Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

MetaStealer a $125 Ticket to Digital Chaos

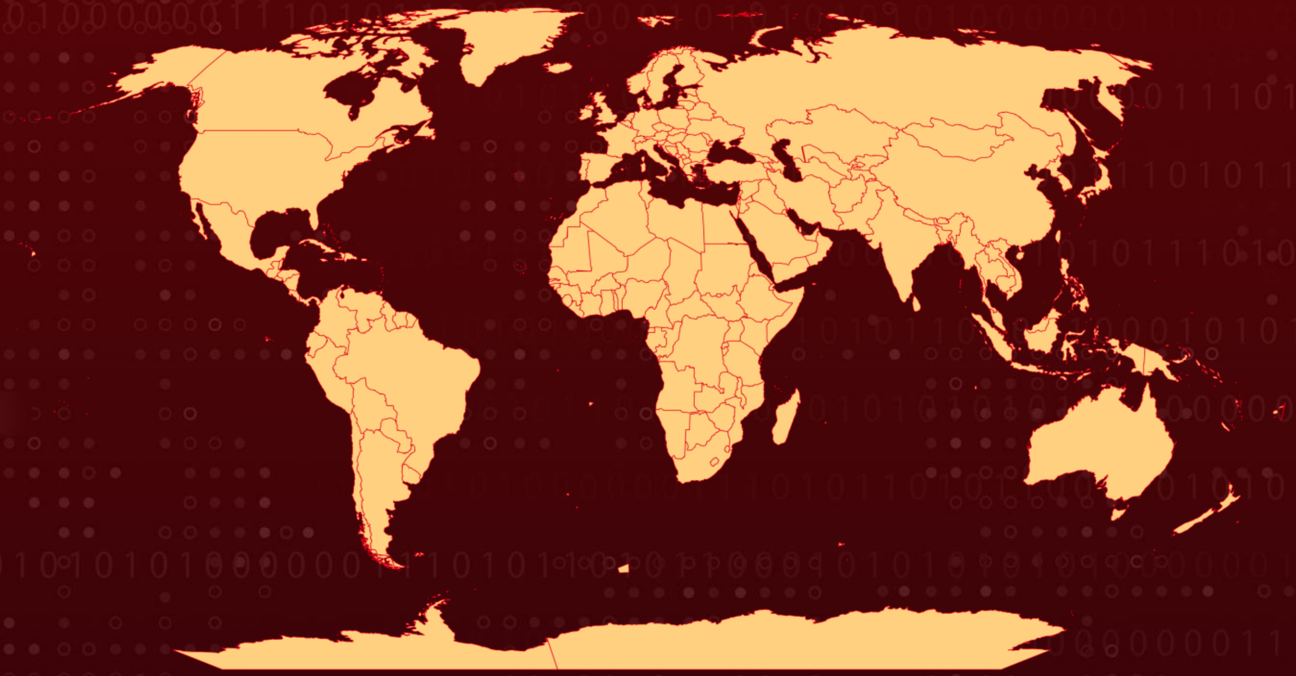
Date of Publication	Admiralty Code	TA Number
December 26, 2023	A1	TA2023520

Summary

First Seen: March 2022
Malware: MetaStealer
Attack Region: Worldwide

Attack: MetaStealer, a nefarious information-stealing malware, initially surfaced in discreet online marketplaces with a pricing structure of USD 125 per month or USD 1000 for an unlimited subscription, subsequently becoming entangled in malvertising campaigns.

Attack Regions



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

Attack Details

#1 MetaStealer, an information-stealing malware, initially surfaced in March 2022 within covert online marketplaces before becoming entangled in malvertising campaigns disseminated through compromised software and pilfered YouTube accounts. The MetaStealer malware is available for purchase at USD 125 per month or USD 1000 for an unlimited subscription.

#2 The malicious actor behind this threat alleges that it shares identical functionality, codebase, and control panel with the Redline stealer, boasting several enhancements. The initial phase of the attack sequence involves the distribution of MetaStealer through deceptive emails disguised as correspondences related to financial transactions or malvertising campaigns, complete with decoy and landing pages.

#3 These emails are equipped with an Excel document containing a VBS macro. Once the target accepts the document, the malware is downloaded and executed. Following a system reboot, the file initiates communication with a command-and-control (C2) server, thereby establishing a persistent mechanism.

#4 MetaStealer is meticulously crafted to stealthily infiltrate target systems, facilitating the potential theft of passwords, cryptocurrency wallets, banking information, identity compromise, and financial losses. The most recent iteration, Meta V4, was unveiled on November 28th, 2023. The emergence of MetaStealer underscores a dynamic threat landscape, with significant implications, particularly within business settings.

