Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Trinity Ransomware Strikes with the Dual Extortion Strategy

Date of Publication	Admiralty Code	TA Number
May 15, 2024	A1	TA2024187

Summary

First Seen: 2024
Malware: Trinity Ransomware
Attack Region: Worldwide
Attack: A newly identified strain of ransomware named Trinity, has surfaced. The ransomware displays pronounced resemblances to the 2023Lock strain. Trinity adopts a dual extortion tactic, beginning with data extraction from victims prior to initiating encryption.

Attack Regions

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

Attack Details

#1 A newly identified strain of ransomware, named Trinity. 2023Lock ransomware displays striking similarities in its ransom note structure and foundational code with Trinity, suggesting it could be a derivative of the latter.

#2 Additionally, noticeable resemblances between Trinity and the Venus ransomware are apparent, particularly in their use of registry values and naming conventions for mutexes. Upon execution, Trinity ransomware initiates various operations, including scanning for a ransom note embedded within its binary file, halting its execution promptly if the note is inaccessible.

#3 Trinity proceeds to collect detailed system information such as processor counts, thread pools, and available drives, crucial for its complex multi-threaded encryption process.

#4 Following this, the ransomware attempts to elevate its privileges by assuming the identity token of a legitimate process, thus bypassing security protocols. It also engages in network reconnaissance and lateral movements, demonstrating its extensive attack capabilities.

#5 Trinity employs a dual extortion strategy to target its victims, with perpetrators seemingly extracting data before initiating encryption. Notably, these malicious actors maintain both a support platform for victims and a platform for leaking sensitive information.

#6 For encryption, Trinity utilizes the robust ChaCha20 algorithm. It delivers ransom demands in both textual and .hta formats, alters desktop wallpapers through registry modifications, and appends a ".trinitylock" extension to encrypted files.

Recommendations

Exercise caution when interacting with online content: Avoid opening untrusted links and email attachments unless their authenticity has been verified through reliable sources.

Data Backup: Establish regular backup protocols for all assets to ensure their utmost security. Utilize the 3-2-1-1 backup framework and specialized tools to enhance backup resilience and accessibility.

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Implement Network Security Measures: Employ robust network security measures, including firewalls and intrusion detection/prevention systems, to help prevent unauthorized access and the spread of ransomware within the network.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0005 Defense Evasion	TA0007 Discovery	TA0008 Lateral Movement
TA0040 Impact	T1204.002 Malicious File	T1204 User Execution	T1134 Access Token Manipulation
T1140 Deobfuscate/Decode Files or Information	T1083 File and Directory Discovery	T1570 Lateral Tool Transfer	T1486 Data Encrypted for Impact
T1491.001 Internal Defacement	T1491 Defacement	T1490 Inhibit System Recovery	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	949c438e4ed541877dce02b38bf593ad
SHA1	4c58d2d624d9bdf6b14a6f8563788785074947a7
SHA256	36696ba25bdc8df0612b638430a70e5ff6c5f9e75517ad401727be03b26d8ec4

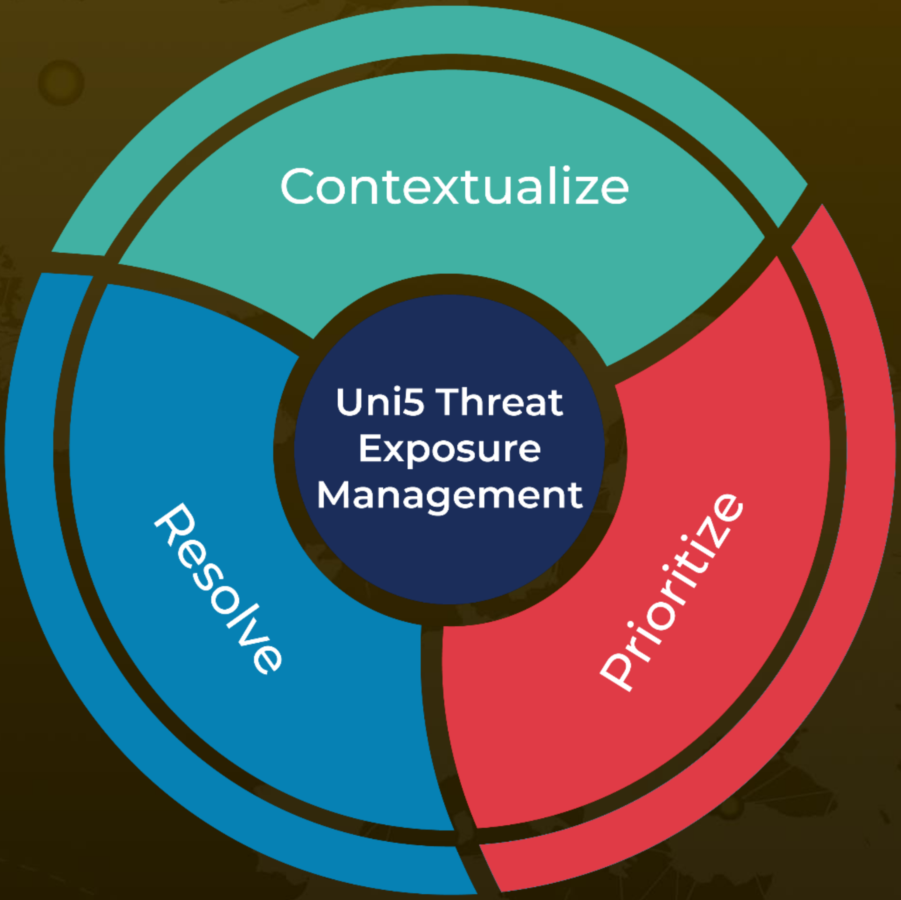
References

https://cyble.com/blog/in-the-shadow-of-venus-trinity-ransomwares-covert-ties/

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 15, 2024 • 4:00 AM

More at www.hivepro.com