Investigadores de seguridad publicaron un informe sobre lo que consideran una botnet de criptominería *«implacable»,* que se esconde detrás de contenido aparentemente legítimo, como imágenes JPEG de Taylor Swift.

La botnet, conocida como MyKings (conocida también como DarkCloud o Smominru), ha estado activa desde 2016, según un comunicado de prensa del 18 de diciembre de Gabor Szappanos en SophosLabs.

Recientemente los actores detrás de MyKings supuestamente agregaron la funcionalidad de bootkit, lo que lo hace aún más resistente a la detección y eliminación.

EL informe de SophosLabs proporciona una visión general completa de las operaciones de la botnet, que Szappanos caracteriza como *«un atacante implacablemente redundante»* que ataca principalmente a los servicios basados en Windows que alojan sistemas de gestión de bases de datos como MySQL y MS-SQL, protocolos de red como Telnet e incluso servidores con almacenamiento de cámaras CCTV.

El informe dice que los creadores de la botnet parecen preferir el uso de código abierto u otro software de dominio público y están altamente capacitados para personalizar y mejorar el código fuente para insertar componentes personalizados que pueden ejecutar ataques y realizar procesos de actualización automatizados.

La botnet lanza una serie de ataques contra un servidor con el objetivo de entregar un ejecutable de malware, frecuentemente un troyano denominado *«Forshare»*, que se encontró que es la carga útil más común en los servidores infectados.

Forshare se utiliza para garantizar que varios criptomineros Monero diferentes se ejecutan en el hardware objetivo, y SophosLabs estima que los operadores de botnets han ganado aproximadamente 3 millones de dólares en Monero hasta ahora. Esto se traduce en un ingreso actual de cerca de 300 dólares por día, debido a la valoración relativa recientemente más baja de la criptomoneda.

En el ejemplo estudiado, una imagen imperceptiblemente modificada de la estrella del pop Taylor Swift, SophosLabs explica que la foto .jpg se había subido a un repositorio público, ocultando dentro de ella un ejecutable que actualizaría automáticamente la botnet cuando se descargara.

La investigación de SophosLabs revela la naturaleza sofisticada del mecanismo de persistencia de MyKings, que se perpetúa por medio de procedimientos agresivos de repetición y auto actualización utilizando múltiples combinaciones de comandos.

> *«Incluso si la mayoría de los componentes de la red de bots se eliminan de la computadora, los restantes tienen la capacidad de restaurarla a su máxima potencia simplemente al actualizarse. Todo esto se organiza utilizando archivos RAR autoextraíbles y archivos por lotes de Windows»*, dice el informe.

También menciona que los países con el mayor número de hosts infectados son actualmente China, Taiwán, Rusia, Brasil, Estados Unidos, India y Japón.

En noviembre, el software disponible para descargar en el sitio web oficial de Monero, se vio comprometido cuando hackers modificaron los binarios con malware que roba criptomonedas.