Hive Pro

Threat Level

Red

THREAT ADVISORY

ACTOR REPORT

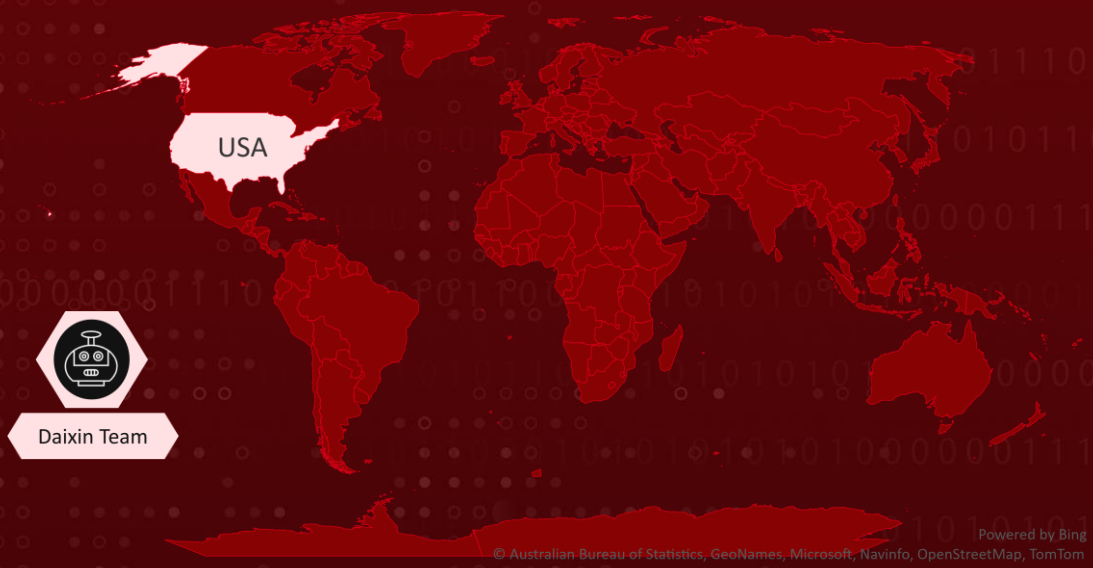
US healthcare organizations targeted by Daixin Team ransomware

Date of Publication	Admiralty code	TA Number
October 25, 2022	A1	TA2022231

Summary

Daixin Team ransomware, and data extortion group has been gaining initial access to victims through virtual private networks (VPN) servers since June 2022, either by exploiting an unpatched vulnerability in the organization's VPN server or using compromised credentials to access a legacy VPN server in order to deploy ransomware and exfiltrate data.

Actor Map



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

Technical Details

#1 As soon as Daixin has gained access to the victim's VPN server, they move laterally via Secure Shell (SSH) and Remote Desktop Protocol (RDP).

#2 Daixin team accessed privileged accounts through credential dumping. Once privileged accounts were accessed, the actors reset account passwords for ESXi servers in the environment using VMware vCenter Server. As a result, the actors used SSH to connect to accessible ESXi servers and deploy ransomware.

#3 A leaked Babuk Locker source code is used by Daixin Team's ransomware. Daixin team has also used Rclone and Ngrok to exfiltrate data from victim systems.

Actor Detail

NAME	ORIGIN	TARGET COUNTRIES	TARGET INDUSTRIES
Daixin Team	Unknown	United States of America	Energy, Media and Healthcare
	MOTIVE		
	Financial gain		

Indicator of Compromise (IOC)

TYPE	VALUE
SHA256	9E42E07073E03BDEA4CD978D9E7B44A9574972818593306BE1F3DCFDEE722238 19ED36F063221E161D740651E6578D50E0D3CACEE89D27A6EBED4AB4272585BD

TYPE	VALUE
SHA256	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

Recent Breaches

https://www.ista.com/corporate/

https://oakbendmedicalgroup.com/

http://tribtotalmedia.com/

http://www.fitzgibbon.org/

References

https://www.cisa.gov/uscert/ncas/alerts/aa22-294a

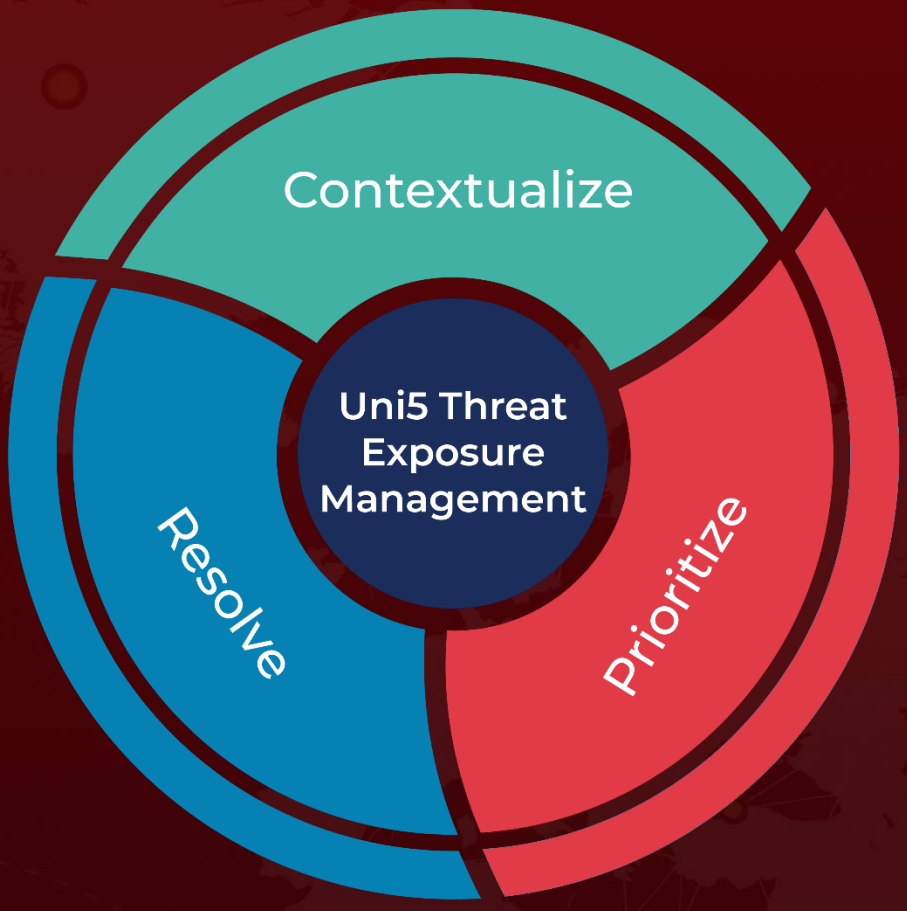
https://thehackernews.com/2022/10/cisa-warns-of-daixin-team-hackers.html

https://healthitsecurity.com/news/daixin-team-ransomware-group-actively-targeting-healthcare-sector

What Next?

At **HivePro**, 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 **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

October 25, 2022 • 6:15 AM

More at www.hivepro.com