Investigadores de seguridad cibernética de Guardicore Labs, publicaron hoy un informe detallado sobre una campaña generalizada de cryptojacking que ataca los servidores de Windows MS-SQL y PHPMyAdmin en todo el mundo.

Nansh0u es el nombre que se le dio a la campaña maliciosa, y está llevándose a cabo por un grupo de piratería chino al estilo de APT que ya ha infectado a casi 50,000 servidores y está instalando un sofisticado rootkit en modo kernel en sistemas comprometidos para evitar que se elimine el malware.

La campaña, que se remonta al 26 de febrero pero fue detectada por primera vez a inicios de abril, cuenta con 20 versiones diferentes de carga útil alojadas en distintos proveedores de alojamiento.

El ataque se basa en la técnica de fuerza bruta luego de encontrar servidores MS-SQL y PHPMyAdmin de acceso público mediante un sistema simple de escáner de puertos.

Después de una autenticación de inicio de sesión exitosa con privilegios administrativos, los atacantes ejecutan una secuencia de comandos de MS-SQL en el sistema comprometido para descargar la carga útil malintencionada desde un servidor de archivos remoto y ejecutarlo con privilegios de sistema.

La carga útil aprovecha en segundo plano, una vulnerabilidad conocida de escalada de privilegios (CVE-2014-4113) para obtener privilegios de sistema en las máquinas comprometidas.

> *«Al usar este privilegio de Windows, el exploit atacante inyecta código en el proceso Winlogon. El código inyectado crea un nuevo proceso que hereda los privilegios del sistema Winlogon, proporcionando permisos equivalentes a la versión anterior».*

Después, la carga útil instala un malware de minería de criptomonedas en servidores comprometidos para extraer la divisa digital TurtleCoin.

Además de esto, el malware también protege su proceso de la terminación mediante el uso de un rootkit de modo de kernel firmado digitalmente para la persistencia.

> *«Descubrimos que el conductor tenía una firma digital emitida por la autoridad de certificación Verisign. El certificado, que está vencido, lleva el nombre de una empresa china falsa: Hanhzhou Hootian Network Technology»*, dicen los investigadores.

Además, los investigadores publicaron una lista completa de IoC (Indicadores de Compromiso) y un script gratuito basado en PowerShell que los administradores de Windows pueden usar para verificar si sus sistemas están infectados o no.

Como el ataque se basa en una combinación de nombre de usuario y contraseña débiles para los servidores MS-SQL y PHPMyAdmin, se recomienda a los administradores que siempre mantengan una contraseña sólida y compleja para sus cuentas.