Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

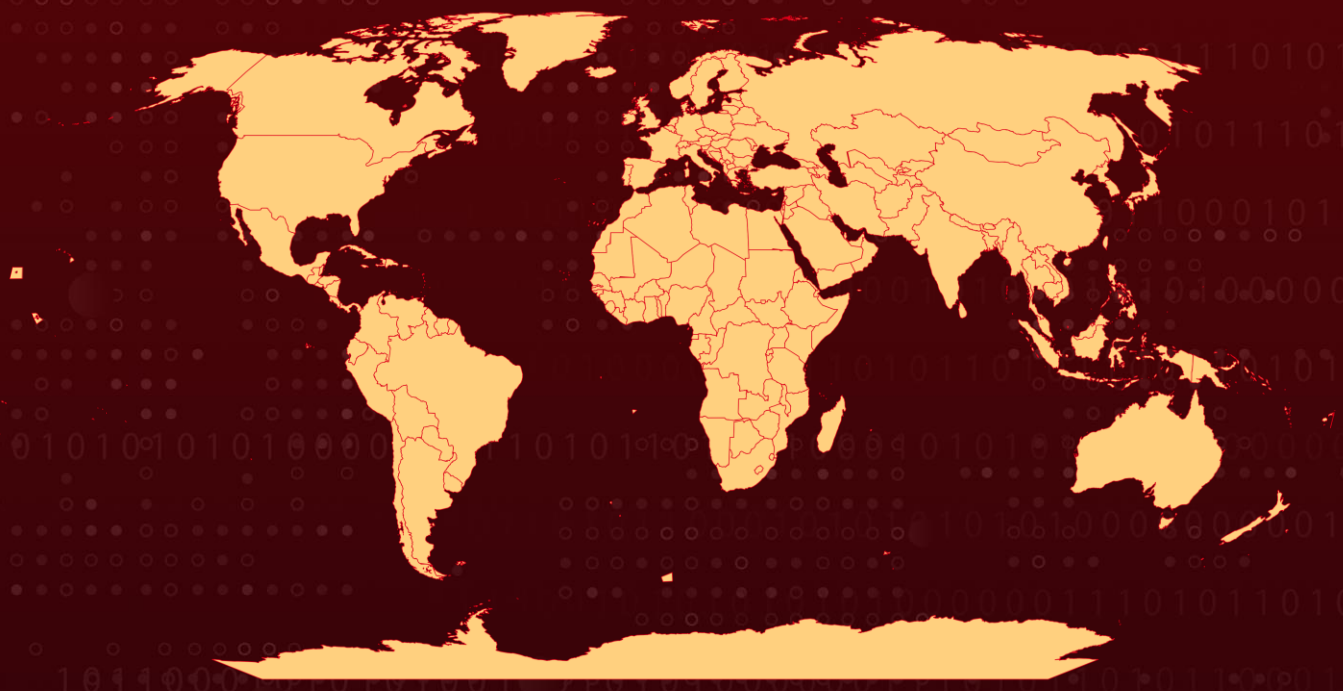
Anonymous Arabic Hacktivist Group Orchestrating Silver RAT

Date of Publication	Admiralty Code	TA Number
January 9, 2024	A1	TA2024008

Summary

Attack Began: November 2023
Attack Region: Worldwide
Malware: Silver RAT
Threat Actor: Anonymous Arabic
Affected Platform: Windows
Attack: Silver RAT, a Windows-based RAT written in C# and developed by a group known as "Anonymous Arabic," exhibits advanced capabilities, including antivirus evasion and ransomware encryption. Despite facing bans, the threat actor's dynamic activities persist, featuring the sharing of cracked versions and hints of a new release targeting Windows and Android platforms.

Attack Regions



Attack Details

#1

Silver RAT is a Windows-based RAT developed by an individual known as 'noradlb1.' This malware written in C#, possesses advanced capabilities, including the ability to bypass antivirus detection, launch hidden applications, deploy keyloggers, and encrypt data using ransomware.

#2

The threat actor behind Silver RAT operates under the name 'Anonymous Arabic' and maintains an active presence on various hacker forums, social media platforms, and e-commerce websites. The RAT was initially observed in the wild in November 2023, and its distribution involved channels such as Telegram, GitHub, and hacker forums. The developer, 'noradlb1,' is known to have a respected reputation on prominent hacking forums.

#3

The Silver RAT v1.0 builder provides users with multiple options, allowing them to customize the payload size and choose various functionalities. The RAT's capabilities include bypassing antivirus, hiding processes, and configuring the payload to execute at a specified time. The payload can be delivered using social engineering tactics, and once executed on the victim's system, it establishes a connection to the attacker's control panel.

#4

The control panel of Silver RAT v1.0 enables the attacker to perform various malicious activities on the compromised system, such as managing installed applications, navigating the file system, modifying registry keys, and initiating actions like data encryption and system restore point deletion.

#5

The Silver RAT developer is associated with a hacktivist group supporting the "Syrian Revolution." The threat landscape involving Silver RAT is dynamic, with ongoing activities such as the sharing of cracked versions, information dissemination on social media and GitHub, and the potential development of a new version capable of targeting both Windows and Android platforms.

