Una nueva operación de ransomware como servicio (RaaS) llamada Eldorado ha surgido, con variantes de bloqueo que permiten cifrar archivos en sistemas Windows y Linux.

Eldorado se presentó por primera vez el 16 de marzo de 2024, cuando se publicó un anuncio para su programa de afiliados en el foro de ransomware RAMP, según informó Group-IB, una empresa de ciberseguridad con sede en Singapur.

La empresa de ciberseguridad, que logró infiltrarse en el grupo de ransomware, indicó que su representante es un hablante de ruso y que el malware no coincide con cepas previamente filtradas como LockBit o Babuk.

> *«El ransomware Eldorado utiliza Golang para capacidades multiplataforma, empleando Chacha20 para el cifrado de archivos y Rivest Shamir Adleman-Optimal Asymmetric Encryption Padding (RSA-OAEP) para el cifrado de claves. Puede cifrar archivos en redes compartidas utilizando el protocolo Server Message Block (SMB)»,* explicaron los investigadores Nikolay Kichatov y Sharmine Low.

El cifrador de Eldorado está disponible en cuatro formatos: esxi, esxi_64, win y win_64, y su sitio de fuga de datos ya ha enumerado 16 víctimas en junio de 2024. Trece de los objetivos se encuentran en los EE. UU., dos en Italia y uno en Croacia.

Estas empresas pertenecen a diversos sectores industriales, como bienes raíces, educación, servicios profesionales, salud y manufactura, entre otros.

Un análisis detallado de la versión de Windows reveló el uso de un comando PowerShell para sobrescribir el bloqueador con bytes aleatorios antes de eliminar el archivo, en un intento de eliminar rastros.

Eldorado es el más reciente de una serie de nuevos actores de ransomware de doble extorsión que han surgido recientemente, incluyendo Arcus Media, AzzaSec, dan0n, Limpopo (también conocido como SOCOTRA, FORMOSA, SEXi), LukaLocker, Shinra y Space Bears,

destacando una vez más la naturaleza persistente de la amenaza.


LukaLocker, vinculado a un operador llamado Volcano Demon por Halcyon, es notable porque no utiliza un sitio de fuga de datos, sino que llama a la víctima por teléfono para extorsionar y negociar el pago después de cifrar estaciones de trabajo y servidores Windows.

Este desarrollo coincide con el descubrimiento de nuevas variantes de Linux del ransomware Mallox (también conocido como Fargo, TargetCompany, Mawahelper) y descifradores asociados con siete diferentes versiones.

Se sabe que Mallox se propaga mediante fuerza bruta en servidores Microsoft SQL y correos electrónicos de phishing para atacar sistemas Windows, con intrusiones recientes que también usan un cargador basado en .NET llamado PureCrypter.

«Los atacantes están utilizando scripts personalizados en Python para la entrega de la carga útil y la exfiltración de la información de la víctima. El malware cifra los datos del usuario y añade la extensión .locked a los archivos cifrados», dijeron los investigadores de Uptycs,

Tejaswini Sandapolla y Shilpesh Trivedi.

Avast también ha desarrollado un descifrador para DoNex y sus predecesores (Muse, falso LockBit 3.0 y DarkRace) aprovechando una vulnerabilidad en el esquema criptográfico. La empresa de ciberseguridad checa ha estado *«proporcionando discretamente el descifrador»* a las víctimas desde marzo de 2024 en colaboración con las autoridades.

> *«A pesar de los esfuerzos de las fuerzas del orden y las mayores medidas de seguridad, los grupos de ransomware continúan adaptándose y prosperando»,* indicó Group-IB.

Datos compartidos por Malwarebytes y NCC Group, basados en las víctimas enumeradas en los sitios de fuga, muestran que se registraron 470 ataques de ransomware en mayo de 2024, frente a 356 en abril. La mayoría de los ataques fueron atribuidos a LockBit, Play, Medusa, Akira, 8Base, Qilin y RansomHub.

> *«El desarrollo continuo de nuevas cepas de ransomware y la aparición de programas de afiliados sofisticados demuestran que la amenaza está lejos de ser contenida. Las organizaciones deben mantenerse vigilantes y proactivas en sus esfuerzos de ciberseguridad para mitigar los riesgos que representan estas amenazas en constante evolución»,* destacó Group-IB.