Los atacantes están explotando las fallas de ProxyLogon en Microsoft Exchange Server, para cooptar máquinas vulnerables a una botnet de criptomonedas llamada Prometei, según una nueva investigación.

> «Prometei explota las vulnerabilidades de Microsoft Exchange recientemente divulgadas asociados a los ataques de hafnio para penetrar en la red para la implementación de software malicioso, la recolección de credenciales y más», dijo Cybereason en un análisis.

Documentado por primera vez por Cisco Talos en julio de 2020, Prometei es una botnet multimodular, con el actor detrás de la operación que emplea una amplia gama de herramientas especialmente diseñadas y exploits conocidos como EternalBlue y BlueKeep para recolectar credenciales, propagarse lateralmente a través de la red y *«aumentar la cantidad de sistemas que participan en su grupo de minería Monero».*

> *«Prometei tiene versiones basadas en Windows y Linux-Unix, y ajusta su carga útil según el sistema operativo detectado en las máquinas objetivo cuando se propaga a través de la red. Está construido para interactuar con cuatro servidores de comando y control (C2) diferentes, lo que fortalece la infraestructura de la botnet y mantiene las comunicaciones continuas, haciéndola más resistente a las caídas»,* dijo Lior Rochberger, investigador de Cybereason.

Las intrusiones aprovechan las vulnerabilidades recientemente parcheadas en los servidores Microsoft Exchange con el objetivo de abusar del poder de procesamiento de los sistemas Windows para minar Monero.

En la secuencia de ataque observada por la compañía, se descubrió que el adversario explotaba las vulnerabilidades del servidor Exchange CVE-2021-27065 y CVE-2021-26858 como un vector de compromiso inicial para instalar el shell web de China Chopper y obtener

acceso a la puerta trasera de la red. Con este acceso en su lugar, el atacante lanzó PowerShell para descargar la carga útil inicial de Prometei desde un servidor remoto.

Las versiones recientes del módulo bot cuentan con capacidades de backdoor que admiten un amplio conjunto de comandos, incluido un módulo adicional llamado *«Microsoft Exchange Defender»*, que se hace pasar por un producto legítimo de Microsoft, que probablemente se encarga de eliminar otros shells web competidores que puedan estar instalados en la máquina para que Prometei tenga acceso a los recursos necesarios para extraer criptomonedas de forma eficiente.

Curiosamente, la evidencia recientemente descubierta recopilada de los artefactos de VirusTotal ha revelado que la botnet puede haber existido ya en mayo de 2016, lo que implica que el malware ha evolucionado constantemente desde entonces, agregando nuevos módulos y técnicas a sus capacidades.

Prometei se ha observado en una gran cantidad de víctimas que abarcan los sectores de finanzas, seguros, comercio minorista, fabricación, servicios públicos, viajes y construcción, comprometiendo redes de entidades ubicadas en Estados Unidos, Reino Unido y varios países de Europa, América del Sur y Asia Oriental, al tiempo que evita explícitamente infectar objetivos en países del antiguo bloque soviético.

No se sabe mucho sobre los atacantes, aparte del hecho de que hablan ruso, y las versiones anteriores de Prometei tienen su código de idioma configurado como «ruso». Un módulo de cliente Tor separado utilizado para comunicarse con un servidor Tor C2 incluía un archivo de configuración que está configurado para evitar el uso de varios nodos de salida ubicados en Rusia, Ucrania, Bielorrusia y Kazajstán.

> *«Los actores de amenazas en la comunidad de delitos cibernéticos continúan adoptando técnicas similares a APT y mejoran la eficiencia de sus operaciones. Como se observó en los recientes ataques de Prometei, los actores de la amenaza aprovecharon la ola de vulnerabilidades de Microsoft Exchange recientemente*

> *descubiertas y las explotaron para penetrar en las redes específicas»,* dijo Rochberger.
>
> *«Esta amenaza representa un gran riesgo para las organizaciones, ya que los atacantes tienen control absoluto sobre las máquinas infectadas, y si así lo desean, pueden robar información, infectar los endpoints con otro malware o incluso colaborar con bandas de ransomware vendiendo el acceso a los puntos finales infectados»*, agregó.