TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 17. No. 2, mayo-agosto, 2018, p.36- 41 ISSN 1729-3804

ENFRENTANDO LOS RANSOMWARES

Autor: Ing. Miguel Ángel Méndez Gil

Empresa Segurmatica

E-mail: miguel@segurmatica.cu

RESUMEN:

El Ransomware (del inglés *ransom* de rescate y *ware* de software) es un tipo de programa maligno que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. Algunos tipos de Ransomware cifran los archivos del Sistema Operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate. Los Ransomwares se hicieron populares en Rusia y su uso creció internacionalmente desde el mes de junio del 2013. En el presente trabajo se analizan las características fundamentales del funcionamiento de estos códigos malignos, así como la forma de prevenir una infección y la conducta a seguir cuando un sistema ha sido contaminado con un programa maligno del tipo Ransomware.

PALABRAS CLAVES*:* Ransomware, ransom, Locky, Zerber, Wanna.

ABSTRACT: A Ransomware (ransom from rescue and ware from software) represents a malignant program to restrict access on certain parts or files of the infected system. Ransomwares ask for a rescue in exchange to remove this restriction. Some types of Ransomware encrypt perating system files disabling devices and coercing the user to pay a demanded ransom. The Ransomware becames popular in Russia and its use grew internationally since June 2013. Current work analyzes main characteristics of functioning of these malignant codes, as well as the way to prevent infection, besides behavior to follow is discussed when a system has been contaminated with a malignant program of the Ransomware.

KeyWords: Ransomware, ransom, Locky, Zerber, Wanna.

1. INTRODUCCION

El Ransomware es un tipo de programa maligno que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. Algunos tipos de Ransomware cifran los archivos del Sistema Operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate. Los Ransomwares se hicieron populares en Rusia y su uso creció internacionalmente desde el mes de junio del 2013.

Por lo general un Ransomware infecta el Sistema Operativo por medio de un archivo descargado o explotando una vulnerabilidad del sistema. El Ransomware se inicia y cifra los archivos del usuario con una determinada clave, que sólo su creador conoce, y solicitará al usuario que la reclame a cambio de un pago.

El presente trabajo utiliza como base información relacionada sobre ataques de Ransomware consultados en informes de encuestas realizadas, informes de análisis, documentos y otros [1]. Se muestra un análisis del funcionamiento general de tres familias de Ransomwares que han adquirido un alto nivel de prevalecencia en los últimos meses, los conocidos

internacionalmente como Win32.Locky, Win32.Wanna y Win32.Zerber. Se analizarán las características fundamentales del funcionamiento de estos códigos malignos, así como la forma de prevenir una infección y la conducta a seguir cuando un sistema ha sido contaminado con un programa maligno del tipo Ransomware.

2. CARACTERÍSTICAS PRINCIPALES DE LA FAMILIA RANSOMWARE WIN32.LOCKY

EL tipo de Ransomware Win32.LOCKY puede impedir el uso de la PC o el acceso a datos personales, solicitando el pago de una cantidad de dinero a cambio de ello. Este código maligno utiliza un archivo infectado de Microsoft Office para descargar el Ransomware en su PC. Puede llegar a su PC como archivo adjunto de correo no deseado, generalmente como un archivo de Word (.doc), aunque también este Ransomware puede ser descargado por los programas malignos TrojanDownloader.JS.Nemucod, JS.Swabfex ó JS.Locky [2].

Información técnica

Este Ransomware se instala cuando se abre un archivo adjunto, generalmente un archivo de Word (.doc), desde un correo electrónico no deseado. Además de los documentos de Office, este código maligno también puede usar otros descargadores como archivos .JS y .BAT como archivos adjuntos en correos electrónicos no deseados. El archivo contiene una macro que descarga el Ransomware y lo ejecuta en su PC.

Existen variantes recientes que se firman digitalmente y llegan como complementos del navegador. Este programa maligno puede crear archivos en su PC, que incluyen:

- _Locky_recover_instructions.txt
- _Locky_recover_instructions.bmp
- % temp% \ svchost.exe - locky ransomware
- [ID] [identificador] .locky (archivos cifrados)

Este Ransomware puede encriptar los archivos en tu PC usando una clave pública. Los archivos se pueden descifrar con una clave privada almacenada en un servidor remoto. Mediante este Ransomware se encriptan los archivos con las siguientes extensiones:

Tabla 1. Extensiones de archivos que encripta el Ransomware Win32.LOCKY.

