AL2024_18 Facebook Ads for Windows Themes Push SYS01 Info-Stealing Malware (16th July 2024)

Description

Cybercriminals are using Facebook business pages and advertisements to promote fake Windows themes that infect users with the SYS01 password-stealing malware. This significant threat leverages the massive reach of the social media platform to distribute the malware widely and effectively.

Details

Researchers from Trustwave have identified campaigns where threat actors promote fake downloads for Windows themes, pirated games, software, Sora AI, 3D image creators, and One Click Active via Facebook advertisements. These ads often stem from newly created or hijacked Facebook business pages, allowing them to reach a large audience by renaming the pages to match the advertised themes.

Once a user clicks on an ad, they are redirected to webpages hosted on Google Sites or True Hosting, which masquerade as download pages for the promoted content. These pages primarily promote a site called Blue-Software, offering supposed free software and game downloads. However, the downloaded ZIP archives contain the SYS01 info-stealing malware instead of the advertised content.

The SYS01 malware, discovered by Morphisec in 2022, employs executables, DLLs, PowerShell scripts, and PHP scripts to install and operate. Upon executing the main file, DLL sideloading is used to load a malicious DLL that sets up the malware's environment, including disabling virtualized environment detection, adding exclusions in Windows Defender, and configuring PHP scripts for malicious operations.

The primary payload includes PHP scripts that create scheduled tasks for persistence and steal data from infected devices, such as browser cookies, saved credentials, browsing history, and cryptocurrency wallets. The malware also exploits Facebook cookies to steal account information, including personal profiles, advertising account data, business details, and page management information.

Trustwave observed that the SYS01 malvertising campaigns extend beyond Facebook to platforms like LinkedIn and YouTube, demonstrating the broad scope and persistence of these attacks.

Indicators of Compromise (IoCs)

Organizations should monitor for the following indicators of compromise:

- Unexpected behavior or performance issues on systems where new themes or free software have been installed.
- Unusual system activity, especially related to DLL sideloading and PowerShell script execution.
- Unauthorized access or suspicious activities linked to browser cookies and saved credentials.
- Reports of phishing emails or messages prompting downloads of fake software or themes.

Remediation

To mitigate this risk organizations can:

- Implement comprehensive security solutions to detect and block malicious activities.
- Regularly update Windows devices to the latest versions.
- Educate users on the dangers of downloading software from untrusted sources and the importance of avoiding phishing scams.
- Monitor network traffic for unusual patterns that may indicate malware activity.
- Ensure anti-malware and anti-tampering measures are up to date and properly configured.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- BleepingComputer. (2024, July 15). Facebook ads for Windows desktop themes push info-stealing malware. Retrieved from

https://www.bleepingcomputer.com/news/security/facebook-ads-for-windows-themes-push-sys01-info-stealing-malware/

- Vumetric Cyber Portal. (2024, July 15). Facebook ads for Windows desktop themes push info-stealing malware. Retrieved from https://cyber.vumetric.com/security-news/2024/07/15/facebook-ads-for-windows-desktop-themes-push-info-stealing-malware/