Investigadores de seguridad cibernética detectaron una cepa de malware previamente indocumentada denominada MosaicLoader, que destaca a las personas que buscan software descifrado como parte de una campaña global.

> *«Los atacantes detrás de MosaicLoader crearon una pieza de malware que puede entregar cualquier carga útil en el sistema, haciéndolo potencialmente rentable como servicio de entrega. El malware llega a los sistemas de destino haciéndose pasar por instaladores crackeados. Descarga un rociados de malware que obtiene una lista de URL del servidor C2 y descarga las cargas útiles de los enlaces recibidos»*, dijeron los investigadores de Bitdefender.

El malware se ha denominado así debido a su sofisticada estructura interna que se orquesta para evitar la ingeniería inversa y evade el análisis.

Los ataques que involucran a MosaicLoader se basan en una táctica bien establecida para la entrega de malware llamada envenenamiento por optimización de motores de búsqueda (SEO), en la que los ciberdelincuentes compran espacios publicitarios en los resultados de los motores de búsqueda para impulsar sus enlaces maliciosos como resultados principales cuando los usuarios buscan términos relacionados con software pirateado.

Luego de una infección exitosa, el cuentagotas inicial basado en Delphi, que se hace pasar por un instalador de software, actúa como un punto de entrada para obtener cargas útiles de la siguiente etapa desde un servidor remoto y también agrega exclusiones locales en Windows Defender para los dos ejecutables descargados en un intento para frustrar el análisis antivirus.

Exclusiones de Windows Defender vía PowerShell

Cabe mencionar que dichas exclusiones de Windows Defender se pueden encontrar en las claves de registro que se enumeran a continuación:

- Exclusiones de archivos y carpetas: HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows Defender \ Exclusions \ Paths
- Exclusiones de tipo de archivo: HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows Defender \ Exclusions \ Extensions
- Exclusiones de procesos: HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows Defender \ Exclusions \ Processes

Uno de los binarios, *«appsetup.exe»*, está hecho para lograr la persistencia en el sistema, mientras que el segundo ejecutable, *«prun.exe»*, funciona como un descargador de un módulo de pulverización que puede recuperar e implementar una variedad de amenazas de una lista de URL, que van desde ladrones de cookies hasta mineros de criptomonedas, e incluso implantes más avanzados como Glupteba.

«prun.exe» también se destaca por su aluvión de técnicas de ofuscación y anti-retroceso, que implican la separación de fragmentos de código con bytes de relleno aleatorios, con el flujo de ejecución diseñado para *«saltar sobre estas partes y solo ejecutar los fragmentos pequeños y significativos».*

Debido a la amplia gama de capacidades de MosaicLoader, los sistemas comprometidos pueden convertirse en una botnet que el actor de la amenaza puede explotar para propagar conjuntos múltiples y en evolución de malware sofisticado, incluyendo el malware personalizado y disponible públicamente, para obtener, expandir y mantener sin autorización el acceso a las computadoras y redes de las víctimas.

> *«La mejor manera de defenderse de MosaicLoader es evitar descargar software descifrado de cualquier fuente. Además de estar en contra de la ley, los*

> *ciberdelincuentes buscan atacar y explotar a los usuarios que buscan software ilegal. Es esencial verificar el dominio de origen de cada descarga para asegurarse de que los archivos sean legítimos»*, dijeron los investigadores.