Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

HexaLocker Ransomware Returns with a Vengeance

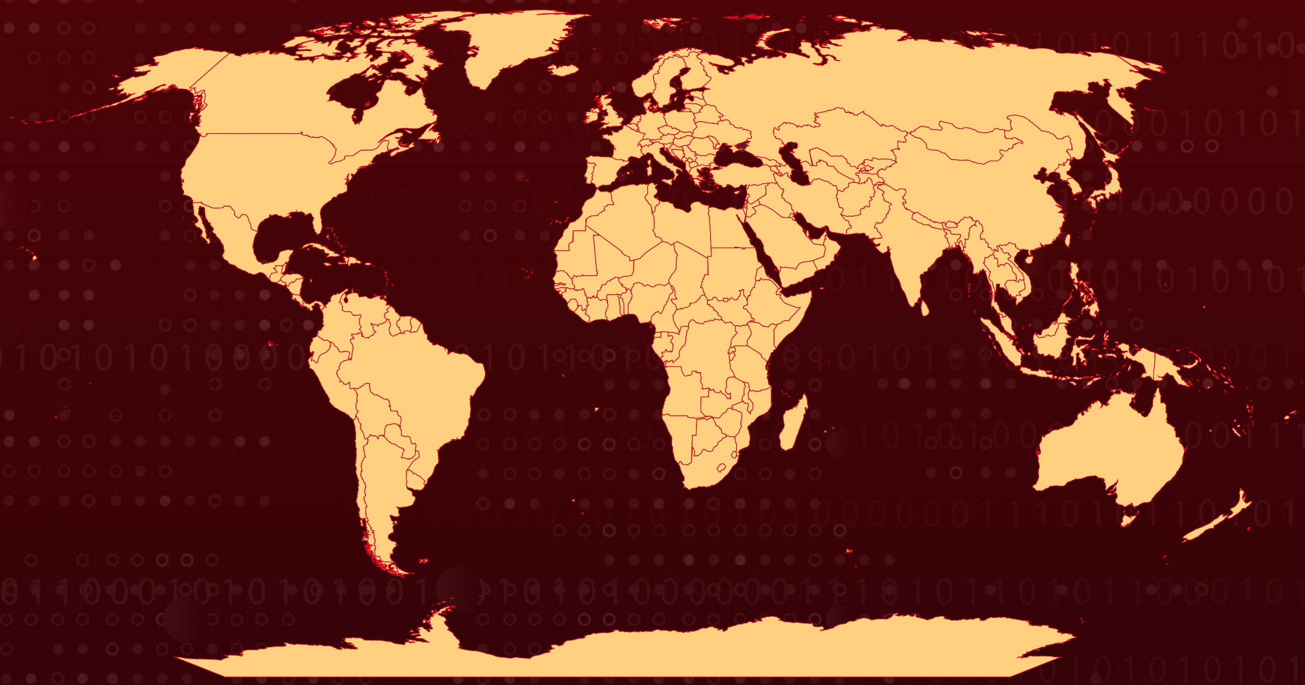
Date of Publication	Admiralty Code	TA Number
January 10, 2025	A1	TA2025009

Summary

First Discovered: Mid-2024
Malware: Hexalocker Ransomware, Skuld Stealer
Affected Platform: Windows
Targeted Region: Worldwide

Attack: HexaLocker ransomware, which emerged in mid-2024, has escalated its operations with a new version that merges data theft and file encryption for maximum impact. Utilizing advanced tactics such as double extortion and anti-analysis tools, it targets sensitive information, locks victims' files, and demands ransom through secure communication channels.

Attack Regions



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

Attack Details

#1 HexaLocker ransomware, first detected in mid-2024, has seen significant advancements with the release of its second version, which introduces notable enhancements and expanded capabilities. A key update in this version is the integration of the open-source Skuld Stealer, a tool designed to extract sensitive data from infected systems before file encryption.

#2 The latest iteration of the Go-based HexaLocker ransomware demonstrates sophisticated functionalities, including the ability to download and execute Skuld Stealer. This infostealer specializes in harvesting critical information such as web browser data, cookies, financial credentials, browsing history, and stored passwords.

#3 Utilizing the infamous double extortion strategy, the ransomware first exfiltrates sensitive data and then encrypts files. Encrypted files are appended with the ".HexaLockerV2" extension, and victims receive a ransom note instructing them to contact the attackers via Telegram or web chat.

#4 HexaLocker employs AES-256-GCM encryption, using a randomly generated password derived via the Argon2ID key derivation algorithm. Decryption keys are AES-encrypted with a hardcoded key and transmitted to a remote HTTPS server, avoiding the use of asymmetric cryptography.

#5 In addition to encryption, the ransomware is capable of stealing files. To further obstruct analysis, the developer has integrated the GoDefender open-source module, which protects the code against dynamic analysis and debugging attempts.

Recommendations

Implement the 3-2-1 Backup Rule: Maintain three total copies of your data, with two backups stored on different devices and one backup, kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

Enforce Application Whitelisting: Implement strict application whitelisting policies to prevent unauthorized or malicious executables from running within your environment.

