Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

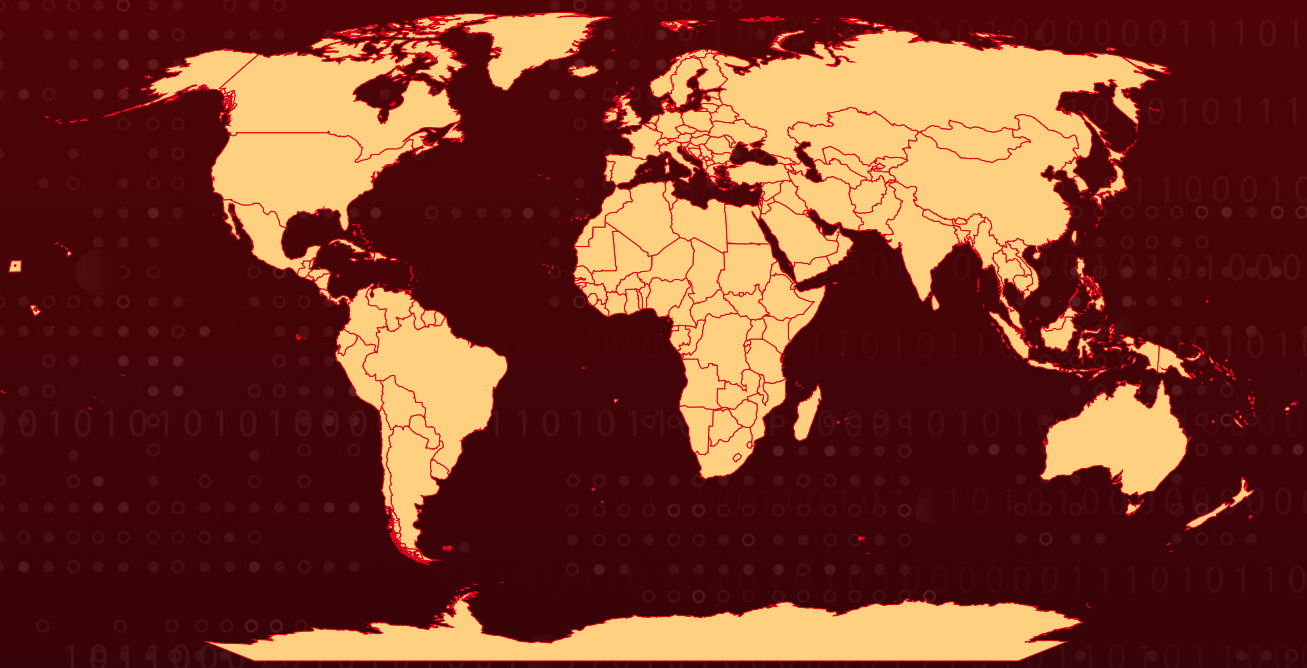
New Embargo Rust-Based Ransomware Threat for Cross-Platform Systems

Date of Publication	Admiralty Code	TA Number
October 28, 2024	A1	TA2024414

Summary

First Appearance: May 2024
Malware: Embargo ransomware
Targeted Countries: Worldwide
Affected Platforms: Windows and Linux
Attack: Embargo ransomware, first identified in mid-2024, operates as a RaaS model, targeting both Windows and Linux systems through the Rust programming language. Its toolkit includes MDeployer, which deploys the ransomware and disables security defenses, and MS4Killer, which terminates security processes using vulnerable drivers for kernel access. The group employs a double-extortion strategy, exfiltrating sensitive data alongside encryption. With ongoing development and adaptability, Embargo poses a significant threat to organizations globally.

Attack Regions



Attack Details

#1

Embargo ransomware is a sophisticated and emerging threat, first identified in June 2024, with its initial public appearance noted in May of the same year. Suspected to operate as a ransomware-as-a-service (RaaS) model, it allows affiliates to deploy the ransomware in exchange for a share of ransom payments. Embargo uses Rust, a preferred language for ransomware, allowing it to target both Windows and Linux systems.

#2

The Embargo ransomware toolkit consists of two primary components, MDeployer and MS4Killer. MDeployer acts as the main loader, responsible for deploying the ransomware and accompanying tools. It decrypts and executes two payloads: MS4Killer, an EDR (Endpoint Detection and Response) killer, and the actual ransomware payload. Notably, MDeployer is actively developed, with different versions observed in single attacks, indicating ongoing refinement and adaptation to bypass security defenses.

#3

MS4Killer specifically targets security products by employing a technique known as "Bring Your Own Vulnerable Driver" (BYOVD). This tool disables security solutions by terminating their processes, allowing the ransomware to execute undetected. MS4Killer is tailored to each victim's environment, using a vulnerable driver embedded within it to gain kernel-level access, which significantly enhances the attack's effectiveness.

#4

Embargo employs a double-extortion strategy, encrypting files and exfiltrating sensitive data to pressure victims into paying ransoms. The group has shown an ability to adapt its tools during attacks, customizing them based on the specific security solutions used by victims. For example, MDeployer can reboot systems into Safe Mode to bypass security measures that are typically active in standard operating modes, enhancing Embargo’s threat potential.

#5

Embargo is linked to several high-profile attacks, including those on the Summerville Police Department and Firstmac Limited, the group communicates with victims through secure messaging platforms like Tox and maintains a leak site to further pressurize victims. Its ongoing development and adaptive strategies make Embargo a significant and growing threat to organizations globally.

Recommendations

Implement Robust Endpoint Protection: Deploy advanced endpoint protection solutions that include behavior-based detection, machine learning algorithms, and threat intelligence. These solutions can detect and block malicious activities associated with Embargo ransomware, such as file encryption and unauthorized processes. Regularly update endpoint security software to ensure protection against the latest threats.

