Clasificando ransomwares para el desarrollo de un detector de código malicioso en ejecución

Iris N. Gastañaga, Fabián A. Gibellini, Pablo S. Frías, Analía L. Ruhl, Leonardo R. Cíceri, Germán N. Parisi, Federico J. Bertola, Paula B. Olmedo, Milagros N. Zea Cárdenas.

Laboratorio de Sistemas / Dpto. de Ingeniería en Sistemas de Información/
Universidad Tecnológica Nacional / Facultad Regional Córdoba
Cruz Roja S/N, 5016

irisg@ciec.com.ar, fgibellini@bbs.frc.utn.edu.ar, pablosfrias@gmail.com, analialorenaruhl@gmail.com, leocic@bbs.frc.utn.edu.ar, germannparisi@gmail.com, federicojbertola@gmail.com, paulabeatrizolmedo@gmail.com, milyzc@gmail.com.

Resumen

En los tiempos actuales, un tipo de software malicioso denominado ransomware, está afectando a muchos usuarios en todo el mundo. Si bien se ha escuchado más sobre aquellos ransomware que cifran archivos del sistema de la computadora infectada y luego piden una recompensa por la clave necesaria para descifrar los archivos, existen múltiples variedades de ransomwares. La recompensa que se pide, generalmente es monetaria y virtual, dentro de las cuales la más conocida es el Bitcoin.

En el presente documento se refuerza y amplía la categorización de ransomwares presentada por Sanggeun et al., buscando comprenderlos para seleccionar un conjunto de estas categorías que permitan definir parámetros e indicadores para desarrollar un detector de ransomwares en ejecución.

Palabras clave: Ransomwares, Cryptoransomwares, Cifrado, Algoritmos.

Contexto

Los resultados presentados en este documento forman parte del Proyecto Homologado “Sistema de Detección de Código malicioso - ransomware”, cuyo código es SIUTNCO0004991. El mismo se lleva a cabo en la UTN - FRC y cuyo objetivo general es “Desarrollar un sistema de detección del malware ransomware durante su ejecución en una computadora víctima y detener su avance antes de cifrar todos los archivos, basado en metodologías abiertas para identificar y analizar sus vulnerabilidades”.

Introducción

Desde finales de la década de los 80 encontramos métodos de ciber-extorsión, especialmente con la llegada del gusano Morris en el año 1988 [1], el primer malware autorreplicable, que afectó a miles de servidores. En el 2004 Young y Yung indicaron, que los futuros ataques, resultarían de una fuerte combinación entre criptografía y malware para atacar los sistemas. En ese año estaba emergiendo una nueva forma de malware en el ciberespacio, conocida como ransomware, que comenzaba a llamar la atención entre investigadores y practicantes de la seguridad informática de sistemas e imponía graves amenazas a la protección de los activos de información [2].

Un ransomware es una forma de software malicioso utilizado en ataques en los que, no se busca destruir irreversiblemente información, sino cifrarla y cobrar por el servicio de recuperación de los datos cifrados [3] [4].

La forma más común de pagar rescates de ataques con ransomwares es a través de criptomonedas, la más conocida y utilizada es el Bitcoin (BTC) [2]. La plataforma sobre la que se maneja el Bitcoin hace que sean

imposible rastrear quién la ha realizado [5]. Este modelo parece ser rentable para las organizaciones criminales que orquestan los ataques sacando provecho a las criptomonedas, asegurándose privacidad al momento de recibir la transferencia de los rescates.

Dentro de los ataques cibernéticos ocurridos antes del 2017 [6] [7] se mencionan el CryptXXX [8], Petya [9], Locky ransomware y Cerber.

En el caso de Cerber, este es conocido como un RaaS (Ransomware as a Service). Un RaaS es un ransomware, que posee parámetros configurables y es ofrecido en la llamada Deep Web a cambio de dinero. Entre los parámetros a configurar de Cerber se encuentra si el origen de la computadora víctima es atacable o no según una lista de países que no deben ser atacadas [10].

Otro ejemplo de RaaS es Philadelphia, al que se le podía configurar la nota que se mostraba en la pantalla de la víctima, detallando la cantidad de bitcoins pedidos por el "rescate" de los archivos y la cantidad de veces que tenía que confirmar la víctima el pago del rescate [11].

