Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

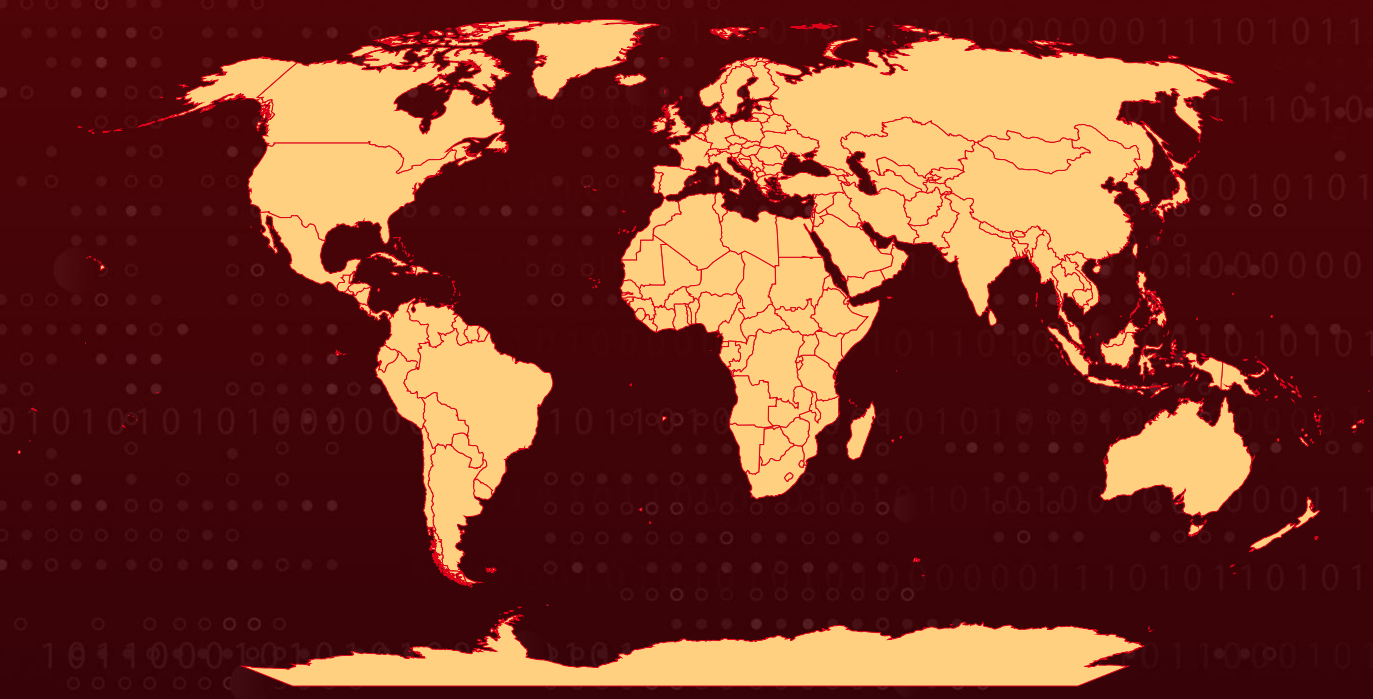
Ymir Ransomware a New Era of In-Memory Execution Tactics

Date of Publication	Admiralty Code	TA Number
November 13, 2024	A1	TA2024426

Summary

First Seen: August 2024
Malware: Ymir ransomware, RustyStealer
Attack Region: Worldwide
Attack: The Ymir ransomware, a new and advanced threat, leverages in-memory execution and sophisticated evasion techniques to bypass traditional detection. Linked with credential-stealing malware like RustyStealer, Ymir was recently used in an attack on a Colombian organization, highlighting a strategic pattern in ransomware and access broker collaboration.

Attack Regions



Attack Details

#1 The Ymir ransomware, a recent addition to the ransomware landscape, demonstrates advanced evasion capabilities, notably executing many functions within system memory by utilizing specific memory management operations.

#2 Attackers target the system through remote PowerShell commands, subsequently deploying a suite of tools, including Process Hacker and Advanced IP Scanner, along with two scripts associated with the SystemBC malware.

#3 These tools established a covert communication channel, enabling malicious actions and weakening the system's defenses. With the necessary permissions obtained, Ymir ransomware was launched to execute encryption and further malicious activities.

#4 Ymir's design incorporates components from CryptoPP, an open-source cryptographic library written in C++. By loading concise instruction sets directly into memory, Ymir leverages memory-only operations—malloc, memmove, and memcmp—to bypass traditional execution patterns and enhance detection evasion.

#5 Using the ChaCha20 stream cipher, Ymir appends the .6C5oy2dVr6 extension to encrypted files. Additionally, it generates a ransom note, "INCIDENT_REPORT.pdf," in every directory containing encrypted files, using the ".data" section of the Ymir binary.

#6 Although the ransom note claims data theft, the malware itself lacks network functionality for data exfiltration. Instead, Ymir scans for PowerShell on the system and then uses it to delete its executable, further reducing the chance of detection.

#7 In a recent attack on an organization in Colombia, threat actors deployed RustyStealer malware to harvest corporate credentials before launching Ymir ransomware. This pattern suggests a connection between credential-stealing botnets acting as initial access brokers and the subsequent execution of ransomware.

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.

Implement Zero Trust Architecture: Adopt a Zero Trust security model that requires verification for every user and device attempting to access network resources, minimizing unauthorized access risks.

Real-Time Network Traffic Analysis and Anomaly Detection: Implement real-time NTA tools with anomaly detection capabilities to identify unusual patterns, such as the creation of covert channels or large data transfers that may indicate exfiltration attempts.

