Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

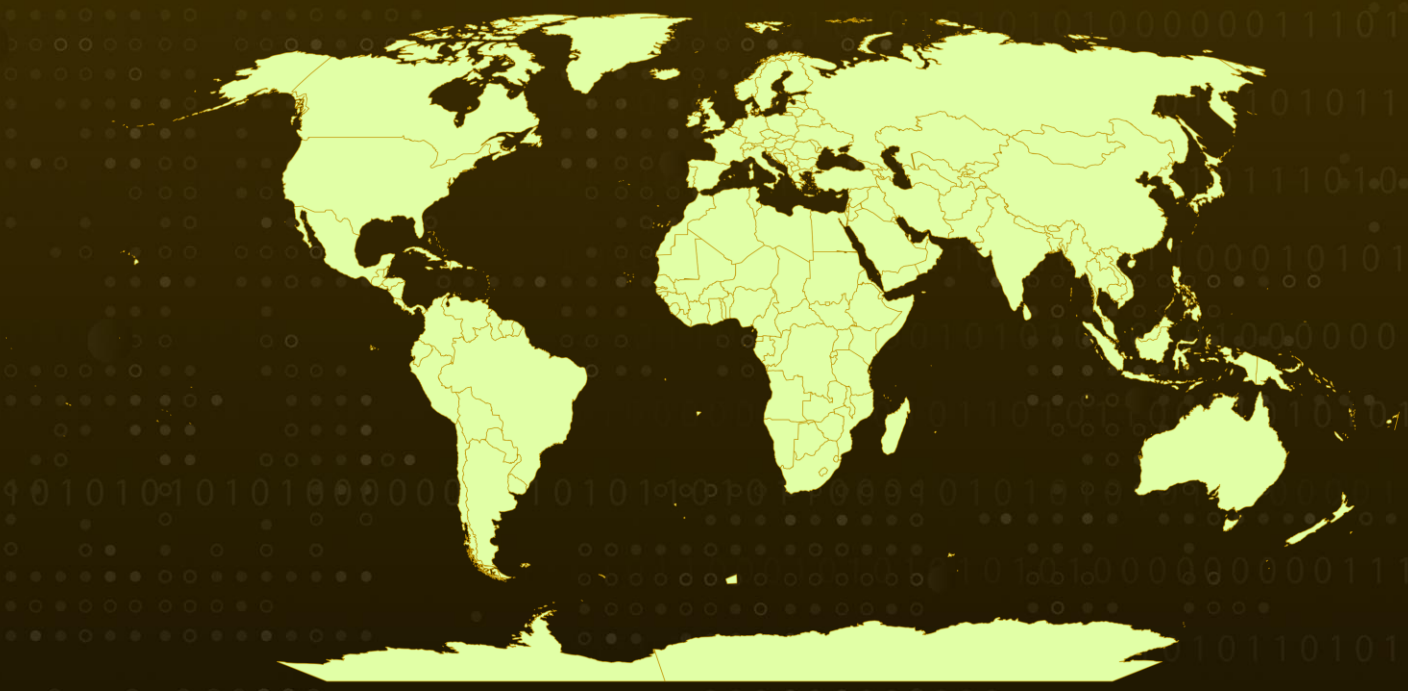
Unveiling the Advanced Rust-based Nevada Ransomware

Date of Publication	Admiralty Code	TA Number
February 3, 2023	A1	TA2023061

Summary

First appeared: December 10th, 2022
Attack Region: Worldwide
Attack: A new type of ransomware named "Nevada Ransomware" has been identified. The creators of this ransomware have established an affiliate program that was initially introduced in the RAMP underground community. This ransomware is quickly enhancing its abilities, as evidenced by its improved performance in locking Windows and VMware ESXi systems.

Attack Regions



Attack Details

#1

The actors behind the Nevada Ransomware have an affiliate platform that was first announced on the RAMP underground community. The ransomware has been upgraded and its functionality has been improved for Windows and Linux/ESXi systems. Updated builds have been made available to affiliates.

#2

Nevada Ransomware is a Rust-based locker that can be controlled from a console using predefined flags. The ransomware features a real-time negotiation chat portal, unique domains on the Tor network for affiliates and victims, and a recursive algorithm in its code to gather information.