Patch and Update Software: Keep all operating systems, applications, and firmware up to date with the latest security patches and updates. By promptly applying patches, organizations can mitigate the risk of these vulnerabilities being exploited and prevent unauthorized access to their networks.

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, store them securely offline. Test restoration processes to ensure backup integrity and availability. In case of a Embargo ransomware attack, up-to-date backups enable recovery without paying the ransom.

Access Control and Least Privilege: Enforce the principle of least privilege, ensuring that users and applications have only the minimum access required to perform their functions. This limits the potential impact of a ransomware attack.

Network Segmentation: Divide the network into segments to limit the spread of ransomware. This can help contain the damage and protect sensitive data.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0040 Impact	T1587 Develop Capabilities	T1587.001 Malware
T1059 Command and Scripting Interpreter	T1059.003 Windows Command Shell	T1059.001 PowerShell	T1053 Scheduled Task/Job
T1053.005 Scheduled Task	T1569 System Services	T1569.002 Service Execution	T1547 Boot or Logon Autostart Execution

T1547.001 Registry Run Keys / Startup Folder	T1136 Create Account	T1136.002 Domain Account	T1562 Impair Defenses
T1562.001 Disable or Modify Tools	T1562.009 Safe Mode Boot	T1070 Indicator Removal	T1070.004 File Deletion
T1112 Modify Registry	T1027 Obfuscated Files or Information	T1027.013 Encrypted/Encoded File	T1135 Network Share Discovery
T1083 File and Directory Discovery	T1490 Inhibit System Recovery	T1486 Data Encrypted for Impact	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	A1B98B1FBF69AF79E5A3F27AA6256417488CC117, F0A25529B0D0AABCE9D72BA46AAF1C78C5B48C31, 2BA9BF8DD320990119F42F6F68846D8FB14194D6, 888F27DD2269119CF9524474A6A0B559D0D201A1, BA14C43031411240A0836BEDF8C8692B54698E05, 8A85C1399A0E404C8285A723C4214942A45BBFF9, 612EC1D41B2AA2518363B18381FD89C12315100F, 7310D6399683BA3EB2F695A2071E0E45891D743B, 7310D6399683BA3EB2F695A2071E0E45891D743B
File Name	dtest.dll, fxc.exe, fdasvc.exe, praxisbackup.exe, praxisbackup.exe, pay.exe, win32.exe, Sysmon64.sys, Sysprox.sys
File Path	C:\Windows\Debug\b.cache, C:\Windows\Debug\a.cache, C:\Windows\Debug\fail.txt, C:\Windows\Debug\stop.exe

Recent Breaches

http://weisermemorialhospital.org
http://summervillepolice.com
http://pioneerworldwide.com
http://diligentusa.com
http://gerard-perrier.com
http://jla.com
http://dmedelivers.com
http://shamrocktradingcorp.com
http://orga-soft.de
http://rexmoore.com
http://firstmac.com.au
http://mulfordconstruction.com

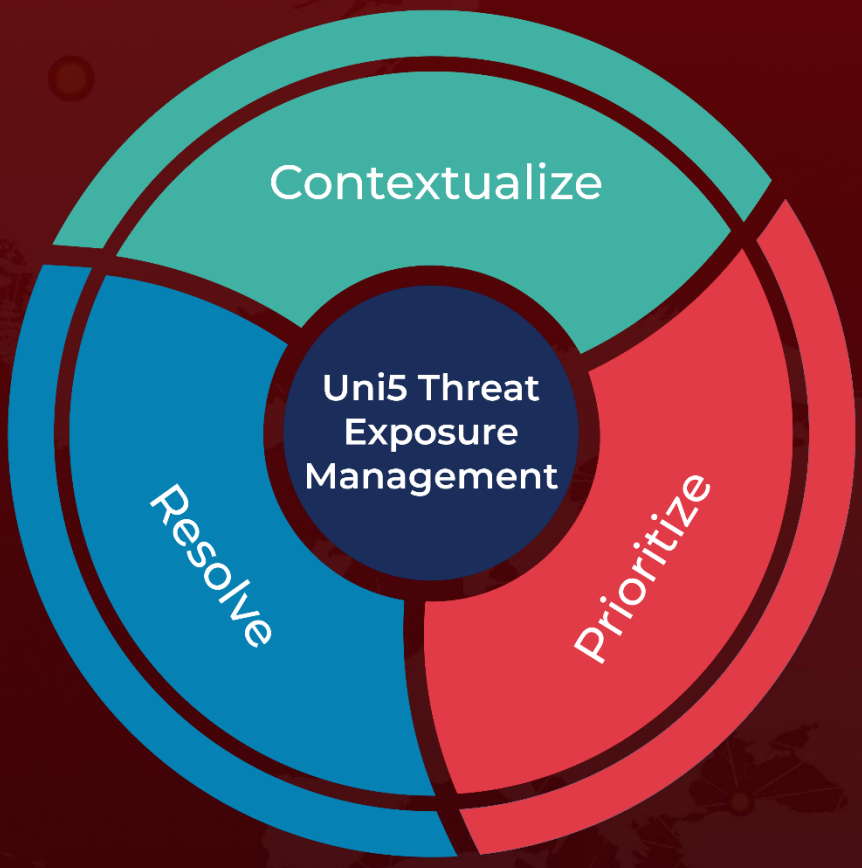
References

https://www.welivesecurity.com/en/eset-research/embargo-ransomware-rocknrust/

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

October 28, 2024 . 7:30 AM

More at www.hivepro.com