Una nueva variante de malware conocida como BundleBot ha estado operando de manera sigilosa aprovechando técnicas de despliegue de archivos únicos de .NET, lo que permite a los actores de amenazas capturar información sensible de los dispositivos comprometidos.

> *«BundleBot está abusando del formato de paquete .NET (archivo único y autónomo), lo que resulta en una detección estática muy baja o incluso nula. Comúnmente se distribuye a través de anuncios en Facebook y cuentas comprometidas que dirigen a sitios web que se hacen pasar por utilidades de programas legítimos, herramientas de inteligencia artificial y juegos»,* informó Check Point en un informe publicado esta semana.

Algunos de estos sitios web buscan imitar a Google Bard, el chatbot de inteligencia artificial generativa y conversacional de la compañía, con el objetivo de atraer a las víctimas para que descarguen un archivo RAR falso («Google_AI.rar») alojado en servicios de almacenamiento en la nube legítimos como Dropbox.

Una vez que se desempaqueta el archivo, se encuentra un archivo ejecutable («GoogleAI.exe»), que es la aplicación .NET de archivo único y autónomo («GoogleAI.exe») que, a su vez, incorpora un archivo DLL («GoogleAI.dll»), el cual se encarga de obtener un archivo ZIP protegido con contraseña desde Google Drive.

El contenido extraído del archivo ZIP («ADSNEW-1.0.0.3.zip») es otra aplicación .NET de archivo único y autónomo («RiotClientServices.exe») que contiene la carga útil de BundleBot («RiotClientServices.dll») y un serializador de datos de paquetes para el control y comando (C2) («LibrarySharing.dll»).

El fabricante RiotClientServices.dll es un malware personalizado y nuevo tipo RAT que utiliza la biblioteca LirarySharing.dll para procesar y serializar los datos de paquetes que se envían al servidor de control y comando (C2) como parte de la comunicación del malware, según informó la compañía israelí de ciberseguridad.

Los artefactos binarios emplean técnicas de ofuscación y código basura personalizado para resistir el análisis, y cuentan con capacidades para extraer datos de navegadores web, capturar capturas de pantalla, obtener tokens de Discord, información de Telegram y detalles de cuentas de Facebook.

Check Point también descubrió una segunda muestra de BundleBot que es virtualmente idéntica en todos los aspectos, excepto que utiliza HTTPS para exfiltrar la información a un servidor remoto en forma de un archivo ZIP.

El uso de señuelos relacionados con Google Bard no debería sorprender, dado que los cibercriminales han estado aprovechando la popularidad de este tipo de herramientas de inteligencia artificial para engañar a los usuarios en plataformas como Facebook y hacer que descarguen malware que roba información, como Doenerium, sin que ellos lo sepan.

> *«La utilización de anuncios en Facebook y cuentas comprometidas como método de distribución ha sido abusada por los actores de amenazas desde hace tiempo. La combinación de esto con una de las capacidades del malware revelado (robar información de cuentas de Facebook de las víctimas) podría servir como una astuta forma de retroalimentación automática»*, señaló la compañía.

Este desarrollo se produce después de que Malwarebytes descubriera una nueva campaña que utiliza publicaciones patrocinadas y cuentas verificadas comprometidas que se hacen pasar por el Administrador de Anuncios de Facebook para atraer a los usuarios a descargar extensiones falsas de Google Chrome diseñadas para robar información de inicio de sesión de Facebook.

Los usuarios que hacen clic en el enlace incrustado son dirigidos a descargar un archivo RAR que contiene un archivo instalador MSI que, a su vez, inicia un script por lotes para abrir una nueva ventana de Google Chrome con la extensión maliciosa cargada utilizando la bandera «–load-extension».

> inicie chrome.exe –load-extension=»%~dp0/nmmhkkegccagdldgiimedpiccmgmiedagg4″ «https://www.facebook.com/business/tools/ads-manager»

> *«Esta extensión personalizada está disfrazada de manera inteligente como Google Translate y se considera 'Desempaquetada' porque se cargó desde la computadora local, en lugar de la Chrome Web Store. Está totalmente enfocada en Facebook y en capturar información importante que podría permitir que un atacante acceda a cuentas»,* explicó Jérôme Segura, director de inteligencia de amenazas de Malwarebytes.

Los datos capturados se envían posteriormente utilizando la API de Google Analytics para evitar las políticas de seguridad de contenido (CSP) implementadas para mitigar los ataques de scripting entre sitios (XSS) y de inyección de datos.

Se sospecha que los actores detrás de esta actividad son de origen vietnamita, quienes han mostrado un agudo interés en los últimos meses en apuntar a cuentas de negocios y publicidad de Facebook. Más de 800 víctimas en todo el mundo han sido afectadas, 310 de ellas ubicadas en los Estados Unidos.

> *«Los estafadores tienen mucho tiempo en sus manos y pasan años estudiando y comprendiendo cómo abusar de las redes sociales y las plataformas en la nube, donde es una carrera constante para mantener a los actores maliciosos fuera. Recuerda que no hay una solución mágica y cualquier cosa que suene demasiado buena para ser verdad podría ser fácilmente una estafa disfrazada»,* dijo Segura.