Un grupo de hackers está atacando dispositivos NAS de Lenovo y pidiendo recompensa por recuperar archivos

Autor: I. Stepanenko

Fecha: Monday 6th of July 2020 01:42:44 AM

Un grupo de hackers bajo el nombre de *«Cl0ud SecuritY»* está accediendo a viejos dispositivos de almacenamiento conectados a la red (NAS) de LenovoEMC (antes Iomega), borrando archivos y dejando notas de rescate pidiendo a los propietarios que paguen entre 200 y 275 dólares para recuperar sus datos.

Los ataques han estado ocurriendo durante al menos un mes, según las entradas en BitcoinAbuse, un sitio web donde los usuarios informan las direcciones de Bitcoin abusadas con referencia a ransomware, extorsiones, entre otros delitos informáticos.

Estos ataques parecen estar dirigidos únicamente a dispositivos LenovoEMC/Iomega NAS, que están exponiendo su interfaz de administración en Internet sin una contraseña.

Muchos de los dispositivos NAS que se encontraron mediante una búsqueda en Shodan, contenían una nota de rescate llamada *«RECOVER YOUR FILES !!!!.TXT».*

Todas las notas de rescate están firmadas con el nombre de Cl0ud SecuritY y se utilizó la misma dirección de correo electrónico *«cloud@mail2pay.com»* como forma de contacto.

Los ataques recientes registrados durante el mes pasado parecen ser una continuación de los ataques que comenzaron el año pasado y que también se han dirigido exclusivamente a

las estaciones NAS de LenovoEMC.

Aunque los ataques del año pasado no fueron firmados ni se utilizó una dirección de correo electrónico como contacto, existen muchas similitudes entre los textos de las notas de rescate utilizados en 2019 y 2020 para creer que se trata del mismo pirata informático.

Victor Gevers, investigador de seguridad cibernética de la GDI Foundation, dijo a ZDNet que ha estado rastreando los ataques por años y que estas intrusiones recientes parecen ser un trabajo de un hacker poco sofisticado.

Gevers agregó que los hackers no confiaron en una hazaña compleja, pues son dispositivos dirigidos que ya estaban abiertos en Internet y no se molestaron en cifrar los datos.

Los piratas informáticos de Cl0ud SecuritY aseguran haber copiado los archivos de la víctima a sus servidores y amenazaron con filtrar los archivos, generalmente en caso de que no se pague el rescate dentro de cinco días.

Sin embargo, no existe evidencia de que los datos hayan sido respaldados en algún lado, tampoco hay datos de víctimas anteriores que hayan realizado el pago.

Gevers también dijo que los ataques contra dispositivos NAS de LenovoEMC no son nuevos e investigó los incidentes desde 1998.

Lenovo ha descontinuado las líneas NAS de LenovoEMC e Iomega en 2018, siendo esta la razón por la que solo existen alrededor de 1000 dispositivos expuestos en línea, ya que la mayoría de las estaciones NAS alcanzaron su EOL hace mucho tiempo.

Aún así, algunos dispositivos NAS siguen en ejecución, y una página de soporte de Lenovo que informa cómo proteger adecuadamente este tipo de dispositivos sigue en línea.

Los ataques a dispositivos NAS de LenovoEMC/Iomega no son los primeros que se han dirigido a dispositivos NAS en los últimos años. Los dispositivos NAS generalmente han sido blanco de malware DDoS, pero también de bandas de ransomware como Muhstik, QSnatch y

eCh0raix.