Una reciente campaña de ciberataques ha afectado a extensiones populares del navegador Chrome, logrando comprometer al menos 16 de ellas y poniendo en riesgo la seguridad de más de 600,000 usuarios al exponer datos sensibles y facilitar el robo de credenciales.

El ataque se enfocó en los desarrolladores de extensiones de la Chrome Web Store mediante correos electrónicos de phishing. Los ciberdelincuentes utilizaron los permisos de acceso de estos desarrolladores para insertar código malicioso en extensiones legítimas, permitiendo así el robo de cookies y tokens de acceso de los usuarios.

Cyberhaven, una empresa de ciberseguridad, fue una de las primeras afectadas cuando un empleado cayó en un ataque de phishing el 24 de diciembre. Esto permitió a los atacantes publicar una versión alterada y maliciosa de su extensión.

El 27 de diciembre, Cyberhaven informó que un actor malicioso había comprometido su extensión del navegador, inyectando código diseñado para comunicarse con un servidor de comando y control (C&C) ubicado en el dominio cyberhavenext[.]pro. Este código descargaba configuraciones adicionales y extraía datos de los usuarios.

El correo electrónico de phishing, que se hacía pasar por un mensaje del equipo de Soporte para Desarrolladores de la Chrome Web Store, advertía falsamente que la extensión estaba en riesgo inminente de ser eliminada por supuestas infracciones a las políticas del Programa para Desarrolladores. Para evitar esto, el mensaje instaba al destinatario a hacer clic en un enlace y otorgar permisos a una aplicación maliciosa llamada «Privacy Policy Extension».

> *«El atacante obtuvo los permisos necesarios a través de esta aplicación maliciosa y subió una extensión comprometida a la Chrome Web Store. Después de pasar por el proceso estándar de revisión de seguridad, la extensión fue aprobada y publicada»,* explicó Cyberhaven.
>
> *«Las extensiones de navegador son un punto débil en la seguridad web. Aunque solemos considerarlas inofensivas, muchas tienen acceso a datos sensibles como*

> *cookies, tokens de acceso e información personal»,* comentó Or Eshed, director ejecutivo de LayerX Security, una empresa especializada en proteger extensiones de navegador.
>
> *«Muchas empresas desconocen las extensiones instaladas en sus dispositivos y no son conscientes del nivel de riesgo que enfrentan»,* agregó Eshed.

Jamie Blasco, director de tecnología de Nudge Security, una empresa enfocada en seguridad SaaS, identificó otros dominios relacionados con la misma dirección IP utilizada por el servidor C&C en el ataque a Cyberhaven.

Investigaciones posteriores han revelado que otras extensiones, incluidas algunas relacionadas con Google Sheets, también podrían estar comprometidas, según el análisis de Secure Annex, una plataforma de seguridad para extensiones de navegador. Estas son:

- 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

- Tackker – online keylogger tool
- AI Shop Buddy
- Sort by Oldest
- Rewards Search Automator
- ChatGPT Assistant – Smart Search
- Keyboard History Recorder
- Email Hunter
- Visual Effects for Google Meet
- Earny – Up to 20% Cash Back

Esto sugiere que el ataque a Cyberhaven no fue un incidente aislado, sino parte de una operación más amplia dirigida a extensiones legítimas del navegador.

John Tuckner, fundador de Secure Annex, declaró a The Hacker News que la campaña pudo haber comenzado el 5 de abril de 2023 o incluso antes, basándose en las fechas de registro de los dominios utilizados. Por ejemplo, nagofsg[.]com fue registrado en agosto de 2022 y sclpfybn[.]com en julio de 2021.

> *«Encontré el mismo código utilizado en los ataques a Cyberhaven en una extensión llamada 'Reader Mode'. Este código incluía el utilizado en Cyberhaven (Código1) y un indicador de compromiso adicional, 'sclpfybn[.]com', con otro conjunto de instrucciones maliciosas (Código2)»*, comentó Tuckner.
>
> *«Al investigar ese dominio, descubrí siete nuevas extensiones. Una de estas extensiones, llamada 'Rewards Search Automator', incluía (Código2), que se presentaba como una funcionalidad de 'navegación segura', pero en realidad estaba enviando datos fuera de la plataforma.»*
>
> *«'Rewards Search Automator' también contenía una funcionalidad oculta de 'comercio electrónico' (Código3) asociada con un nuevo dominio 'tnagofsg[.]com',*

> *que era muy similar en funcionalidad a la de 'navegación segura'. Al profundizar en este dominio, encontré la extensión 'Earny – Hasta un 20% de Reembolso en Efectivo', que aún incluye el código de 'comercio electrónico' (Código3) y tuvo su última actualización el 5 de abril de 2023.»*

En el caso de la extensión comprometida de Cyberhaven, el análisis sugiere que el código malicioso estaba diseñado para robar datos de identidad y tokens de acceso de cuentas de Facebook, con un enfoque específico en los usuarios de anuncios de Facebook.

Según Cyberhaven, la versión maliciosa de la extensión fue retirada aproximadamente 24 horas después de que se publicara. Otras extensiones afectadas también han sido

actualizadas o eliminadas de la Chrome Web Store.

No obstante, el hecho de que se haya eliminado de la tienda no significa que la amenaza haya desaparecido, señala Or Eshed. *«Mientras la versión comprometida de la extensión siga activa en los dispositivos de los usuarios, los atacantes aún tendrán acceso y podrán extraer datos»,* explica.

Los investigadores de seguridad continúan analizando otras extensiones que podrían estar comprometidas, pero la complejidad y el alcance de esta campaña han incrementado los desafíos para las organizaciones que buscan proteger sus extensiones de navegador.