Europol anunció el viernes la desmantelación de la infraestructura relacionada con el ransomware Ragnar Locker, junto con la detención de un *«objetivo importante»* en Francia.

> *«Entre el 16 y el 20 de octubre, se llevaron a cabo operaciones de búsqueda en la República Checa, España y Letonia. El principal perpetrador, sospechoso de ser un desarrollador del grupo Ragnar, fue llevado ante los magistrados del Tribunal Judicial de París»,* informó la agencia.

Cinco cómplices adicionales relacionados con la banda de ransomware fueron interrogados en España y Letonia, mientras que los servidores y el portal de filtración de datos fueron confiscados en los Países Bajos, Alemania y Suecia.

Este es el más reciente ejercicio coordinado que involucra a autoridades de la República Checa, Francia, Alemania, Italia, Japón, Letonia, los Países Bajos, España, Suecia, Ucrania y Estados Unidos. Dos sospechosos vinculados a la banda de ransomware fueron arrestados previamente en Ucrania en 2021. Un año después, otro miembro fue aprehendido en Canadá.

Ragnar Locker, que surgió por primera vez en diciembre de 2019, es conocido por una serie de ataques dirigidos a entidades de infraestructura crítica en todo el mundo. Según Eurojust, el grupo ha perpetrado ataques contra 168 empresas internacionales en todo el mundo desde 2020.

> *«El grupo Ragnar Locker era conocido por emplear una táctica de doble extorsión, solicitando pagos exorbitantes a cambio de herramientas de descifrado y para evitar la divulgación de datos sensibles robados»,* declaró Europol.

La Policía Cibernética de Ucrania informó que realizó redadas en las instalaciones de uno de los miembros sospechosos en Kiev, incautando computadoras portátiles, teléfonos móviles y medios electrónicos.

Esta acción policial coincide con la infiltración y cierre del sitio de filtración dirigido por el grupo de ransomware Trigona por parte de la Alianza Cibernética de Ucrania (UCA), y la eliminación de 10 de los servidores, aunque no antes de exfiltrar los datos almacenados en ellos. Hay evidencia que sugiere que los actores de Trigona utilizaron Atlassian Confluence para sus actividades.

Al igual que la desarticulación de Hive y Ragnar Locker representa esfuerzos continuos para abordar la amenaza del ransomware, también lo son las iniciativas emprendidas por actores de amenazas para evolucionar y cambiar de nombre. Hive, por ejemplo, ha resurgido como Hunters International.

Este desarrollo coincide con una operación de la Oficina Central de Investigación de la India, basada en información compartida por Amazon y Microsoft, que llevó a cabo redadas en 76 ubicaciones de 11 estados en una operación a nivel nacional destinada a desmantelar la infraestructura utilizada para facilitar delitos financieros habilitados por la cibertecnología, como estafas de soporte técnico y fraudes con criptomonedas.

La operación, llamada Operación Chakra-II, condujo a la incautación de 32 teléfonos móviles, 48 computadoras portátiles/discos duros, imágenes de dos servidores, 33 tarjetas SIM y unidades USB, así como la adquisición de 15 cuentas de correo electrónico.

También sigue a la extradición de Sandu Diaconu, un ciudadano moldavo de 31 años, desde el Reino Unido a los Estados Unidos para enfrentar cargos relacionados con su papel como administrador de E-Root Marketplace, un sitio web que ofrecía acceso a más de 350,000 credenciales de computadoras comprometidas en todo el mundo para ataques de ransomware, transferencias no autorizadas y fraude fiscal.

El sitio web, que comenzó a operar en enero de 2015, fue cerrado en 2020, y Diaconu fue arrestado en el Reino Unido en mayo de 2021 mientras intentaba huir del país.

> *«El E-Root Marketplace operaba en una red ampliamente distribuida y tomaba*

> *medidas para ocultar las identidades de sus administradores, compradores y vendedores»*, dijo el Departamento de Justicia de los Estados Unidos esta semana.

En una acción policial relacionada, Marquis Hooper, un exgerente de TI de la Marina de los Estados Unidos, fue condenado a cinco años y cinco meses de prisión por obtener ilegalmente información personal identificable (PII) de 9,000 ciudadanos estadounidenses y venderla en la web oscura por $160,000 en bitcoin.