MyCERT : Advisories - Ransomware Group Daixin Team

Archived: 2026-04-05 17:12:14 UTC

1.0 Introduction

On 21 October 2022, The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and Department of Health and Human Services (HHS) released a joint Cyber Security Advisory (CSA) to provide information on the “Daixin Team”.

The Daixin Team is a ransomware and data extortion group that has targeted the Healthcare and Public Health (HPH) Sector with ransomware and data extortion operations since at least June 2022.

MyCERT has also received an incident report this year with similar activities by Daixin Team within the constituency, targeting the Critical National Information Infrastructure (CNII) organisation. Based on the incident report, we discovered that the Threat Actor (TA) is not only targeting companies based on particular industry type, geo-location, or political motivation.

Ransomware is a type of malicious software (malware) that infects a computer or any system and restricts access to it until a ransom is paid. This type of malware, which has now been observed for several years, attempts to extort money from victims by displaying an on-screen ransom note. These ransom notes often state that their computer or system has been locked or that all their files have been encrypted and demand that a ransom be paid to restore access. In some instances, the threat actors also threaten victims if a ransom is not paid, their data will be exposed on the Internet.

The present advisory provides the Technique, Tactic and Procedure (TTP) and Indicator of Compromise (IOCs) associated with the Daixin TA, primarily obtained from FBI threat response activities and MyCERT incident report.

2.0 Impact

- Deployed ransomware to encrypt servers responsible for services in the organisation — i.e. electronic health records services, diagnostics services, imaging services, and intranet services.
- Exfiltrated personal identifiable information (PII) and other sensitive information such as patient data, employee personal details.
- Leave an on-screen ransom note to request the victim organisation to pay a ransom and threaten to leak the information if a ransom is not paid.
- Leak the victim organisation's personal information and put the information for sale on the dark web.

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.

3.0 Indicators of Compromise (IoCs)

Daixin TA gained initial access to victims' networks through virtual private network (VPN) servers. In one confirmed compromise, the actors likely exploited an unpatched vulnerability in the organisation's VPN server. In another confirmed compromise, the actors used previously compromised credentials to access a legacy VPN server 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 sent to potential staff members with a malicious attachment.

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

According to some trusted information, the ransomware used by the Daixin TA is based on leaked Babuk Locker ransomware source code. Based on some trusted information and FBI analysis show that the ransomware targets ESXi servers and encrypts files 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 the targeted file system path and Figure 2 for the targeted file extensions list. Figure 3 includes a sample of a ransom note. In Figure 3, it is noticeable that Daixin TA misspells "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

