# Seguridad Informática

EL Ramsonware

El ransomware es un programa de software malicioso que infecta tu computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema. Este tipo de malware es un sistema criminal para ganar dinero que se puede instalar a través de enlaces engañosos incluidos en un mensaje de correo electrónico, mensaje instantáneo o sitio web. El ransomware tiene la capacidad de bloquear la pantalla de una computadora o cifrar archivos importantes predeterminados con una contraseña.

Ejemplos de ransomware

El scareware es el tipo más simple de ransomware. En concreto, utiliza tácticas de amedrentamiento o intimidación para hacer que las víctimas paguen. Este tipo de malware puede adoptar la forma de un programa de software antivirus que muestra un mensaje en el que se informa que la computadora tiene varios problemas y el usuario debe efectuar un pago en línea para corregirlos.

El nivel de este tipo de ataque es variable. En ocasiones, abruma a los usuarios con alertas y mensajes emergentes interminables. En otros, la computadora deja de funcionar por completo. Existe otro tipo de ransomware que se hace pasar por una fuerza de seguridad y abre una página aparentemente perteneciente a la oficina de un organismo de seguridad. Aparece un mensaje que afirma que el usuario de la computadora fue atrapado realizando actividades ilegales en línea. A continuación, los archivos se bloquean con cifrados complejos difíciles de recuperar por los usuarios a menos que paguen un rescate.

Los ataques típicos suelen pedir montos de $100 a $200. Otros ataques son mucho más ambiciosos, especialmente si el atacante es consciente de que los datos que capturó pueden causar pérdidas financieras directas y

considerables a una empresa. Como resultado, los cibercriminales que orquestan estas estafas pueden ganar mucho dinero.

Independientemente de la situación, incluso si el usuario paga el rescate, no existe garantía de que volverá a acceder completamente a sus sistemas. Aunque algunos hackers indican a las víctimas que deben pagar a través de Bitcoin, MoneyPak u otros métodos en línea, los atacantes también pueden exigir información de tarjetas de crédito, lo que supone otra vía de pérdida financiera.

## Historia del ransomware

Los primeros casos se denunciaron en Rusia en 2005. Sin embargo, desde entonces, las estafas se han propagado a todo el mundo y nuevas variantes siguen sumando víctimas. En septiembre de 2013, apareció CryptoLocker, que dirige sus ataques a todas las versiones de Windows. Este ransomware ha logrado infectar cientos de miles de computadoras personales y sistemas empresariales. Las víctimas, de manera inconsciente, abrieron correos electrónicos procedentes supuestamente de servicios de soporte al cliente de FedEx, UPS, DHS y otras empresas. Después de activarse, se muestra un cronómetro en la pantalla que exige un pago promedio de $300 en un plazo de 72 horas. Algunas versiones afectaron a archivos locales y medios extraíbles. El Equipo de respuesta a emergencias informáticas de Estados Unidos advirtió que el malware era capaz de desplazarse de equipo en equipo y recomendó a los usuarios de las computadoras infectadas que eliminaran de inmediato los equipos infectados de sus redes.

Los expertos en seguridad de Kaspersky han podido descifrar los datos secuestrados, pero admiten que esto no siempre es posible si el cifrado es muy potente, como en el caso de CryptoLocker. Es fundamental que los usuarios privados y las empresas realicen copias de seguridad periódicas de sus computadoras para evitar la pérdida de datos importantes.

## Prevención y eliminación

Los usuarios de computadoras deben comprobar que sus firewalls estén activados, evitar visitar sitios web de dudosa reputación y tener cuidado cuando abran cualquier mensaje de correo electrónico sospechoso. Si eliges una solución de software antivirus de eficacia certificada provista por una empresa de prestigio, podrás proteger tu computadora contra las amenazas de ransomware más recientes.

## AIDS Info Disk: el primer ransomware de la historia

El primer ransomware que pasó a la historia fue el trojan AIDS, también conocido como PC Cybor. Fue programado en QuickBasic 3.0 en 1989 por el biólogo estadounidense Joseph Popp y distribuido a través de disquetes enviados a través de servicios postales. Popp envió 20.000 disquetes de 5,25 pulgadas a investigadores fuera de los Estados Unidos que estaban investigando el SIDA. “PC Cybor Corporation” fue el remitente ficticio de las cartas en las que llegaron los disquetes con “Información sobre el SIDA – Disquetes de introducción” escrito en los sobres. Los disquetes fueron acompañados por un folleto informativo que indica la necesidad de comprar una licencia para usar el software. Dentro de los disquetes habían dos tipos de software instalables: “INSTALL.EXE” y “AIDS.EXE”. El primero fue el malware real. Una vez que el malware entró en el PC reemplazando el archivo AUTOEXEC.BAT, el archivo de arranque del sistema Windows MS-DOS mostró un mensaje pidiéndole al usuario que renovara la licencia para continuar usando la computadora. Las impresoras conectadas imprimieron un documento invitando al usuario a enviar $189 dólares a un buzón en Panamá para obtener una licencia anual y obtener instrucciones sobre la recuperación de datos. La instalación del ransomware fue realizada por el 5% de los usuarios, lo que equivale a alrededor de 1.000 computadoras.

AIDS Info Disk Ransomware

Mensaje que aparece en el PC después de ser infectado por el AIDS ransomware. Fuente: Wikipedia.

El ransomware causó daños considerables en el campo científico. Una organización italiana para la investigación sobre el tratamiento del SIDA perdió alrededor de 10 años de resultados del estudio debido al

ransomware. Joseph Popp fue arrestado por el FBI en enero de 1990 después de ser visto por un oficial de seguridad en el aeropuerto Schiphol de Amsterdam. Esto evitó que enviara 2 millones de disquetes que contenían el ransomware. Fue liberado de la prisión prematuramente en 1991 debido a su inestable salud mental.

Actividad:

Investigar sobre dos virus ramsonware (tomando como ejemplo la información del virus anteriormente planteada). Describir cada uno en su modo de atacar, de lucrar y ubicarlo en el tiempo. Si es posible, describir el método de prevención para cada uno.

Recuerden que para la entrega la fecha límite es el 05/10 a mi Mail.

Sebasleclercq2@gmail.com

Espero que estén bien y les mando un saludo.