Limit User Privileges: Apply the principle of least privilege by limiting user access rights to only those necessary for their role. This minimizes the risk of unauthorized access and potential data breaches.

Endpoint Hardening: Implement endpoint hardening by disabling unnecessary services, ports, and protocols, particularly those often exploited by malware, such as Remote Desktop Protocol (RDP).

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
TA0008 Lateral Movement	TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact

T1083 File and Directory Discovery	**T1082** System Information Discovery	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell
T1486 Data Encrypted for Impact	**T1497** Virtualization/Sandbox Evasion	**T1497.003** Time-Based Evasion	**T1070** Indicator Removal
T1070.004 File Deletion	**T1057** Process Discovery	**T1129** Shared Modules	**T1027** Obfuscated Files or Information
T1055 Process Injection	**T1048** Exfiltration Over Alternative Protocol	**T1005** Data from Local System	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	12acbb05741a218a1c83eaa1cfc2401f, 5ee1befc69d120976a60a97d3254e9eb, 5384d704fadf229d08eab696404cbba6, 39df773139f505657d11749804953be5, 0fd79133bd46b420056204b475719cd5, dd7799d822f052cfa8ad1e16b33bb2cb
SHA1	3648359ebae8ce7cacae1e631103659f5a8c630e, e6c4d3e360a705e272ae0b505e58e3d928fb1387, 0d65b15d30fdbbd3c4a338a3233eee48802d4458, 3bf56d07fd29be12fb2c604de343a43d51f25391, 79e581dee9b2a19943fe79136d58859e4ac5dffa, fe6de75d6042de714c28c0a3c0816b37e0fa4bb3, f954d1b1d13a5e4f62f108c9965707a2aa2a3c89
SHA256	cb88edd192d49db12f444f764c3bdc287703666167a4ca8d533d51f86ba428d8, 7c00152cc68f0104e7436f9ce8b4c99e685d05f4361f50af307d4bfdbc90bca0, 2c0a52d2fc26c5d9130b9efd4e6557945883f4c8d08c98febb3ac5b101980d5d, 732121b220f0bb69f08bd01be85b4d1f43c1766322f50791d5ffecc12aaa8eaf, 8287d54c83db03b8adcdf1409f5d1c9abb1693ac8d000b5ae75b3a296cb3061c,

TYPE	VALUE
SHA256	51ffc0b7358b7611492ef458fdf9b97f121e49e70f86a6b53b93ed923b707a03, b087e1309f3eab6302d7503079af1ad6af06d70a932f7a6ae1421b942048e28a, 04dce8eb632250f64f1741f47707e6cb991926d35f4157d540c2fc3230b6a92f
File Name	AudioDriver2.0.exe, INCIDENT_REPORT.pdf
IPv4	74[.]50[.]84[.]181, 94[.]158[.]244[.]69, 85[.]239[.]61[.]60, 5[.]255[.]117[.]134
URL	hxxps[:]//github[.]com/qTox/qTox/releases/download/v1[.]17[.]6/setup-qtox-x86_64-release[.]exe

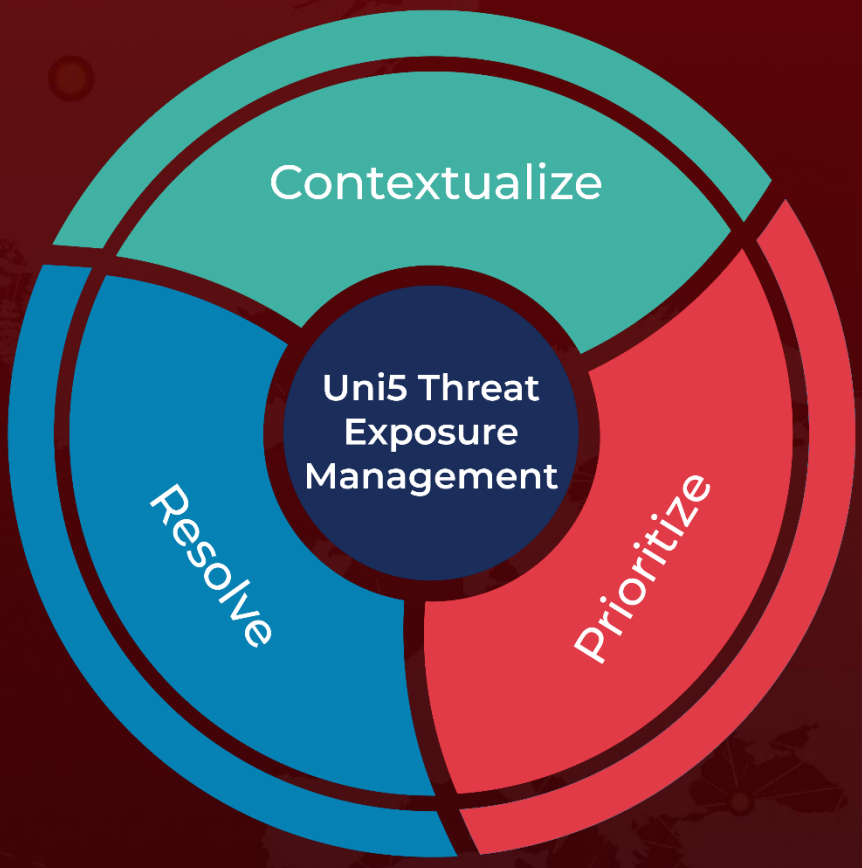
References

https://securelist.com/new-ymir-ransomware-found-in-colombia/114493/

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

November 13, 2024 . 5:00 AM

More at www.hivepro.com