مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

SamsStealer - Information Stealer Targeting Windows Users

Tracking #:432315885

Date:24-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a new information stealer, "SamsStealer," targeting Windows systems to steal sensitive information from victims' computers, including passwords, cookies, cryptocurrency wallet data, and more.

TECHNICAL DETAILS:

A new information stealer, "SamsStealer," targeting Windows systems users worldwide and this malware, written in .NET, is designed to steal sensitive information from victims' computers, including passwords, cookies, cryptocurrency wallet data, and more. It operates stealthily, targeting various browsers and applications including Discord, Chrome, and Microsoft Edge. The stolen data is compressed and uploaded to a file-sharing service before the download link is sent to the attacker via Telegram.

SamsStealer employs asynchronous techniques to efficiently steal information from various sources. It targets a wide range of browsers and applications, such as Discord variants, Telegram, Chrome, Firefox, Opera, Brave, Chromium, EpicPrivacy, OperaGx, Vivaldi, and Yandex. Additionally, it targets popular cryptocurrency wallets, including Bitcoin, Zcash, Armory, Bytecoin, Jaxx, Exodus, Ethereum, Electrum, AtomicWallet, Guarda, and Coinomi.

The malware uses a multi-step process to manage the stolen data. First, it compresses the gathered information into a ZIP file named "Backup.zip". Then, it leverages the "gofile.io" online file-sharing platform to upload the compressed file. Finally, it utilizes the Telegram messaging service to send the download link of the uploaded file to the attacker for retrieval

SamsStealer employs concurrency for efficiency and removes unnecessary files from the stolen data. The extracted information is stored in the Temp folder as different text files.

INDICATORS OF COMPROMISE(IOCs):

Attached in Excel File

RECOMMENDATIONS:

- Layered Security: Combine endpoint security with robust antivirus/anti-malware for advanced threat detection, prevention, and removal.
- Patch Management: Prioritize regular updates for operating systems, applications, and security software to address vulnerabilities.
- Network Segmentation & Monitoring: Limit lateral movement with segmentation and use firewalls to block malicious network traffic.
- Security Awareness Training: Educate employees on phishing, social engineering, and how to identify suspicious activity.
- Enhanced Network Defenses: Implement application whitelisting, behaviour-based monitoring, and monitor for anomalous data transfers.
- Incident Response & Threat Intelligence: Develop a plan for incidents and stay informed about current malware threats and indicators of compromise (IOCs).

- Data Backups & Least Privilege: Regularly back up data and implement the principle of least privilege to minimize potential damage.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

https://www.cyfirma.com/research/samsstealer-unveiling-the-information-stealer-targeting-windows-systems/