Existe una campaña activa, motivada por intereses financieros, que tiene como objetivo atacar servidores SSH vulnerables para capturarlos de manera encubierta en una red de proxy.

> *«Esta campaña en curso implica que el atacante aproveche SSH para obtener acceso remoto y ejecutar scripts maliciosos que silenciosamente reclutan servidores víctimas en una red de proxy peer-to-peer (P2P), como Peer2Profit o Honeygain»,* informó el investigador de Akamai, Allen West, en un informe publicado el jueves.

A diferencia del cryptojacking, en el que los recursos de un sistema comprometido se utilizan de manera ilícita para minar criptomonedas, el proxyjacking permite a los actores de amenazas aprovechar el ancho de banda no utilizado de las víctimas para ejecutar servicios diversos de forma encubierta como un nodo P2P.

Esto ofrece beneficios dobles: no solo permite al atacante obtener ganancias del ancho de banda adicional con una carga de recursos considerablemente reducida en comparación con el cryptojacking, sino que también reduce las posibilidades de detección.

> *«Es una alternativa más sigilosa al cryptojacking y presenta implicaciones serias que pueden agravar los problemas ya causados por los ataques proxy en la capa 7«*, afirmó West.

Para empeorar la situación, el anonimato brindado por los servicios de proxy puede ser una espada de doble filo, ya que los actores maliciosos pueden abusar de ellos para ocultar el origen de sus ataques, redirigiendo el tráfico a través de nodos intermediarios.

Akamai, que descubrió la última campaña el 8 de junio de 2023, informó que esta actividad en curso tiene como objetivo atacar servidores SSH vulnerables para infiltrarse de manera encubierta en una red de proxy.

> *«Esta es una campaña activa en la que el atacante utiliza SSH para acceder de forma remota, ejecutando scripts maliciosos que secretamente incorporan servidores víctimas en una red de proxy peer-to-peer (P2P), como Peer2Profit o Honeygain»,* afirmó el investigador de Akamai, Allen West, en un informe publicado el jueves.

A diferencia del cryptojacking, en el cual se utilizan los recursos de un sistema comprometido para minar criptomonedas ilícitamente, el proxyjacking ofrece a los actores de amenazas la capacidad de aprovechar el ancho de banda no utilizado de la víctima para ejecutar servicios diferentes como un nodo P2P.

Esto ofrece dos beneficios principales: no solo permite al atacante monetizar el exceso de ancho de banda con una carga de recursos significativamente reducida en comparación con el cryptojacking, sino que también reduce las posibilidades de ser descubierto.

> *«Es una alternativa más sigilosa al cryptojacking y tiene serias implicaciones que pueden aumentar los problemas que ya presentan los ataques de capa 7 con proxy»,* dijo West.

Para empeorar las cosas, la anonimidad proporcionada por los servicios de proxyware puede ser de doble filo, ya que puede ser aprovechada por actores maliciosos para ocultar el origen de sus ataques al enrutarse a través de nodos intermediarios.