Una botnet de adware y minería de criptomonedas dirigida a Rusia, Ucrania, Bielorrusia y Kazajstán, al menos desde 2012, ya está apuntando a servidores Linux.

Según un nuevo análisis publicado por Intezer, el troyano se hace pasar por HTTPd, un programa de uso común en servidores Linux, y es una nueva versión del malware perteneciente a un actor de amenazas rastreado como Stantinko.

En 2017, investigadores de ESET detallaron una botnet masiva de adware que funciona al engañar a los usuarios que buscan software pirateado para que descarguen ejecutables maliciosos disfrazados de torrents para instalar extensiones de navegador fraudulentas que realizan la inyección de anuncios y fraude de clics.

La campaña encubierta, que controla un ejército de medio millón de bots, ha recibido desde entonces una actualización sustancial en forma de un módulo de criptominería con el objetivo de sacar provecho de las computadoras bajo su control.

Aunque Stantinko ha sido tradicionalmente un malware para Windows, la expansión de su conjunto de herramientas para apuntar a Linux no pasó desapercibida, y ESET observó un proxy troyano de Linux implementado a través de binarios maliciosos en servidores comprometidos.

La última investigación de Intezer ofrece nuevos conocimientos sobre el proyecto de Linux, específicamente una versión más reciente (v2.17) del mismo malware (v1.2) llamada https, con una muestra del malware cargada en VirusTotal el 7 de noviembre desde Rusia.

Después de la ejecución, httpd valida un archivo de configuración ubicado en *«etc/pd.d/proxy.conf»* que se entrega junto con el malware, y crea un socket y un oyente para aceptar conexiones de lo que los investigadores creen que son otros sistemas infectados.

Una solicitud HTTP Post de un cliente infectado allana el camino para que el proxy pase la

solicitud a un servidor controlado por el atacante, que luego responde con una carga útil adecuada que el proxy reenvía al cliente.

En el caso de que un cliente no identificado envíe una solicitud HTTP Get al servidor comprometido, se devuelve un redireccionamiento HTTP 301 a una URL preconfigurada especificada en el archivo de configuración.

Al afirmar que la nueva versión del malware solo funciona como un proxy, los investigadores de Intezer dijeron que la nueva variante comparte distintos nombres de funciones con la versión anterior y que algunas rutas codificadas tienen similitudes con campañas anteriores de Stantinko.

> *«Stantinko es el último malware que ataca a servidores Linux volando bajo el radar, junto con amenazas como Doki, IPStorm y RansomEXX. Creemos que este malware es parte de una campaña más amplia que aprovecha los servidores Linux comprometidos»*, dijo la compañía.