Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

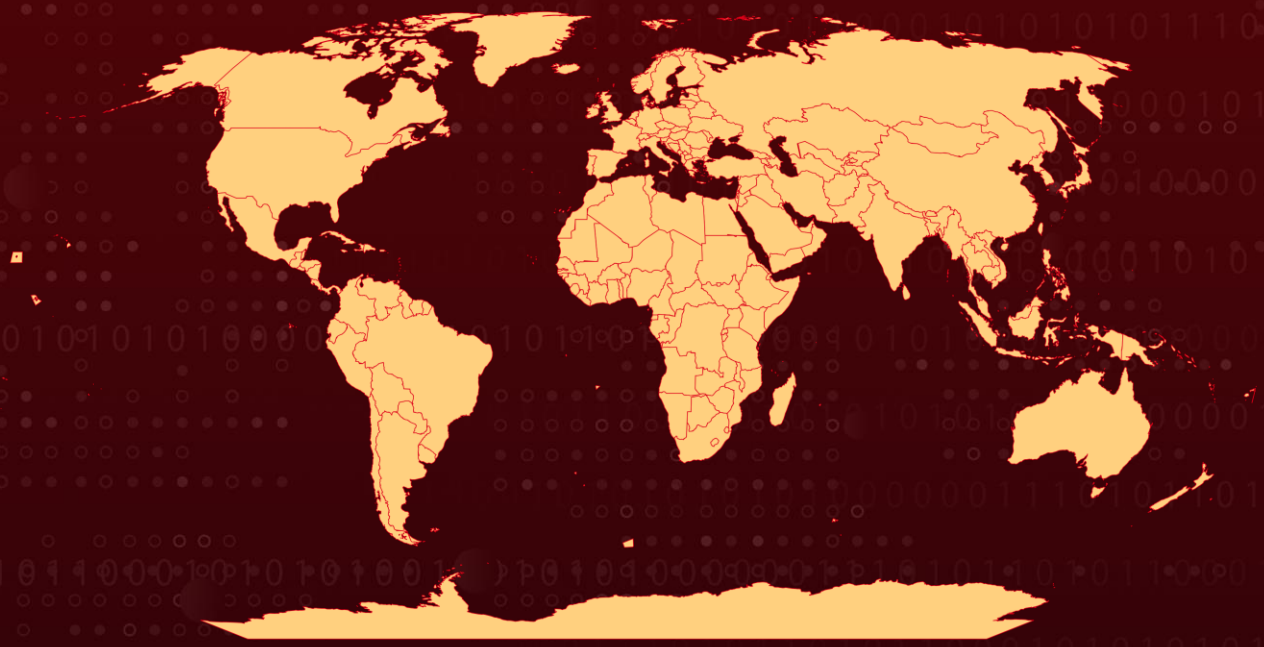
Adversaries Leverage Social Media to Disseminate New Python-Based Stealer

Date of Publication	Admiralty Code	TA Number
December 13, 2023	A1	TA2023500

Summary

Attack Discovered: December 2023
Attack Region: Worldwide
Targeted Industries: Social Media
Malware: Editbot Stealer
Attack: A recently identified malicious campaign involves the use of WinRAR archive files with minimal detection to execute a multi-stage attack. The payload, known as Editbot, is a newly discovered Python-based stealer. Editbot is specifically designed to extract process information and data stored in web browsers, including passwords, cookies, and other web-related information. The stolen data is then exfiltrated to threat actors through a Telegram channel.

Attack Regions



Attack Details

#1 In a recently discovered campaign targeting social media users, threat actors utilized a WinRAR archive file with minimal detection on VirusTotal. The campaign employs a multi-stage attack strategy, with each phase aimed at evading detection, downloading additional payloads, or establishing persistence on the victim's system.

#2 The final payload known as Editbot is a Python-based malware that steals sensitive information and browser-stored data via the Telegram channel. The Python script collects data from various browsers and sends it to a specified TAs Telegram channel. The malware executes a batch file, enumerates running processes, and saves the output in a file extracting country code, IP address, and timestamp.

#3 In early December, a phishing campaign revolving around the theme of a "defective product to be sent back" was observed. Malicious actors exploit the attractiveness of popular products and engaging content to lure users into interacting with deceptive pages or groups. As users engage with these fraudulent pages or groups, such as by commenting or liking posts, they unintentionally expand the reach of the deceptive content, making it visible in the news feeds of their network.

#4 Threat actors leverage open-source code-sharing platforms like GitLab to acquire payloads for subsequent stages. Using the obtained BAT file, the TAs have sought to implement a multi-phase infection approach, aiming to deploy their final payload onto the victim's system. Editbot, the ultimate payload, is a Windows-specific Python-based stealer meticulously crafted to adeptly collect a diverse range of sensitive data.

