RANSOMWARE

El ransomware es un tipo de código malicioso que, tras infectar un equipo, secuestra su información para extorsionar a las víctimas, solicitando el pago de una suma de dinero para recuperar esos datos.

La información secuestrada es cifrada utilizando procedimientos criptográficos, que incluso pueden alterar los archivos de manera irrevocable. En el último tiempo, el ransomware ha cobrado una mayor relevancia en el panorama de la seguridad de la información y ha infectado tanto a usuarios como empresas.

¿Qué archivos pueden correr riesgo?

Las extensiones más perjudicadas son las de archivos de ofimática y multimedia:

- Procesadores de texto
- Hojas de cálculo
- Diapositivas
- Imágenes
- Correos electrónicos

¿CÓMO FUNCIONA?

1. **Explotación del sistema**
   Propagación por correo, pendrive u otros.
2. **Instalación**
   En la mayoría de los casos, tras abrir un archivo adjunto infectado en un correo electrónico.
3. **Identificación de archivos a cifrar**
4. **Cifrado de datos**
   Las últimas variantes de Filecoder usan RSA de 2048 bits.
5. **Notificación a usuario**
   Puede usar trucos como hacerse pasar por la policía para asustar a la víctima.
6. **Espera por pago**
   Los métodos aceptados van desde tarjetas prepagas hasta bitcoins o cupones de MoneyPak, Ukash y cashU, para otorgar anonimato.
7. **Entrega de las claves de descifrado**
   Nada asegura que el atacante devuelva el control del equipo infectado.

TIPOS DE RANSOMWARE

RANSOMWARE QUE CIFRA ARCHIVOS

Se comunica con el atacante a través de Tor mientras exige la transferencia de dinero.

Cryptolocker, CTB-Locker y **TorrentLocker** son los más resonantes. Estas variantes son detectadas por los productos de ESET bajo el nombre Win32/FileCoder.

RANSOMWARE DE PANTALLA DE BLOQUEO

No es posible usar el equipo hasta haber pagado el rescate.

Reveton es una de las familias más encontradas en entornos virtuales.

RANSOMWARE PARA DISPOSITIVOS MÓVILES

Las mismas amenazas llegan a nuevas plataformas.

En Android encontramos a **Simplocker**, en iOS a **WireLurker y**, además, nuevas variantes del **"Virus de la Policía"**.

2.500
Dólares le costó a una compañía argentina recuperar sus datos

15%
De las detecciones de CTB-Locker fueron en países hispanoparlantes

500.000
Es el número estimado de víctimas de Cryptolocker

1.44%
De las víctimas de TorrentLocker terminó pagando el rescate

¿CÓMO PROTEGERSE?

- Contar con una solución integral de seguridad que pueda detectar y bloquear amenazas conocidas de manera temprana.
- Actualizar aplicaciones y componentes del sistema operativo a su última versión, porque el ransomware aprovecha vulnerabilidades.
- Los correos electrónicos son un importante vector de propagación, por eso es importante: evitar divulgar la dirección, revisar el remitente, tener cuidado con ofertas tentadoras, verificar si se trata de un correo dirigido y filtrar los archivos ejecutables.
- Educar al personal para que no sucumba ante las técnicas de Ingeniería Social que se utilizan como puerta de entrada para la infección.
- Una adecuada política de backup asegurará la restitución de bases de datos y la continuidad del negocio incluso en los escenarios más sombríos.

¡NO PAGAR!

Si bien es posible que se restituya el acceso a los archivos una vez pagado el rescate, desalentamos esta práctica. Los criminales pueden aun así dejar malware en el equipo y ahora saben que la víctima está dispuesta a pagar dinero, por lo que podría ser blanco de otro ataque.

Además, hacer el pago motivaría a otros cibercriminales a continuar con este tipo de operaciones, y no hay garantía de que "cumplan su parte" del trato y realmente devuelvan los archivos.