uc3m | Universidad Carlos III de Madrid

Máster Universitario en Ciberseguridad
2017/2018

Trabajo Fin de Máster

OpenRansim

Íñigo Serrano Salgado

Tutor
Juan Tapiador

Lugar y fecha de presentación prevista

Palabras clave: Ransomware, simulation, security, malware, encryption.
Resumen: En este documento, se va a presentar una herramienta de código abierto que sirve para comprobar la protección de un sistema informático frente a ataques de Ransomware.

Índice

Índice de figuras

Resumen

Hoy en día, uno de los ataques más comunes y eficaces que existen en el mundo de Internet, es el llamado Ransomware. Este tipo de ataques empezó a surgir en 1989 con AIDS Trojan. El Ransomware, se basa en secuestrar los datos de un sistema informático y pedir un rescate por estos. Técnicamente no requiere grandes conocimientos de seguridad para desarrollar un ejecutable, aunque, es cierto, que muchos emplean exploits para la fase de propagación. Lo cual lo convierte en uno de los ataques más efectivos y que suele obtener sus objetivos.

Es, por este motivo, que se ha decidido llevar a cabo este Trabajo de Fin de Máster, con el objetivo de aportar facilidades, para poder así evitar una infección en nuestros equipos y la consecuente remuneración para poder acceder de nuevo a nuestros archivos.

1. Introducción

El desarrollo del proyecto en cuestión, se centrará en la presentación de una nueva herramienta creada para facilitar la protección de sistemas informáticos frente a ataques de Ransomware. La idea en la que se basará este trabajo, surgió al descubrir algo similar en el mercado. Una aplicación llamada Ransim. Ésta, ejecuta una serie de escenarios, los más comunes, intentando asemejarse a un programa de Ransomware real.

El objetivo, es llevar a cabo los procedimientos necesarios para que, dicha herramienta, sea capaz de realizar la misma función que la previamente descubierta, aunque con una diferencia, y es que esta nueva herramienta presentaría un código abierto con posibilidad de ejecutar escenarios ad hoc. Por este motivo, el nombre elegido, ha sido OpenRansim. OpenRansim podrá encontrarse en la siguiente URL: Github. Al tratarse de una aplicación de código abierto, cualquier persona con un cierto interés en el tema, podrá colaborar en su desarrollo, lo cual, será clave y podrá favorecer al correcto funcionamiento de la misma.

2. Ransomware, historia y motivación del proyecto

2.1. Introducción

Como en muchas facetas de la vida real, la posibilidad de ganar dinero de forma fácil y a costa de los demás, ha llegado ya al mundo Online, como no podía ser de otro modo.

Con el paso de los años, han ido apareciendo muchos ciberdelincuentes o, incluso, mafias que están actuando a través de Internet. El secuestro de información, el ciberespionaje, el tráfico de cualquier dato sensible o la venta de piezas de malware, son cada vez más habituales en los tiempos que corren. Debido a esta serie de factores, es de vital importancia que exista, a disposición del usuario una ayuda como la presentada en este ensayo.

Figura 1: Imagen que aparece en un ordenador infectado

De todas las opciones que existen, los ataques de Ransomware, quizás sean los más rentables en términos económicos. Su único objetivo es secuestrar los datos de un ordenador para poder pedir un rescate por ellos. El uso de la criptografía y de las nuevas formas de pago, que garantizan el anonimato, son fundamentales para realizar un buen ataque.

2.2. Historia

El primer Ransomware que apareció, fue AIDS Trojan en 1989. Este malware escondía y cifraba los nombres de todos los ficheros que se encontrasen en el disco C. Esto hacia que el ordenador se quedase inservible, teniendo que pagar 189$ a una oficina de correos en Panamá.

En 2011 apareció el primer Trojan, que se aprovechaba de la moda de los pagos anónimos como medio de pago del rescate de los datos. Actualmente, el uso de medios de pago anónimos es algo muy común, aunque no siempre es fácil para el atacante recuperar el dinero.

