Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

New ResolverRAT Malware Targets Global Pharma and Healthcare Sectors

Date of Publication

April 15, 2025

Admiralty Code

A1

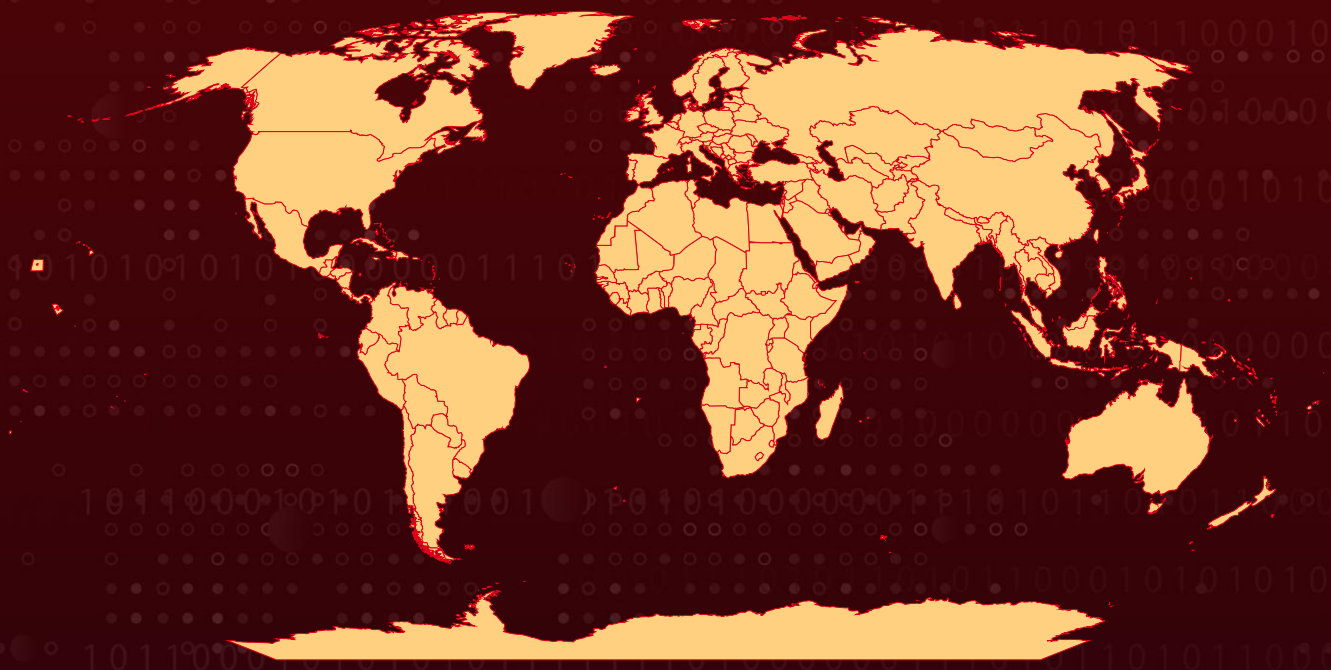
TA Number

TA2025114

Summary

First Seen: March 10, 2025
Targeted Countries: Worldwide
Malware: ResolverRAT
Targeted Platforms: Windows
Targeted Industries: Healthcare and Pharmaceutical
Attack: ResolverRAT is a sophisticated remote access trojan (RAT) identified in March 2025, employing advanced in-memory execution and runtime API resolution to evade detection. It targets corporate employees via phishing emails, leading to stealthy in-memory execution and secure command-and-control communications. The malware exfiltrates data in segments using a chunking mechanism, minimizing detection during large transfers.

Attack Regions



Attack Details

#1

ResolverRAT is a highly sophisticated remote access Trojan (RAT) that has recently emerged as a serious threat, especially targeting global enterprises in sectors like healthcare and pharmaceuticals. It is designed to operate stealthily by executing entirely in memory, using strong encryption and compression to avoid detection. This malware employs advanced evasion techniques, including obfuscation and dynamic resource decryption, making it difficult for traditional security tools to identify and remove.

#2

The infection typically begins through carefully crafted phishing campaigns that are localized to the target's language and culture. These emails often use urgent themes such as legal investigations or copyright issues to trick victims into opening malicious attachments or links. Once inside the system, ResolverRAT uses DLL side-loading, a method that leverages legitimate executables to load malicious code, helping it bypass many security defenses.

#3

ResolverRAT communicates with its command-and-control (C2) servers using custom certificate-pinned channels, ensuring secure and resilient connections. It also employs IP rotation and fallback servers to maintain persistent communication even if some servers are disrupted. For persistence, the malware modifies the Windows Registry with obfuscated keys and places copies of itself in multiple system locations, allowing it to survive reboots and removal attempts.

#4

The malware's capabilities include chunked data exfiltration, where large files are split into smaller pieces to blend with normal network traffic, and parallel command processing, which enables it to execute multiple commands simultaneously without crashing. Its global phishing campaigns, tailored to various languages such as Hindi, Italian, and Turkish, indicate a well-coordinated operation with a broad reach, although the specific threat actor remains unknown.

