مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

SYS01 Infostealer Malware Campaign

Tracking #:432316468

Date:04-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a sophisticated malvertising campaign leveraging Meta's advertising platform to spread the SYS01 InfoStealer malware.

TECHNICAL DETAILS:

A sophisticated malvertising campaign, dubbed "SYS01 Infostealer," is targeting millions of users worldwide by leveraging compromised Facebook Business accounts to distribute malicious ads. The campaign leverages social engineering techniques, impersonating popular brands to trick users into downloading malware. The malware, delivered as an ElectronJS application, can steal sensitive information, including login credentials and financial data.

Attack Vector

The attackers use compromised Facebook Business accounts to create and distribute malicious advertisements. These ads impersonate popular brands and software, including:

- Productivity tools (e.g., Office 365)
- Video/photo editing software (e.g., CapCut, Canva, Adobe Photoshop)
- Streaming services (e.g., Netflix)
- VPN providers (e.g., Express VPN)
- Messaging platforms (e.g., Telegram)
- Video games

Malware Delivery

When users interact with these malicious ads, they are directed to fake websites hosted on platforms like Google Sites or True Hosting. These sites offer free downloads of the advertised software, which actually contain the SYS01 Infostealer malware

Distribution Method

1. Malicious ads are created using hijacked Meta Business accounts.
2. Ads typically link to MediaFire or direct download links.
3. Users download a ZIP archive containing an Electron application.
4. The Electron app's embedded JavaScript code drops and executes the malware

Malware Capabilities

SYS01 Infostealer is designed to:

- Evade detection using sandbox detection techniques
- Disable security solutions
- Maintain persistence through scheduled tasks
- Steal personal data and credentials, particularly targeting Facebook Business accounts

Indicators of Compromise (IOC's):

- **Malware Hosting Domains**
  - hxxps[:]//krouki.com
  - hxxps[:]//kimiclass.com
  - hxxps[:]//goodsuccessmedia.com
  - hxxps[:]//wegoodmedia.com
  - hxxps[:]//socialworldmedia.com

- hxxps[:]//superpackmedia.com
- hxxps[:]//wegoodmedia.com
- hxxps[:]//eviralmedia.com
- hxxps[:]//gerymedia.com
- hxxps[:]//wakomedia.com

- **C2 Domains**
  - hxxps[:]//musament.top
  - hxxps[:]//enorgutic.top
  - hxxps[:]//untratem.top
  - hxxps[:]//matcrogir.top
  - hxxps[:]//ubrosive.top
  - hxxps[:]//wrust.top
  - hxxps[:]//lucielarouche.com
  - hxxps[:]//ostimatu.top

RECOMMENDATIONS:

- Review the Indicators of Compromise (IOCs) and implement the necessary security measures.
- **User Awareness:**
  - Educate users about the risks of clicking on suspicious ads, especially those that appear out of context or offer unrealistic deals.
  - Encourage users to be cautious of unsolicited downloads and to verify the legitimacy of software sources.
  - Promote the importance of strong, unique passwords for all online accounts.
- **Network Security:**
  - Implement robust network security measures, including firewalls, intrusion detection systems, and web filtering solutions.
  - Keep all software and operating systems up-to-date with the latest security patches.
  - Use reliable antivirus and anti-malware software to detect and block malicious threats.
- **Email Security:**
  - Train users to identify and avoid phishing emails.
  - Use email security solutions to filter out malicious emails and attachments.
- **Incident Response:**
  - Have a comprehensive incident response plan in place to address security breaches promptly and effectively.
  - Conduct regular security audits and penetration testing to identify vulnerabilities.

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.bitdefender.com/en-us/blog/labs/unmasking-the-sys01-infostealer-threat-bitdefender-labs-tracks-global-malvertising-campaign-targeting-meta-business-pages/