Nombres y Apellidos

Vladimir Antonio González Dotel

Matrícula

1098139

Materia

Algoritmos Maliciosos

Tema

Informe de proyecto final: ransomware

Docente

Harold Marzán

Sección

01

Sábado 16 de julio, 2022

Santo Domingo, República Dominicana

Contenido

Introducción

A lo largo de la evolución de la computación y el uso común 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.

A continuación, veremos el informe correspondiente al proyecto final de la asignatura ICS202 – Algoritmos Maliciosos, consistente en un ransomware creado exclusivamente con fines académicos llamado “What a good day, isn’t it?”. Grosso modo, está desarrollado en C#, utilizando la tecnología de Windows Forms para mostrar un mensaje al usuario.

Marco teórico

Concepto de ransomware

El malware de rescate, o ransomware, es un tipo de malware que impide a los usuarios acceder a su sistema de archivos personales y que, como medio de recuperación, exige un pago para poder acceder de nuevo a ellos.

Historia

La primera iteración registrada de virus ransomware fue creada por un estudiante de Harvard llamado Joseph L. Popp en el año 1989. Bautizado como AIDS Trojan, unos 20,000 discos infectados fueron distribuidos a los asistentes de la Conferencia Internacional sobre SIDA de la Organización Mundial de la Salud. El arma principal del Trojan fue criptografía simétrica; sin embargo, a las herramientas de cifrado no les tomó mucho tiempo para recuperar los nombres de los archivos, pero esta acción puso en marcha casi más de tres décadas de ataques de ransomware.

Entre 2005 y 2006, comenzamos a ver ataques de ransomware hacia puntos de datos dentro de otros países. Estos fueron creados por organizaciones criminales de Rusia, y alcanzaron a muchas víctimas dentro de ese país, al igual que en naciones vecinas como Bielorrusia, Ucrania y Kazajstán.

En 2006 (antes de que el término ransomware fuera usado) se descubrió una de sus variantes, llamada Troj_Cryzip A. En su mayor parte, esta variante afectó a las máquinas que utilizaban Windows 98, ME, NT, 2000, XP y Server 2003. Una vez descargada y ejecutada, identificar a los archivos con un cierto tipo de archivo, moviéndolos a una carpeta ZIP protegida con contraseña, habiendo eliminado a los originales. Para que la víctima recupere sus archivos, debía transferir cierto pago a una cuenta E-Gold (precursor del moderno Bitcoin, una pauta para la historia del ransomware).

En 2012, Trend Micro descubrió un nuevo tipo de variante de ransomware: TROJ_RANSOM.AQB. Incrementando el peligro y siendo más sofisticado, su método de infección fue reemplazar el registro de arranque principal (MBR) de Windows con un malicioso código único. Cuando la computadora arrancaba, el usuario vería un mensaje de rescate escrito en Ruso, demandando el pago. Tras pagar, las víctimas obtendrían un código que les permitiría restaurar sus computadoras a la normalidad.

Ahora, existen más formas de obtener rescates de la víctima o de la organización a la que ésta pertenece. Los atacantes pueden usar Vouchers, BitCoins, Paysafecard, MoneyPak, UKash, CashU y MoneXy para demandar el pago. Todo esto hace que sea más fácil recolectar el pago, y más fácil para que la víctima pueda realizarlo; sin embargo, al igual que con cualquier otro crimen monetario, mientras más víctimas paguen, más ataques seguiremos viendo. Por lo tanto, sin importar lo que usted decida hacer, evite pagar el rescate si puede.

Quanty, 25 de enero, 2022.

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.

Métodos de infección

Un virus informático puede alojarse en un computador de varias maneras. En el caso del ransomware, estas son las más populares:

- **Malspam**. Es un correo electrónico no solicitado que se utiliza para distribuir malware.

- **Malvertising**. Publicidad online para distribuir malware sin interacción del usuario

- **Spear phishing**. Email dirigido a un individuo dentro de una organización que parece provenir de una fuente confiable

- **Ingeniería social**. Los hackers la usan para asustar a los usuarios y hacerles pagar una suma de dinero para desbloquear sus archivos

Desarrollo

Metodología

Este malware requiere de varios procedimientos: localizar archivos del sistema y encriptar archivos. Para acceder, escribir y leer directorios del sistema operativo, se importa la librería Systerm.IO. Para encriptar los archivos, se hace uso de las funciones y utilidades que incluye la librería System.Security.Critography de C#. Esta permite codificación y decodificación de data y realizar operaciones como hashing, generación de números aleatorios y realizar autenticaciones.

