Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

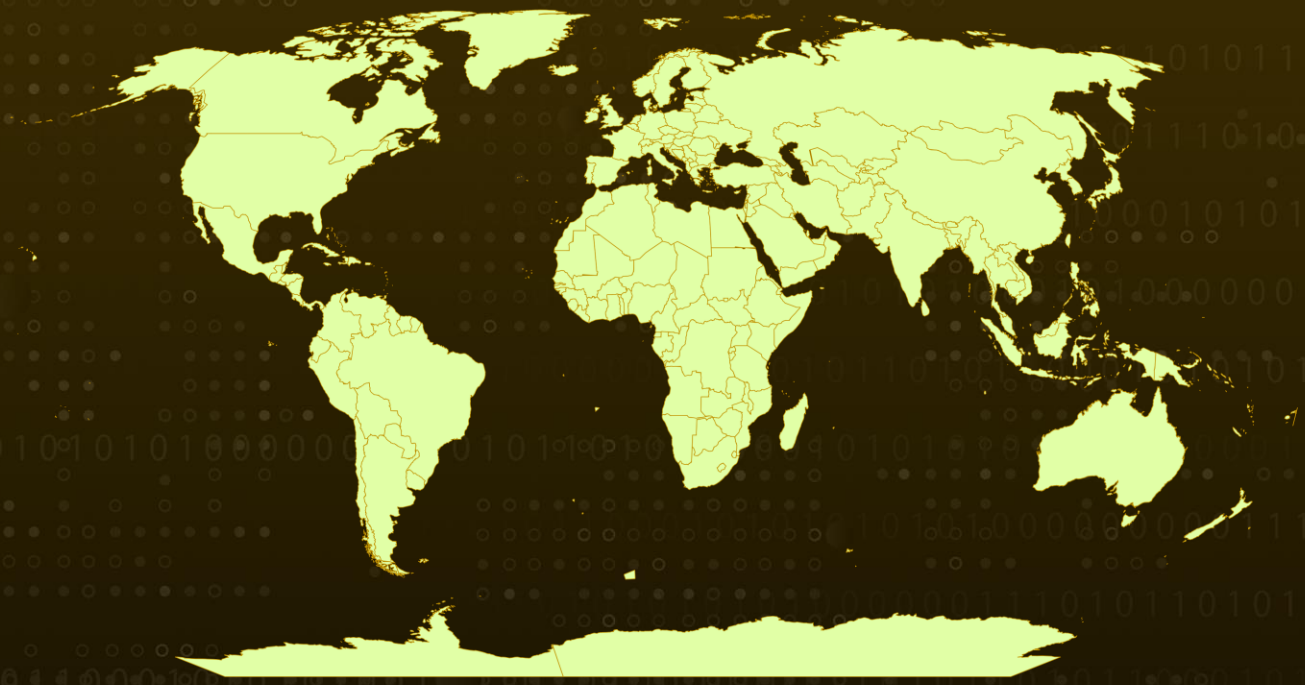
VCURMS and STRRAT Trojans Using AWS and GitHub as Launchpads

Date of Publication	Admiralty Code	TA Number
March 13, 2024	A1	TA2024098

Summary

First Appearance: December 2022
Malware: VCURMS and STRRAT
Affected Platforms: AWS and GitHub
Attack Region: Worldwide
Attack: A sophisticated phishing campaign is targeting personnel, enticing them to click on a seemingly innocuous button to authenticate payment details. However, this action initiates the download of a harmful JAR file from Amazon Web Services (AWS) onto the victim's device. This malicious file serves as a gateway for installing a Java downloader, with the intent of distributing VCURMS and STRRAT remote access trojans (RATs).

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 A phishing campaign targets personnel, suggesting an ongoing payment transaction and urging them to click a specified button to authenticate payment details, thereby delivering remote access trojans (RAT) via downloader. Upon clicking, a harmful JAR file hosted on AWS is downloaded onto the victim's device.

#2 These downloaded files appear as typical phishing attachments with altered names, crafted strategically to entice individuals into opening them, thus initiating the download of a malicious Java downloader to spread VCURMS and STRRAT remote access trojans (RATs).

#3 The perpetrators exploit public services such as Amazon Web Services (AWS) and GitHub to store malware, employing a commercial protector to avoid detection. Upon activation, the JAR file obtains two additional JAR files, each executed separately to release the twin trojans.

#4 VCURMS bears similarities to another Java-based infostealer called Rude Stealer, which emerged in the wild towards the end of the previous year. This similarity encompasses the ability to execute arbitrary commands, gather system data, search and transmit files of interest, and acquire additional information stealer and keylogger modules from the same AWS endpoint. In contrast, STRRAT, also a Java-built RAT, has been observed in the wild since 2020, frequently propagated through deceptive JAR files.

Recommendations

Email Filtering and Monitoring: Strengthen email filtering systems to detect and quarantine phishing attempts, especially those involving malicious PDFs. Regularly monitor email communications for potential threats and provide timely alerts to users.

