Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

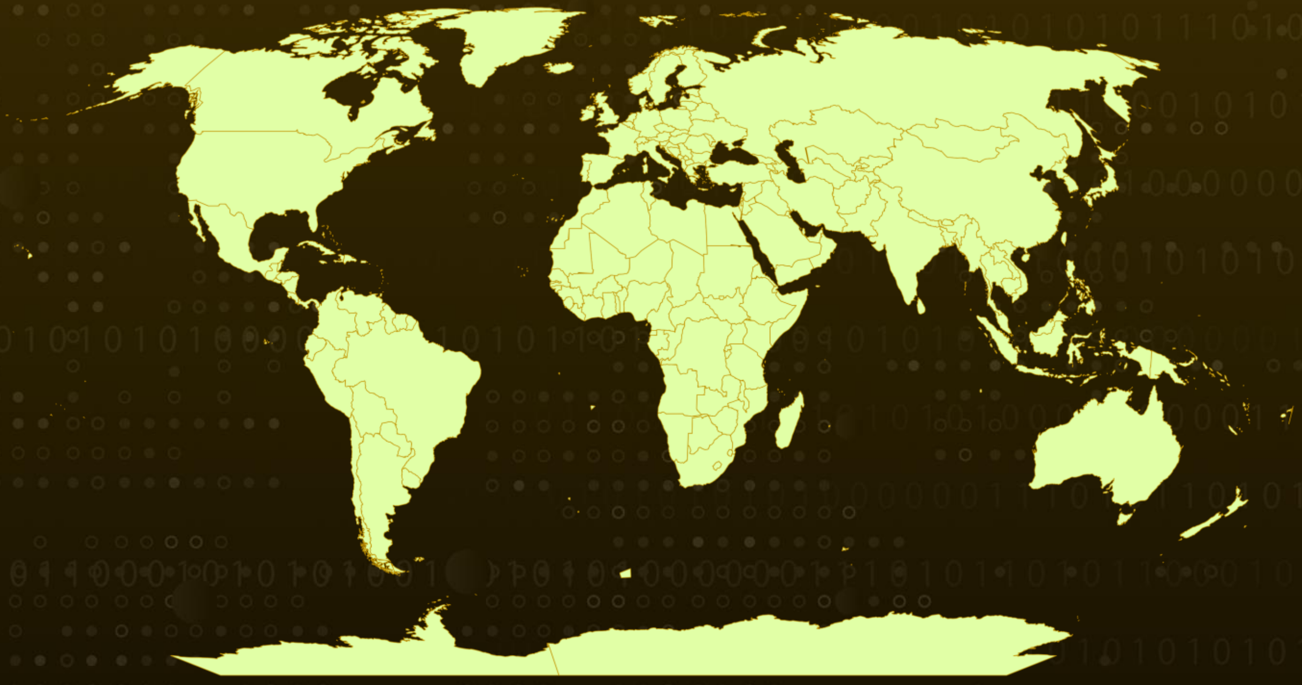
New Variant of RedLine Stealer Uses Batch Script to Evade Detection

Date of Publication	Admiralty Code	TA Number
September 26, 2023	A1	TA2023386

Summary

First appeared: March 2020
Attack Region: Worldwide
Affected Platform: Windows
Malware: RedLine Stealer
Attack: A new variant of RedLine Stealer is being distributed as a batch script. This latest variant of RedLine Stealer is more sophisticated than its previous versions and employs number of techniques to evade detection. Notably, the malware is highly obfuscated, uses multiple encryption layers and also uses different techniques to hide its presence on the victim's system, including the creation of hidden files and folders.

Attack Regions



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

Attack Details

#1

A new variant of RedLine Stealer that is being distributed as a batch script file. The batch script file is typically disguised as a legitimate document, such as a PDF or Word file. When the victim opens the document, the batch script file is executed and installs the RedLine Stealer malware on the victim's system.

#2

This new variant of RedLine Stealer is more sophisticated than previous versions and uses a number of techniques to evade detection. For example, the malware is obfuscated and uses multiple layers of encryption. It also uses a variety of techniques to hide its presence on the victim's system, such as creating hidden files and folders.

#3

RedLine Stealer, initially discovered in March 2020, has gained notoriety as a potent malware specializing in the theft of sensitive data from compromised systems. This malicious tool is widely available as a service on underground forums, known for its adaptability and versatility. RedLine Stealer is coded in C# and employs a SOAP API to communicate with its C2 server.

#4

It is most notorious for its capability to extract a wide array of information from targeted systems. This includes data from web browsers, email clients, and various applications, encompassing valuable financial data such as credit card details and cryptocurrency wallet information. Additionally, RedLine Stealer collects comprehensive system data, ranging from hardware specifications and software inventory to VPN configurations and user-related information.

#5

One of the key findings regarding RedLine Stealer is its sophisticated evasion tactics. It employs multi-level obfuscation techniques to avoid detection and operates by disguising itself as an obfuscated PowerShell script, often appearing as a legitimate system file. This malware is typically distributed through phishing emails and communicates with a command-and-control (C2) server located in Russia.

#6

The analysis of RedLine Stealer reveals its extensive capabilities, making it a formidable threat. Beyond data theft, it excels at credential theft, extracting sensitive information from web browsers and communication applications, harvesting user profiles, and targeting financial data. Moreover, it collects network and FTP login credentials and conducts a thorough system profile.

Recommendations

Implement Advanced Threat Detection: Given the sophisticated nature of RedLine Stealer and its ability to evade traditional security measures, it is crucial to invest in advanced threat detection systems. These systems can employ behavior-based analytics and anomaly detection to identify and respond to the unique characteristics of RedLine Stealer attacks.

