Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

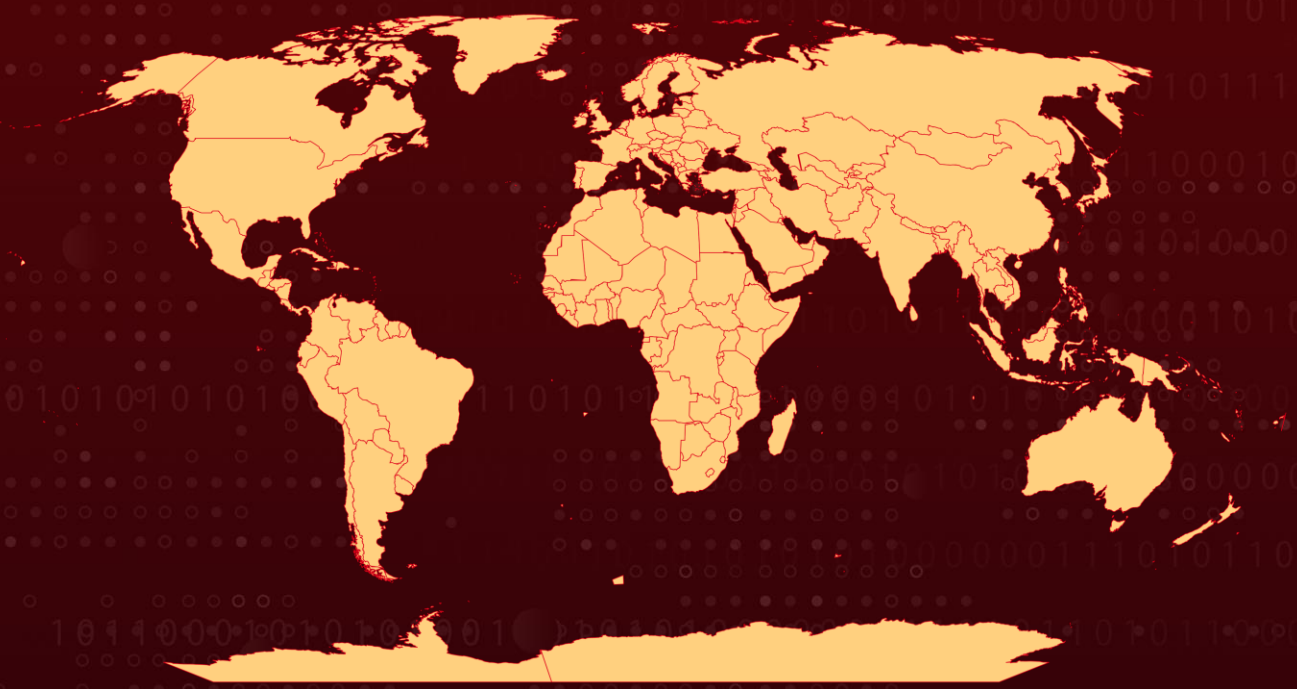
Monti Ransomware's New Linux Variant Enhanced Encryption

Date of Publication	Admiralty Code	TA Number
August 17, 2023	A1	TA2023334

Summary

First Appearance: June 2022
Attack Region: Worldwide
Affected Platform: Windows, and Linux
Targeted Industries: Legal, Financial services, Government, and Healthcare
Malware: Monti Ransomware
Attack: Monti ransomware, resembling Conti, resurfaces after a break, targeting legal and government sectors. A new Linux variant diverges significantly, using distinct tactics for encryption and virtual machine termination. Organizations must enhance defenses and backup measures to counter evolving ransomware threats.

Attack Regions



Attack Details

#1

Monti is a ransomware group that emerged in June 2022 and targets Linux and Windows systems. It encrypts files with a ".monti" extension and demands a ransom for decryption. Monti is believed to be a rebranded version of Conti, a notorious ransomware.

#2

Monti employs similar tools and tactics as Conti, such as exploiting the Log4Shell vulnerability, dumping credentials, scanning the network, and using remote access agents. However, Monti also features unique elements, including a more discreet encryption process and a distinct ransom note. Monti has targeted various sectors, including public, legal, and virtualization domains.

#3

After a two-month hiatus, Monti ransomware activities have resumed, now with a focus on legal and government sectors. A new Linux-based variant, distinct from its predecessors, has emerged. This variant deviates significantly from the older versions, with only a 29% similarity rate compared to the 99% similarity rate between the older variants and Conti.

