STORMSHIELD

Informe de amenazas

Stormshield Endpoint Security Evolution

Su **empresa** Con Stormshield Endpoint Security Evolution
está protegida frente al ransomware

LockBit 2.0

EXFILTRACIÓN Y CIFRADO DE DATOS EN LAS MÁQUINAS INFECTADAS

LOCKBIT 2.0

LockBit es un grupo de ciberatacantes que opera bajo un modelo de Ransomware-as-a-Service (RaaS), como un producto listo para funcionar.

LockBit ofrece su plataforma de ransomware a otras entidades o particulares que la utilizan en un modelo de afiliación.

Se dice que LockBit es el grupo de ransomware más activo, con una impresionante lista de 203 víctimas solo en el tercer trimestre de 2021.

Acceso inicial
Ingeniería social para obtener privilegios elevados para cifrar archivos y exigir un rescate.

Objetivos
Empresas de cualquier tamaño sin una protección eficaz contra el ransomware. Especialmente en Estados Unidos, Canadá y Europa.

Riesgos
Cifrado de datos (impacto en la integridad), robo de información sensible (impacto en la confidencialidad), pérdida de productividad (impacto en la disponibilidad), etc.

Descubra nuestra solución de protección contra el ransomware

#1 Infección primaria

Fase 1

El ciberatacante **accede a la empresa objetivo** , ya sea comprando un exploit a otro grupo, o a través de su propia campaña de phishing.

Stormshield Endpoint Security Evolution ***le ofrece una protección eficaz contra diversas técnicas de ataque*** *(desbordamiento del búfer, malware empaquetado y vaciado de procesos).*

#2 Movimiento lateral y búsqueda de valor (expansión)

Fase 2

El ciberatacante **se infiltra en profundidad** en la red. A continuación, se desplaza **lateralmente** mientras busca identificar las máquinas que contienen información valiosa..

Stormshield Endpoint Security Evolution ***detecta y neutraliza las operaciones de descubrimiento*** *(por ejemplo, la ejecución de comandos para obtener direcciones IP, cuentas de usuario, servidores DNS, recursos compartidos de red, etc.).*

#3 Impacto

Fase 3

Exfiltración de datos hacia la infraestructura del grupo LockBit

Stormshield Endpoint Security Evolution ***bloquea el acceso a archivos confidenciales*** *como contraseñas, claves privadas, cámaras acorazadas digitales, credenciales, etc.*

Cifrado de archivos y publicación de una nota de rescate

Este paso no se realiza nunca. *Stormshield Endpoint Security Evolution neutraliza el malware que se comporta como ransomware, evitando el cifrado de datos.*

Destrucción de puntos de recuperación del servicio de instantáneas de volumen

Detecta y bloquea los intentos de manipulación *del servicio de instantáneas de volumen, impidiendo que el ransomware se ejecute.*