Estado de Internet
Volumen 09 | Número 04

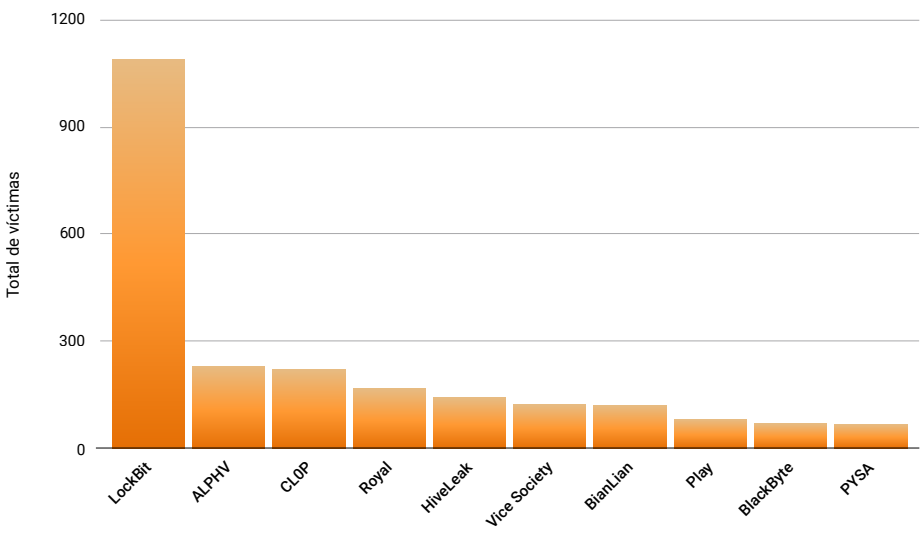
El ransomware en movimiento:

evolución de las técnicas de explotación y la búsqueda activa de día cero

Los grupos de ransomware están en movimiento y utilizan métodos de victimización, como el abuso de vulnerabilidades de día cero y de primer día, así como varios esquemas de extorsión para maximizar sus daños a las empresas.

LockBit controla el panorama del ransomware y está detrás del 39 % de las empresas víctimas

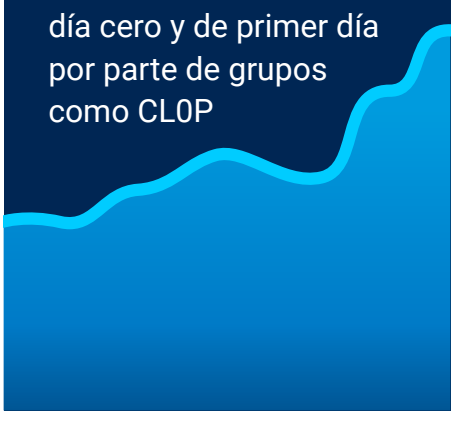
Volumen de víctimas de grupos de ransomware
Del 1 de octubre de 2021 al 31 de mayo de 2023



El éxito de LockBit se puede atribuir a las mejoras constantes introducidas en su software. Sin embargo, CL0P está ganando terreno y se está labrando un nombre gracias a un creciente abuso de las vulnerabilidades de día cero en el software de transferencia de archivos.

143 % ↑

Aumento del número de víctimas de ransomware debido al abuso activo de vulnerabilidades de día cero y de primer día por parte de grupos como CL0P



Las víctimas de diferentes grupos de ransomware tienen casi seis veces más probabilidades de sufrir otro ataque durante los primeros tres meses

77 %

Aumento del número de víctimas de ransomware en Europa, Oriente Medio y África (EMEA)

204 %

Aumento del número de víctimas de ransomware en Asia-Pacífico y Japón (APJ)

¿Cómo logran los atacantes optimizar sus tácticas de extorsión?

Acceso inicial
(Spear) phishing, vulnerabilidades de día cero y de primer día, abuso de credenciales

Movimiento lateral
Difusión por la red para lograr el mayor impacto y el mayor daño posibles

Exfiltración
Búsqueda y robo de datos valiosos: se está convirtiendo en uno de los principales métodos de extorsión

Cifrado
Cifrado eficaz y seguro para evitar la recuperación e interrumpir las operaciones

Petición de rescate
Las víctimas pagan el rescate; de lo contrario, los atacantes publican sus datos confidenciales en sitios de filtración

Los grupos de ransomware exploran las vulnerabilidades que pueden conducirles de manera directa al robo de datos

En los últimos meses, algunos autores de ataques de ransomware solo han utilizado los datos filtrados con fines extorsionadores

Ataques DDoS
Ataques DDoS para interrumpir las operaciones, que sirven como táctica de extorsión adicional

Intimidación y acoso
Los atacantes llaman o envían correos electrónicos a los clientes o partners de la víctima para ejercer más presión

Presión adicional para obligar a las víctimas a pagar un rescate

Para obtener más información sobre las tendencias en ransomware, el cambio en las técnicas de ataque y las estrategias de mitigación, lea nuestro informe completo.

Descargar el informe completo