Una versión actualizada de un malware de botnet denominado Prometei, ha infectado a más de 10,000 sistemas en todo el mundo desde noviembre de 2022.

Las infecciones son geográficamente indiscriminadas y oportunistas, con la mayoría de las víctimas reportadas en Brasil, Indonesia y Turquía.

Prometei, observado por primera vez en 2016, es una botnet modular que presenta un gran repertorio de componentes y varios métodos de proliferación, algunos de los cuales también incluyen la explotación de las vulnerabilidades de ProxyLogon Microsoft Exchange Server.

También es notable por evitar atacar a Rusia, lo que sugiere que los hackers detrás de la operación probablemente tengan su sede en el país.

Las motivaciones de la botnet multiplataforma son financieras, principalmente aprovechando su grupo de hosts infectados para extraer criptomonedas y recolectar credenciales.

La última variante de Prometei (llamada v3) mejora sus características existentes para desafiar el análisis forense y profundizar aún más su acceso en las máquinas de las víctimas, dijo Cisco Talos en un informe.

La secuencia de ataque procede de la siguiente forma: al obtener un punto de apoyo exitoso, se ejecuta un comando de PowerShell para descargar la carga útil de la red de bots desde un servidor remoto. Después, el módulo principal de Prometei se usa para recuperar la carga útil real de criptominería y otros componentes auxiliares en el sistema.

Algunos de estos módulos de soporte funcionan como programas propagadores diseñados para propagar el malware por medio del Protocolo de Escritorio Remoto (RDP), Secure Shell (SSH) y Server Message Block (SMB).

Prometei v3 también se destaca por usar un algoritmo de generación de dominios (DGA) para construir su infraestructura de comando y control (C2). Incluye además un meanismo de actualización automática y un conjunto ampliado de comandos para recopilar datos

confidenciales y controlar el host.

Finalmente, el malware implementa un servidor web Apache que se incluye con un shell web basado en PHP, que es capaz de ejecutar comandos codificados en Base64 y realizar cargas de archivos.

> *«Esta reciente adición de nuevas capacidades indica que los operadores de Prometei están continuamente actualizando la botnet y agregando funcionalidad»,* dijeron los investigadores de Talos, Andrew Windsor y Vanja Svajcer.