Investigadores de seguridad cibernética encontraron una nueva familia de ransomware dirigida a dispositivos de almacenamiento NAS, fabricados por los sistemas QNAP con sede en Taiwán, el ataque encripta los datos hasta que la empresa pague un rescate.

Los dispositivos NAS son unidades de almacenamiento dedicados conectados a una red, que permiten a los usuarios o empresas almacenar y compartir sus datos y copias de seguridad con distintas computadoras.

Descubierto por el equipo de investigación de Anomali, el nuevo ransomware, apodado eCh0raix, apunta a dispositivos NAS de QNAP mal protegidos o inseguros, ya sea por fuerza bruta o forzando credenciales débiles, así como explotando vulnerabilidades conocidas.

eCh0raix está escrito en el lenguaje de programación Go, y cifra todos los archivos con extensiones dirigidas utilizando el cifrado AES y agrega la extensión .encrypt a todos los archivos infectados.

Sin embargo, si un dispositivo NAS comprometido se encuentra en Bielorrusia, Ucrania o Rusia, el ransomware finaliza el proceso de cifrado de archivos y finaliza sin realizar daño alguno.

Después de la ejecución, el ransomware de cifrado de archivos primero se conecta a su servidor remoto de comando y control, protegido detrás de la red Tor, utilizando un proxy Tor SOCKS5 y notifica a los atacantes sobre las nuevas víctimas.

> *«Según el análisis, está claro que el autor del malware ha configurado el proxy para proporcionar a la red Tor el acceso al malware sin incluir la funcionalidad de Tor»*, dicen los investigadores.

En un dispositivo infectado, el ransomware genera una cadena aleatoria de 32 caracteres para crear una clave secreta AES-256 y luego utilizarla para cifrar todos los archivos almacenados en el dispositivo NAS seleccionado con el algoritmo AES con el Modo de Cifrado

de Retroalimentación (CFB) y luego elimina los archivos originales.

Algo interesante, es que ya que el módulo de cifrado utiliza el paquete matemático para generar la clave secreta, es probable que los investigadores escriban un descifrador para la nueva familia de ransomware porque la función no es completamente aleatoria.

> *«El malware inicializa la página aleatoria matemática utilizando la hora actual. Dado que está utilizando el paquete matemático para generar la clave secreta, no es criptográficamente aleatorio, y es posible escribir un descifrador»,* agregan los investigadores.
>
> *«El actor de amenazas apunta a los dispositivos QNAP NAS que se usan para el almacenamiento de archivos y las copias de seguridad. No es común que estos dispositivos ejecuten productos antivirus, y actualmente, las muestras solo son detectadas por 2-3 productos en VirusTotal, lo que permite que el ransomware corra sin problemas»*.

Los investigadores también mencionaron que antes de cifrar los archivos almacenados en las NAS específicas, el ransomware también intenta eliminar una lista específica de procesos, incluidos apache2, httpd, nginx, MySQL, mysql y PostgreSQL.