Durante el 2017 aparecieron nuevos y múltiples variaciones de los ransomwares ya existentes, entre los que se puede mencionar: Cryptoblock, Sage, WannaCry y NotPetya. Un ejemplo notable fue WannaCry, lanzado en mayo y que se expandió rápidamente a nivel mundial. Hasta el momento es el mayor ataque de ransomware mundialmente hablando y es por esto que consideramos el año 2017 como un punto de inflexion para los ataques de ransomwares. Aquellos equipos que no poseían el parche de actualización, brindado en marzo por Microsoft eran vulnerables a WannaCry, inclusive se crearon parches para versiones que se encontraban fuera de soporte, como Windows XP debido a la magnitude del ataque.

Para empezar a comprender este ransomware hay que empezar por entender las "piezas" que lo componen. WannaCry explota la vulnerabilidad CVE-2017-0144 (CVE, 2017) [10], haciendo uso del exploit EternalBlue, junto con la herramienta DoublePulsar. EternalBlue es un script creado por la National Security Agency (NSA) y liberado por un grupo conocido como Shadow Brokers que permite explotar la vulnerabilidad CVE-2017-0144 de los bloques de mensajes del servidor (SMBv1) [14] y ejecutar código remotamente [11]. DoublePulsar es una puerta trasera para Windows a través de la cual se puede subir archivos al sistema donde está instalado. Cuando Wannacry inicia su propagación a una máquina víctima no infectada, primero verifica que ésta tenga instalado DoublePulsar, si no se encuentra instalado utiliza el exploit EternalBlue para descargarlo e instalarlo. Una vez instalado DoublePulsar inicia la descarga del ransomware en la máquina víctima [12].

NotPetya es una variante del ya conocido ransomware Petya que copia el modus operandi de WannaCry explotando la vulnerabilidad EternalBlue. A pesar del potencial daño que podría haber causado, varios investigadores llegaron a la conclusión de que realmente no cifraba los archivos, como inicialmente se creía.

Según Sanggeun et al, se puede clasificar los ransomware según su funcionalidad [13]:

Scareware: alerta falsamente al usuario sobre la presencia de malware en el equipo, ofreciéndole la posibilidad de comprar un falso antivirus para la eliminación de dicho malware. Puede ser distribuido mediante correos electrónicos, ventanas emergentes o alertas internas cuando se navega por internet.

Locker-ransomware: bloquea el acceso al sistema operativo del equipo, de modo que el usuario no tiene posibilidad de usar la computadora, ni siquiera con sucesivos reinicios. Muestran una advertencia indicando que el usuario ha cometido un delito y debe abonar una multa para recuperar el normal funcionamiento del equipo.

Cryptoransomware: escanea el sistema de archivos y/o las unidades de red del equipo con el fin de cifrar el contenido (suele centrarse en las extensiones más comunes, como por ejemplo jpg, txt o mp3). Naturalmente, el acceso al mismo queda inhabilitado. Actualmente los ransomware de este tipo, exigen el pago en bitcoins.

corresponden a la clasificación dada por Sanggeun [13]:

- Scarewares.
- Locker-ransomwares.
- Cryptoransomwares: para esto utilizan algoritmos de cifrado simétrico, asimétrico o ambos. Existen casos en los que utilizan algoritmos de curva elíptica.

