Un hombre con ciudadanía rusa e israelí ha sido acusado en Estados Unidos por presuntamente ser el creador del ransomware como servicio (RaaS) LockBit, una operación ahora desactivada que operó desde su inicio en 2019 hasta al menos febrero de 2024.

Rostislav Panev, de 51 años, fue detenido en Israel en agosto de este año y actualmente se encuentra a la espera de ser extraditado, según informó el Departamento de Justicia de Estados Unidos (DoJ). Se sospecha que Panev obtuvo cerca de $230,000 entre junio de 2022 y febrero de 2024 mediante transferencias a una billetera de criptomonedas vinculada a él.

> *«Durante años, Rostislav Panev desarrolló y gestionó herramientas digitales que permitieron a sus socios de LockBit causar estragos y pérdidas económicas valoradas en miles de millones de dólares en todo el mundo»*, afirmó Philip R. Sellinger, fiscal de Estados Unidos.

LockBit, considerado uno de los grupos de ransomware más activos, vio su infraestructura desmantelada en febrero de 2024 durante una operación policial internacional denominada Cronos. Este grupo es conocido por atacar a más de 2,500 organizaciones en al menos 120 países, incluyendo 1,800 en Estados Unidos.

Las víctimas del ransomware iban desde particulares y pequeñas empresas hasta grandes corporaciones, hospitales, escuelas, organizaciones benéficas, infraestructuras críticas, gobiernos y fuerzas de seguridad. Se estima que el grupo generó al menos $500 millones en ganancias ilícitas.

Según los documentos presentados en el tribunal, el ordenador de Panev, analizado tras su arresto, contenía credenciales de administrador para un repositorio en la dark web que almacenaba el código fuente de varias versiones del constructor de LockBit. Este software era utilizado por afiliados para crear variantes personalizadas del ransomware.

También se hallaron credenciales para el panel de control de LockBit y una herramienta llamada StealBit, que facilitaba a los afiliados extraer datos confidenciales de los sistemas

infectados antes de proceder al cifrado de la información.

Además de escribir y mantener el código del ransomware LockBit, Panev brindó asesoramiento técnico al grupo y supuestamente intercambió mensajes con Dmitry Yuryevich Khoroshev, conocido como «*LockBitSupp*«, sobre el desarrollo del constructor y el panel de control.

> *«En declaraciones a las autoridades israelíes tras su detención, Panev admitió haber realizado trabajos de programación, desarrollo y consultoría para el grupo LockBit, recibiendo pagos frecuentes en criptomonedas por estos servicios»,* señaló el DoJ.
>
> *«Entre las tareas que Panev reconoció haber realizado están el desarrollo de herramientas para desactivar programas antivirus, la implementación de malware en múltiples dispositivos de una red comprometida y la impresión automática de las notas de rescate de LockBit en todas las impresoras conectadas a la red de las víctimas».*

Con este arresto, ya son siete los miembros de LockBit procesados en Estados Unidos, incluidos Mikhail Vasiliev, Ruslan Astamirov, Artur Sungatov, Ivan Gennadievich Kondratiev y Mikhail Pavlovich Matveev.

A pesar de estos reveses, los operadores de LockBit parecen planear un regreso con una nueva versión, LockBit 4.0, programada para lanzarse en febrero de 2025. Sin embargo, el futuro del grupo sigue siendo incierto tras los recientes arrestos y operaciones policiales.

Segundo miembro de NetWalker condenado a 20 años de prisión

En un caso relacionado, Daniel Christian Hulea, un rumano de 30 años vinculado a la

operación de ransomware NetWalker, fue sentenciado a 20 años de cárcel y obligado a renunciar a $21,500,000, además de sus intereses en una empresa en Indonesia y una propiedad de lujo adquirida con fondos obtenidos ilícitamente.

Hulea se declaró culpable en junio de 2024 de conspirar para cometer fraude informático y fraude electrónico. Fue arrestado en Rumanía el 11 de julio de 2023 y extraditado a Estados Unidos.

> *«Como parte de su declaración, Hulea reconoció haber usado NetWalker para obtener aproximadamente 1,595 bitcoins en pagos de rescate, valorados en $21,500,000 en el momento de los pagos»,* indicó el DoJ.

La operación NetWalker se enfocó particularmente en el sector salud durante la pandemia de COVID-19 y fue desmantelada en enero de 2021, cuando las autoridades estadounidenses y búlgaras confiscaron los sitios web utilizados por el grupo.

Desarrollador de Raccoon Stealer recibe 5 años de prisión

En otras noticias, el DoJ anunció la condena de Mark Sokolovsky, un ucraniano de 28 años acusado de ser el principal desarrollador del malware Raccoon Stealer, a 60 meses de prisión por conspirar para cometer intrusión informática.

Sokolovsky ofrecía Raccoon Stealer como un servicio de malware (MaaS) a otros criminales por $200 al mes. Estos utilizaban el software para robar información confidencial mediante técnicas como correos electrónicos de phishing.

Extraditado de los Países Bajos en febrero de 2024, Sokolovsky se declaró culpable y aceptó entregar $23,975 y pagar al menos $910,844.61 en compensación.

> *«Mark Sokolovsky fue una pieza clave en una conspiración criminal internacional que afectó a innumerables víctimas, facilitando el acceso al malware que permitió incluso a delincuentes amateurs cometer crímenes complejos»*, declaró Jaime Esparza, fiscal del distrito oeste de Texas.

El FBI (Buró Federal de Investigaciones) de los Estados Unidos ha lanzado un sitio web donde las personas pueden comprobar si su dirección de correo electrónico está incluida en los datos robados por el malware Raccoon Stealer. Esta operación de Malware-como-Servicio (MaaS) fue desmantelada en marzo de 2022, coincidiendo con la detención de Sokolovsky por parte de las autoridades de los Países Bajos.

Neoyorquino sentenciado a casi 6 años por tráfico de tarjetas de crédito y lavado de dinero

Recientemente, también se dictó sentencia contra Vitalii Antonenko, un residente de Nueva York de 32 años, quien fue condenado a tiempo cumplido y días adicionales por su implicación en un esquema delictivo que utilizaba ataques de inyección SQL para comprometer sistemas, robar información de tarjetas de crédito y datos personales, y vender estos datos en mercados ilegales en línea.

> *«Una vez que los datos eran vendidos por un cómplice, Antonenko y otros empleaban Bitcoin, transferencias bancarias tradicionales y dinero en efectivo para blanquear las ganancias, ocultando su origen, naturaleza, ubicación, propiedad y control. Entre las víctimas de esta conspiración se encuentran una empresa del sector hotelero y una institución de investigación científica sin ánimo de lucro, ambas situadas en el este de Massachusetts»*, explicó el Departamento de Justicia en mayo de 2020.

Antonenko fue detenido en marzo de 2019 cuando regresaba a Estados Unidos desde

Ucrania con «*computadoras y dispositivos digitales que contenían cientos de miles de números de tarjetas de pago robados*».

En septiembre de 2024, se declaró culpable de los cargos de conspiración para acceder ilegalmente a redes informáticas y traficar con dispositivos de acceso no autorizados, así como de conspiración para lavar dinero.