SECURITY ADVISORY

CYBER STASH

February, 2023

MULTIPLE CVEs

Vector Stealer Malware

Context

VectorStealer is modular malware that emerged in 2020 and steals .rdp files using phishing emails and malicious websites, enabling threat actors to perform RDP hijacking and propagate across connected systems. Its primary goal is to exfiltrate sensitive information, including log-in credentials and financial and personal data, through popular channels like SMTP, Discord, or Telegram.

VectorStealer uses advanced anti-analysis techniques, including the KGB Crypter tool, which encrypts and modifies the code with each compilation, making it challenging to detect and remove. It can also recover sensitive data from popular browsers, like Firefox, Chrome, and Safari. By leveraging KGB Crypter, VectorStealer can evade traditional security measures and successfully infiltrate systems, posing a severe threat to targeted individuals and organisations.

Mitigation

To reduce the chances of being affected by VectorStealer malware, it is advised to implement the following measures for risk mitigation:

- Keep all software up-to-date, including anti-virus and anti-malware software.
- Implement multi-factor authentication on all accounts accessible remotely.

- Enforce application whitelisting policies to control which applications can run on your systems and how they interact with their environment.
- Control and monitor the use of .rdp files, PowerShell scripts and VBA macros.
- Minimise exposure to high-risk infrastructures by limiting network access of systems using tactical and operational threat intelligence.

Technical Details

Tactics, Techniques and Procedures

After gaining access inside the victim network, VectorStealer malware uses the following post-exploitation adversary techniques:

- T1027.002: Obfuscated Files or Information: OLE stream embedded VBA macros de-obfuscate PowerShell script, which is executed via the Shell() function.
- T1105: Ingress Tool Transfer: PowerShell used to drop and execute 2nd stage payload from a remote server.
- T1053: Scheduled Task: Creates a copy of itself in the %appdata% folder and sets up a task scheduler to ensure persistence on the victim's system.
- T1027.003: Virtualization/Sandbox Evasion : The use of KoiVM to virtualize and obfuscate .NET opcodes is a technique employed by adversaries to evade detection and hinder analysis. This technique involves the use of virtualization to create an environment in which the malware can run undetected, making it more difficult for defenders to identify and respond to the threat. KoiVM specifically is designed to work with ConfuserEx, a popular open-source obfuscation tool used by malware authors to obfuscate .NET assemblies.

Cyber Threat Intelligence

The Vector Stealer payload can be easily created through a web panel available for purchase at USD 63 in Bitcoin, allowing threat actors to generate customized malware without requiring advanced programming skills. The web panel provides several options for customization, including defining the malware's actions and behavior.

The creators of KGB Crypter, who are of Russian origin, offer a paid service for USD 145 per month through their website. They claim that several notorious malware variants, including Redline, Quasar RAT, Venom RAT, and Pandora RAT, use their crypter. KGB Crypter features a metamorphic generator that modifies the malware code to make it more challenging for antivirus software to detect.

References

Related IOC's

https://www.hivepro.com/vectorstealer-malware-steals-sensitive-information-via-rdp-hijacking-and-phishing-attacks/

Sandbox Report Sample

https://www.joesandbox.com/analysis/729182/0/html

Public Intelligence

https://blog.cyble.com/2023/02/01/vector-stealer-a-gateway-for-rdp-hijacking/

https://www.bypasshacker.com/vectorstealer-malware/#how_to_protect_against_VectorStealer_malware

https://www.infosecurity-magazine.com/news/remote-desktop-protocol-attacks/