MOORE ULA

Artículo

La Lucha contra el Ransomware

Por: Emmanuel De La Cruz,
Gerente de TI

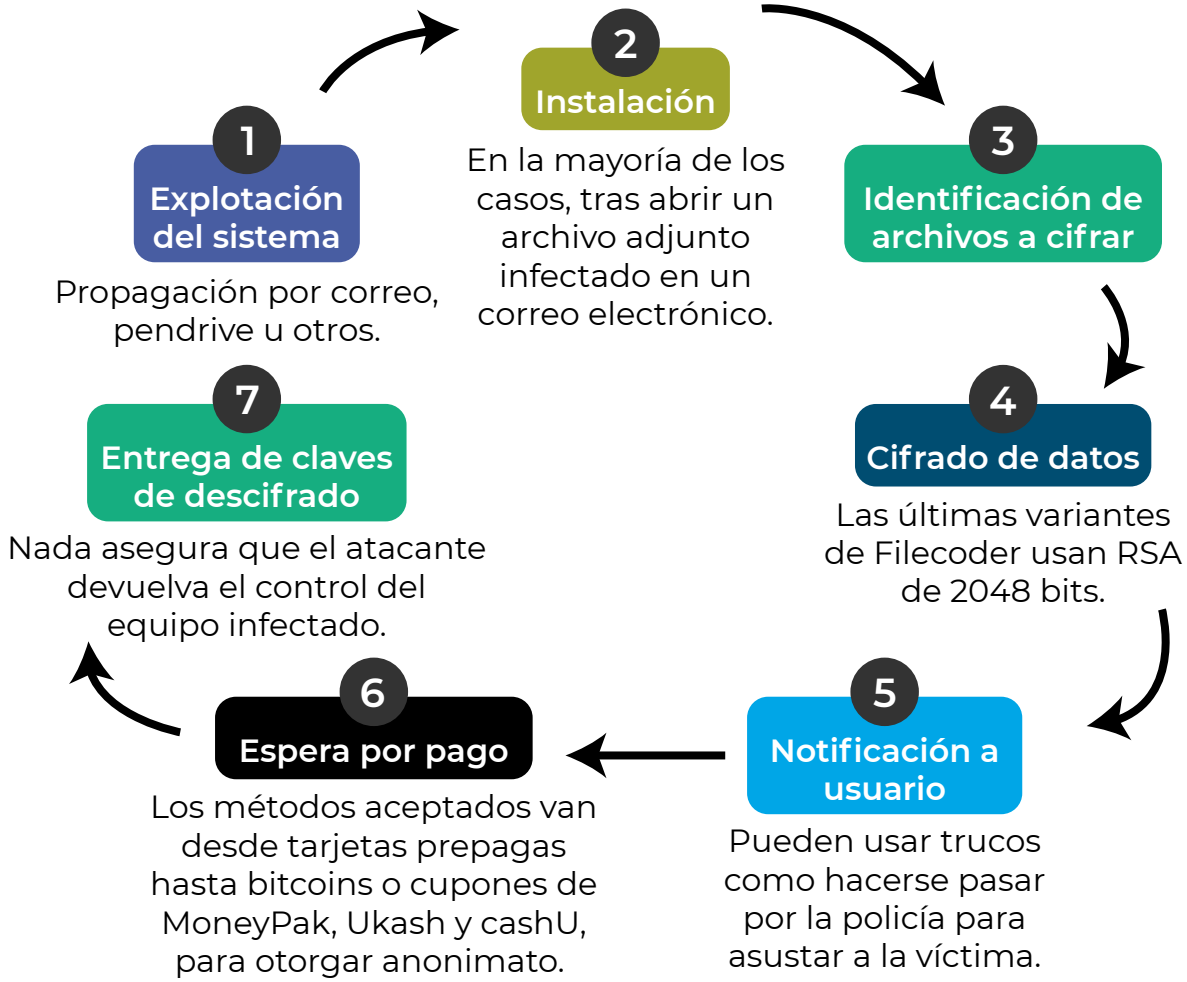
“LA LUCHA CONTRA EL RANSOMWARE”

Empecemos por definirlo, ¿qué es ransomware? El también conocido como “Secuestro de datos” en español, es un tipo de programa dañino que infecta tu computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema.

Un ransomware tiene la capacidad de bloquear la pantalla de una computadora o cifrar archivos importantes con una contraseña.

En los últimos años el ransomware se ha convertido en la principal amenaza de seguridad, tecnológicamente hablando.

¿Cómo funciona un ransomware?:



Tipos de Ransomware:

Los ransomware se pueden clasificar en 3 grandes grupos

1. Bloqueadores de computadoras.
2. Bloqueadores de Datos.
3. Ransomware para dispositivos móviles.

Bloqueadores de Computadoras: Este tipo de ransomware normalmente solo impide el acceso a la interfaz de la computadora y no afecta sus archivos o el sistema. Por lo tanto, tal vez pueda eliminar el ransomware y mantener todos sus archivos intactos.

Bloqueadores de Datos: Este es el tipo más común, conocido como criptoransomware, son potencialmente más peligrosos que los bloqueadores de computadora. Este escanea su computadora en busca de archivos valiosos y cambia su extensión, a una que el ordenador no sea capaz de reconocer. En definitiva, un secuestro de datos, incluso los ciberdelincuentes amenazan con borrar la clave, para que estos archivos se queden cifrados definitivamente.

Ransomware para dispositivos móviles: Las mismas amenazas, pero en las plataformas móviles, en Android Simplocker y en iOS Wirelurker, además de algunas variantes del ''Virus Policía''.

Los 10 ransomware más peligrosos de los últimos años son: Cryptolocker, WannaCry, SimpleLocker, TeslaCrypt, Bad Rabbit, Cerber, Ryuk, Petya y NotPetya, GrandCrab y SamSam.

CÓMO PROTEGERNOS

Los correos electrónicos son la principal fuente de propagación de ransomware, por lo que les dejo 3 consejos a la hora de trabajar con el correo corporativo:

1. No ejecutar los archivos adjuntos que provengan de remitentes desconocidos.
2. Evitar hacer clic en los enlaces incrustados en los correos que provienen de desconocidos o directamente no confiables.
3. Evitar acceso al correo electrónico desde equipos públicos.

Otras formas de protegernos:

Actualizaciones
Actualizar el Sistema Operativo y todas las aplicaciones a su última versión, esto porque los ransomware aprovechan las vulnerabilidades.

Ingeniería Social
Educar al personal para que no caiga ante las técnicas de ingeniería social, que utilizan los ransomware como puerta de entrada para la infección.

Antivirus y Backup
Contar con una solución integral de seguridad, que pueda detectar y bloquear amenazas de manera temprana, así como una eficiente política de backup.

Estos hechos cada vez son más frecuentes y les cuestan mucho dinero a las empresas, ya sea en pérdidas o en multas para recuperar su información.

Actualmente se estima que se produce un ataque de ransomware cada 11 segundos, con daños proyectados por un total de 20.000 millones de dólares para finales de 2020.

En caso de enfrentarse a un ataque de ransomware, las autoridades aconsejan no pagar el rescate. Algunos antivirus son capaces de detectar y eliminar el ransomware y recuperar sus archivos, esto puede que no funcione con algunos ransomware avanzados, y es por lo que recomendamos seguir las formas de protegernos mencionadas.

Autor:
Emmanuel De La Cruz
Gerente de TI
Moore ULA - República Dominicana.