Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

CryptNet A Novel Ransomware-as-a-Service

Date of Publication	Admiralty Code	TA Number
May 19, 2023	A1	TA2023238

Summary

First seen: April 2023
Malware: CryptNet
Attack Region: Worldwide
Targeted Sectors: Internet Software & Services, Trading Companies & Distributors
Attack: CryptNet is a new ransomware-as-a-service group that employs data exfiltration and .NET code. Currently, it has two victims listed on its data leak site.

Attack Regions

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 In April 2023, a newly surfaced ransomware-as-a-service entity called CryptNet emerged. This group asserts its ability to extract data before encrypting files, and it operates a data leak site on a Tor hidden service, presently featuring two victims. The CryptNet ransomware employs the .NET framework and utilizes obfuscation through .NET Reactor.

#2 Upon removing the obfuscation layer, similarities between CryptNet and the Chaos ransomware families, specifically the latest variant known as Yashma, become apparent. These similarities encompass encryption techniques, the ability to disable backup services, and the deletion of shadow copies.

#3 As CryptNet carries out the encryption procedure, it leaves behind a ransom note named "RESTORE-FILES-[9 random characters].txt". Additionally, if the ransomware possesses administrator privileges, it will eliminate Windows shadow copies and delete the backup catalog.

Recommendations

Strengthen Backup Systems: Given CryptNet's capability to disable backup services and delete shadow copies, it is crucial to reinforce backup systems by implementing robust security measures and regularly testing the effectiveness of backup and recovery processes.

Heighten Security Awareness: As CryptNet leverages data exfiltration and operates a data leak site, organizations should prioritize security awareness training for employees, emphasizing the importance of identifying suspicious emails, practicing safe browsing habits, and adhering to strict data protection protocols.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0009 Collection	TA0011 Command and Control	TA0040 Impact
T1047 Windows Management Instrumentation	T1053 Scheduled Task/Job	T1129 Shared Modules	T1027 Obfuscated Files or Information
T1027.002 Software Packing	T1036 Masquerading	T1070 Indicator Removal	T1070.004 File Deletion
T1070.006 Timestomp	T1140 Deobfuscate/Decode Files or Information	T1222 File and Directory Permissions Modification	T1497 Virtualization/Sandbox Evasion
T1562 Impair Defenses	T1562.001 Disable or Modify Tools	T1010 Application Window Discovery	T1033 System Owner/User Discovery
T1057 Process Discovery	T1082 System Information Discovery	T1083 File and Directory Discovery	T1087 Account Discovery
T1518 Software Discovery	T1518.001 Security Software Discovery	T1560 Archive Collected Data	T1486 Data Encrypted for Impact
T1490 Inhibit System Recovery	T1491 Defacement		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	2e37320ed43e99835caa1b851e963ebbf153f16cbe395f259bd2200d14c7b775 1cc7283ee218081f2f056bd2ec70514e86b8dcb921342dc9aed69e7480dec18e

Recent Breaches

http://www.urbanimport.com

http://www.exporthub.com

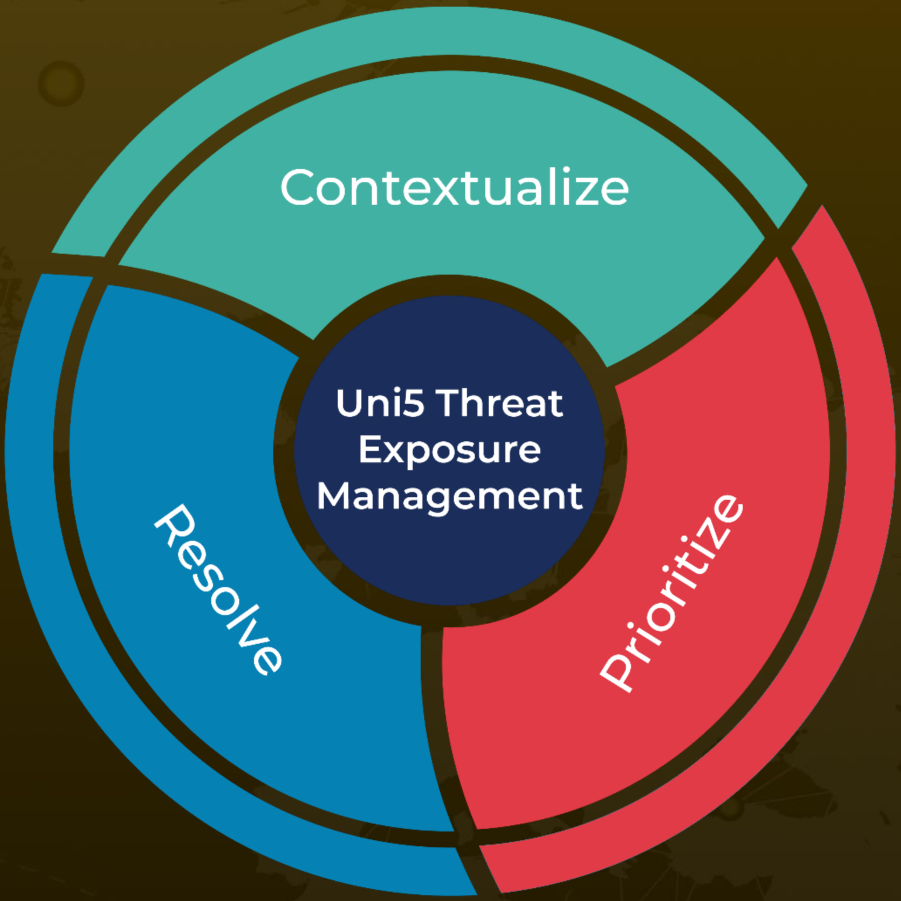
References

https://www.zscaler.com/blogs/security-research/technical-analysis-cryptnet-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

May 19, 2023 • 6:24 AM

More at www.hivepro.com