Ransomware: Muchas víctimas, muy pocas soluciones

El renacimiento de una lucrativa técnica de ataque

Los ataques de este tipo son conocidos desde hace mucho tiempo, y son ampliamente utilizados por su potencial lucrativo, así como por su capacidad de propagarse de forma rápida y devastadora. Actualmente estamos asistiendo a un aumento de este tipo de amenazas. Las cifras de la agencia francesa de ciberseguridad ANSSI muestran que el **número de ataques aumentó un 37% entre 2020 y 2021**. Del mismo modo, ha habido una tendencia a lo largo del tiempo hacia el ransomware como servicio (RaaS).

El ransomware es un malware que toma sus datos como rehenes.

La primera categoría: el clásico ransomware "Browlock" que **"cuelga" su navegador** o paraliza completamente su ordenador.

La segunda: el cripto-ransomware más dañino ("Cryptoware") **cifra los documentos de su ordenador**, haciéndolos ilegibles sin la clave de descifrado, en poder del hacker, que luego pide un rescate a cambio de esta clave.

En esta última categoría, más reciente, el malware **exfiltra datos y amenaza con revelarlos**, exigiendo un pago en bitcoin al propietario.

7.000 Euros

Coste medio de un ciberataque

Fuente: Usine Digitale

Las infraestructuras críticas como objetivo para el sabotaje sigue siendo una amenaza constante.

SEGÚN DATOS101 **LOS ATAQUES DE RANSOMWARE HAN AUMENTADO EN UN 253%**

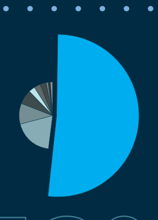
NOS AFECTA **A TODOS**

Particulares y empresas de todos los sectores y tamaños

Casi dos tercios de las víctimas de ransomware fueron víctimas de phishing (65%), muy por delante del robo de credenciales (39%), según un informe de Hiscox.

UNA FAMILIA ACTIVA Y DIVERSA

...
GPcode (.AG, .AK)
LOCKBIT 2.0
TROJ.RANSOM.A
Archiveus
Krotten
RSA4096
Cerber
Cryzip
MayArchive
Petya
CryptoLocker
TorrentLocker
Cryptowall
TeslaCrypt
Locky Ransomware
KeRanger
CTB-Locker
WinLock
Reveton
Winwebsec
...



El 52% de la víctimas son PYMEs

Afecta a todos los SO

KERANGER
EL PRIMER RANSOMWARE DIRIGIDO A MAC OS X (2016)

CTB-LOCKER
(VARIANTE)
DIRIGIDO A SERVIDORES WEB CORRIENDO EN GNU/LINUX

COMUNIDAD DE HACKERS
Las diversas campañas de ransomware ya no son llevadas a cabo por un solo grupo, sino **por varios grupos de hackers.**

LA CAMPAÑAS SON DIRIGIDAS
Un claro ejemplo: Locky
Locky se dirige a las empresas, y se propaga a través de campañas de correo electrónico malicioso (correos con facturas falsas, móviles gratuitos, etc.). **Su eficacia aumenta gracias a la personalización.**

CRYPTOWARE
Los efectos del ransomware son cada vez más difíciles de descifrar, lo que reduce las posibilidades de recuperar los datos sin pagar el rescate.

En muy poco tiempo, el tamaño y la fuerza de las llaves han aumentado considerablemente.

OBSERVACIÓN
Este tipo de ataque está aumentando constantemente (nuevos ataques o variantes)

CREE SU PROPIO RANSOMWARE SIN CONOCIMIENTOS TÉCNICOS

RANSOMWARE-AS-A-SERVICE

Ahora todo el mundo puede usarlo ***la generación de código malicioso está disponible para su uso*** *en el dark web.*

¿CÓMO FUNCIONA?

Con herramientas muy sencillas, paso a paso, los hackers pueden construir rápidamente su propio ransomware. Pagan al proveedor de este servicio el 25% de las transacciones llevadas a cabo en la campaña.

LOCKBIT 2.0

LockBit es un grupo cibercriminal que opera bajo un modelo de ransomware como servicio (RaaS).

El ransomware LockBit 2.0 sigue adaptándose y evolucionando en la actualidad, con ataques dirigidos en Estados Unidos, Canadá y Europa.

Las variantes más recientes han adoptado el modelo de doble extorsión: primero localizar y exfiltrar los datos, para luego cifrar los sistemas.

Paso 1
Personalización

1. El hacker elige **el método de ataque**
   - [x] Bloqueo
   - [x] Cifrado
   - [ ] Cuenta atrás
2. a continuación escribe **el mensaje**

   Message
   Sus datos personales están cifrados
   Su dispositivo acaba de ser bloqueado. Para recuperar sus datos, realice un pago de 200€ en la siguiente dirección:
3. a continuación proporciona **la información para el pago**

   bitcoin

PARA MÁS INFORMACIÓN

Descubra cómo el ataque LockBit amenaza la infraestructura **con la exfiltración y el cifrado de datos.**

Y la respuesta de Stormshield, con **el componente de protección anti-ransomware de su solución Endpoint Security Evolution.**

Paso 2
Creación

4. El servicio **prepara el malware** según las opciones seleccionadas
5. El código está **listo para ser usado**

   </>

Paso 3
Distribución

¡EMPIEZA EL ESPECTÁCULO!

El ransomware empleará múltiples métodos de propagación, como el uso de un "kit de explotación" para explotar vulnerabilidades.

...

RANSOMWARE YA NO SOLO SE DISTRIBUYE POR CORREO ELECTRÓNICO

- un sitio web malicioso o comprometido,
- una memoria USB,
- un software/aplicación instalado desde una fuente no segura,
- redes sociales (que facilitan la ingeniería social), etc.

GUSANO DE ORDENADOR
MALWARE EN EL CORREO ELECTRÓNICO
ATAQUE SIN FICHERO
HACKER
DISPOSITIVOS INFECTADOS
VULNERABILIDADES DE SOFTWARE
TROYANO

EXISTEN
SOLUCIONES FRENTE AL RANSOMWARE

STORMSHIELD
Endpoint Security Evolution

Esta protección proactiva evita que el malware se ejecute en su ordenador y/o que explote una vulnerabilidad (a través de un kit de explotación).

Stormshield Endpoint Security Evolution cuenta con una tecnología de identificación de malware proactiva que puede bloquear el ransomware incluso antes de que sea identificado por la comunidad de ciberseguridad.

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

Más información
www.stormshield.com/es/productos-y-servicios/productos/endpoint-protection/

ALGUNOS CONSEJOS INDISPENSABLES
para protegerse de los ransomware

Tango cuidado con los correos electrónicos sospechosos con archivos adjuntos

Haga copias de seguridad a menudo

Actualice sus aplicaciones, complementos y el sistema operativo