Un sitio web de gestión de descargas dirigido a usuarios de Linux entregó malware de manera sigilosa que durante más de tres años robó contraseñas y otra información confidencial como parte de un ataque a la cadena de suministro.

La táctica utilizada consistió en establecer una conexión inversa hacia un servidor controlado por actores maliciosos e instalar un programa Bash en el sistema comprometido. La campaña, que tuvo lugar entre 2020 y 2022, ya no está en curso.

> *«Este software malicioso recopila datos como detalles del sistema, historial de navegación, contraseñas almacenadas, archivos de carteras de criptomonedas, así como credenciales para servicios en la nube (AWS, Google Cloud, Oracle Cloud Infrastructure, Azure)»*, señalaron los investigadores de Kaspersky, Georgy Kucherin y Leonid Bezvershenko.

El sitio web en cuestión es freedownloadmanager[.]org, que, según la firma de ciberseguridad rusa, ofrece un software legítimo para Linux llamado *«Free Download Manager».* Sin embargo, a partir de enero de 2020, comenzó a redirigir a algunos usuarios que intentaban descargarlo a otro dominio, deb.fdmpkg[.]org, que proporcionaba un paquete Debian con una trampa.

Se presume que los autores del malware diseñaron el ataque basándose en ciertos criterios de filtrado predefinidos (por ejemplo, una huella digital del sistema) para dirigir selectivamente a posibles víctimas hacia la versión maliciosa. Las redirecciones engañosas cesaron en 2022 por razones inexplicables.

El paquete Debian contiene un script de posinstalación que se ejecuta después de su instalación para copiar dos archivos ELF, /var/tmp/bs y un backdoor basado en DNS (/var/tmp/crond) que inicia una conexión inversa hacia un servidor de comando y control (C2) en respuesta a una solicitud DNS a uno de los cuatro dominios siguientes:

- 2c9bf1811ff428ef9ec999cc7544b43950947b0f.u.fdmpkg[.]org

- c6d76b1748b67fbc21ab493281dd1c7a558e3047.u.fdmpkg[.]org
- 0727bedf5c1f85f58337798a63812aa986448473.u.fdmpkg[.]org
- c3a05f0dac05669765800471abc1fdaba15e3360.u.fdmpkg[.]org

> *«El protocolo de comunicación varía dependiendo del tipo de conexión, siendo ya sea SSL o TCP. En el caso de SSL, el backdoor crond ejecuta el archivo /var/tmp/bs y transfiere todas las comunicaciones posteriores a él. En otro caso, el backdoor crond crea la conexión inversa por sí mismo»,* informaron los investigadores.

El objetivo último del ataque es implementar un malware roba-información y recopilar datos confidenciales del sistema. La información recolectada se carga luego en el servidor del atacante utilizando un programa de carga descargado desde el servidor C2.

Según Kaspersky, crond es una variante de un backdoor conocido como Bew que ha estado circulando desde 2013, mientras que una versión temprana del malware roba-información Bash ya fue documentada por Yoroi en junio de 2019.

No está claro de inmediato cómo se produjo el compromiso en realidad y cuáles eran los objetivos finales de la campaña. Lo que es evidente es que no todos los que descargaron el software recibieron el paquete malicioso, lo que permitió evadir la detección durante años.

> *«Aunque la campaña está actualmente inactiva, este caso de Free Download Manager demuestra que puede ser bastante complicado detectar ataques cibernéticos en curso en máquinas Linux a simple vista. Por lo tanto, es crucial que las máquinas Linux, tanto de escritorio como de servidor, estén equipadas con soluciones de seguridad confiables y eficaces»,* afirmaron los investigadores.

Actualización

El equipo de Free Download Manager contactó a Masterhacks para incluir una actualización con la declaración oficial de la organización. Puedes ver dicha declaración en su página oficial.

> *«Para investigar este problema, accedimos a datos de las copias de seguridad de nuestro proyecto que datan de 2020 y encontramos esta página modificada, que contenía un algoritmo que elegía si daba a los usuarios el enlace de descarga correcto o el que conducía al dominio falso deb.fdmpkg.org que contenía un archivo malicioso. Archivo .deb. Tenía una «lista de excepciones» de direcciones IP de varias subredes, incluidas las asociadas con Bing y Google. Los visitantes de estas direcciones IP siempre recibieron el enlace de descarga correcto»,* es algo de lo que se puede leer en la declaración oficial de FDM.

Actualización 22 de septiembre

En seguimiento al incidente ocurrido con el sitio de Free Download Manager, el equipo de mantenedores del proyecto ha lanzado un script bash para buscar malware en los equipos de los usuarios.

> *«A la luz de las recientes preocupaciones de seguridad relacionadas con FDM, hemos desarrollado un script bash que permite a los usuarios comprobar si hay malware en sus sistemas. El script y las instrucciones ya están disponibles en nuestro sitio web oficial:»,* https://www.freedownloadmanager.org/blog/?p=664

Se espera que este script ayude a los usuarios a identificar malware en sus sistemas y evitar la propagación de malware. Agradecemos al equipo de FDM por la constante comunicación con Masterhacks para lograr publicar las actualizaciones a tiempo.