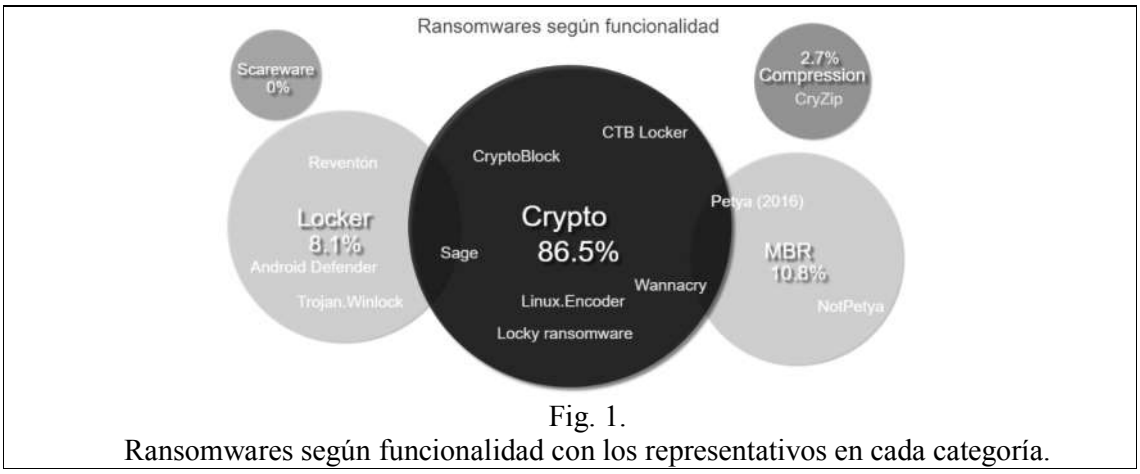

Fig. 1.
Ransomwares según funcionalidad con los representativos en cada categoría.

Partiendo de esta clasificación y estudiando los distintos ransomwares que aparecieron hasta el 2017, se definieron los siguientes objetivos:

- Verificar que la clasificación dada por Sanggeun contemple todos los ransomwares conocidos hasta el momento del estudio.
- Identificar los algoritmos de cifrados más utilizados por los cryptoransomware.
- Identificar una/s categoría predominante para enfocarse en la necesidad de detener estos ataques.

Líneas de Investigación, Desarrollo e Innovación

Este proyecto se inscribe dentro de la línea de Seguridad Informática, más precisamente dentro defensas contra código malicioso ransomware.

Resultados y Objetivos

Para la clasificación de ransomwares se tuvo en cuenta el modo de ataque y cómo funcionan, agrupándolos en familias o categorías. Las categorías son listadas a continuación, donde las tres primeras se

Borra los archivos originales.

- MBR ransomwares: consiguen permisos de administrador de modo que sea posible modificar el contenido de la Master Boot Record y así impedir el acceso al sistema. Pueden ser clasificado también como un caso específico de Locker-ransomware.
- Compression ransomwares: impide el acceso a los archivos de usuario, mediante la compresión de estos en ficheros cifrados y protegidos con contraseña. Borra los archivos originales.

Para arrivar a conclusions feacientes se realizó un análisis teórico a una muestra aleatoria de 41 ransomwares identificando a qué categoría pertenecen, su característica más distintiva, el año en que se los detectó, sistema operativo sobre el que se ejecuta y su modo de propagación. Se descartaron aquellos que no fueron considerados como ransomwares modernos y herramientas que sirven para la creación de ransomwares, entre estos One Half y Citadel. Quedando un total de 37 ransomwares.

Los resultados de la Fig. 1 expusieron cierta predominancia de los cryptoransomwares sobre el resto, además se puede observar que el porcentaje total

sobrepasa el 100%, esto se debe a que hay ransomwares que se los consideró incluidos en más de una categoría, como por ejemplo Petya del 2016 es tanto de tipo cryptoransomware y MBR.

El siguiente paso, fue clasificar los algoritmos de cifrado que utilizan los cryptoransomwares. De un total de 37 ransomwares, 32 resultaron cryptoransomwares.

En los resultados de la Tabla 1, se observa que los cryptoransomwares usan tanto algoritmos de cifrado simétrico como asimétrico y de hecho hay algunos que usan ambos tipos de cifrado. Es por esto que, sumando los totales, este valor da 39 ransomwares, superando el total de ransomwares analizados.

Dentro de los que utilizan un algoritmo asimétrico, el más usado es el RSA 2048, mientras que, el AES CBC es el más usado dentro de los algoritmos simétricos.

Algoritmos de de cifrado					
Cifrado asimétrico		Cifrado simétrico			
Algroritmos	Cantidad	Algoritmos	Cantidad	Tamaño de bloque	Cantidad
RSA 56	1	#XOR	1		
RSA 512	1	AES CBC	13	256	5
RSA 2048	5			128	5
RSA 4096	1	AES ECB	1	256	1
Curva elíptica	2			128	0
No idenficados	8	Salsa20	2		
TOTAL	18	No idenficados	4		
		TOTAL	21		

Tabla 1.
Clasificación de algoritmos de cifrado utilizados por cryptoransomwares.

Se inició este proyecto en el contexto del ataque cibernético mundial producido por el Wannacry, por lo cual aludir a la palabra "ransomware" era una asociación directa al cifrado masivo de datos.

