Investigadores de seguridad cibernética de por lo menos dos empresas, revelaron los detalles de una nueva variedad de malware que se dirige a los sistemas operativos Windows y MacOS, con un malware de minería de criptomonedas basado en Linux.

Denominado como LoudMiner o Bird Miner, el ataque aprovecha el software de virtualización basado en la línea de comandos en sistemas específicos para iniciar silenciosamente una imagen del sistema operativo Tiny Core Linux que ya contiene un software de minería de criptomonedas activado por un pirata informático.

Descubiertos por investigadores de ESET y Malwarebytes, los atacantes distribuyen el malware junto con copias pirateadas del software VST (Virtual Studio Technology) en Internet y a través de la red de Torrent desde agosto de 2018.

Las aplicaciones VST contienen sonidos, efectos, sintetizadores y otras funciones de edición avanzadas que permiten a los profesionales de audio centrados en la tecnología, la creación de música.

> *«Con respecto a la naturaleza de las aplicaciones dirigidas, es interesante observar que su propósito está relacionado con la producción de audio, por lo tanto, las máquinas en las que están instaladas deben tener una buena capacidad de procesamiento y un alto consumo de CPU»*, dijeron los investigadores de ESET.

También encontraron versiones maliciosas de casi 137 aplicaciones relacionadas con VST, 42 de estas son para Windows y 95 son para MacOS, incluyendo Propellerhead Reason, Ableton Live, Sylenth1, Nexus, Reaktor 6 y AutoTune.

Para los sistemas MacOS, el software ejecuta múltiples scripts de shell y utiliza la utilidad de código abierto Quick Emulator (QEMU) para iniciar el sistema operativo virtual de Linux, y para Windows, se basa en VirtualBox para la emulación.

Una vez instalado y activado, el malware también gana persistencia en el sistema al instalar

archivos adicionales y luego inicia las máquinas virtuales en segundo plano.

Estas imágenes del sistema operativo Linux ya fueron preconfiguradas por los atacantes para iniciar el software de minerías de criptomonedas automáticamente en el inicio sin necesidad de que un usuario inicie sesión y se conecte a los servidores de comando y control del pirata informático.

> «El archivo OVF incluido en la imagen de Linux describe la configuración de hardware de la máquina virtual: utiliza 1 GB de RAM y 2 núcleos de CPU (con un máximo del 90%). La imagen de Linux es Tiny Core Linux 9.0, configurado para ejecutar XMRig, así como algunos archivos y scripts para mantener el minero actualizado continuamente», dijeron los investigadores de ESET.

El malware *«puede ejecutar dos imágenes a la vez, cada una de las cuales toma 128 MB de RAM y un núcleo de CPU»* para explotar de forma simultánea.

> *«Además, el hecho de que el malware ejecute dos mineros separados, cada uno de ellos ejecutando su propio archivo de imagen QEMU de 130 MB, significa que el malware consume muchos más recursos de los necesarios»*, dijo Malwarebytes.

El ataque es otra buena razón por la que nunca se debe confiar en software no oficial y pirateado disponible en Internet, siempre es necesario asegurarse de descargar programas legítimos de fuentes confiables.