Según las últimas tendencias de Ransomware, el uso de criptografía simétrica es la forma más empleada para hacer que los datos no puedan recuperarse, a menos que se tenga la contraseña. Pero esto no siempre ha sido así, hubo un tiempo en

el que la idea principal no era cifrar los datos de un ordenador, sino bloquearlo y hacer que su uso fuera limitado. Estos son los llamados "Lockers", que se valen de exploits y ciertas vulnerabilidades del sistema operativo anulando cualquier interacción con la máquina afectada.

Históricamente, este tipo de ataques ha estado siempre dirigido a ordenadores personales, por lo que los ordenadores con un sistema operativo de la familia Microsoft, eran más propensos a este tipo de ataque. Con la llegada de los Smartphone y la capacidad que tienen para ser ordenadores personales portátiles, en 2014 salió un Ransomware centrado en el sistema operativo Android.

2.3. Motivación del proyecto

Parece ser, que nos encontramos en un nuevo mundo, el mundo de la digitalización. En este nuevo mundo, uno de los elementos más valiosos, ha pasado a ser la disposición de datos y su control. Por este motivo, el Ransomware, se ha convertido, en la opción con más posibilidades de hacer negocio para los ciberdelincuentes.

A comienzos del año 2017, apenas se conocía la existencia de este tipo de ataques, hasta que saltó a la fama WannaCry. En Mayo del mismo año, se lanzó un ataque masivo que afectó a nivel mundial, incluyendo grandes empresas españolas. El 27 de Junio de 2017 salió a la luz otro Ransomware llamado NotPetya. Este último también se propagó a escala mundial afectando a Ucrania, Estados Unidos e Italia, principalmente.

Debido al notable aumento de este tipo de ataques, la existencia de una herramienta que pueda medir, de forma fiable, como de protegido se encuentra un ordenador frente a este tipo de amenazas, pasa a convertirse en un recurso vital para compañías de todo el mundo. OpenRansim, ha sido desarrollado, para que cualquier persona, sea capaz de cubrir sus necesidades de protección ante posibles ataques de Ransomware.

3. OpenRansim

3.1. Introducción

OpenRansim es una herramienta de línea de comando, desarrollada en Golang bajo la licencia GPL 3.0 de uso libre. La puesta en marcha, se ha llevado a cabo, mediante la utilización de 10 escenarios básicos, aunque su diseño, basado en módulos, permite la creación de escenarios nuevos, haciendo que sea personalizable.

3.2. Pre task & Post task

Para comprobar que un escenario se ha ejecutado correctamente, y poder así dictaminar si existe una posibilidad de infección o no, se han añadido al desarrollo de la herramienta, las llamadas: pre-task y post-task. Antes de empezar a ejecutar un escenario, la herramienta crea una carpeta especifica donde se van a realizar

las pruebas definidas por cada escenario. De esta forma se ejecuta la prueba bajo un entorno controlado sin que afecte a ningún archivo real.

Una vez ejecutado un escenario, es necesario comprobar si éste se ha completado correctamente o si, por el contrario, el sistema operativo ha interrumpido la ejecución, detectando y bloqueando, de esta manera, la posible acción maliciosa.

3.3. Escenarios

Para esta primera versión de OpenRansim se han llevado a cabo una serie de escenarios, que intentan simular las ejecuciones de varios tipos de Ransomware. Para ello, se han estudiado cuales son las formas de funcionar de las familias de Ransomware más representativas. Estos son los 10 escenarios:

- InsideCryptor – Cifra los datos y sobrescribe los archivos originales.
- LockyVariant – Simula una de las incontables variables del Ransomware Locky.
- Mover – Cifra los datos en una carpeta diferente a la original y elimina los ficheros originales.
- Replacer – Reemplaza el contenido de los archivos.
- Streamer – Cifra todos los datos y los agrupa en un único fichero.
- StrongCryptor – Cifra los datos y borra los ficheros originales de forma segura.
- StrongCryptorFast – Cifra los datos y borra los archivos originales.
- StrongCrytptorNet – Cifra los datos, borra los ficheros originales y simula una conexión HTTP.
- ThorVariant – Simula una de las incontables variables del Ransomware Thor.
- WeakCryptor – Utiliza un cifrado débil para cifrar los datos y elimina los archivos originales.

3.4. BYOS, Build Your Own Scenario

Aquí se habla de como te puedes crear tu propio escenario.

4. Conclusión

No siempre se devuelven los archivos después de pagar