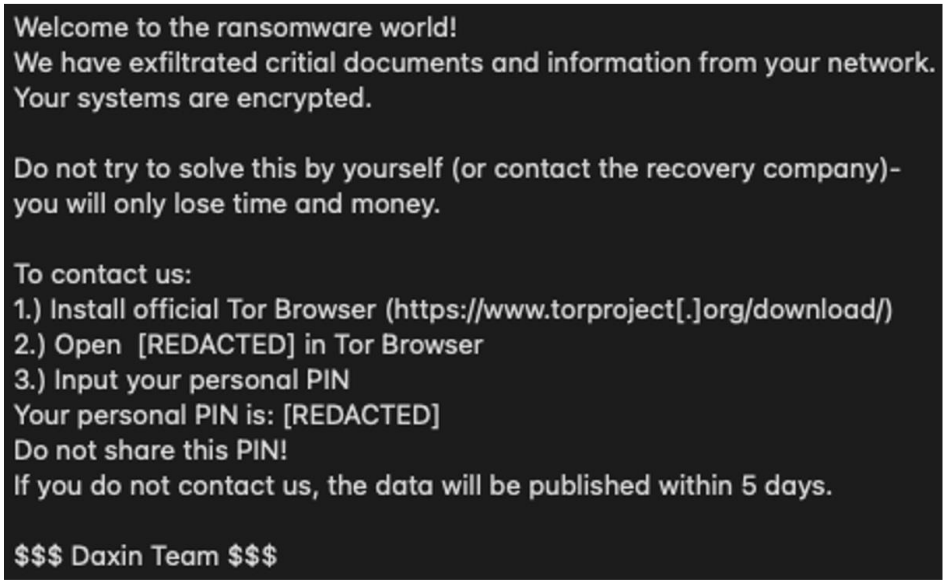

Figure 3: Example 1 of Daixin Team Ransomware Note

```
db 'Welcome to the ransomware world!',0Ah
                        ; DATA XREF: __Files_and_encryption+A8↑o
db 'We have exfiltrated critial documents and information from your n'
db 'etwork.',0Ah
db 'Your systems are encrypted.',0Ah
db 0Ah
db 'Do not try to solve this by yourself (or contact the recovery com'
db 'pany)-',0Ah
db 'you will only lose time and money.',0Ah
db 0Ah
db 'To contact us:',0Ah
```

Figure 4: Example 2 of Daixin Team Ransomware Note

In addition to deploying ransomware, Daixin actors have exfiltrated data [TA0010] from victim systems. In one confirmed compromise, the actors used Rclone—an open-source program to manage files on cloud storage—to exfiltrate data to a dedicated virtual private server (VPS). In another compromise, the actors used Ngrok—a reverse proxy tool for proxying an internal service out onto an Ngrok domain—for data exfiltration [T1567].

MITRE ATT&CK TACTICS AND TECHNIQUES

See Table 1 for all referenced threat actor tactics and techniques included in this advisory.

Table 1: Daixin Actors' ATT&CK Techniques for Enterprise

Reconnaissance		
Technique Title	**ID**	**Use**
Phishing for Information: Spearphishing Attachment	T1598.002	Daixin actors have acquired the VPN credentials (later used for initial access) by a phishing email with a malicious attachment.
Initial Access		
Technique Title	**ID**	**Use**
Exploit Public-Facing Application	T1190	Daixin actors exploited an unpatched vulnerability in a VPN server to gain initial access to a network.

Valid Accounts	T1078	Daixin actors use previously compromised credentials to access servers on the target network.
Persistence		
Technique Title	**ID**	**Use**
Account Manipulation	T1098	Daixin actors have leveraged privileged accounts to reset account passwords for VMware ESXi servers in the compromised environment.
Credential Access		
Technique Title	**ID**	**Use**
OS Credential Dumping	T1003	Daixin actors have sought to gain privileged account access through credential dumping.
Lateral Movement		
Technique Title	**ID**	**Use**
Remote Service Session Hijacking: SSH Hijacking	T1563.001	Daixin actors use SSH and RDP to move laterally across a network.
Remote Service Session Hijacking: RDP Hijacking	T1563.002	Daixin actors use RDP to move laterally across a network.
Use Alternate Authentication Material: Pass the Hash	T1550.002	Daixin actors have sought to gain privileged account access through pass the hash.
Exfiltration		

Technique Title	ID	Use
Exfiltration Over Web Service	T1567	Daixin Team members have used Ngrok for data exfiltration over web servers.
Impact		
Technique Title	**ID**	**Use**
Data Encrypted for Impact	T1486	Daixin actors have encrypted data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources.