Respecto a los objetivos planteado como partida, se revalidó la clasificación de Sanggeun [13] y se agregaron dos categorías, los ransomware de tipo MBR y de Compression. Esta clasificación no se la considera absoluta y está sujeta a cambios, tanto en categorías como subcategorías, dependiendo de los nuevos ransomwares que vayan surgiendo posteriormente.

En cuanto al segundo objetivo, los algoritmos asimétricos son los más utilizados porque son más difíciles de "romper", lo que genera mayor dificultad en los intentos para desencriptar los archivos cifrados por un ransomware.

Si bien actualmente los algoritmos más usados son los RSA, se ha comenzado a utilizar algoritmos de curva elíptica que son intrínsicamente más complejos. Otro punto importante respecto a los algoritmos, es que para lograr ransomwares más eficientes, es decir con una encriptación más rápida y al mismo tiempo difícil de romper, se están usando los dos tipos de algoritmo, el simétrico para cifrar los archivos y el asimétrico para cifrar la llave del algoritmo simétrico.

Los resultados ratifican la predominancia de los cryptoransomwares, lo que manifestó la necesidad de enfocarse en descubrir una forma de detectar cryptoransomwares mientras se ejecuten en una computadora víctima de manera que sirva como última barrera de defensa durante un ataque y se minimicen la cantidad de arhivos cifrados.

Si bien fue un estudio teórico, este ha cumplido un propósito mayor, dando una clara descripción de los ransomwares ya conocidos en el mundo cibernético y su evolución, clasificándolos y exponiendo la familia de ransomwares en la que los atacantes se han enfocado.

Basado en estos datos se puede comenzar a trabajar de manera detallada sobre aquellos Malwares de tipo ransomware que sean compatibles en este caso con algoritmos tales como AES (algoritmos simétricos) y RSA (algoritmos asimétricos) preferentemente RSA 2048.

Formación de Recursos Humanos

El grupo está compuesto, ademas de Director, Co-Director, investigadores de apoyo, profesores aspirantes a incorporarse a la carrera de investigador, técnicos de soporte, estudiantes investigadores de la carrera de Ingeniería en Sistemas de Información y becarios que forman parte del equipo. Este proyecto contribuirá a la formación y crecimiento de la carrera de los integrantes del mismo. En el caso de los estudiantes y algunos integrantes se iniciarán en la línea de seguridad informática.

Referencias

[1] Spafford E., "The Internet Worm Program: An Analysis". Purdue University. (1988).

[2] Young A., Yung M., "Malicious Cryptography Exposing Cryptovirology". Wiley Publishing, Inc. (2004).

[3] Moore C., "Detecting Ransomware with Honeypot techniques". Cybersecurity and Cyberforensics Conference, IEEE. (2016).

[4] Savage K., Coogan P., "The evolution of ransomware". Symantec. (2015).

[5] Mehmood S., "Enterprise Survival Guide for Ransomware Attacks". The SANS Institute. (2016).

[6] Richardson R., North N., "Ransomware: Evolution, Mitigation and Prevention". International Management Review. Vol. 13. No. 1. (2017).
http://scholarspress.us/journals/IMR/pdf/IMR-1-2017.%20pdf/IMR-v13n1art2.pdf

[7] Hampton N., Baig Z., "Ransomware: Emergence of the cyber-extortion menace". Edith Cowan University Australian Information Security Management Conference. (2015).
http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1179&context=ism

[8] Lupu E., Sgandurra D., Muñoz-González M., Mohsen R., "Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection". arXiv.org E-print Archive arXiv:1609.03020 [cs.CR]. (2016).

[9] MalwareLabs, "Petya – Taking Ransomware To The Low Leve". (2017).

[10] Scott J., Spaniel D., "Cerber & KeRanger: The Latest Examples of Weaponized Encryption". Institute for Critical Infrastructure Technology (ICIT). (2016).

[11] Proofpoint Staff, "Philadelphia Ransomware Brings Customization to Commodity Malware". (abril 2017).

[12] Fact Sheet: ETERNALBLUE exploit and DOUBLEPULSAR backdoor. Australian Cyber Security Centre. (mayo 2017).

[13] Sanggeun S., Bongjoon K., Sangjun L., "The effective Ransomware Prevention Technique Using Process Monitoring on Android Platform. Soongsil University. (2016).

[14] Microsoft. “Server Message Block Overview”. Documentación official: https://docs.microsoft.com/es-es/previous-versions/windows/server/hh831795(v=ws.11)