Los usuarios que buscan juegos populares fueron engañados para descargar instaladores trojanizados que resultaron en la instalación de un minero de criptomonedas en equipos Windows comprometidos.

Esta actividad a gran escala ha sido denominada StaryDobry por la empresa rusa de ciberseguridad Kaspersky, que la detectó por primera vez el 31 de diciembre de 2024. La actividad duró un mes.

Los objetivos de la campaña incluyen tanto a individuos como a empresas de todo el mundo, con la telemetría de Kaspersky revelando mayores concentraciones de infecciones en Rusia, Brasil, Alemania, Bielorrusia y Kazajistán.

> *«Este enfoque permitió a los atacantes maximizar el uso del implante del minero, apuntando a poderosas máquinas de juegos capaces de soportar la actividad de minería»,* comentaron los investigadores Tatyana Shishkova y Kirill Korchemny en un análisis publicado el martes.

La campaña del minero de criptomonedas XMRig utiliza juegos populares de simulación y física como BeamNG.drive, Garry's Mod, Dyson Sphere Program, Universe Sandbox y Plutocracy como señuelos para lanzar una cadena de ataques compleja.

El proceso incluye la subida de instaladores de juegos contaminados creados con Inno Setup a varios sitios de torrents en septiembre de 2024, lo que sugiere que los atacantes detrás de la campaña planearon cuidadosamente los ataques.

Los usuarios que descargan estos archivos, también conocidos como «repacks», ven una pantalla de instalación que los incita a continuar con el proceso de configuración, durante el cual se extrae y ejecuta un dropper («unrar.dll»).

El archivo DLL solo sigue ejecutándose después de realizar una serie de verificaciones para determinar si está en un entorno de depuración o sandbox, lo que muestra su

comportamiento altamente evasivo.

A continuación, el malware consulta varios sitios como api.myip [.]com, ip-api [.]com e ipwho [.]is para obtener la dirección IP del usuario y estimar su ubicación. Si no puede completar este paso, establece el país como China o Bielorrusia por razones que no están completamente claras.

La siguiente fase involucra la recopilación de una huella digital de la máquina, el descifrado de otro archivo ejecutable («MTX64.exe») y la escritura de su contenido en un archivo en el disco denominado «Windows.Graphics.ThumbnailHandler.dll» en la carpeta %SystemRoot% o %SystemRoot%\Sysnative.

Basado en un proyecto legítimo de código abierto llamado EpubShellExtThumbnailHandler, MTX64 modifica la funcionalidad del controlador de miniaturas del Windows Shell Extension para su propio beneficio, cargando una carga útil de siguiente etapa, un ejecutable llamado Kickstarter que luego descomprime un blob cifrado incrustado en él.

El blob, al igual que en el paso anterior, se guarda en el disco bajo el nombre «Unix.Directory.IconHandler.dll» en la carpeta %appdata\Roaming\Microsoft\Credentials%InstallDate%.

El DLL recién creado está configurado para descargar el binario de última etapa desde un servidor remoto que maneja el implante del minero, mientras verifica continuamente si los procesos taskmgr.exe y procmon.exe están presentes en la lista de procesos activos. El artefacto se cierra inmediatamente si se detecta alguno de estos procesos.

El minero es una versión modificada de XMRig que utiliza una línea de comando preconfigurada para comenzar la minería en máquinas con CPUs que tienen 8 o más núcleos.

> *«Si hay menos de 8, el minero no se ejecuta. Además, los atacantes optaron por alojar un servidor de minería en su propia infraestructura en lugar de usar uno*

> *público»*, explicaron los investigadores.
>
> *«XMRig analiza la línea de comando utilizando su funcionalidad incorporada. El minero también crea un hilo separado para comprobar si hay monitores de procesos en el sistema, utilizando el mismo método que en la etapa anterior.»*

StaryDobry sigue sin ser atribuido debido a la falta de indicios que lo vinculen a actores de crimen cibernético conocidos. Sin embargo, la presencia de cadenas de texto en ruso en las muestras sugiere que el atacante podría ser un actor de habla rusa.