#6

The threat actor continues to share information on social media and development platforms, indicating ongoing underground activity. Despite facing platform bans, their active presence across different forums and platforms persists, emphasizing the need for continued monitoring and response to mitigate potential threats.

Recommendations

Keep Software Up-to-Date: Ensure that all software, including operating systems, applications, and security tools, is regularly updated with the latest patches and security updates. This helps to address known vulnerabilities that attackers may exploit.

Enhance Endpoint Security: Employ reputable antivirus and anti-malware solutions to detect and block known RAT signatures. Regularly update and patch operating systems and software to address vulnerabilities that threat actors may exploit.

Network Segmentation: Implement network segmentation to isolate critical systems and sensitive data. This can limit the lateral movement of a RAT within a network, reducing the potential impact of a successful intrusion.

Network Monitoring and Intrusion Detection: Deploy network monitoring and intrusion detection systems to detect unusual or suspicious activities. Anomalies in network traffic and behavior can be indicative of a security incident.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	TA0002 Execution	TA0005 Defense Evasion	TA0009 Collection
TA0006 Credential Access	TA0010 Exfiltration	TA0003 Persistence	TA0004 Privilege Escalation
T1027 Obfuscated Files or Information	T1053 Scheduled Task/Job	T1053.005 Scheduled Task	T1059 Command and Scripting Interpreter
T1055 Process Injection	T1112 Modify Registry	T1497 Virtualization/Sandbox Evasion	T1056 Input Capture
T1539 Steal Web Session Cookie	T1552 Unsecured Credentials	T1528 Steal Application Access Token	T1057 Process Discovery
T1083 File and Directory Discovery	T1082 System Information Discovery	T1041 Exfiltration Over C2 Channel	T1567 Exfiltration Over Web Service

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	79a4605d24d32f992d8e144202e980bb6b52bf8c9925b1498a1da59e50ac51f9, a9fa8e14080792b67a12f682a336c0ea9ff463bbcb27955644c6fcaf80023641, 7a9aeea5e65a0966894710c1d9191ba4cbd6415cba5b10b3b75091237a70a5b8, 0ace7ae35b7b44a3ec64667983ff9106df688c24b52f8fcb25729c70a00cc319, 3b06b4aab7f6f590aeac5afb33bbe2c36191aeee724ec82e2a9661e34679af0a, 27b781269be3b0d2f16689a17245d82210f39531e3bcb88684b03ae620ac5007, 0ace7ae35b7b44a3ec64667983ff9106df688c24b52f8fcb25729c70a00cc319

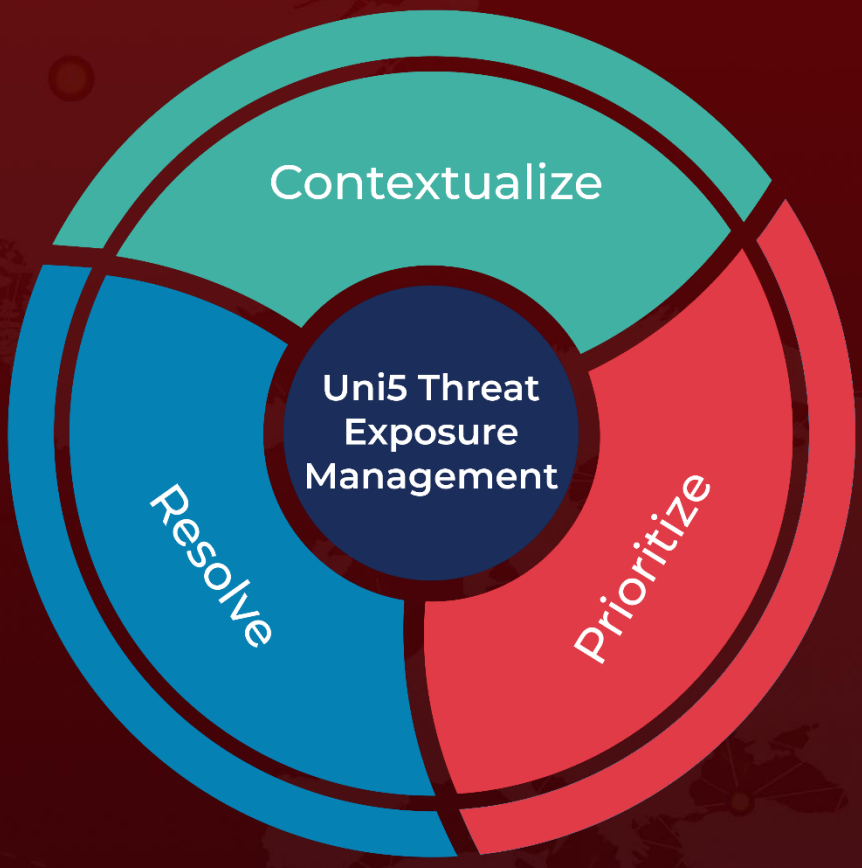
References

https://www.cyfirma.com/outofband/a-gamer-turned-malware-developer-diving-into-silverrat-and-its-syrian-roots/

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 9, 2023 . 4:30 AM

More at www.hivepro.com