Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

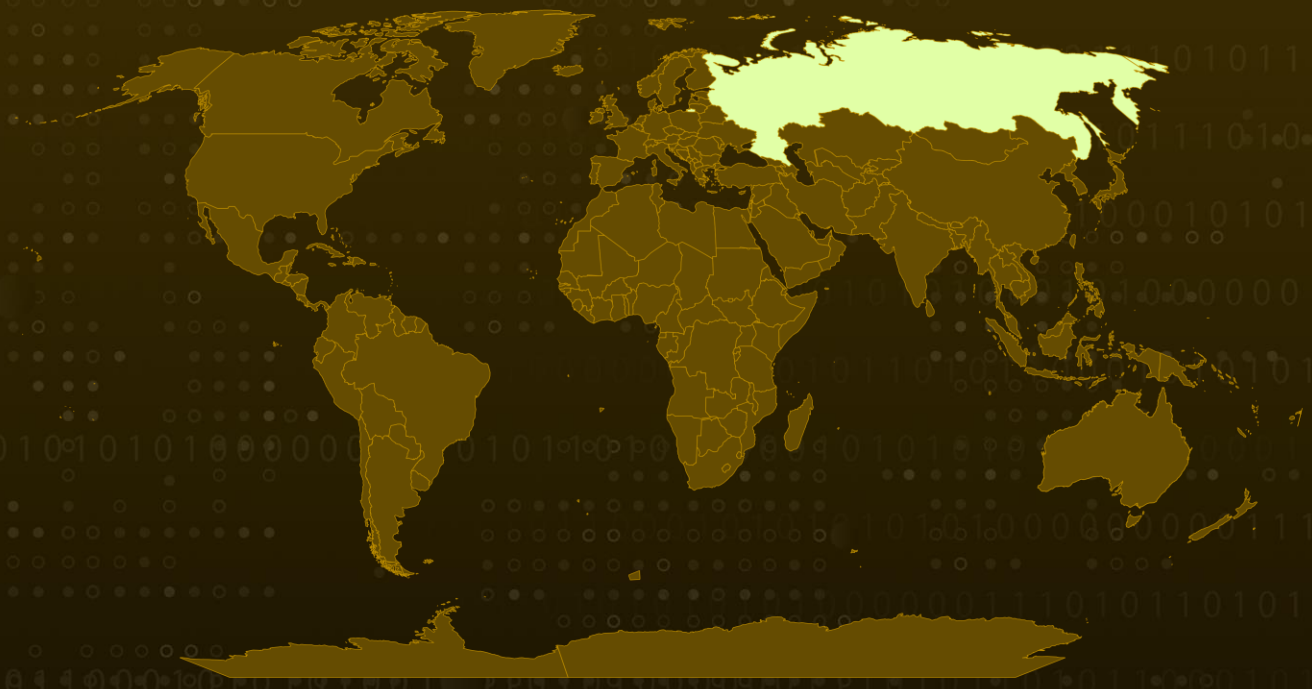
SapphireStealer's Stealthy Invasion via Deceptive Legal Documents

Date of Publication	Admiralty Code	TA Number
March 8, 2024	A1	TA2024092

Summary

First Appearance: December 2022
Malware: SapphireStealer
Attack Region: Russia
Targeted Industry: Government
Attack: An intricate campaign aimed at Russian individuals has emerged, showcasing the SapphireStealer malware, a publicly available information-stealing tool introduced in December 2022. The incorporation of social engineering techniques significantly enhances the efficacy of these campaigns, allowing attackers to evade detection by assuming the guise of trustworthy entities.

Attack Regions



Attack Details

#1 In late February, a sophisticated campaign emerged, specifically targeting Russian individuals with the SapphireStealer malware. SapphireStealer, an open-source information-stealing tool that debuted in December 2022, has been progressively spreading across various public malware repositories.

#2 Presumably distributed through spam emails, the downloaded executable file disguises itself as a PDF icon, deceptively leading users to believe it is a harmless document. Upon closer inspection, the misleading PDF reveals scanned images resembling a directive for enforcing a court order against a debtor, and another simulating a subpoena summoning an individual as a witness in a Russian administrative violation case.

#3 Upon execution, the executable file not only reveals the embedded lure PDF document but also quietly engages in a covert data-stealing operation in the background. Crafted in C#, the simplicity of SapphireStealer belies its effectiveness, granting even novice hackers the ability to capture screenshots and extract credentials from web browsers.

#4 The malware is equipped with features to collect host information, browser data, files, and screenshots, subsequently exfiltrating the acquired data in the form of a ZIP file via Simple Mail Transfer Protocol (SMTP). Following the data transfer, SapphireStealer meticulously erases any traces of its activity and terminates itself.

#5 Several iterations of this information-stealing malware are already circulating in the digital landscape, with threat actors continually refining its efficiency and effectiveness. This deliberate use of social engineering techniques enhances the success of malware campaigns by allowing attackers to elude detection, presenting themselves as trustworthy and benign entities.

