Se ha observado que un nuevo malware de Linux desarrollado con el compilador de scripts de shell (shc) implementa un minero de criptomonedas en sistemas comprometidos.

> *«Se presume que después de una autenticación exitosa por medio de un ataque de diccionario en servidores Linux SSH administrados de forma inadecuada, se instalaron varios malware en el sistema de destino»,* dijo AhnLab Security Emergency Response Center (ASEC) en un informe.

Shc permite que los scripts de shell se conviertan directamente en archivos binarios, lo que ofrece protección contra modificaciones no autorizadas del código fuente. Es similar a la utilidad BAT2EXE en Windows que se usa para convertir cualquier archivo por lotes en un ejecutable.

En una cadena de ataque detallada por la compañía de seguridad cibernética de Corea del Sur, un compromiso exitoso del servidor SSH conduce a la implementación de un malware de descarga shc junto con un bot DDoS IRC basado en Perl.

Posteriormente, el descargador shc procede a obtener el software minero XMRig para extraer criptomonedas, con el bot IRC capaz de establecer conexiones con un servidor remoto para obtener comandos para montar ataques distribuidos de denegación de servicio (DDoS).

> *«Este bot admite no solo ataques DDoS como inundación TCP, inundación UDP e inundación HTTP, sino también otras características que incluyen ejecución de comandos, shell inverso, escaneo de puertos y eliminación de registros»,* dijeron los investigadores de ASEC.

El hecho de que todos los artefactos del descargador de shc se hayan subido a VirusTotal desde Corea del Sur sugiere que la campaña se centra principalmente en los servidores SSH de Linux con poca seguridad en el país.

Se recomienda que los usuarios sigan las pautas de seguridad de contraseñas y las cambien periódicamente para evitar intentos de fuerza bruta y ataques de diccionario. También se recomienda mantener los sistemas operativos actualizados.