Strengthen Web Application Security: RedLine Stealer targets prominent platforms and banks, making web application security paramount. Conduct regular security assessments and penetration testing for web applications, especially if they are linked to financial transactions. Ensure that security patches for web frameworks and content management systems are promptly applied to prevent vulnerabilities that RedLine Stealer can exploit.

Network Segmentation and Access Control: Segment your network to limit lateral movement for malware like RedLine Stealer. Restrict user and application access to sensitive areas of the network through proper access control measures. Implement the principle of least privilege (PoLP), which ensures that users and applications have only the minimum access necessary to perform their tasks. This limits the potential impact of a breach and helps contain malware infections.

Potential MITRE ATT&CK TTPs

TA0006 Credential Access	**TA0005** Defense Evasion	**TA0001** Initial Access	**TA0002** Execution
TA0007 Discovery	**TA0010** Exfiltration	**TA0009** Collection	**TA0011** Command and Control
TA0040 Impact	**T1566** Phishing	**T1204.002** Malicious File	**T1204** User Execution
T1204.002 Malicious File	**T1059.003** Windows Command Shell	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell

T1564.001 Hidden Files and Directories	**T1555.003** Credentials from Web Browsers	**T1087** Account Discovery	**T1217** Browser Bookmark Discovery
T1046 Network Service Discovery	**T1057** Process Discovery	**T1012** Query Registry	**T1518** Software Discovery
T1016 System Network Configuration Discovery	**T1083** File and Directory Discovery	**T1082** System Information Discovery	**T1102** Web Service
T1113 Screen Capture	**T1041** Exfiltration Over C2 Channel	**T1102.002** Bidirectional Communication	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	28caece68c96bec864c5b61d09a8ad06, B4c53eb42fac3e0c8770a4704171cfb6, 8248867e6d42d41cfdea624f87e14fa6, 6018d10792d2e5717b4e3aaff9310a6a
SHA256	e0f0449aae4dc117e34517e8c83fd49faf2b379dc4f2fd35ff291dd5003864e2, f4f093e1c950a233464a6a17a2040630c9e4f69b282f4a34510b3de35d5723b0, 197b50f15375335928e08c5cc5b6f50cd93864655237b8db85556d4057f3b988, 83db86d7872e467513f186adcc02f5408e50b6a3d3aa14cbf7dd5d1fb6affb34

References

https://www.cyfirma.com/outofband/redline-stealer-a-new-variant-surfaces-deploying-using-batch-script/

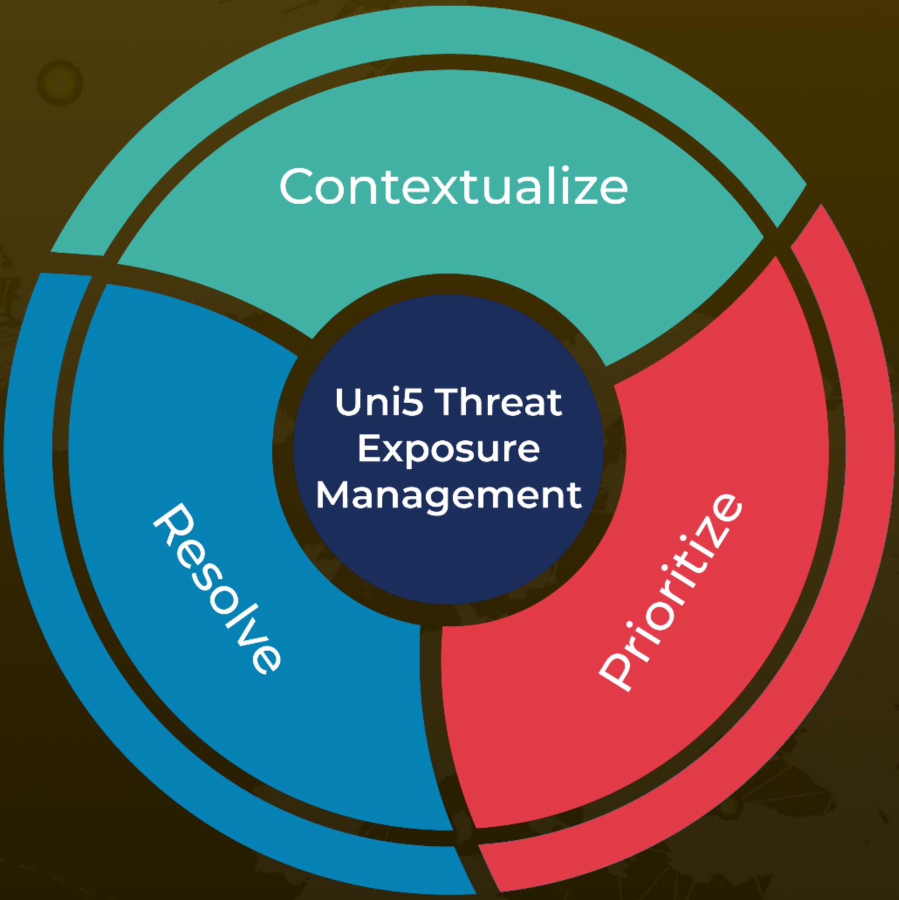
https://www.hivepro.com/google-chromes-second-zero-day-in-2022/

https://www.hivepro.com/redline-stealer-used-in-spear-phishing-campaign-targeting-hospitality-industry/

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

September 26, 2023 • 5:30 AM

More at www.hivepro.com