Recommendations

Enhance Network Security Measures: Strengthen network security protocols to guard against potential infiltrations by MetaStealer and related threat clusters. Employ robust firewalls and intrusion detection systems, and regularly update security software to mitigate vulnerabilities.

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Email Security Enhancements: Implement advanced measures to filter out malicious emails, especially those carrying attachments with VBS macros, and utilize email authentication protocols to verify the legitimacy of incoming emails.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0011 Command and Control
TA0010 Exfiltration	T1657 Financial Theft	T1018 Remote System Discovery	T1059 Command and Scripting Interpreter
T1053 Scheduled Task/Job	T1053.005 Scheduled Task	T1055 Process Injection	T1059.001 PowerShell
T1083 File and Directory Discovery	T1082 System Information Discovery	T1071 Application Layer Protocol	T1071.001 Web Protocols
T1659 Content Injection	T1566 Phishing	T1566.001 Spearphishing Attachment	T1562 Impair Defenses
T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution	T1555 Credentials from Password Stores	T1078 Valid Accounts

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps[:]//rawnotepad[.]com/notepad++.zip, hxxps[:]//startworkremotely[.]com/Anydesk.zip
SHA256	949c5ae4827a3b642132faf73275fb01c26e9dce151d6c5467d3014f208f77ca, 991230636 90e244f95b89d96759ec7dbc28d4079a56817f3152834047ab047eb, c5597da40dee419696ef2b32cb937a11fcad40f4f79f9a80f6e326a94e81a90f, 7ce94c2008d904e10ddecb401307f4cb5182b5989d594e416c9891b817c3d356

TYPE	VALUE
Domains	rawnotepad[.]com, startworkremotely[.]com, wgcuwcgociewewoo[.]xyz, ockimqekmwecocug[.]xyz, kiqewcsyeyaeusag[.]xyz, cewgwsyookogmmki[.]xyz, startworkremotely[.]com, csyeywqwyikqaiim[.]xyz, iqaeaoeueeqouweo[.]xyz, mmswgeewswyyywqk[.]xyz, accounts[.]google[.]com, iqwgwsigmigiqgoa[.]xyz
MD5	32d319d9677635f995f4e009db2e85a1
SHA1	4770af11a733c00ee8c1e7613f64690361f7d9af

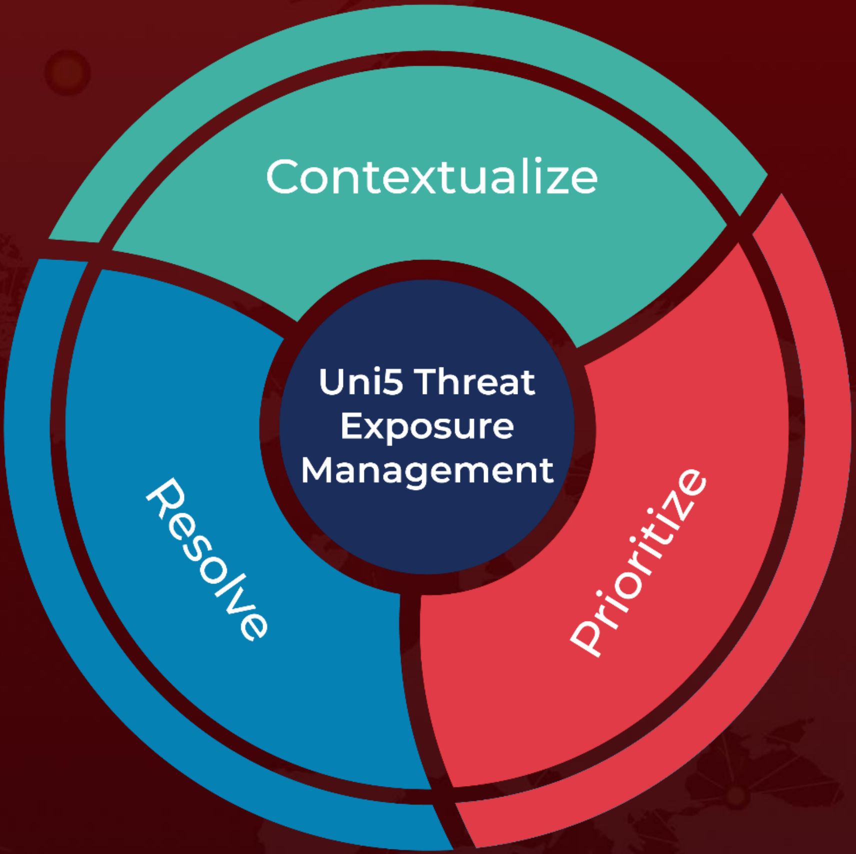
References

https://www.malwarebytes.com/blog/threat-intelligence/2023/12/new-metastealer-malvertising-campaigns

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 26, 2023 • 4:00 AM

More at www.hivepro.com