Recommendations

Email Filtering and Monitoring: Strengthen email filtering systems to detect and quarantine phishing attempts, especially those involving malicious PDFs. Regularly monitor email communications for potential threats and provide timely alerts to users.

Continuous Monitoring and Analysis: Implement continuous monitoring and analysis of network traffic and system logs. This proactive approach can help identify anomalies and potential threats before they escalate.

Disable Unnecessary Services: Review and disable unnecessary services and features on systems to minimize potential attack vectors. Restrict user privileges to limit the impact of potential breaches.

Heighten Awareness: Familiarize yourself with common social engineering tactics and deceptive strategies employed by threat actors. Knowing the signs of malicious activity can help you avoid falling victim to scams.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**T1203** Exploitation for Client Execution
T1027 Obfuscated Files or Information	**T1027.002** Software Packing	**T1140** Deobfuscate/Decode Files or Information	**T1003** OS Credential Dumping
T1082 System Information Discovery	**T1083** File and Directory Discovery	**T1005** Data from Local System	**T1560** Archive Collected Data
T1036 Masquerading	**T1071** Application Layer Protocol	**T1566** Phishing	**T1566.001** Spearphishing Attachment
T1113 Screen Capture	**T1204.001** Malicious Link	**T1555** Credentials from Password Stores	**T1555.003** Credentials from Web Browsers

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	5c025a9e86a125bf2f2ca5c1b29b42a6, 55bb772aea4303ca373fd8940663b6bd
SHA1	6b44ab6c246c077ee0e6f51300654b3eec2fddc7, b396a8d5e30fb179f3139d28b843b57bb8ae3f47
SHA256	850a99d2039dadb0c15442b40c90aa4dac16319114455ab5904aa51e062fe6e1, c816d0be8d180573d14d230b438a22d7dda6368b1ef1733754eda9804f295a2f
Domain	govermentu[.]ru
URL	hxxp://govermentu[.]ru/media/FederalnoeUpravlenie_postanovlenie_o_vozbuzdenie_ispolnitelnogo_proizvodstava[.]exe
IPv4	193[.]39[.]185[.]4

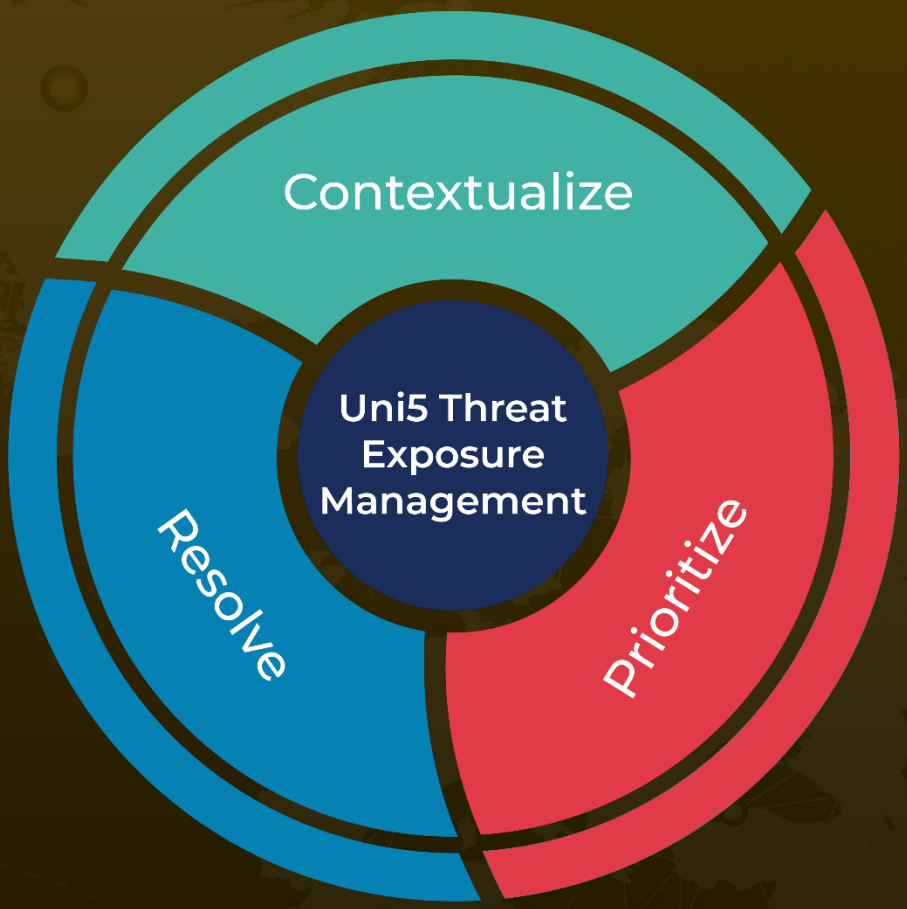
References

https://cyble.com/blog/sapphirestealer-sneaks-in-deceptive-legal-documents-prey-on-russians/

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 8, 2024 • 3:00 AM

More at www.hivepro.com