Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

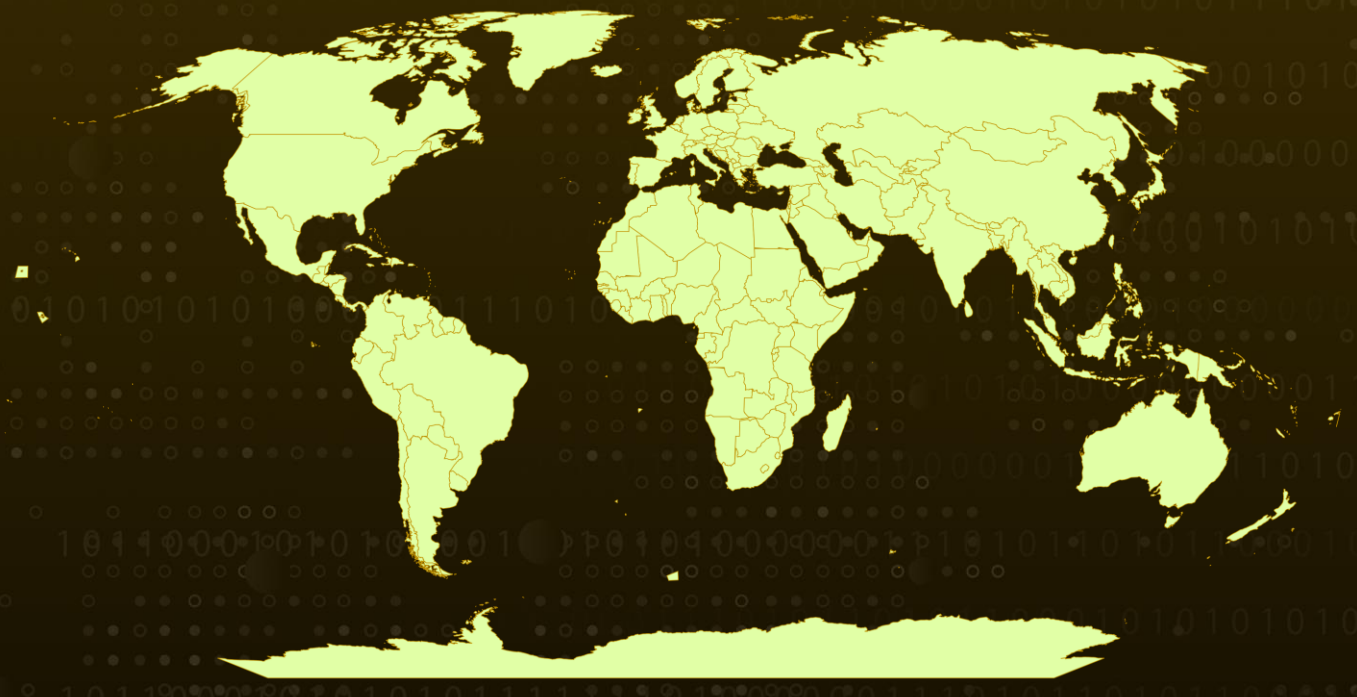
InnoLoader Malware Stealth Mastery, Unique Instances per Download

Date of Publication	Admiralty Code	TA Number
June 28, 2024	A2	TA2024249

Summary

Attack Began: June 2024
Targeted Countries: Worldwide
Malware: InnoLoader
Affected Platform: Windows
Attack: InnoLoader is a new unique malware that generates a distinct version with each download, complicating detection. It disguises itself as an installer, executing malicious actions and downloading additional payloads like StealC Infostealer and Socks5Systemz proxy malware. The malware adapts its behavior based on C2 server instructions to evade detection.

Attack Regions



Attack Details

#1

A new type of InnoSetup based malware named "InnoLoader," is unique as it creates a distinct version of itself with every download attempt. This technique makes it especially challenging for security solutions to detect and mitigate the threat. The malware is disguised as a legitimate installer and initiates its malicious activities when the user interacts with the installation prompts. Inno Setup is a free and popular tool for creating software installers specifically for Windows.

#2

InnoLoader's primary function is to download and execute additional malicious payloads. Among these are the StealC Infostealer, which is designed to harvest sensitive information, the Socks5Systemz proxy malware, which facilitates network-based attacks, and masquerades as a security browser plugin, and transforms into a commercial proxy resource and clicker. These payloads enable the attacker to perform a variety of malicious activities, from stealing data to controlling infected systems remotely.

#3

One of the most concerning aspects of InnoLoader is its ability to adapt its behavior based on instructions from its command-and-control (C2) server. This feature allows the malware to change its tactics to evade detection and analysis, making it a highly versatile and persistent threat. The dynamic nature of its operations means that it can continually evolve, posing ongoing challenges for cybersecurity professionals.

Recommendations

Monitoring and Detection: Deploy advanced threat detection and monitoring tools capable of identifying and mitigating malware attacks in real-time. This includes behavior-based analytics, intrusion detection systems, and endpoint protection solutions.

Regular Software Updates: Keep all software, including operating systems and applications, updated with the latest patches to close vulnerabilities that malware can exploit.

Network Segmentation: Segment networks to limit the spread of malware infections. Restrict access to sensitive systems and data, and implement firewalls and access controls to prevent lateral movement by attackers.