El funcionamiento del ransomware a nivel detallado consiste en:

1. Indicar las rutas del sistema operativo cuyos archivos serán encriptados (en este caso: Escritorio, Documentos y Descargas).

2. Encriptar las carpetas y archivos contenidos en las ubicaciones identificadas en el paso anterior.

3. Mostrar una ventana indicando que el usuario ha sido víctima de un ataque de ransomware, indicándole que, para que autor del virus le envíe el software para desencriptar sus archivos, este debe transferirle un Bitcoin a una dirección especificada.

4. Escribir un archivo .txt el detalle sobre el total de archivos encriptados y el nombre de estos con su respectiva ubicación.

Proceso de encriptado

Comprendiendo el proceso general que lleva a cabo el malware, es preciso conocer con un grado de detalle superior el procedimiento para encriptar los archivos de las rutas, implementando las funciones de System.Security.Critography:

1. Llena un array de 32 bytes con una secuencia criptográfica fuerte de números aleatorios.

2. Crea un archivo con el mismo nombre del que se pretende encriptar con la extensión .jcrypt.

3. Convierte la contraseña definida como constante en el programa a un array de bits.

4. Aplica el algoritmo de encriptado simétrico de Rijndael, indicándole sus propiedades: KeySize (256), BlockSize (128) y el espaciado entre sus elementos (2).

5. Para el objeto de encriptado Rinjdael, le asigna una llave (usando el método Rfc2898DeriveBytes) y la encripta en dos ocasiones.

6. Crea un buffer de un mega (1 MB) para solo asignar esta cantidad de memoria y no el tamaño completo del archivo.

7. En un archivo .txt, se agregan iteradamente los archivos encriptados y se eliminan los originales de la ruta del ordenador que está siendo intervenida.

Conclusión

Con este proyecto, se ha puesto en evidencia el conocimiento teórico adquirido a lo largo de la asignatura de Algoritmos Maliciosos; en conjunto con la práctica, se ha creado un malware que realmente afecta al dispositivo infectado en caso de que este carezca de software protección como McAfee, Kaspersky, Windows Defender, entre otros conocidos.

Es un hecho que la generación Z (nacida después del 2000) fue la primera en tener presencia directa con ordenadores personales capaces de conectarse a la internet, por lo cual, se asume que, para este punto (2022), todos conocen lo que es un virus informático. No obstante, este acercamiento permitió ver con mayor cercanía esta clase de malware y observar cómo son sus algoritmos de operación.

Resulta inquietante ver cómo este es un "primer palazo" para obtener lucro personal con la informática de manera deshonesta, sin embargo, este tipo de prácticas son más fructíferas vistas desde el punto de vista del aprendizaje y conocimiento. Más que utilizar estos conocimientos para ciber-delinquir, son útiles para conocer cómo funcionan este tipo de virus (ransomware, en este caso), cómo prevenirlos y entender cuáles son los métodos de ataque por parte de los autores de dicho malware.

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

Kamaruzzaman, M. (2021, 11 diciembre). *Microservice Architecture: A brief overview and why you should use it in your next project*. Medium. https://towardsdatascience.com/microservice-architecture-a-brief-overview-and-why-you-should-use-it-in-your-next-project-a17b6e19adfd

Kamaruzzaman, M. (2022, 12 abril). *Microservice Architecture and its 10 Most Important Design Patterns*. Medium. https://towardsdatascience.com/microservice-architecture-and-its-10-most-important-design-patterns-824952d7fa41

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

Microsoft. (s. f.-a). *Rfc2898DeriveBytes Class (System.Security.Cryptography)*. Microsoft Docs. https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.rfc2898derivebytes?view=net-6.0

Microsoft. (s. f.-b). *RNGCryptoServiceProvider Class (System.Security.Cryptography)*. Microsoft Docs. https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.rngcryptoserviceprovider?view=net-6.0

Microsoft. (s. f.-c). *RNGCryptoServiceProvider.GetBytes Method (System.Security.Cryptography)*. Microsoft Docs. https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.rngcryptoserviceprovider.getbytes?view=net-6.0

Microsoft. (s. f.-d). *System.Security.Cryptography Namespace*. Microsoft Docs. https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography?view=net-6.0

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/

Tarek, A. (2022, 8 enero). *.NET C# Covariance & Contravariance - Ahmed Tarek - Medium | Level Up Coding*. Medium. https://levelup.gitconnected.com/covariance-and-contravariance-in-net-c-c2b8576b2155?gi=46e3d5589205