Se ha descubierto una nueva botnet en la naturaleza explotando el protocolo SMB de Microsoft Windows para moverse de forma lateral a través de los sistemas mientras mina criptomonedas de forma encubierta.

En un informe, Cisco Talos explicó que el malware Prometei ha estado en funcionamiento desde marzo de 2020.

La nueva red de bots se considera peligrosa ya que utiliza un sistema modular extenso y una variedad de técnicas para comprometer los sistemas y ocultar su presencia a los usuarios finales para extraer la criptomoneda Monero (XMR).

La cadena de infección de Prometei comienza con el intento de compromiso del protocolo de Bloqueo de Mensajes de Windows Server (SMB) de una máquina a través de vulnerabilidades que incluyen Eternal Blue.

Mimikatz y otros ataques de fuerza bruta se utilizan para buscar, almacenar y probar credenciales robadas, y las contraseñas descubiertas se envían al servidor de comando y control (C2) del operador para su reutilización por *«otros módulos que intentan verificar la validez de las contraseñas en otros sistemas que utilizan protocolos SMB y RDP»,* según los investigadores.

En total, la botnet cuenta con más de 15 módulos ejecutables que son controlados por un módulo principal. La botnet está organizada en dos ramas de funciones principales: una rama C++ dedicada a las operaciones de minería de criptomonedas, y otra, basada en .NET, que se centra en el robo de credenciales, el abuso de SMB y la ofuscación.

Sin embargo, la rama principal puede operar de forma independiente de la segunda, ya que contiene funcionalidad para comunicarse con un C2, robo de credenciales y minería de criptomonedas.

También se le agregaron módulos auxiliares que pueden ser utilizados por el malware para comunicarse por medio de redes TOR o I2P, para recopilar información del sistema, verificar

puertos abiertos, extenderse a través de SMB y escanear la existencia de cualquier billetera de criptomonedas.

Una vez que un sistema se compromete y se agrega a la red esclava, el atacante puede realizar una variedad de tareas, como la ejecución de programas y comandos, el lanzamiento de shells de comandos, la configuración de claves de cifrado RC4 para comunicación, apertura, descarga y robo de archivos, y lanzamiento de operaciones de minería de criptomonedas, entre otras funciones.

Según los análisis de Cisco Talos en el módulo de minería, el número actual de sistemas infectados con Prometei está en los *«miles bajos».* La botnet solo ha estado funcionando durante cuatro meses, por lo que las ganancias no son altas actualmente, generando solo 1,250 dólares por mes en promedio.

Se han detectado solicitudes del C2 de Prometei en países como Estados Unidos, Brasil, Turquía, China y México.

Uno de los servidores C2 fue incautado en junio, pero esto parece no haber tenido ningún impacto material en la operación de Prometei.

> *«Aunque las ganancias de 1250 dólares por mes no parecen ser una cantidad significativa en comparación con otras operaciones cibercriminales, para un desarrollador en Europa del Este, esto proporciona más que el salario mensual promedio para muchos países. Quizás por eso, si miramos las rutas incrustadas a los archivos de la base de datos del programa en muchos componentes de botnet, vemos una referencia a la carpeta C:Work»,* dijeron los investigadores.