Agencias de seguridad cibernética del Reino Unido y Estados Unidos, publicaron hoy una alerta de seguridad conjunta acerca de QSnatch, una variante de malware que ha estado infectando dispositivos de almacenamiento conectado a la red (NAS) del fabricante taiwanés QNAP.

En las alertas de la Agencia de Seguridad Cibernética e Infraestructura de Estados Unidos (CISA), y el Centro Nacional de Seguridad Cibernética (NCSC) de Reino Unido, ambas agencias afirman que los ataques con el malware QSnatch se remontan a 2014, pero los ataques se intensificaron durante el último año cuando el número de infecciones reportadas aumentó de 7000 en octubre de 2019, a más de 62 mil a mediados de junio de 2020.

De estos reportes, CISA y NSCS aseguran que aproximadamente 7,600 de los dispositivos infectados se encuentran en Estados Unidos, mientras que unos 3,900 se encuentran en Reino Unido.

> *«La primera campaña probablemente comenzó a inicios de 2014 y siguió hasta mediados de 2017, mientras que la segunda comenzó a fines de 2018 y todavía seguía activa a fines de 2019»,* dijeron las agencias.

Capacidades del malware QSnatch

CISA y NCSC informan que las dos campañas utilizaron diferentes versiones del malware QSnatch, también rastreado bajo el nombre de Derek.

La alerta conjunta se centra en la última versión, utilizada en la campaña más reciente. Según los informes, la nueva versión de QSnatch tiene un conjunto mejorado y amplio de características que incluyen funcionalidades para módulos como:

- Registrador de contraseña CGI: Instala una versión falsa de la página de inicio de sesión de administrador de dispositivo, registra autenticaciones exitosas y las pasa a la página de inicio de sesión legítima.
- Raspador de credenciales.
- Puerta trasera SSH: Esto permite al atacante ejecutar código arbitrario en un dispositivo.
- Exfiltración: Al ejecutarse, QSnatch roba una lista predeterminada de archivos, que incluye configuraciones del sistema y archivos de registro. Estos se cifran con la clave pública del actor y se envían a su infraestructura por medio de HTTPS.
- Funcionalidad de shell web para acceso remoto.

Sin embargo, aunque los investigadores de CISA y de NCSC lograron analizar la versión actual del malware QSnatch, dicen que aún no saben exactamente cómo el malware infecta inicialmente los dispositivos.

Los hackers podrían estar explotando vulnerabilidades en el firmware QNAP o podrían estar utilizando contraseñas predeterminadas para la cuenta de administrador, sin embargo, no se ha podido verificar esto.

Una vez lograda la infección, los investigadores afirman que QSnatch se inyecta en el firmware, desde donde toma el control total del dispositivo y bloquea futuras actualizaciones del firmware para permanecer en la NAS víctima.

Según la alerta conjunta, la infraestructura del servidor del grupo QSnatch que se utilizó en la segunda serie de ataques, está ahora inactiva, pero las infecciones de QSnatch aún siguen activas en Internet y dispositivos infectados.

Las agencias recomiendan a las compañías y usuarios domésticos que utilizan dispositivos QNAP, seguir los pasos para remediar y mitigar los ataques, enumerados en la página de soporte del proveedor.

Omitir la eliminación del malware significa permitir a los hackers el uso de una puerta trasera

en las redes de la empresa y acceso directo a los dispositivos NAS.