La empresa rumana de seguridad cibernética Bitdefender, en colaboración con Europol, el proyecto No More Ransom y las autoridades policiales de Zúrich, puso a disposición un descifrador para el ransomware LockerGoga.

Identificado en enero de 2019, LockerGoga acaparó titulares por sus ataques contra la compañía noruega del aluminio, Norsk Hydro. Se dice que infectó a más de 1800 víctimas en 71 países, causando daños estimados en 104 millones de dólares.

La operación de ransomware recibió un golpe significativo en octubre de 2021 cuando 12 personas relacionadas con el grupo, junto con MegaCortex y Dharma, fueron detenidas como parte de un esfuerzo internacional de aplicación de la ley.

Los arrestos, que tuvieron lugar en Ucrania y Suiza, también incluyeron la incautación de dinero en efectivo por un valor de $52,000 dólares, cinco vehículos de lujo y una serie de dispositivos electrónicos. Uno de los acusados se encuentra actualmente en prisión preventiva en Zúrich.

La Policía Cantonal de Zúrich dijo además que pasó los últimos meses examinando los dispositivos de almacenamiento de datos confiscados al individuo durante los arrestos de 2021 e identificó numerosas claves privadas que se utilizaron para bloquear los datos.

También se espera que se publique una utilidad de descifrado para MegaCortex en los siguientes meses. Se recomienda a las partes víctimas que presenten una denuncia penal en sus respectivos países de origen.

> *«Estas claves permiten a las empresas e instituciones agraviadas recuperar los datos que fueron cifrados previamente con el malware LockerGoga o MegaCortex»,* dijo la agencia.

Como un medio para prevenir las infecciones de ransomware, el departamento de policía insta a las organizaciones a manejar de forma segura los correos electrónicos, bloquear los

archivos adjuntos de correo electrónico sospechosos, crear copias de seguridad periódicas, hacer cumplir la autenticación de dos factores y mantener los sistemas de TI actualizados.