Continuous Monitoring and Analysis: Implement continuous monitoring and analysis of network traffic and system logs. This proactive approach can help identify anomalies and potential threats before they escalate.

Disable Unnecessary Services: Review and disable unnecessary services and features on systems to minimize potential attack vectors. Restrict user privileges to limit the impact of potential breaches.

Heighten Awareness: Familiarize yourself with common social engineering tactics and deceptive strategies employed by threat actors. Knowing the signs of malicious activity can help you avoid falling victim to scams.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**TA0010** Exfiltration
T1027 Obfuscated Files or Information	**T1033** System Owner/User Discovery	**T1140** Deobfuscate/Decode Files or Information	**T1059.001** PowerShell
T1566 Phishing	**T1566.001** Spearphishing Attachment	**T1036** Masquerading	**T1547.001** Registry Run Keys / Startup Folder
T1082 System Information Discovery	**T1083** File and Directory Discovery	**T1005** Data from Local System	**T1560** Archive Collected Data
T1113 Screen Capture	**T1056.001** Keylogging	**T1105** Ingress Tool Transfer	**T1041** Exfiltration Over C2 Channel
T1204 User Execution	**T1204.002** Malicious File	**T1036** Masquerading	

Indicators of Compromise (IOCs)

TYPE	VALUE
Emails	copier@ferrellengineering[.]com, sacriliage@proton[.]me
Domains	bankofindustry[.]s3[.]us-east-2[.]amazonaws[.]com, riseappbucket[.]s3[.]ap-southeast-1[.]amazonaws[.]com, ofornta[.]ddns[.]net, jbfrost[.]live, backinghof[.]ddns[.]net
SHA256	97e67ac77d80d26af4897acff2a3f6075e0efe7997a67d8194e799006ed5efc9, 8d72ca85103f44742d04ebca02bff65788fe6b9fc6f5a411c707580d42bbd249, 588d6f6feefa6273c87a3f8a15e2089ee3a063d19e6a472ffc0249298a72392d, 8aa99504d78e88a40d33a5f923caf7f2ca9578031d004b83688aafdf13b3b59f, c0d0dee9b8345da3c6cf3e1c3ce5b5b6e8c9e4002358517df1e3cd04c0f0b3d1

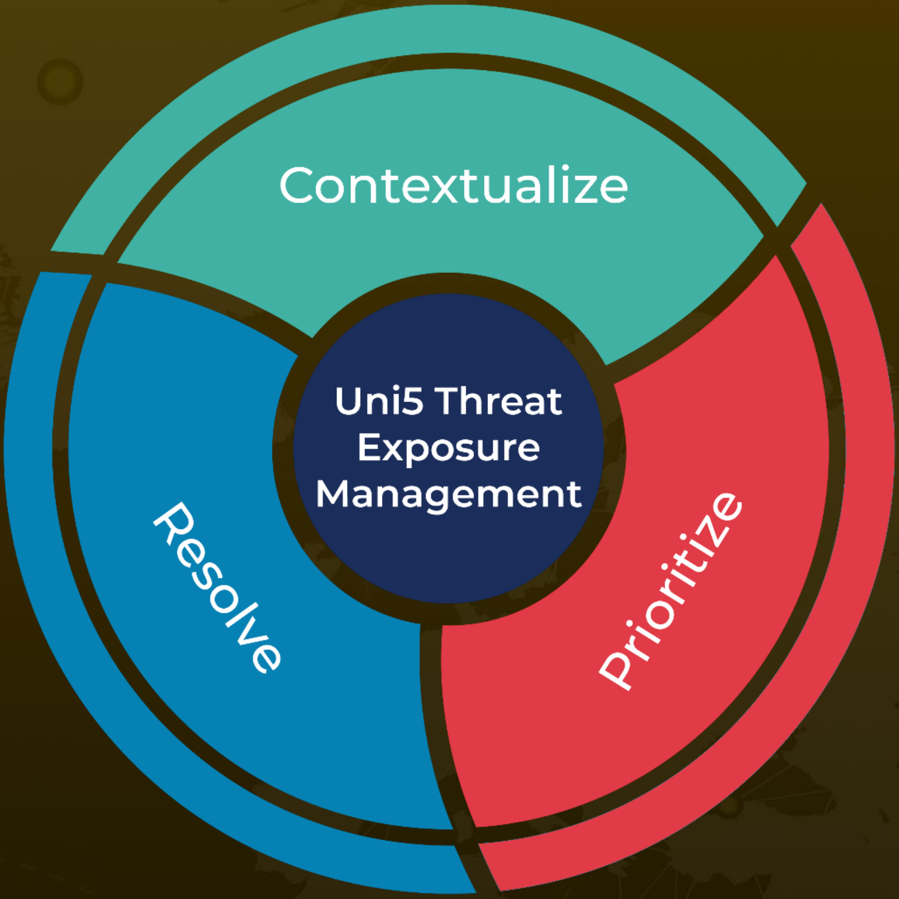
References

https://www.fortinet.com/blog/threat-research/vcurms-a-simple-and-functional-weapon

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

March 13, 2024 • 6:30 AM

More at www.hivepro.com