Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

LOCKBIT SUFRE FILTRACIÓN SE EXPONEN MENSAJES DE NEGOCIACIÓN Y CONTRASEÑAS DE AFILIADOS

09 / 05 / 2025

CONTENIDO

INTRODUCCIÓN

En un nuevo golpe contra el cibercrimen, el temido grupo de ransomware LockBit ha sido hackeado y expuesto públicamente. Su panel de afiliados en la dark web fue intervenido y reemplazado por un mensaje burlón que incluía un enlace con su base de datos interna. Entre los datos filtrados se encuentran miles de direcciones de Bitcoin, configuraciones de ataques, mensajes de negociación con víctimas y hasta contraseñas de sus miembros. Esta filtración pone en jaque la reputación del grupo y demuestra que, incluso en el mundo del crimen digital, nadie está a salvo.

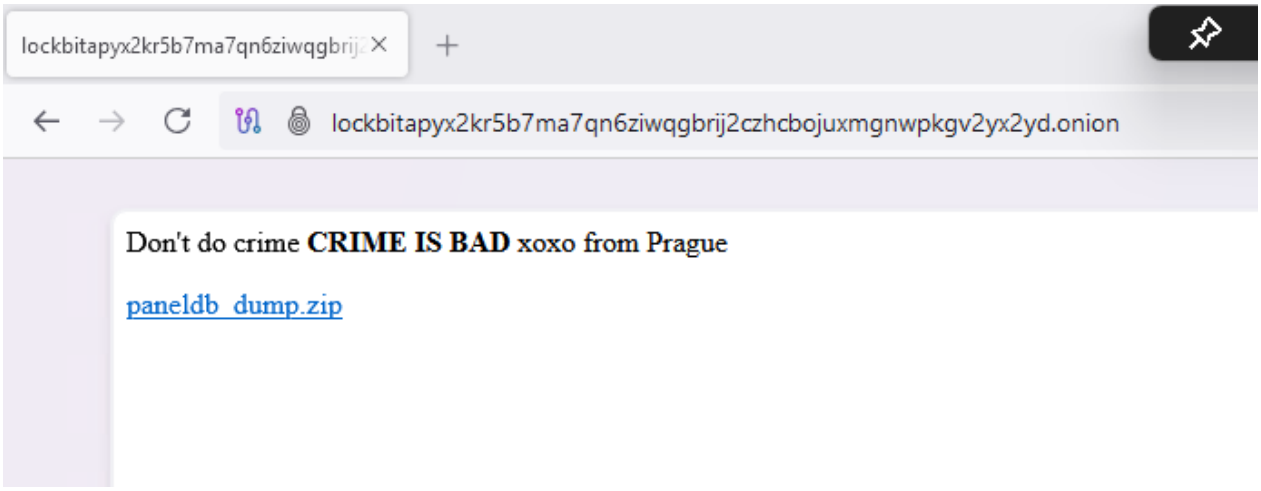
LOCKBIT SUFRE FILTRACIÓN: SE EXPONEN MENSAJES DE NEGOCIACIÓN Y CONTRASEÑAS DE AFILIADOS

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_05_09_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	09/05/2025
Es día cero (0 day):	No

RESUMEN

El grupo de ransomware LockBit, uno de los más conocidos en el mundo del cibercrimen, ha sido víctima de una nueva filtración de datos. Esta vez, su panel de afiliados en la dark web fue hackeado y reemplazado por un mensaje que decía: *"Don't do crime. CRIME IS BAD. xoxo from Prague"* ("No cometas crímenes. El crimen es malo. Con cariño, desde Praga"). El mensaje incluía un enlace para descargar un archivo con la base de datos interna del grupo.



El archivo, llamado paneldb_dump.zip, contiene un volcado (dump) de su base de datos MySQL. Según el análisis realizado, la base de datos incluye:

- **59,975 direcciones de Bitcoin** posiblemente usadas para recibir pagos de rescate.
- **Una tabla de "builds"** con los ataques personalizados que los afiliados lanzaron, incluyendo en algunos casos los nombres de las empresas atacadas.
- **Configuraciones técnicas de los ataques**, como servidores que debían evitarse o tipos de archivos que debían cifrarse.
- **Más de 4,400 mensajes de negociación** entre las víctimas y los operadores del ransomware, intercambiados entre diciembre de 2024 y abril de 2025.
- **Una lista de 75 usuarios**, entre administradores y afiliados del grupo, donde incluso se descubrieron contraseñas guardadas en texto plano. Algunas contraseñas filtradas incluyen "Weekendlover69", "MovingBricks69420" y "Lockbitproud231".

El operador de LockBit conocido como *LockBitSupp* confirmó la brecha a través de una conversación por Tox, pero aseguró que no se filtraron claves privadas ni se perdió información importante para sus operaciones.

Esta filtración se suma a los problemas que LockBit ha enfrentado en el último año. En 2024, la operación internacional **Operation Cronos**, liderada por agencias de seguridad, ya había logrado desmantelar parte

de su infraestructura. A pesar de que el grupo logró volver a operar tras ese golpe, esta nueva exposición pública pone en duda su capacidad para mantener la confianza de sus afiliados.
Todavía no se sabe quién está detrás del hackeo actual, pero el mensaje dejado en el sitio coincide con uno usado recientemente para atacar al grupo Everest, lo que sugiere que podría tratarse del mismo autor o grupo.

Grupos como Conti, Black Basta y Everest también han sufrido filtraciones similares en el pasado, lo que muestra una tendencia creciente: los propios cibercriminales no están a salvo de ser atacados y expuestos.

NOTICIA COMPLETA

https://devel.group/blog/lockbit-sufre-filtracion-se-exponen-mensajes-de-negociacion-y-contrasenas-de-afiliados/

CONTACTOS DE SOPORTE

Correo electrónico: soporte@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group/