INDICATORS OF COMPROMISE

See Table 2 for IOCs obtained from third-party reporting.

Table 2: Daixin Team IOCs – Rclone Associated SHA256 Hashes

File	SHA256
rclone-v1.59.2-windows-amd64\git-log.txt	9E42E07073E03BDEA4CD978D9E7B44A9574972818593306BE1F3DCFDEE722238
rclone-v1.59.2-windows-amd64\rclone.1	19ED36F063221E161D740651E6578D50E0D3CACEE89D27A6EBED4AB4272585BD
rclone-v1.59.2-windows-amd64\rclone.exe	54E3B5A2521A84741DC15810E6FED9D739EB8083CB1FE097CB98B345AF24E939
rclone-v1.59.2-windows-amd64\README.html	EC16E2DE3A55772F5DFAC8BF8F5A365600FAD40A244A574CBAB987515AA40CBF
rclone-v1.59.2-windows-amd64\README.txt	475D6E80CF4EF70926A65DF5551F59E35B71A0E92F0FE4DD28559A9DEBA60C28

MITIGATIONS

FBI, CISA, and HHS urge HPH Sector organizations to implement the following to protect against Daixin and related malicious activity:

- Install updates for operating systems, software, and firmware as soon as they are released. Prioritize patching VPN servers, remote access software, virtual machine software, and known

exploited vulnerabilities. Consider leveraging a centralized patch management system to automate and expedite the process.

- Require phishing-resistant MFA for as many services as possible—particularly for webmail, VPNs, accounts that access critical systems, and privileged accounts that manage backups.
- If you use Remote Desktop Protocol (RDP), secure and monitor it.
    - 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 business purposes (e.g., RDP Transmission Control Protocol Port 3389).
- Turn off SSH and other network device management interfaces such as Telnet, Winbox, and HTTP for wide area networks (WANs) and secure with strong passwords and encryption when enabled.
- Implement and enforce multi-layer network segmentation with the most critical communications and data resting on the most secure and reliable layer.
- 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.
- Secure PII/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.
- 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 HHS 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 applicable state data breach laws and consult legal counsel when necessary.
        - 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

- 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.
- 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.
- Use strong passwords and avoid reusing passwords for multiple accounts. See CISA Tip Choosing and Protecting Passwords and the National Institute of Standards and Technology's (NIST's) 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 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: FBI, CISA, and HHS strongly discourage paying ransoms as doing so does not guarantee files and records will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities.

REFERENCES

- Stopransomware.gov is a whole-of-government approach that gives one central location for ransomware resources and alerts.
- Resource to mitigate a ransomware attack: CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide.
- No-cost cyber hygiene services: Cyber Hygiene Services and Ransomware Readiness Assessment.

- Ongoing Threat Alerts and Sector alerts are produced by the Health Sector Cybersecurity Coordination Center (HC3) and can be found at hhs.gov/HC3
- For additional best practices for Healthcare cybersecurity issues see the HHS 405(d) Aligning Health Care Industry Security Approaches at 405d.hhs.gov

REPORTING

The FBI is seeking any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, a sample ransom note, communications with Daixin Group actors, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file. Regardless of whether you or your organization have decided to pay the ransom, the FBI, CISA, and HHS urge you to promptly report ransomware incidents to a local FBI Field Office, or CISA at cisa.gov/report.

ACKNOWLEDGEMENTS

FBI, CISA, and HHS would like to thank CrowdStrike and the Health Information Sharing and Analysis Center (Health-ISAC) for their contributions to this CSA.

DISCLAIMER

The information in this report is being provided “as is” for informational purposes only. FBI, CISA, and HHS do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by FBI, CISA, or HHS.