Hive Pro

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

# Snip3 Crypter an Advanced RAT Loader Targeting Multiple Industries

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| March 2, 2023 | A1 | TA2023114 |

# Summary

**First appeared:** 2021
**Malware:** Snip3 Crypter
**Attack Region:** Worldwide
**Attack Sector:** Healthcare, Energy, Oil and gas, Manufacturing, Raw materials, Finance, Retail, and Technology
**Attack:** A multi-stage remote access trojan (RAT) loader called Snip3 crypter was recently discovered deploying RAT families, including QuasarRAT and DcRAT, to target victims across multiple industry verticals.

## Attack Regions

# Attack Details

**#1**

Snip3 Crypter is a crypter-as-a-service offering that has been available since 2021. It employs advanced evasion, obfuscation, and reflective code-loading techniques in its multi-stage infection chain. The crypter has been enhanced with sophisticated techniques that enable it to effectively deploy the final Remote Access Trojan (RAT) payload while evading detection. The attack begins with a spear-phishing email that uses bait related to "tax statements" to entice victims into executing the multi-staged infection chain.

**#2**

The initial VBS payloads were downloaded as an attachment via a phishing email. When executed, it creates an ADODB connection and a record object to connect to a database. To evade detection from static string-based signatures, the script decodes a Downloader PowerShell script.

**#3**

After the decoded downloader PowerShell script is executed, the Stage-2 PowerShell script is downloaded in byte format. The Stage-3 PowerShell script then collects system information, organizes the data, and stores it. Once persistence is established, the Stage-4 PowerShell script is executed from the download server by invoking Powershell.exe with a hidden window style from the temp path. Finally, the "Snip3 Crypter crew" acts as the ultimate loader in the infection chain, delivering and executing QuasarRAT and DcRAT on the target machines.

# Recommendations

**Security Leaders**

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

**Security Engineers**

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

# Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0002<br>Execution | TA0004<br>Privilege Escalation | TA0005<br>Defense Evasion | TA0006<br>Credential Access |
| TA0007<br>Discovery | TA0009<br>Collection | TA0011<br>Command and Control | T1055<br>Process Injection |
| T1056<br>Input Capture | T1562<br>Impair Defenses | T1059<br>Command and Scripting Interpreter | T1497<br>Virtualization/Sandbox Evasion |
| T1027<br>Obfuscated Files or Information | T1027.002<br>Software Packing | T1036<br>Masquerading | T1003<br>OS Credential Dumping |
| T1082<br>System Information Discovery | T1518<br>Software Discovery | T1518.001<br>Security Software Discovery | T1010<br>Application Window Discovery |
| T1057<br>Process Discovery | T1005<br>Data from Local System | T1095<br>Non-Application Layer Protocol | T1566<br>Phishing |

# Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| URLs | hxxp[:]//$IP:Port/Vre<br>pastetext[.]net/raw/lcscgt0mss<br>toptal[.]com/developers/hastebin/raw/buliforayu |
| MD5 | bd23ae38590d87243af890505d6fbeec<br>a41de1ef870e970e265cc35b766a5ec8<br>a5b76ca780ddff061db6f86f03d3b120<br>b78c9bb6070340bb4d352c712a0a28b7<br>923f46f8a9adfd7a48536de6f851d0f7<br>dda2ba195c9ebc9f169770290cd9f68a<br>ef2236c85f915cae6380c64cc0b3472a<br>0bbc89719ff3c4a90331288482c95eac |
| IPV4 | 185[.]81[.]157[.]59<br>185[.]81[.]157[.]172<br>185[.]81[.]157[.]136<br>185[.]81[.]157[.]117<br>185[.]81[.]157[.]203 |

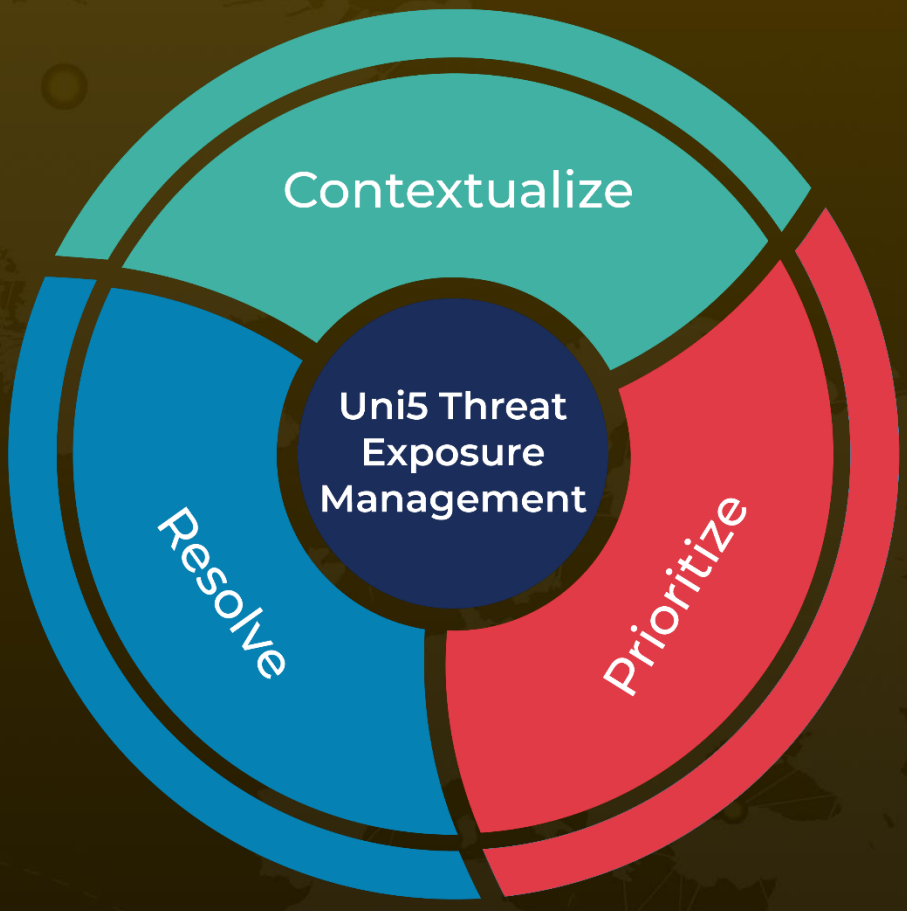
# References

https://www.zscaler.com/blogs/security-research/snip3-crypter-reveals-new-ttps-over-time

# 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 2, 2023 • 3:33 AM**

© 2023 All Rights are Reserved by HivePro

More at www.hivepro.com