Nombres y Apellidos

Vladimir Antonio González Dotel

Matrícula

1098139

Materia

Algoritmos Maliciosos

Tema

Ensayo sobre Ransonware

Docente

Harold Marzán

Sección

01

Sábado 23 de julio, 2022

Santo Domingo, República Dominicana

Contenido

Introducción

Con la evolución de la computación y el uso popularizado de los computadores de uso personal, se han creado distintos tipos de malware con funciones de corte benigno o maligno. No obstante, uno de los tipos de software malicioso más utilizados para obtener beneficios por parte del infectado, es el ransomware. Este tipo de malware se caracteriza por encriptar los archivos del usuario en ubicaciones de almacenamiento del dispositivo infectado para, posteriormente, solicitar una remuneración para desbloquear los archivos.

Es una amenaza que afecta no solo a particulares, sino a organizaciones completas. Con el objetivo de ampliar los conocimientos teóricos sobre esta clase de malware, el informe a continuación describirá el ransomware a nivel de concepto, antecedentes puntuales, tipos de ataques, métodos de infección, objetivos de los autores de malware y cómo prevenir infecciones.

Desarrollo

Definición

El ransomware o software de secuestro es un tipo de malware que, en esencia, limita las funciones de un usuario en un dispositivo, principalmente, privándolo de acceder a sus archivos personales, exigiendo un pago o remuneración de otra naturaleza para liberar los archivos del usuario.

Las versiones más tempranas de ransomware aparecieron a finales de los años 80; el medio de pago era enviado por correo electrónico. Actualmente, el medio de pago más común suelen ser las criptomonedas, debido a que no dejan rastro en entidades bancarias, en consecuencia, no se revela información personal del atacante.

Métodos de infección del ransomware

- **Malspam**. El spam malicioso, o malspam, es un correo electrónico no solicitado que se utiliza para distribuir malware. El correo electrónico puede incluir archivos adjuntos con trampas, como archivos PDF o documentos de Word. También puede contener enlaces a sitios web maliciosos.

- **Malvertising**. El malvertising, o publicidad maliciosa, es el uso de la publicidad online para distribuir malware sin apenas interacción por parte del usuario. Mientras navegan por la web, incluso por sitios legítimos, los usuarios pueden ser dirigidos a servidores criminales sin ni siquiera hacer clic en un anuncio. Estos servidores catalogan los detalles de los ordenadores de las víctimas y su ubicación, y luego seleccionan el malware más adecuado para distribuirlo.

- **Spear phishing**. Un medio más dirigido a un ataque de ransomware es a través del spear phishing; un ejemplo de esto sería el envío de correos electrónicos a los empleados de una determinada empresa, alegando que el director general le pide que realice una importante encuesta a los empleados, o que el departamento de recursos humanos le exige que descargue y lea una nueva política.

- **Ingeniería social**. El malspam, malvertising y spear phishing pueden, y a menudo lo hacen, contener elementos de ingeniería social. Los actores de la amenaza pueden utilizar la ingeniería social para engañar a la gente para que abra los archivos adjuntos o haga clic en los enlaces aparentando ser legítimos, ya sea aparentando ser de una institución de confianza o de un amigo. Los ciberdelincuentes utilizan la ingeniería social en otros tipos de ataques de ransomware, como hacerse pasar por el FBI para asustar a los usuarios y hacerles pagar una suma de dinero para desbloquear sus archivos.

Tipos de ransomware

- **Scareware**. Este ransomware actúa de manera variada, pero intentando generar el miedo del usuario, indicándole que debe realizar acciones con el fin de librarse de una falsa amenaza. Cuando el usuario accede a lo que le indica el virus, descarga en esencia el malware y da paso al inicio del atraque.

- **Bloqueadores de pantalla**. Provoca que la víctima no pueda iniciar el sistema operativo con normalidad ni tenga acceso a su sistema de archivos. En ocasiones, el ransomware de bloqueo de pantalla solo afecta a funciones puntuales del ordenador en lugar de todas.

- **Ransomware de cifrado**. Es el tipo más común; bloquea los archivos del usuario en direcciones de memoria determinadas. Este malware elimina los archivos originales del usuario y los sustituye por una versión encriptada de estos. Para poder obtener el programa o la llave para desencriptar los archivos, el individuo detrás del virus solicita una compensación económica.

Objetivos a los que apuntan los autores de malware

Cuando se introdujo el malware, las víctimas iniciales eran personas regulares, no obstante, los cibercriminales incursionaron en otros medios más lucrativos para ellos, como son las empresas. Debido a los costos que tenía la información en los sistemas empresariales, los autores de malware centraron sus ataques hacia estos medios.

Geográficamente hablando, los ataques de ransomware están enfocados en mercados del oeste, incluyendo al Reino Unido, Estados Unidos y Canadá. Debido a sus intereses lucrativos, los autores de ransomware se enfocan en mercados con una alta densidad de ordenadores personales, donde los ciudadanos tengan una riqueza relativa. A lo sumo, también aumenta el ransomware en mercados emergentes, con crecimiento económico, de Asia y Suramérica.

¿Cómo prevenir el ransomware?

En primer lugar, lo mejor es prevenir el ransomware, no obstante, con la infección presente, debe saberse que, si accedemos al pago por el rescate de nuestros archivos secuestrados, no existe seguridad de que el atacante enviará la llave de acceso o el código fuente para desencriptar dichos archivos; existe la posibilidad de que el ransomware no sea reciente, y su autor no cumpla con su palabra por medios diversos (está sentenciado, muerto o no desea cooperar).

En consecuencia, lo ideal es prevenirlo mediante:

- Instalación de software antivirus.
- Realizar copias de seguridad de los archivos importantes.
- Si se es víctima de una infección, no pagar por el rescate.

En caso de ser infectado con ransomware, puede intentarse instalando y ejecutando software para desencriptado de archivos, de todos modos, esto no tiene por qué funcionar en todos los casos. Lo ideal es prevenir la infección de este tipo de malware, teniendo cuidado con los dispositivos que permitimos conectar en nuestro ordenador y siendo precavidos con las descargas que realizamos.

Conclusión

Con el desglose observado, hemos visto con mayor profundidad no solo la naturaleza del ransomware, sino de los métodos que utilizan los atacantes para encontrar nuevas víctimas. Si algo podemos recoger como positivo y mandatorio de este proceso comprensivo, es tener alta precaución con los archivos o unidades de almacenamiento externos a los que exponemos nuestro ordenador, pues, estas son una de las vías de infección más sencillas, y en consecuencia comunes, para infectar dispositivos. Sucede lo mismo con los programas de pago “gratuitos” que encontramos en internet; son gratuitos en costo, pero no se conoce con certeza si estos instaladores traen consigo malware de una determinada naturaleza.

Con esta perspectiva, se entiende mejor por qué se debe navegar con precaución en internet y mostrar un mínimo nivel de escepticismo cuando terceros inserten unidades de almacenamiento desconocidas en nuestros ordenadores; las verdaderas intenciones de tales individuos solo son de su propio conocimiento, y ya sea adrede o no, esto puede mortificar el funcionamiento de nuestro ordenador y dejarlo al merced del autor del virus y su conciencia y ética.

Referencias bibliográficas

Malwarebytes. (s. f.). *What is Ransomware? | How to Protect Against Ransomware*. https://www.malwarebytes.com/ransomware

Quanti. (2022, 25 enero). *La historia del ransomware: Historia, tipos de ransomware y futuros impactos*. Quanty. https://quanti.com.mx/articulos/la-historia-del-ransomware-historia-tipos-de-ransomware-y-futuros-impactos/