#4

The older versions of Monti ransomware were based on the Golang programming language and utilized the Salsa20 encryption algorithm. The new versions of the ransomware are built on the Rust programming language and use the AES-256-CTR encryption algorithm. This shift makes the decryption of the new ransomware versions considerably more challenging.

#5

The new variant introduces changes such as a different encryption method, and alterations to the ransom note message. It tampers with the motd (aka message of the day) file to display the ransom note. It has a significantly lower similarity rate to Conti than previous versions of Monti. The ransomware appends an "infection marker" to files before initiating encryption and employs various methods to determine the size of files to be encrypted.

Recommendations

Keep your systems and software up to date: Regularly install updates for your operating system, applications, and security software. This helps patch vulnerabilities that adversaries can exploit.

Conduct Regular Data Backups: Implement a robust data backup strategy that includes regular backups of critical data and systems, ad hoc and periodic backup restoration test. In the event of a ransomware attack, having up-to-date backups will allow organizations to restore their systems and data without paying the ransom.

Protect your Backups: Ensure backups are adequately protected, employ 3-2-1-1 back up principle and Deploy specialized tools to ensure backup protection.

Potential MITRE ATT&CK TTPs

TA0040 Impact	TA0007 Discovery	TA0005 Defense Evasion	TA0002 Execution
TA0009 Collection	TA0010 Exfiltration	T1005 Data from Local System	T1059 Command and Scripting Interpreter
T1083 File and Directory Discovery	T1027 Obfuscated Files or Information		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	F1c0054bc76e8753d4331a881cdf9156dd8b812a, a0c9dd3f3e3d0e2cd5d1da06b3aac019cdbc74ef
URLs	hxxp://monti5o7lvyrpyk26lqofnfvajtyqruwatlfaazgm3zskt3xiktudwid[.]onion, hxxp://mblogci3rudehaagbryjznltdp33ojwzkq6hn2pckvjq33rycmzczpid[.]onion

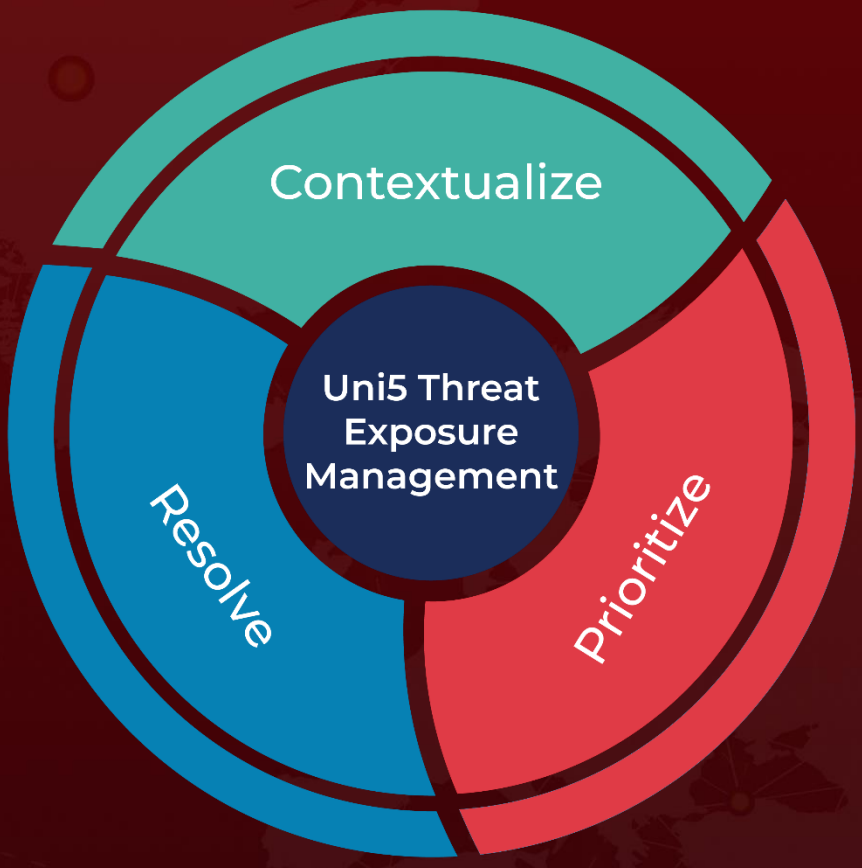
References

https://www.trendmicro.com/en_us/research/23/h/monti-ransomware-unleashes-a-new-encryptor-for-linux.html

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

August 17, 2023 • 7:30 AM

More at www.hivepro.com