Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Daixin Team Ransomware: A Growing Cyber Threat

Date of Publication	Admiralty Code	TA Number
January 31, 2025	A1	TA2025028

Summary

First Appearance: 2022
Malware: Daixin Team ransomware
Targeted Region: Worldwide
Affected Platforms: Windows, Linux and VMware ESXi
Targeted Industries: Healthcare, Media, Government, Hospitality, Agriculture, Technology, Manufacturing, Energy, and Aviation
Attack: The Daixin Team is a ransomware group known for targeting healthcare, government, and enterprise sectors, especially VMware ESXi servers. They exploit VPN vulnerabilities, phishing, and weak authentication to gain access, then exfiltrate and encrypt sensitive data. Notably, they claimed responsibility for a June 2024 attack on Dubai Municipality, stealing up to 80GB of sensitive information. Their expanding attacks highlight the need for strong cybersecurity measures, including MFA, regular patching, and network monitoring.

Attack Regions

Daixin Team
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 The Daixin Team is a ransomware and data extortion group that has emerged as a significant threat, particularly targeting Healthcare and Government sectors since at least June 2022. This group has gained notoriety for double extortion tactics, where they not only encrypt files but also steal sensitive data, threatening to leak it unless a ransom is paid. Their primary targets include Windows and Linux environments, with a specific focus on VMware ESXi servers, which are widely used in enterprise and government IT infrastructure.

#2 The Daixin Team typically gains entry through Virtual Private Network (VPN) servers by exploiting vulnerabilities, using phishing emails, or leveraging the absence of Multi-Factor Authentication (MFA). In some cases, they use compromised credentials to access legacy VPN systems. After initial access, the group moves laterally within the network using protocols such as Remote Desktop Protocol (RDP) and Secure Shell (SSH). They often achieve privileged access through techniques like credential dumping and pass-the-hash attacks.

#3 Before deploying ransomware, Daixin actors exfiltrate sensitive data, including Personally Identifiable Information (PII) and Patient Health Information (PHI). This data is used as leverage to coerce victims into paying ransoms. The ransomware used by Daixin is based on the leaked Babuk Locker source code. It specifically targets ESXi servers, encrypting files with extensions such as .vmdk, .vmem, .vswp, .vmsd, .vmx, and .vmsn. A ransom note is typically left in the encrypted directories.

#4 In June 2024, the Daixin Team claimed responsibility for a cyberattack on Dubai Municipality, reportedly stealing between 60 to 80 GB of sensitive data. The stolen information included government employee ID cards, passports, personal details, housing records, business documents, and land ownership data. However, as of now, Dubai Municipality has not released an official statement regarding the incident, and their website remains operational.

#5 In recent months, the Daixin Team has claimed responsibility for various attacks beyond healthcare, including incidents involving media and hospitality sectors, indicating their expanding target range. The Daixin Team's activities highlight an ongoing trend in cybercrime where attackers target high-profile entities to maximize their impact.

Recommendations

Implement Robust Endpoint Protection: Deploy advanced endpoint protection solutions that include behavior-based detection, machine learning algorithms, and threat intelligence. These solutions can detect and block malicious activities associated with Daixin Team ransomware, such as file encryption and unauthorized processes. Regularly update endpoint security software to ensure protection against the latest threats.

Patch and Update Software: Keep all operating systems, applications, and firmware up to date with the latest security patches and updates. By promptly applying patches, organizations can mitigate the risk of these vulnerabilities being exploited and prevent unauthorized access to their networks.

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, store them securely offline. Test restoration processes to ensure backup integrity and availability. In case of a Daixin Team ransomware attack, up-to-date backups enable recovery without paying the ransom.

Strengthen Access Controls: Implement Multi-Factor Authentication (MFA) for all remote access solutions, including VPNs and administrative accounts, to prevent unauthorized access. Enforce strong password policies with complex, unique passwords and regular rotation. Limit privileged access by following the principle of least privilege (PoLP) to restrict administrative rights to only essential users.