Potential MITRE ATT&CK TTPs

TA0011 Command and Control	TA0002 Execution	TA0003 Persistence	TA0010 Exfiltration
TA0005 Defense Evasion	TA0009 Collection	TA0006 Credential Access	TA0007 Discovery
T1036 Masquerading	T1204 User Execution	T1204.002 Malicious File	T1059.003 Windows Command Shell
T1059 Command and Scripting Interpreter	T1218 System Binary Proxy Execution	T1218.007 Msiexec	T1041 Exfiltration Over C2 Channel
T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers	T1082 System Information Discovery	T1027 Obfuscated Files or Information
T1547.009 Shortcut Modification	T1547 Boot or Logon Autostart Execution	T1105 Ingress Tool Transfer	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	b4c9d60f0e2c57c34ec6cb4a564c7ee1, 2e85211a7ab36e6d7e2a4a4b5d88b938, 6b5730e49a37d6ffee273790449ac037, 0283c9517cfb46faec1735262bd58654, fa24733f5a6a6f44d0e65d7d98b84aa6, 95007206c6b2407fb69748ef7c93612 , 1b3ad155c454d3351cfc107344bc4ad5, f8bb5272ce5d5b2e767f85e788dd4c5c , 0738205d5a1472662b94561e004d9803, ff640a60d25e4bcf1ef290c3d1893a17
Hostname	d9500682396017175017969210108a04a635094d7af3f018356690047bce5.aoa.aent78[.]sbs, e38ee82150cc00a8627814c6.bag.sack54[.]net

TYPE	VALUE
URL	hxxp://monkeyagreement[.]fun/coo.php?paw=883174&spot=1&a=2857&on=444&o=1678, hxxp://240601155506901.try.kyhd08[.]buzz/f/fvgbm0601901.txt, hxxp://monkeyagreement[.]fun/coo.php?paw=762694&spot=2&a=2857&on=458&o=1688, hxxps://cdn-edge-node[.]com/online_security_mkl.exe, hxxp://monkeyagreement[.]fun/coo.php?paw=401610&spot=3&a=2857&on=420&o=1662, hxxp://monkeyagreement[.]fun/coo.php?paw=895836&spot=4&a=2857&on=418&o=1660, hxxps://song.oaksfoxes[.]ltd/tid/202.exe, hxxp://monkeyagreement[.]fun/coo.php?paw=956684&spot=5&a=2857&on=460&o=1690, hxxp://monkeyagreement[.]fun/coo.php?paw=787557&spot=6&a=2857&on=244&o=331, hxxp://kapetownlink[.]com/installer.exe, hxxp://93.123.39[.]135/129edec4272dc2c8.php,
Domains	valuescent[.]website, caretouch[.]hair, whipunit[.]hair, eyesnose[.]hair, nightauthority[.]xyz, cattlebusiness[.]icu, monkeyagreement[.]fun, laughvein[.]hair, brotherpopcorn[.]website, selectionword[.]xyz

References

https://asec.ahnlab.com/en/67502/

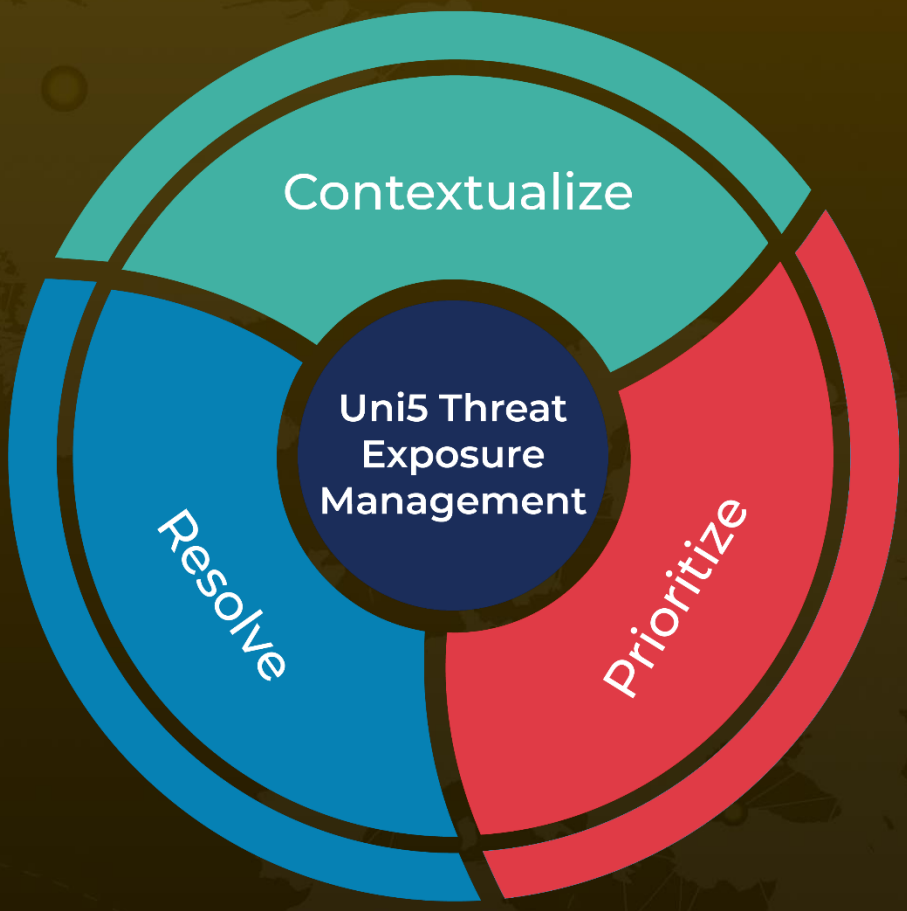
https://www.hivepro.com/a-new-info-stealing-malware-named-stealc-targeting-cryptocurrency-wallets/

https://www.hivepro.com/threat-advisory/socks5systemz-proxy-botnet-infects-10000-systems/

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

June 28, 2024 • 5:00 AM

More at www.hivepro.com