Network and File Share Security: Secure shared network resources by limiting write access and enforcing strict access controls. Isolate critical shared drives to minimize the impact of ransomware propagating across the network.

Conduct Ransomware Simulation Drills: Test the organization's resilience against ransomware attacks by conducting simulated scenarios to identify gaps in preparedness.

Regularly Test Backup Restores: Conduct frequent tests to verify the integrity of backup data and ensure that restoration processes work as intended. This practice helps identify any issues before an actual data recovery scenario arises.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion	TA0007 Discovery
TA0040 Impact	TA0006 Credential Access	TA0006 Credential Access	TA0009 Collection
TA0010 Exfiltration	T1204 User Execution	T1204.002 Malicious File	T1547.001 Registry Run Keys / Startup Folder
T1140 Deobfuscate/Decode Files or Information	T1083 File and Directory Discovery	T1486 Data Encrypted for Impact	T1555 Credentials from Password Stores
T1560 Archive Collected Data	T1555.003 Credentials from Web Browsers	T1560.001 Archive via Utility	T1041 Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps[:]//hexalocker[.]xyz/SGDYSRE67T43TVD6E5RD[.]exe, hxxps[:]//hexalocker[.]xyz/upload[.]php, hxxps[:]//hexalocker[.]xyz/receive[.]php, hxxps[:]//darkslategray-baboon-853641[.]hostingersite[.]com/index[.]php, hxxps[:]//darkslategray-baboon-853641[.]hostingersite[.]com/receive[.]php
SHA256	8b347bb90c9135c185040ef5fdb87eb5cca821060f716755471a637c350988d8, 0347aa0b42253ed46fdb4b95e7ffafa40ba5e249dfb5c8c09119f327a1b4795a, 28c1ec286b178fe06448b25790ae4a0f60ea1647a4bb53fb2ee7de506333b960, d0d8df16331b16f9437c0b488d5a89a4c2f09a84dec4da4bc13eab15aded2e05, 87c1869871e9be8adaacb41a16c8fff691f86591416a592a77e308c4b7c041be, be759e58413431dbe40d29ea5e399b1ebbfe75847c19a5a8f2610dab9f78ca8b, d1dc3aa5d2701a9c611126da9b5d1809d1306c24b988325787ce01db15fdf856, 75601d6fee42e2af8ec80d2c18a9b5fb48466084745d119286ff1a03221a37fa, 87f11be87275147a118544b10396c932dfd7e244cf07826d2707561c8e0f25e8

References

https://cyble.com/blog/hexalocker-v2-being-proliferated-by-skuld-stealer/

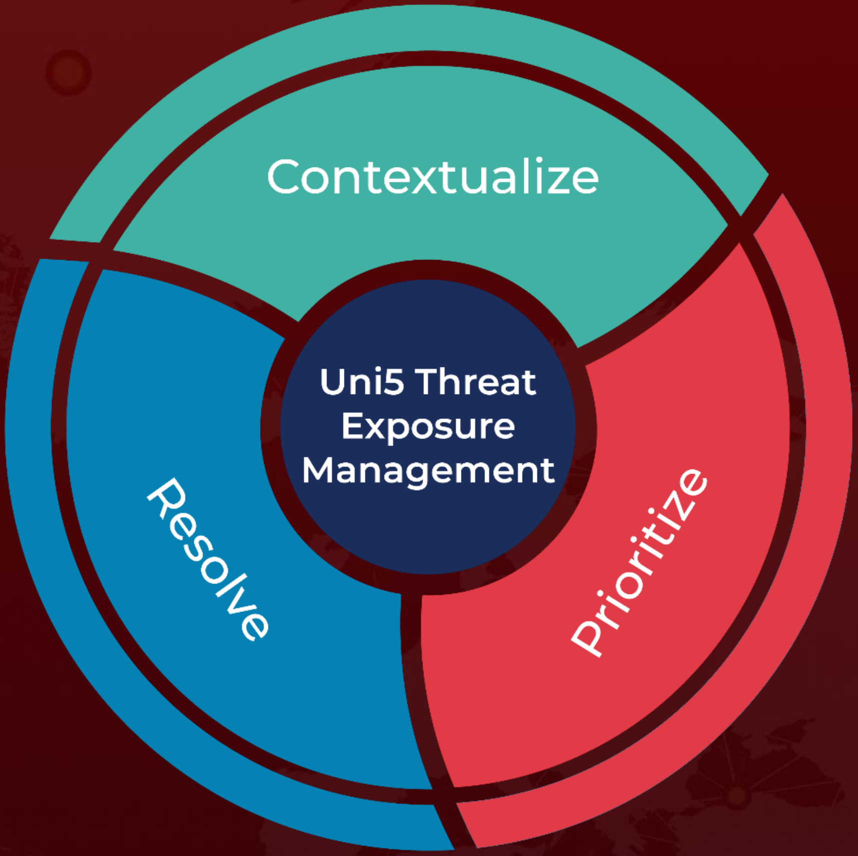
https://www.synacktiv.com/publications/lapsus-is-dead-long-live-hexalocker.html

https://github.com/synacktiv/hexalocker-analysis/blob/main/HexaLocker.yar

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 10, 2025 • 7:00 AM

More at www.hivepro.com