Network Segmentation: Divide the network into segments to limit the spread of ransomware. This can help contain the damage and protect sensitive data.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0003 Persistence	TA0006 Credential Access
TA0008 Lateral Movement	TA0010 Exfiltration	TA0040 Impact	T1598 Phishing for Information
T1598.002 Spearphishing Attachment	T1190 Exploit Public-Facing Application	T1078 Valid Accounts	T1098 Account Manipulation
T1003 OS Credential Dumping	T1563 Remote Service Session Hijacking	T1563.001 SSH Hijacking	T1563.002 RDP Hijacking

T1550 Use Alternate Authentication Material	**T1550.002** Pass the Hash	**T1567** Exfiltration Over Web Service	**T1486** Data Encrypted for Impact

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	9E42E07073E03BDEA4CD978D9E7B44A9574972818593306BE1F3DCFDEE722238, 19ED36F063221E161D740651E6578D50E0D3CACEE89D27A6EBED4AB4272585BD, 54E3B5A2521A84741DC15810E6FED9D739EB8083CB1FE097CB98B345AF24E939, EC16E2DE3A55772F5DFAC8BF8F5A365600FAD40A244A574CBAB987515AA40CBF, 475D6E80CF4EF70926A65DF5551F59E35B71A0E92F0FE4DD28559A9DEBA60C28
File Path	rclone-v1.59.2-windows-amd64\git-log.txt, rclone-v1.59.2-windows-amd64\rclone.1, rclone-v1.59.2-windows-amd64\rclone.exe, rclone-v1.59.2-windows-amd64\README.html, rclone-v1.59.2-windows-amd64\README.txt
TOR Address	7ukmkdtyxdkdivtjad57klqnd3kdsmq6tp45rrsxqnu76zzv3jvitlqd[.]onion, 232fwh5cea3ub6qguz3pynijxfzl2uj3c73nbrayipf3gq25vtq2r4qd[.]onion

Recent Breaches

https://communicare.org
https://www.sgsco.com
https://acadianambulance.com
https://www.dm.gov.ae
https://www.omnihotels.com

References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-294a

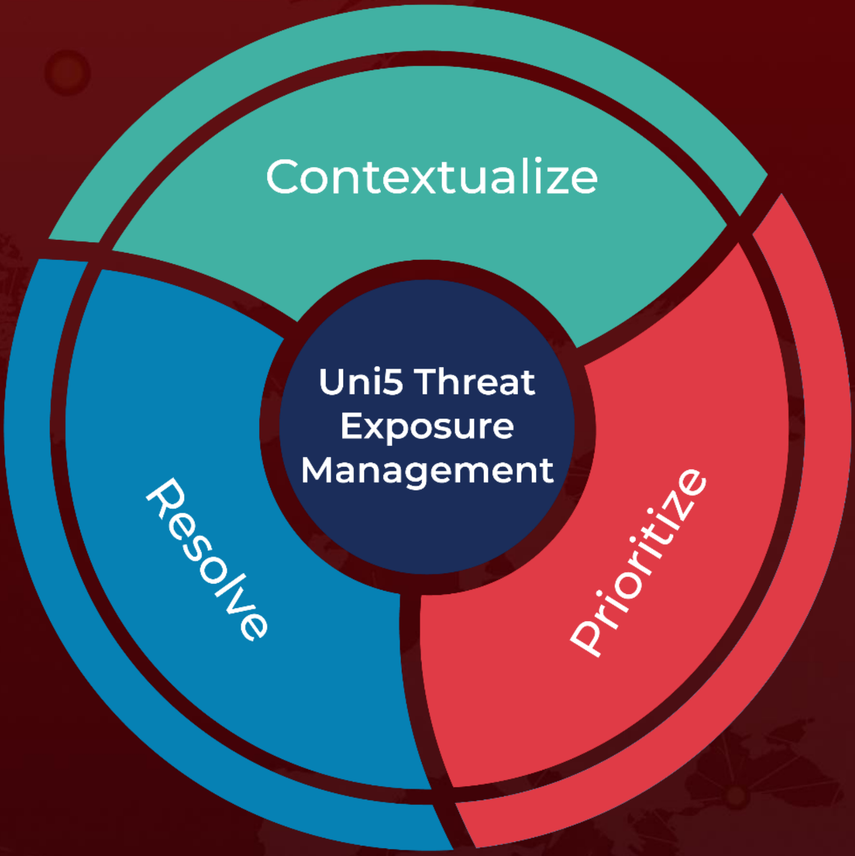
https://cybernews.com/news/dubai-government-ransomware-attack-daixin/

https://hivepro.com/threat-advisory/us-healthcare-organizations-targeted-by-daixin-team-ransomware/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 31, 2025 • 9:30 AM

More at www.hivepro.com