Los actores de amenazas están utilizando anuncios de empleo falsos en Facebook como cebo para engañar a posibles víctimas y lograr que instalen un nuevo malware ladrón llamado Ov3r_Stealer, diseñado para sistemas Windows.

Según un informe por Trustwave SpiderLabs, este malware tiene la capacidad de robar credenciales y carteras criptográficas, enviándolas a un canal de Telegram que el actor de amenazas monitorea.

Ov3r_Stealer es capaz de extraer información como la ubicación basada en la dirección IP, datos de hardware, contraseñas, cookies, información de tarjetas de crédito, autocompletados, extensiones de navegador, carteras criptográficas, documentos de Microsoft Office, y una lista de productos antivirus instalados en el host comprometido.

Aunque el objetivo final de la campaña no se conoce con certeza, es probable que la información robada se ofrezca a la venta a otros actores de amenazas. También existe la posibilidad de que Ov3r_Stealer se actualice con el tiempo para funcionar como un cargador similar a QakBot, llevando a cabo cargas útiles adicionales, incluido el ransomware.

El ataque comienza con un archivo PDF manipulado que se presenta como un documento alojado en OneDrive. El usuario es instado a hacer clic en un botón de *«Acceder al documento»* incrustado en el archivo.

Trustwave identificó que el PDF se compartía a través de una cuenta falsa de Facebook que pretendía ser el CEO de Amazon, Andy Jassy, así como a través de anuncios en Facebook para trabajos en publicidad digital.

Los usuarios que hacen clic en el botón son redirigidos a un archivo de acceso directo a Internet (.URL) que simula ser un documento de DocuSign alojado en la red de entrega de contenido (CDN) de Discord. Este archivo de acceso directo sirve como un conducto para entregar un archivo de elemento de panel de control (.CPL), que se ejecuta utilizando el proceso binario del Panel de control de Windows («control.exe«).

La ejecución del archivo CPL conduce a la descarga de un cargador de PowerShell («DATA1.txt») desde un repositorio de GitHub, que finalmente lanza Ov3r_Stealer.

Es relevante señalar que recientemente, Trend Micro reveló una cadena de infección casi idéntica utilizada por actores de amenazas para distribuir otro ladrón llamado Phemedrone Stealer, aprovechando una vulnerabilidad de bypass en Microsoft Windows Defender SmartScreen (CVE-2023-36025, puntuación CVSS: 8.8).

Las similitudes incluyen el uso del mismo repositorio de GitHub (nateeintanan2527) y el hecho de que Ov3r_Stealer comparte similitudes a nivel de código con Phemedrone.

> *«Este malware se informó recientemente, y podría ser que Phemedrone haya sido adaptado y renombrado como Ov3r_Stealer. La principal diferencia entre ambos es que Phemedrone está programado en C#»,* según Trustwave.

Estos descubrimientos coinciden con la revelación de Hudson Rock de que los actores de amenazas están anunciando su acceso a portales de solicitud de cumplimiento policial de importantes organizaciones como Binance, Google, Meta y TikTok, aprovechando credenciales obtenidas de infecciones por ladrones de información.

Además, siguen la aparición de una categoría de infecciones denominada CrackedCantil, que utiliza software pirateado como un vector de acceso inicial para distribuir cargadores como PrivateLoader y SmokeLoader. Estos actúan como mecanismos de entrega para ladrones de información, mineros de criptomonedas, botnets de proxy y ransomware.