Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Venom Spider's Victim-Specific Malware Tactics Decoded

Date of Publication	Admiralty Code	TA Number
December 5, 2024	A1	TA2024452

Summary

Attack Commenced: August 2024
Threat Actor: Venom Spider (aka GOLDEN CHICKENS)
Malware: RevC2, Venom Loader
Targeted Region: Worldwide

Attack: Venom Spider, is a notorious threat actor offering advanced Malware-as-a-Service (MaaS) tools, which have also been used by other threat groups such as FIN6 and Cobalt. Their arsenal now includes two new malware families, RevC2 and Venom Loader, specifically designed for highly targeted cyberattacks.

Attack Regions

Attack Details

#1 Venom Spider, also known as GOLDEN CHICKENS, is a prominent threat actor specializing in offering Malware-as-a-Service (MaaS) tools. Their portfolio includes VenomLNK, TerraLoader, TerraStealer, and TerraCryptor, which have been leveraged by notorious threat groups such as FIN6 and Cobalt in the past.

#2 These tools are designed to facilitate the deployment of advanced malware and enable sophisticated cyberattacks. Two newly identified malware families, RevC2 and Venom Loader, have been deployed using Venom Spider's MaaS tools.

#3 RevC2 is a backdoor designed to exfiltrate sensitive data while maintaining covert communication with its command-and-control (C2) server through WebSockets. It possesses diverse capabilities, including stealing cookies and passwords, proxying network traffic, and executing remote code (RCE).

#4 In contrast, Venom Loader acts as a customizable malware loader tailored for each victim by encoding the payload with the victim's computer name. Upon execution, RevC2 performs two system checks to confirm specific criteria before proceeding with a measure designed to evade detection in analysis environments such as sandboxes.

#5 The backdoor’s functionality includes communicating with its C2 server via the websocketpp C++ library, exfiltrating passwords and cookies from Chromium-based browsers, capturing screenshots, proxying network traffic through the SOCKS5 protocol, and executing commands under different user contexts using stolen credentials.

#6 A distinctive feature of Venom Loader is its highly targeted approach. Each DLL file used in observed campaigns is uniquely built for the intended victim, ensuring the payload is specifically tailored to the target. This customization enhances the stealth and effectiveness of the malware, making it a key tool in Venom Spider's arsenal.

Recommendations

Implement Endpoint Detection and Response (EDR): Deploy advanced EDR solutions to monitor and respond to suspicious activities, including sandbox evasion and C2 communications.

Monitor Anomalous File Execution: Continuously track the execution of unknown or suspicious DLL files, as malware like Venom Loader uses custom-built DLLs for targeted attacks. Use file integrity monitoring (FIM) to detect and alert on unrecognized files. Implement application control to block unauthorized files and use sandboxing or behavioral analysis to assess unknown DLLs before execution. This helps prevent malicious payloads from activating and ensures early detection of suspicious activity.

Audit Third-Party Tools: Regularly review and assess the security of third-party software, services, and integrations to identify potential vulnerabilities that could be exploited by malware like Venom Loader. Prioritize auditing tools used for remote access, file sharing, or browser extensions, as these can be potential entry points for attackers. Limit usage to trusted, verified tools, and ensure that they are updated with the latest security patches.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**TA0010** Exfiltration
T1547 Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1140** Deobfuscate/Decode Files or Information	**T1574** Hijack Execution Flow
T1574.002 DLL Side-Loading	**T1539** Steal Web Session Cookie	**T1555** Credentials from Password Stores	**T1113** Screen Capture
T1090 Proxy	**T1059** Command and Scripting Interpreter	**T1571** Non-Standard Port	**T1071** Application Layer Protocol
T1071.001 Web Protocols	**T1041** Exfiltration Over C2 Channel		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	153cd5a005b553927a94cc7759a8909bd1b351407d8d036a1bf5fcf9ee83192e, 46a982ec4ea400f8df403fa8384e1752dca070bd84beef06284f1d412e159e67, 8e16378a59eb692de2c3a53b8a966525b0d36412bfd79c20b48c2ee546f13d04, 9b0b58aa10577244bc0e174d588ffa8d34a54a34c1b59371acba52772b584707, cf45f68219c4a105fffc212895312ca9dc7f4abe37306d2f3b0f098fb6975ec7, f93134f9b4ee2beb1998d8ea94e3da824e7d71f19dfb3ce566e8e9da65b1d7a2
URLs	hxxp[:]//170[.]75[.]168[.]151[:]8080/transaction[.]pdf[.]lnk/, hxxp[:]//65[.]38[.]121[.]211/api/infos, ws[:]//208[.]85[.]17[.]52[:]8082, ws[:]//nopsec[.]org[:]8082/

References

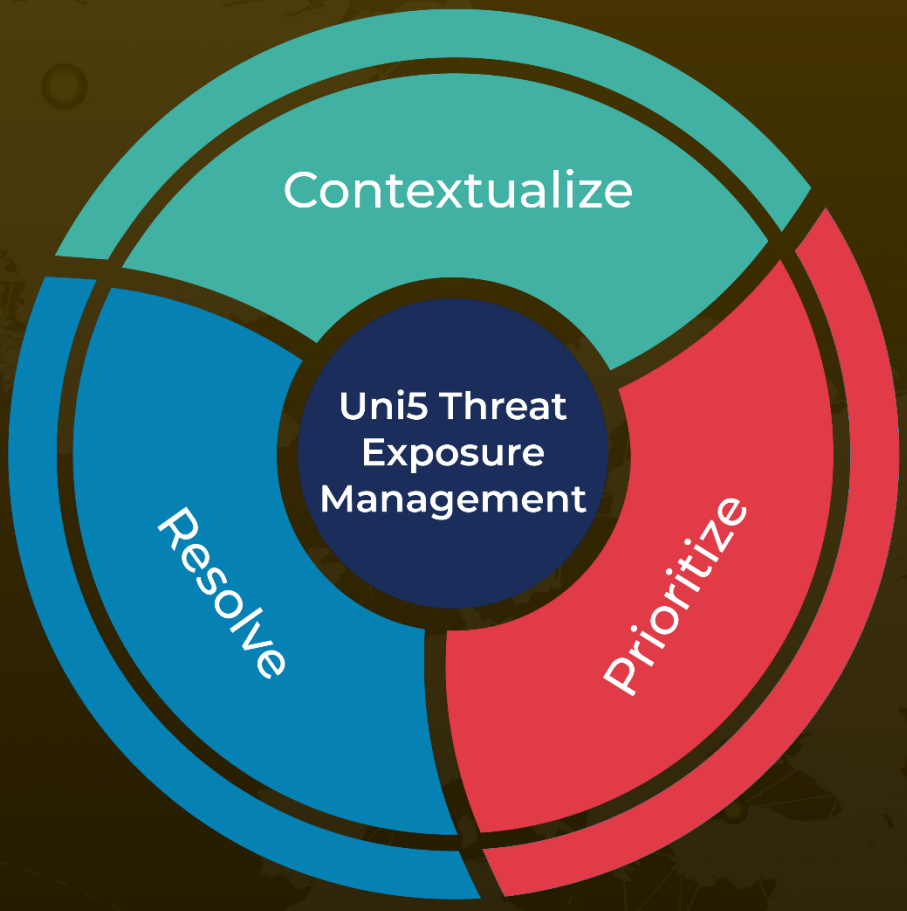
https://www.zscaler.com/blogs/security-research/unveiling-revc2-and-venom-loader

https://github.com/ThreatLabz/tools/tree/main/revc2

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

December 5, 2024 • 3:30 AM

More at www.hivepro.com