Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

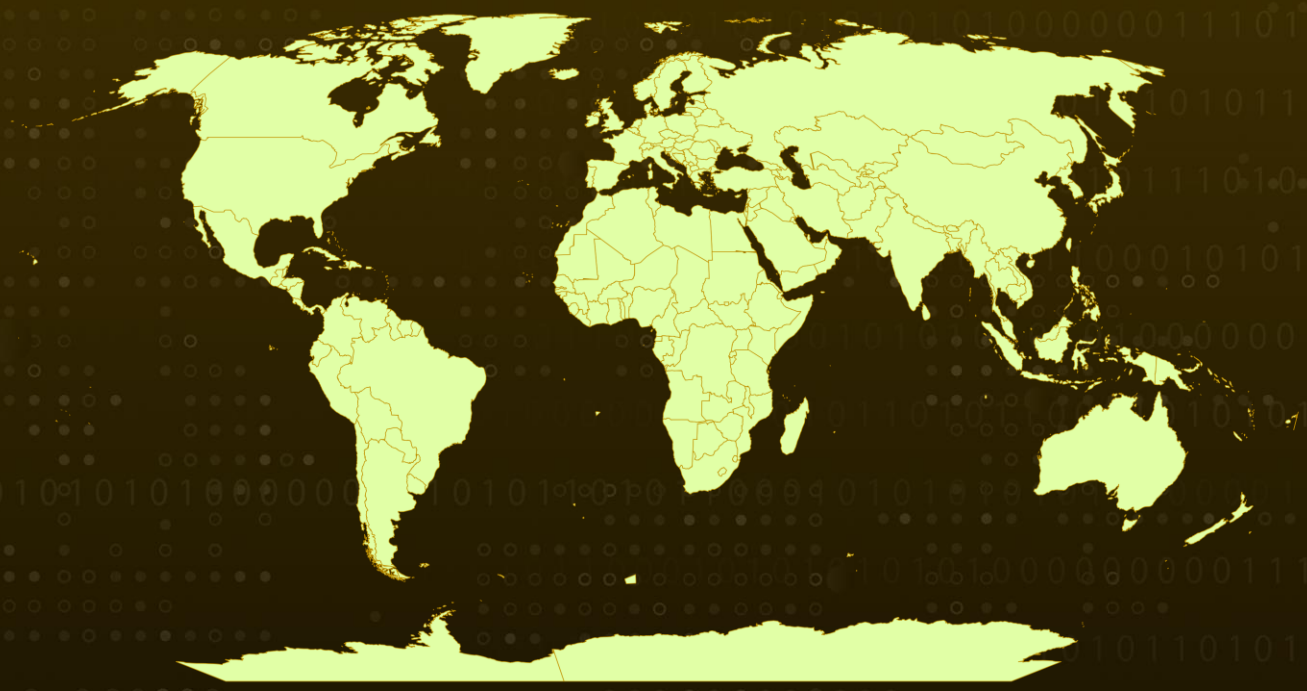
Rhadamanthys: A New Evasive Information Stealer

Date of Publication	Admiralty Code	TA Number
January 17, 2023	A1	TA2023027

Summary

First appeared: January 2023
Attack Region: Worldwide
Attack: Rhadamanthys Evasive Infostealer is spread through phishing emails and prevalent Google ads that lead to fake download pages for popular workforce software.

Attack Regions



Attack Details

#1

Rhadamanthys Stealer is a new malware strain that is still active today. It is marketed as "malware-as-a-service" (MaaS) and spreads through Google Ads, directing victims to phishing websites that mimic Zoom, AnyDesk, Notepad++, and Bluestacks. It can also be distributed through spam email attachments containing malicious payload.

#2

When the file is executed, a folder containing two hidden binary executable files is created in the %temp% directory. The initial installation files are obfuscated Python code, and the end payload of the Rhadamanthys stealer is decoded as a 32-bit executable file compiled with the Microsoft Visual C/C++ compiler.

#3

It captures information from the victim's crypto wallet browser extensions that are hard-coded into the stealer binary and sends all of the stolen information to the attacker's command and control server. It is crucial for users to be vigilant when receiving spam emails or visiting phishing websites and to verify the source before downloading any software.