#5 The threat actors then employed Editbot to retrieve sensitive information from RAR archive files. The stealer extracts data from the browser profile folder, encompassing cookies, login details, web data, and local state, and saves it in a text file named "pass.txt." Subsequently, it generates a ZIP archive, housing the victim's information in the identical directory. To exfiltrate the pilfered data, the threat actors utilize Telegram bots.

#6 The surge in social media attacks can be linked to threat actors utilizing payloads, introducing complexity to the identification process. The sophisticated, multi-stage structure of these attacks implies possible participation by organizations or individuals with proficiency in obtaining and reselling credentials or gaining access to compromised systems, resembling the characteristics of Initial Access Brokers.

Recommendations

Remain vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Update Browser Settings: Adjust your browser settings to not save passwords. Most browsers offer an option to disable password saving. This ensures that even if someone gains access to your computer, they won't have easy access to your stored credentials.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0006 Credential Access
TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration	T1566 Phishing
T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1057 Process Discovery	T1547 Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	T1005 Data from Local System	T1539 Steal Web Session Cookie	T1555 Credentials from Password Stores
T1567 Exfiltration Over Web Service			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	fd8391a1a0115880e8c3ee2e76fbce741f1b3c5fbcb728b9fac37c21e9f6d7b7, d13aba752f86757de6628e833f4fdf4c625f480056e93b919172e9c309448b80, 3f7bd47fbbf1fb0a63ba955c8f9139d6500b6737e5baf5fdb783f0cedae94d6d, 9d048e99bed4ced4f37d91a29763257a1592adb2bc8e17a66fa07a922a0537d0, bc3993769a5f82e454acef92dc2362c43bf7d6b6b203db7db8803faa996229aa
SHA1	feff390b99dfe7619a20748582279bc13c04f52a, 18e96d94089086848a0569a1e1d8051da0f6f444, eed59a282588778ffbc772085b03d229a5d99e35, 93d70f02b2ee2c4c2cd8262011ed21317c7d92de, cf019e96e16fdaa504b29075aded36be27691956
MD5	ca5bee4607ddd920729e5c2b4fc89bbc, e9e4cd111cadcf94c469365354df3fdc, 669e7ac187fb57c4d90b07d9a6bb1d42, f23465088d26e90514b5661936016c05, c3a447c5c6c73d80490347c1b4afe9d5

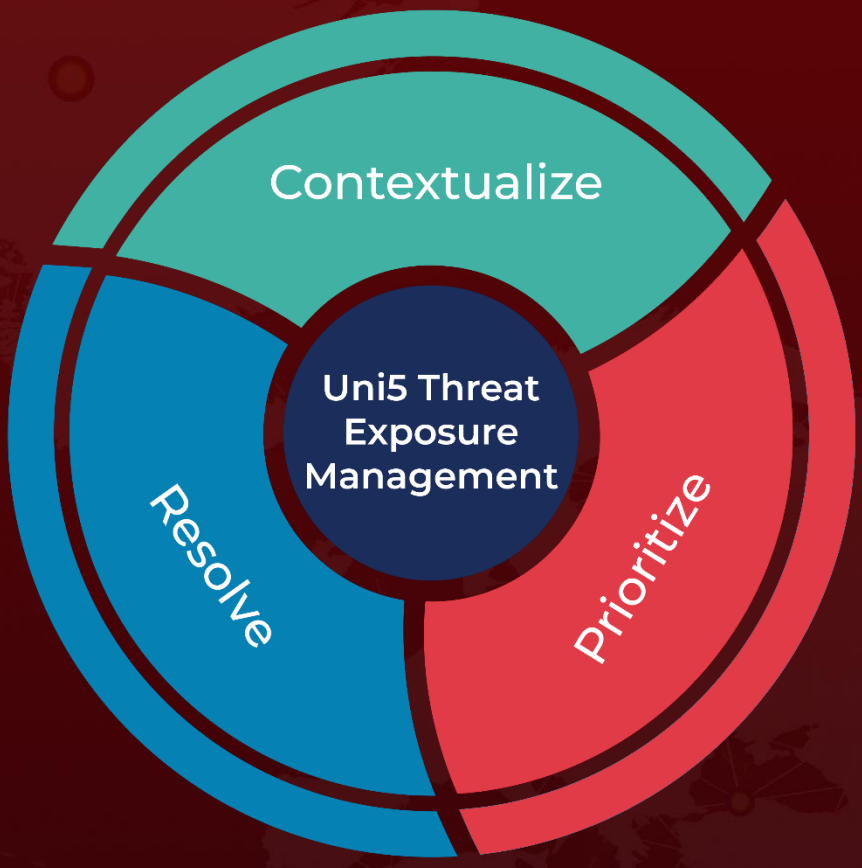
References

https://cyble.com/blog/new-editbot-stealer-spreads-via-social-media-messages/

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 13, 2023 . 4:45 AM

More at www.hivepro.com