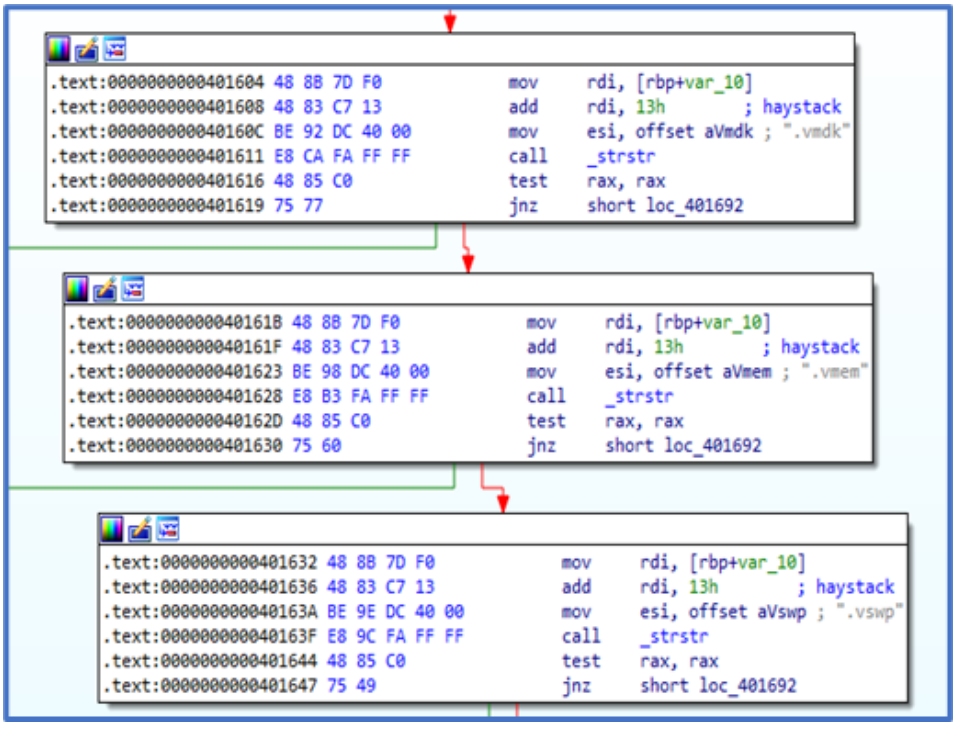

Figure 2: Daixin Team – Ransomware Targeted File Extensions

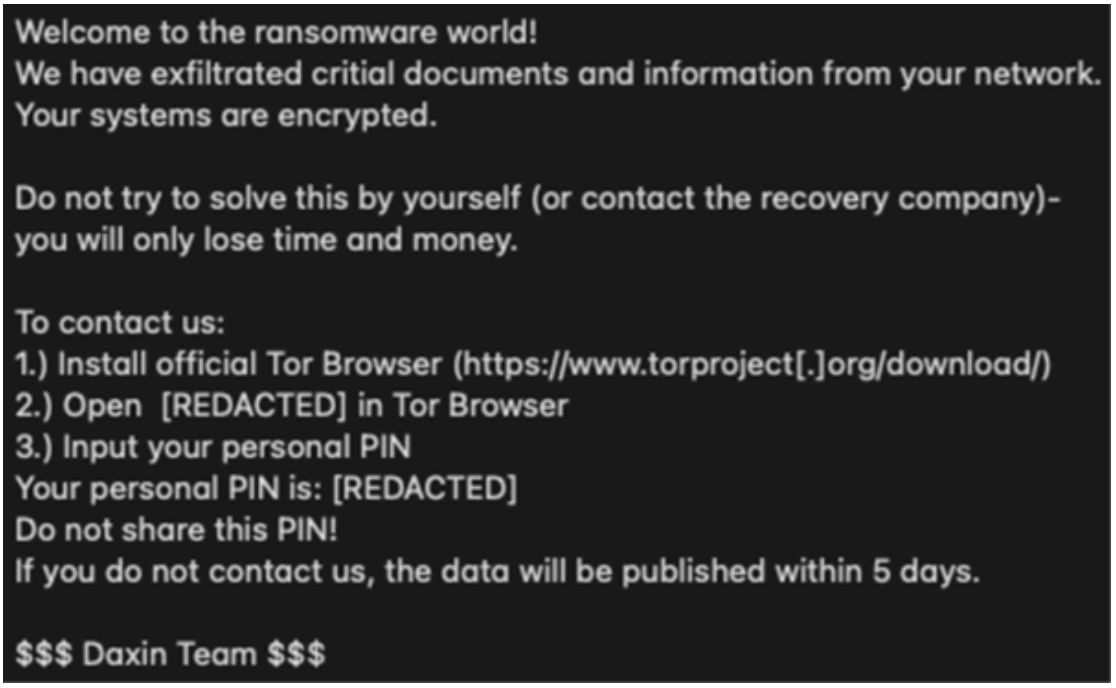

Figure 3: Example 1 of Daixin Team Ransom Note

In addition to deploying ransomware, Daixin TA has exfiltrated data 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 a Ngrok domain—for data exfiltration.

The table below shows the IOCs associated with the Daixin TA activities.

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

Table 2: *Daixin Team IOCs – Rclone Associated SHA256 Hashes*

4.0 Recommendations

MyCERT urges organisations to implement the following best practices to defend against malicious activities associated with the Daixin TA:

- Install updates for operating systems, software, and firmware as soon as they are released. Prioritise patching VPN servers, remote access software, virtual machine software, and known exploited vulnerabilities. Consider leveraging a centralised patch management system to automate and expedite the process.
- Consider 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 the 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 devices management interfaces such as Telnet, Winbox, and HTTP for wide area networks (WANs) and secure with strong passwords and encryption when enabled.
- In general, it is best to disable services that are not in use and whitelist applications that are only allowed to be used.
- 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 the least privilege.
- Secure PII at collection points and encrypt the data at rest and in transit by using technologies such as Transport Layer Security (TPS). Only store personal 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.
- Use monitoring tools to observe whether IoT devices are behaving erratically due to a compromise.
- Establish and regularly review internal security policies that regulate the collection, storage, access, and monitoring of personal and sensitive data belonging to the organisations.
- Implement network segmentation to separate critical areas from non-critical areas to prevent threat propagation and strengthen organisations' security policies.
- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
- Organisations are recommended to educate their employees on safe email practices and general security awareness, which helps to prevent attacks targeting end-users or employees.

4.0 Best Practices for Business Continuity after any Ransomware Attack:

- Identify affected machines and isolate affected systems. Disconnect them immediately to prevent the attack becomes widespread in the network.
- Identify the ransomware variant using Crypto Sheriff by The No More Ransom! Project to understand the tactics and techniques used by the ransomware variant to infiltrate the network.
- Reimage infected machines for investigation and postmortem analysis.
- Restore systems using clean, good working backup and perform a password reset exercise to all systems after restoration is completed.
- Review existing security tools and logs to detect vectors/vulnerabilities that caused the attack and patch them during the recovery process to prevent future attacks.
- Implement Business Continuity Plan (BCP). Ideally, operational departments, key decision-makers, and relevant stakeholders are familiar with the plan and able to execute it accordingly.
- In principle, we advise victims to avoid paying the ransom as this increases malicious activity, and more often, the decryption key does not guarantee full recovery of the encrypted data. However, the decision to pay or not to pay a ransom is within the victim.

For further enquiries, please get in touch with MyCERT through the following channels:

E-mail: cyber999[at]cybersecurity.my
Phone: 1-300-88-2999 (monitored during business hours)
Mobile: +60 19 2665850 (24x7 call incident reporting)
Business Hours: Mon - Fri 09:00 -18:00 MYT
Web: https://www.mycert.org.my
Twitter: https://twitter.com/mycert
Facebook: https://www.facebook.com/mycert.org.my

5.0 References

- https://www.cisa.gov/uscert/ncas/alerts/aa22-294a
- https://www.mycert.org.my/portal/advisory?id=MA-824.122021
- https://www.bleepingcomputer.com/news/security/us-govt-warns-of-daixin-team-targeting-health-orgs-with-ransomware/amp/
- https://www.mitre.org
