Una herramienta legítima de Windows llamada Advanced Installer, utilizada para crear paquetes de software, está siendo mal utilizada por actores de amenazas para propagar malware de minería de criptomonedas en máquinas infectadas desde al menos noviembre de 2021.

> *«El atacante emplea Advanced Installer para empacar otros instaladores legítimos de software, como Adobe Illustrator, Autodesk 3ds Max y SketchUp Pro, junto con scripts maliciosos, y aprovecha la función de Acciones Personalizadas de Advanced Installer para que los instaladores de software ejecuten los scripts maliciosos»*, explicó Chetan Raghuprasad, investigador de Cisco Talos, en un informe técnico.

La naturaleza de las aplicaciones troyanizadas sugiere que las víctimas probablemente se encuentran en sectores como arquitectura, ingeniería, construcción, fabricación y entretenimiento. Los instaladores de software predominantemente se encuentran en francés, lo que indica que los usuarios de habla francesa son el objetivo principal.

Esta campaña estratégica se enfoca en industrias que dependen en gran medida de computadoras con una poderosa Unidad de Procesamiento Gráfico (GPU) para sus operaciones diarias, lo que las convierte en objetivos atractivos para el cryptojacking.

El análisis de Cisco de los datos de solicitudes DNS enviadas a la infraestructura del atacante muestra que las víctimas se encuentran principalmente en Francia y Suiza, seguidas de infecciones esporádicas en los Estados Unidos, Canadá, Argelia, Suecia, Alemania, Túnez, Madagascar, Singapur y Vietnam.

Los ataques culminan con la implementación de un M3_Mini_Rat, un script de PowerShell que probablemente actúa como una puerta trasera para descargar y ejecutar amenazas adicionales, así como varias familias de malware de minería de criptomonedas, como PhoenixMiner y lolMiner.

En cuanto al vector de acceso inicial, se sospecha que se utilizaron técnicas de

envenenamiento de motores de búsqueda (SEO) para entregar los instaladores de software manipulados a las máquinas de las víctimas.

Una vez que se ejecuta el instalador, se inicia una cadena de ataque de múltiples etapas que descarga el cliente M3_Mini_Rat y los binarios del minero.

> *«El cliente M3_Mini_Rat es un script de PowerShell con capacidades de administración remota que se enfoca principalmente en realizar reconocimiento del sistema y descargar y ejecutar otros binarios maliciosos»,* señaló Raghuprasad.

El troyano está diseñado para comunicarse con un servidor remoto, aunque actualmente no responde, lo que dificulta determinar la naturaleza exacta del malware que podría haberse distribuido a través de este proceso.

Los otros dos componentes maliciosos se utilizan para minar criptomonedas de forma ilícita utilizando los recursos de GPU de la máquina. PhoenixMiner es un malware de minería de criptomonedas de Ethereum, mientras que lolMiner es un software de minería de código abierto que puede utilizarse para minar dos monedas virtuales al mismo tiempo.

En otro caso de abuso de herramientas legítimas, Check Point advierte sobre un nuevo tipo de ataque de phishing que utiliza Google Looker Studio para crear sitios falsos de phishing de criptomonedas en un intento de eludir las protecciones.

> *«Los hackers están empleando esta técnica para crear páginas falsas de criptomonedas diseñadas para robar dinero y credenciales»*, advirtió el investigador de seguridad Jeremy Fuchs.

> *«En resumen, los hackers están aprovechando la autoridad de Google. Un servicio*

> *de seguridad de correo electrónico analizará todos estos factores y tendrá un alto grado de confianza en que no se trata de un correo electrónico de phishing y que proviene de Google».*