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	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
T1598 Phishing for Information	T1598.002 Spearphishing Attachment	T1204 User Execution	T1059 Command and Scripting Interpreter
T1055 Process Injection	T1218 System Binary Proxy Execution	T1218.011 Rundll32	T1027 Obfuscated Files or Information
T1497 Virtualization/Sandbox Evasion	T1003 OS Credential Dumping	T1056 Input Capture	T1552 Unsecured Credentials
T1552.002 Credentials in Registry	T1082 System Information Discovery	T1518 Software Discovery	T1083 File and Directory Discovery
T1087 Account Discovery	T1005 Data from Local System	T1114 Email Collection	T1071 Application Layer Protocol
T1095 Non-Application Layer Protocol	T1105 Ingress Tool Transfer		

Indicators of Compromise (IOCs)

TYPE	VALUE
URL	hxxps[:]\\zolotayavitrina[.]com/Jan-statement[.]exe
Domains	bluestacks-install[.]com zoomus-install[.]com install-zoom[.]com install-anydesk[.]com install-anydeslk[.]com zoom-meetings-install[.]com zoom-meetings-download[.]com anydleslk-download[.]com zoomvideo-install[.]com zoom-video-install[.]com istaller-zoom[.]com noteepad.hasankahrimanoglu[.]com[.]tr

TYPE	VALUE
SHA256	046981c818bd26e7c28b12b998847038e6b64c44df6645438dae689d75fb0269 4f4b5407d607ee32e00477a9f4294600ca86b67729ff4053b95744433117fccf 4a55c833abf08ecfe4fb3a7f40d34ae5aec5850bc2d79f977c8ee5e8a6f450d4 093a58f36c075644d1dc8856acdefad7fd22332444b6aa07fee2ad615d50b743 db66fc58c07ba0ccbe1b9c2db770179d0d931e5bf73838da9c915581661d4c1a fe99a49596fc6f841b7605021da6fce7f6c817d5247d880227f790388a7cabe4

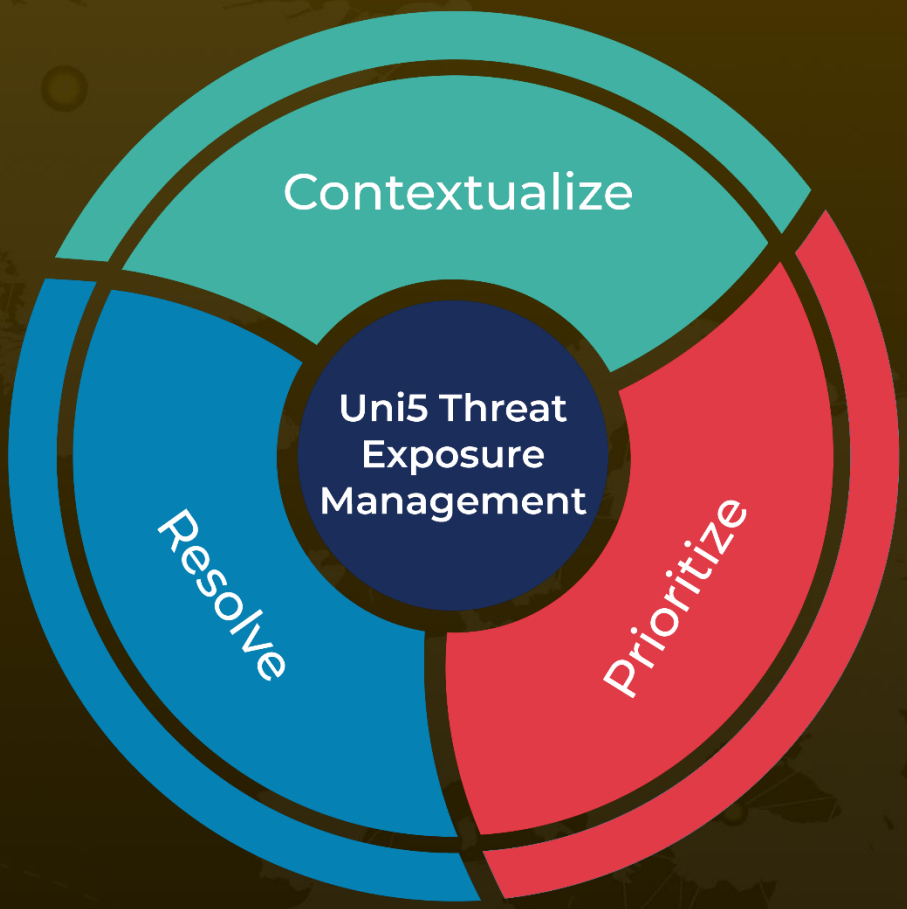
References

https://blog.cyble.com/2023/01/12/rhadamanthys-new-stealer-spreading-through-google-ads/

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

January 17, 2023 . 2:22 AM

More at www.hivepro.com