Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

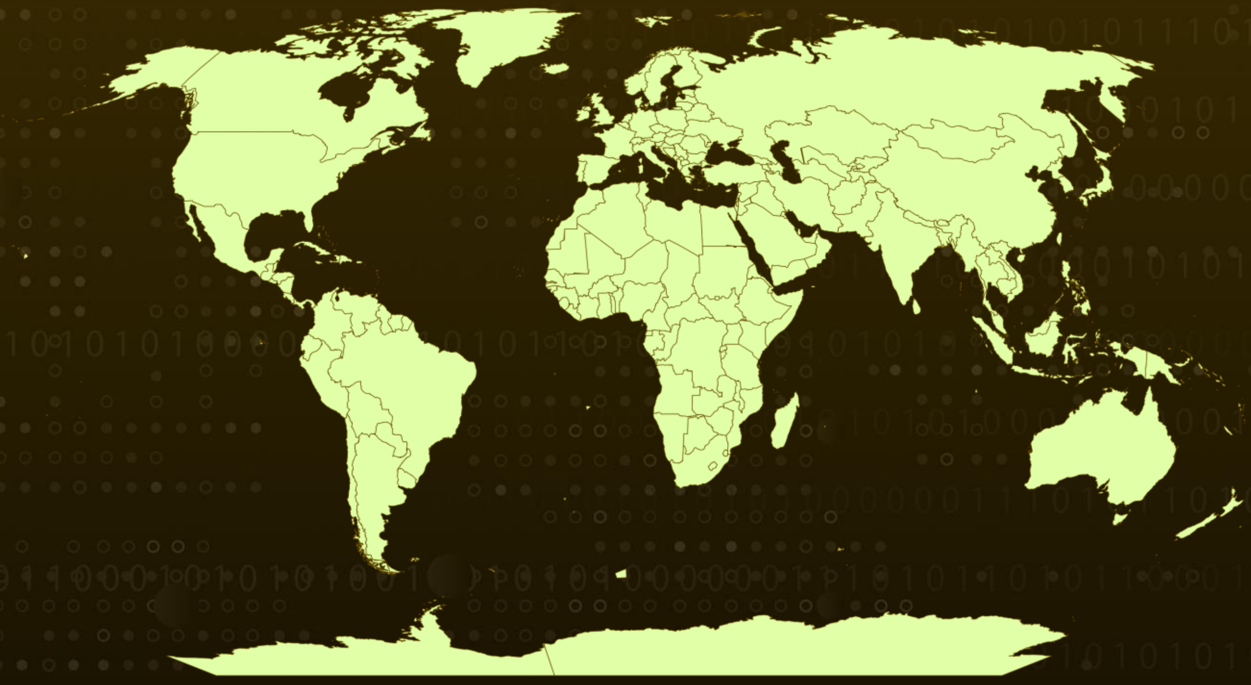
HookSpoofer A Novel Infostealer with Advanced Capabilities

Date of Publication	Admiralty Code	TA Number
March 20, 2023	A1	TA2023146

Summary

First appeared: March 2023
Malware: HookSpoofer Infostealer
Attack Region: Worldwide
Attack: HookSpoofer, the latest Infostealer with keylogging and clipper functionalities, has been disseminated by multiple bundlers.

Attack Regions



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

Attack Details

#1

Several bundlers are spreading HookSpoofer, a novel Infostealer with keylogging and clipper capabilities. HookSpoofer is written in C# and is an enhanced version of Stormkitty, an open-source stealer available on GitHub. This bundler contains 17 files, with the primary executable being distributed as "spotify checker.exe," which is the HookSpoofer stealer.

#2

HookSpoofer includes AntiAnalysis strategies for detecting VirtualBox, SandBox, Debugger, VirusTotal, and Any.Run. Every piece of information captured in %Appdata% is saved in a folder and then archived as a password-protected zip file. This zip file is then uploaded to "anonfile.com/message id>" and the resulting link is sent to the Telegram bot.

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 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
T1047 Windows Management Instrumentation	T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading	T1027 Obfuscated Files or Information
T1027.002 Software Packing	T1036 Masquerading	T1003 OS Credential Dumping	T1010 Application Window Discovery
T1560 Archive Collected Data	T1071 Application Layer Protocol	T1105 Ingress Tool Transfer	T1095 Non-Application Layer Protocol

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	bd4345c3a7cc6f6e261986e1f5f1e8bc de90466d983da595e863339c34ee4b6b 7fce055a581c0b116a9679291bf89b7d 474e0cd6bc1f0fb71bbffa1ae7dd8e66

References

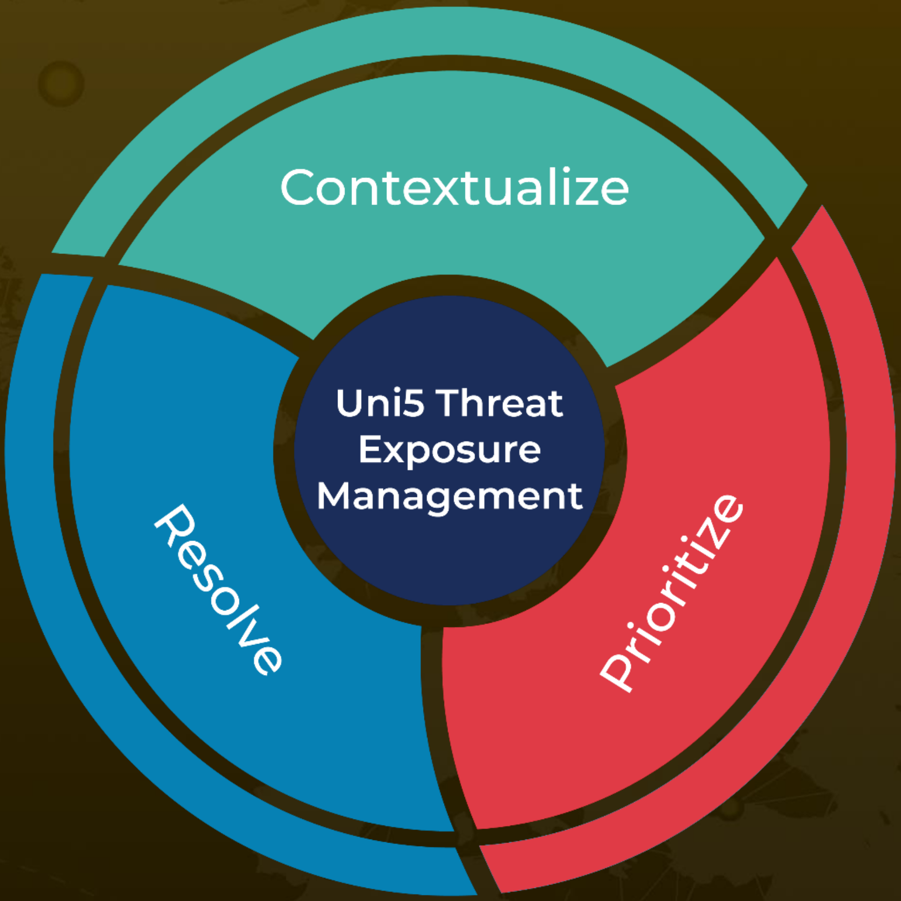
https://www.uptycs.com/blog/threat-research-hookspoofer

https://github.com/LimerBoy/StormKitty

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 20, 2023 • 6:30 AM

More at www.hivepro.com