مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Raccoon Stealer - Malware Targeting Windows

Tracking #:432316001

Date:01-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a resurgence of the Raccoon Stealer, indicating the emergence of a new variant.

TECHNICAL DETAILS:

Raccoon Stealer, an information-stealing malware, has resurfaced after a hiatus. It targets Windows systems, harvesting sensitive data like browser passwords, credit card info, and crypto-wallet data. Its adaptive tactics and communication with command-and-control servers pose a persistent threat.

Features:

- **Information Stealing:** Raccoon Stealer targets sensitive data saved in users' browsers and cryptocurrency wallets.
- **Browser Data:** It seeks cookies, saved login details, and credit card information from browsers.
- **Crypto-Wallet Data:** It harvests public keys, private keys, and seed phrases from crypto-wallets.

Targeted Platform:

- **Windows Systems:** Raccoon Stealer primarily infects Windows (32-bit and 64-bit) systems.

Propagation Methods:

- **Phishing Emails:** Cybercriminals distribute Raccoon Stealer via phishing emails.
- **Exploit Kits:** It leverages exploit kits to infiltrate vulnerable systems.
- **Malicious Ads:** Raccoon Stealer camouflages as legitimate software updates or applications.

Impact:

- **Identity Theft:** Stolen data can lead to identity theft.
- **Cryptocurrency Theft:** Crypto-wallet data compromise risks financial losses.
- **Credit Card Fraud:** Exfiltrated credit card details may be misused

The latest version of Raccoon Stealer **(v2.3.0)** comes with several enhancements to improve user experience and stealth. The features are as listed below:

- **Improved Stealth:** Raccoon Stealer now operates more discreetly, making detection harder for security tools.
- **Ease of Use:** The user interface has been refined, simplifying configuration and usage.
- **Pricing Update:** The subscription fees have changed to $125 per week or $275 per month.

A few of the targeted applications which are commonly used include:

- Google Chrome
- Internet Explorer
- Microsoft Edge
- Firefox
- Outlook

INDICATORS OF COMROMISE:

Attached File

RECOMMENDATIONS:

- App Source Verification: Install from trusted sources only. Review app permissions before installation. Avoid apps that request excessive access.
- Patch Management: Prioritize regular updates for operating systems, applications, and security software to address vulnerabilities.
- Security Awareness Training: Educate employees on phishing, social engineering, and how to identify suspicious activity. Encourage strong password practices and multi-factor authentication.
- Email Hygiene: Be cautious with email attachments and links. Avoid opening suspicious emails or downloading attachments from unknown senders.
- Browser Security: Disable unnecessary browser extensions. Clear cookies and cache regularly to minimize data exposure.
- Security Software: Use reputable security apps to detect and remove malware. Run periodic scans to identify any malicious activity.

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://socradar.io/raccoon-stealer-resurfaces-with-new-enhancements/
- https://cyberint.com/blog/financial-services/raccoon-stealer/