مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Chrome Extension Supply Chain Attack

Tracking #:432316684

Date:30-12-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed security researchers reported a sophisticated phishing campaign has compromised at least 16 Chrome browser extensions, potentially exposing over 600,000 users to data theft and credential harvesting.

TECHNICAL DETAILS:

A sophisticated phishing campaign has compromised at least 16 Chrome browser extensions, potentially exposing over 600,000 users to data theft and credential harvesting. The attack, which began in mid-December 2024, targeted extension developers through the Chrome Web Store, allowing threat actors to inject malicious code into legitimate extensions. This code communicates with a command and control (C&C) server, exfiltrating sensitive user data including cookies, access tokens, and identity information.

The cybersecurity firm Cyberhaven was among the first victims, with their extension compromised on December 24, 2024. Subsequent investigation revealed a wider campaign affecting multiple extensions, including those related to AI assistants, VPNs, and productivity tools.

Compromised Extensions:
The following browser extensions have been confirmed or are suspected to be compromised:

- AI Assistant - ChatGPT and Gemini for Chrome
- Bard AI Chat Extension
- GPT 4 Summary with OpenAI
- Search Copilot AI Assistant for Chrome
- TinaMind AI Assistant
- Wayin AI
- VPNCity
- Internxt VPN
- Vindoz Flex Video Recorder
- VidHelper Video Downloader
- Bookmark Favicon Changer
- Castorus
- Uvoice
- Reader Mode
- Parrot Talks
- Primus
- Cyberhaven

Indicators of Compromise:
Malicious Extension Version: 24.10.4

- Hash: DDF8C9C72B1B1061221A597168f9BB2C2BA09D38D7B3405E1DACE37AF1587944

Network Traffic to C&C Servers:

- Domains: cyberhavenext[.]pro, api.cyberhaven[.]pro
- IPs: 149.28.124[.]84, 149.248.2[.]160

RECOMMENDATIONS:

- Immediately remove or disable all affected extensions from corporate and personal devices or If users still need to use certain extensions, they should ensure that they are updated to the latest, secure versions.
- Credential Rotation: Users of affected extensions should immediately revoke and rotate all passwords and API tokens.
- Immediate Extension Audit: Organizations should conduct a thorough audit of all Chrome extensions installed on corporate devices.
- Implement a strict whitelist policy for approved browser extensions in corporate environments.
- Enhanced Monitoring: Implement advanced monitoring for suspicious browser activity and data exfiltration attempts.
- User Education: Conduct awareness training on the risks associated with browser extensions and phishing attacks.
- Extension Management Policy: Develop and enforce a strict policy for approving and managing browser extensions in corporate environments.

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.cyberhaven.com/engineering-blog/cyberhavens-preliminary-analysis-of-the-recent-malicious-chrome-extension