Recommendations

Use Advanced Endpoint Security: Deploy endpoint detection and response (EDR) solutions that monitor for unusual behaviors such as in-memory execution, DLL side-loading, and encrypted payloads. Keep antivirus and anti-malware software updated to detect sophisticated and obfuscated threats.

Enhance Network Monitoring: Monitor network traffic for anomalies, including encrypted communications to unfamiliar IP addresses and segmented data transfers that may indicate data theft. Implement firewall and intrusion detection/prevention systems to block or alert on connections to known malicious command-and-control servers.

Strengthen Email Security and Filtering: Implement advanced email filtering solutions to block malicious attachments, links, and phishing attempts. Technologies such as SPF, DKIM, and DMARC can authenticate senders and reduce the risk of email-based attacks.

Strengthen Phishing Awareness: Provide ongoing cybersecurity training focused on identifying phishing emails, especially those crafted in local languages and using culturally relevant themes. Conduct regular phishing simulations to help employees recognize and respond appropriately to suspicious messages.

Potential MITRE ATT&CK TTPs

TA0008 Lateral Movement	TA0005 Defense Evasion	TA0010 Exfiltration	TA0002 Execution
TA0003 Persistence	TA0001 Initial Access	TA0009 Collection	TA0011 Command and Control
T1566 Phishing	T1204 User Execution	T1204.001 Malicious Link	T1574.002 DLL Side-Loading

T1574 Hijack Execution Flow	T1027 Obfuscated Files or Information	T1140 Deobfuscate/Decode Files or Information	T1620 Reflective Code Loading
T1566.002 Spearphishing Link	T1059.001 PowerShell	T1059 Command and Scripting Interpreter	T1218 System Binary Proxy Execution
T1055 Process Injection	T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution	T1041 Exfiltration Over C2 Channel
T1008 Fallback Channels	T1030 Data Transfer Size Limits	T1027.007 Dynamic API Resolution	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	ec189b7ce68cb308139f6a5cf93fd2dc91ccf4432dc09ccaecb9de403a000c73, 6c054f9013c71ccb7522c1350995066ef5729371641a639a7e38d09d66320bf4, c3028a3c0c9b037b252c046b1b170116e0edecf8554931445c27f0ddb98785c1, 19a4339a4396e17fece5fd5b19639aa773c3bb3d8e2f58ee3b8305b95d969215, 05313e81e28f4c4a13e5f443cd2641181d5de95cdc7e450e097ee23c09758a15, 80625a787c04188be1992cfa457b11a166e19ff27e5ab499b58e8a7b7d44f2b9, e78505de8436a1d9978fd03a4e374518be6f3f6f7f4bf18ae59e3f23301ce927
IPv4	38[.]54[.]6[.]120, 192[.]30[.]241[.]106

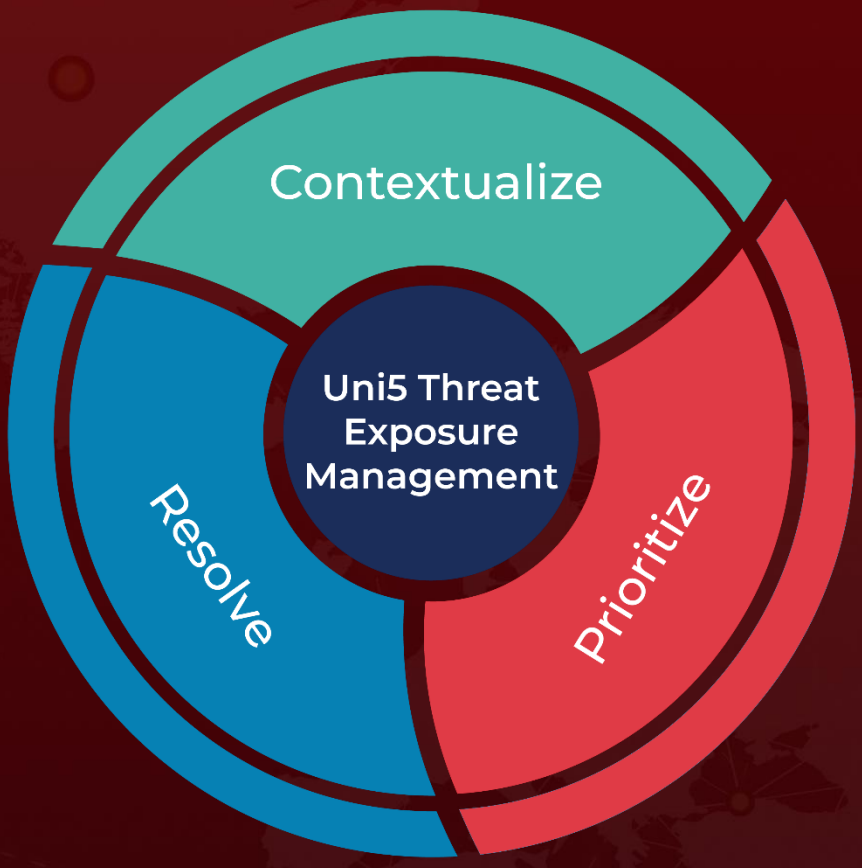
References

https://www.morphisec.com/blog/new-malware-variant-identified-resolverrat-enters-the-maze/

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

April 15, 2025 • 6:30 AM

More at www.hivepro.com