#3

The payload collects information about network resources using MPR.dll, adding shared folders to the encryption queue. Each disk, including hidden ones, is assigned a letter, and the files on them are added to the queue as well. After this, the encryptor is installed as a service and the compromised system reboots into Windows safe mode with an active network connection. To speed up the encryption process, the locker employs the Salsa20 algorithm to perform intermittent encryption on files larger than 512KB.

#4

To avoid rendering the victim host unbootable, executables, DLLs, LNKs, SCRs, URLs, and INI files in Windows system directories and the user's Program Files are excluded from encryption. The Nevada Ransomware will leave a 'readme.txt' file after successful encryption, and the encrypted files will be given the extension '.NEVADA'.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

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
T1082 System Information Discovery	**T1059** Command and Scripting Interpreter	**T1129** Shared Modules	**T1569** System Services
T1574 Hijack Execution Flow	**T1574.002** DLL Side-Loading	**T1543** Create or Modify System Process	**T1055** Process Injection
T1027 Obfuscated Files or Information	**T1070** Indicator Removal	**T1135** Network Share Discovery	**T1518** Software Discovery
T1489 Service Stop	**T1490** Inhibit System Recovery	**T1112** Modify Registry	**T1140** Deobfuscate/Decode Files or Information

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	nevcorps5cvivjf6i2gm4uia7cxng5ploqny2rgrinctazjlnqr2yiyd[.]onion/
MD5	99549bcea63af5f81b01decf427519af fb5dcf0b880b57b10a2093f164f2ed27 709ba88e758454f097959c3e62997000 f1f569c6e4f961007f7411fca131bbe0 1396ab93e9104faaf138ac64211471ba

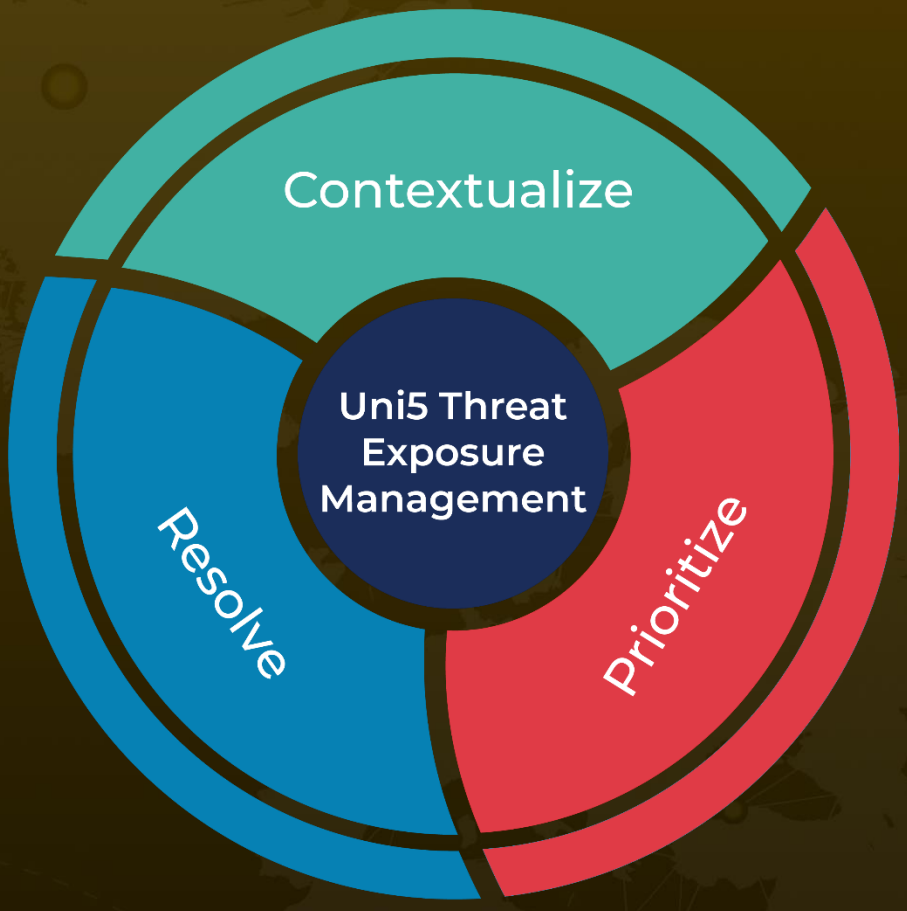
References

https://resecurity.com/blog/article/nevada-ransomware-waiting-for-the-next-dark-web-jackpot

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

February 3, 2023 • 1:30 AM

More at www.hivepro.com