Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

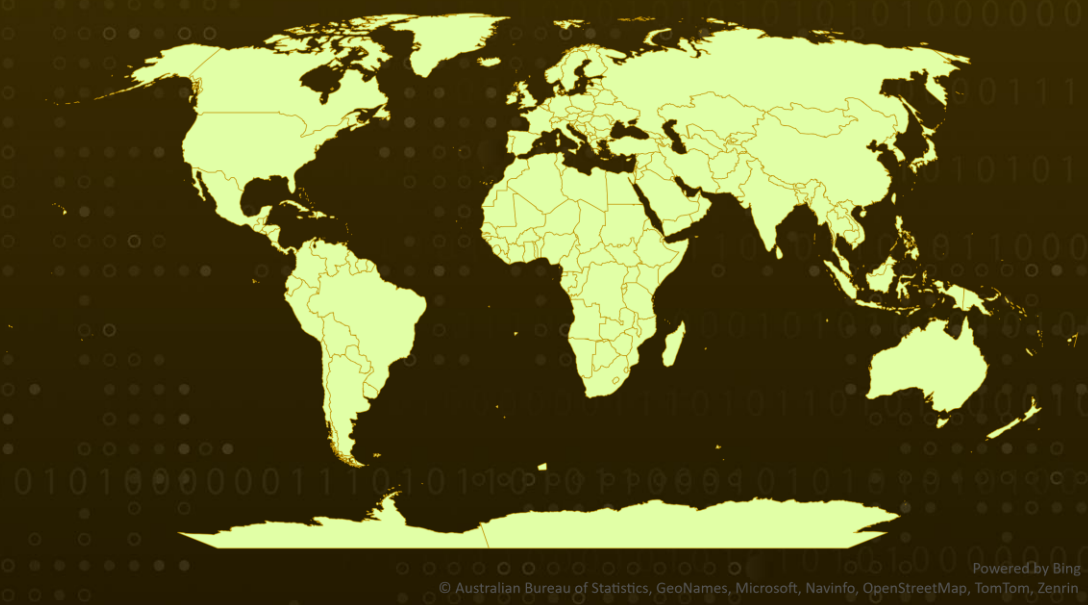
Malware Impersonating Websites Spread via Google Ads

Date of Publication	Admiralty Code	TA Number
March 16, 2023	A1	TA2023139

Summary

First Appeared: February 2023
Attack Region: Worldwide
Malware: Vidar, Ursnif, & BatLoader
Attack: Multiple Malware were found on newly registered websites impersonating various applications, likely originating from malicious Google Search Ads.

Attack Regions



Attack Details

#1 In February 2023, it was discovered that a number of newly registered websites were pretending to be different applications. These websites were hosting fake download pages and using a malware called BatLoader to launch hidden Python scripts.

#2 The Python files were protected with PyArmor and designed to retrieve an encrypted payload and execute either Ursnif or Cobalt Strike. BatLoader has been associated with other payloads like Redline Stealer, SystemBC RAT, Syncro RMM, and Vidar Stealer. It is suspected that the malware originated from malicious ads on Google Search Ads.

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

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	T1055 Process Injection	T1036 Masquerading
T1016 System Network Configuration Discovery	T1547 Boot or Logon Autostart Execution	T1059 Command and Scripting Interpreter	T1199 Trusted Relationship

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	3db1edc5b5550f54abdcb5520cf91d75 0cb75b1192b23b8e03d955f1156ad19e 85fbc743bb686688ce05cf3289507bf7 11ae3dabdb2d2458da43558f36114acb 9ebbe0a1b79e6f13bfca014f878ddeec
Domains	chatgpt-t[.]com zoomvideor[.]com adobe-l[.]com freecad-l[.]com microso-t[.]com spotify-uss[.]com quickbooks-q[.]com freecad-f[.]com2 java-s[.]com adobe-e[.]com anydesk-o[.]com anydesk-r[.]com java-r[.]com tableau-r[.]com java-a[.]com basecamp-a[.]com adobe-a[.]com visualstudio-t[.]com openoffice-a[.]com bitwarden-t[.]com gimp-t[.]com figma-t[.]com6 shvarcnegerhistory[.]com Pixelarmada[.]su uelcoskdi[.]ru iujdhsndjfks[.]ru isoridkf[.]ru gameindikdowd[.]ru jhgfdlkjhaoiu[.]su reggy506[.]ru reggy914[.]ru

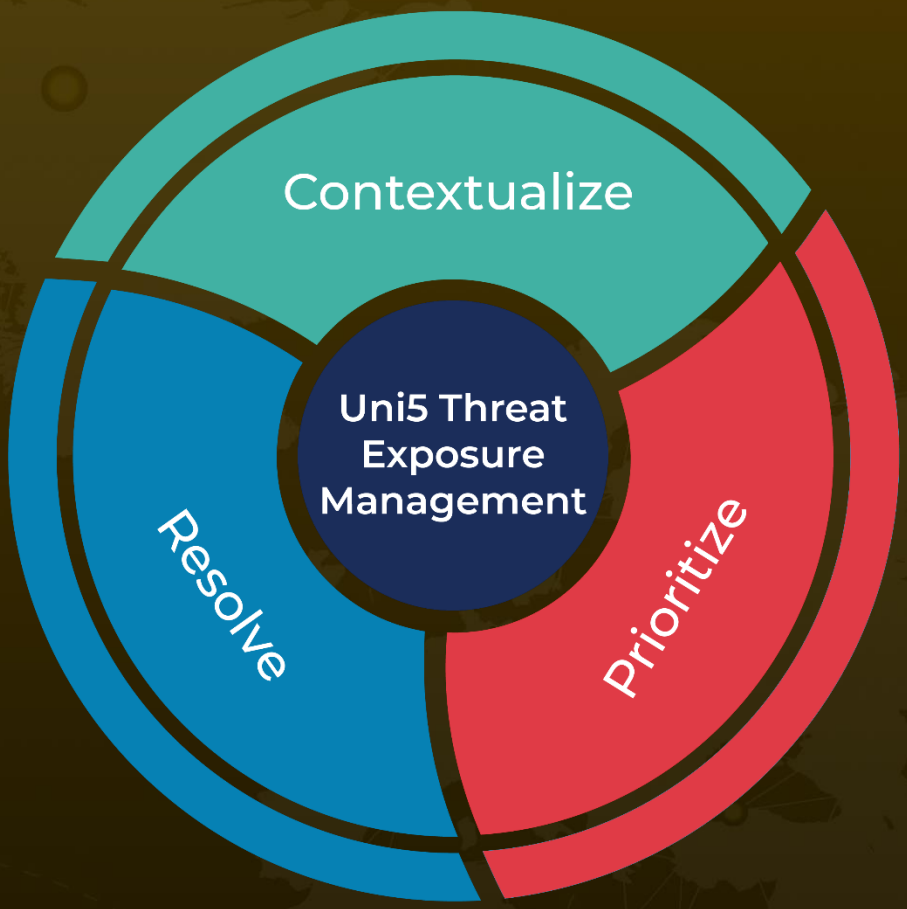
References

https://www.esentire.com/blog/batloader-continues-to-abuse-google-search-ads-to-deliver-vidar-stealer-and-ursnif

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 16, 2023 • 1:20 AM

More at www.hivepro.com