.123	.djvu	.mml	.ppsm	.tgz
.602	.DOC	.mov	.ppsx	.tif
.3dm	.docb	.mp3	.PPT	.tiff
.3ds	.docm	.mp4	.pptm	.txt
.3g2	.docx	.mpeg	.pptx	.uop
.3gp	.DOT	.mpg	.psd	.uot
.7z	.dotm	.ms11	.qcow2	.vb

Este Ransomware también renombra los ficheros infectados utilizando el siguiente formato:

- [ID][identificador].locky
- [ID][identificador].zepto

Ejemplos de esta operación constan por los siguientes:

- 8C05983C8B06FC65A0A9F44EDE9CA812.locky
- 8C05983C8B06FC65A1E1405B2324F5A5.locky

También cambia el fondo de escritorio, abre el fichero "_Locky_recover_instructions.txt" y muestra la misma imagen de rescate para indicarle que puede recuperar los archivos mediante un enlace personal que lo dirige a una página TOR que solicita el pago.

El código maligno accede a las siguientes URL:

- hxxp://vjwmpxseu.fr/main.php
- hxxp://jywdohhfkypg.de/main.php
- hxxp://blydeylrayu.it/main.php
- hxxp://obvpxgcohmpsou.it/main.php
- hxxp://cqvgwp.uk/main.php
- hxxp://tdxgp.eu/main.php
- hxxp://109.234.38.35/main.php

Como prevenir una infección por Win32.LOCKY

Este ataque de Ransomware puede evitarse ya que es portado por una macro y se recibe a través del correo electrónico. Configure su Centro de Confianza en los programas de Microsoft Office para "Deshabilitar todas las macros excepto las firmadas digitalmente", esto le permite controlar posibles macroinstalaciones en las máquinas de su red [3]. Tenga en cuenta que algunos programas maliciosos tratarán de ingresar a su sistema a través de macros utilizando el correo electrónico.

Las macros que deshabilitan administrativamente pueden ayudar a evitar que las macros cargadas de malware descarguen Ransomware u otras amenazas en su máquina o su red. Si el sistema ya ha sido víctima del Ransomware, no existe una respuesta única para todos los casos. No hay garantía de que pagar el rescate le otorgue acceso a sus archivos.

3. CARACTERÍSTICAS PRINCIPALES DE LA FAMILIA RANSOMWARE WIN32. WANNA

Este es uno de los Ransomware más peligrosos que existe en la actualidad. El ataque de este Ransonware muestra el resultado de ignorar las actualizaciones del Sistema Operativo. Los daños ocasionados por el Win32.Wanna se estiman en todo el mundo en $ 5 mil millones en el pasado año 2017[4].

Síntomas del programa maligno Win32.WANNA.zbu:

- Es capaz de desactivar el firewall y bloquear programas antivirus.
- Degrada significativamente el rendimiento de la computadora.
- Puede descargar otros programas malignos en su PC [5].
- Puede alterar su navegador y cambiar su configuración predeterminada.
- Puede conectarse con hackers y violar su información confidencial.

El código maligno Ransom.Win32.wanna.zbu se propaga principalmente a través de programas de descarga gratuita y otros archivos gratuitos. Los fabricantes de estos códigos malignos acostumbran a descargar cosas gratuitas en línea, incluidas aplicaciones, juegos, música gratis, películas y actualizaciones de software. Mediante la descarga de estas aplicaciones gratuitas se incrustan todo tipo de virus en sitios web para compartir archivos, y luego cuando se descarga el servicio gratuito, algún código malicioso como Ransom.win32.wanna.zbu pueden entrar en la PC. Además, esta amenaza también se difunde a través de correo electrónico no deseado y sitios web pornográficos. He aquí la importancia de tomar todas las precauciones necesarias cuando navegamos por Internet [6].

4. CARACTERÍSTICAS PRINCIPALES DE LA FAMILIA RANSOMWARE WIN32. ZERBER

Zerber es un software malicioso de tipo criptográfico que se introduce en el sistema y encripta varios archivos (.jpg, .doc, .raw, .avi etc.) posteriormente (cabe resaltar que Zerber agrega la extensión .cerber (.beef) a cada archivo encriptado)[7]. Tras realizarse la encriptación, Zerber exige a los usuarios pagar un rescate para desencriptar esos archivos. Se insta a los usuarios a pagar el rescate dentro del plazo dado (7 días); de lo contrario, se duplicará la suma del rescate.

Durante el proceso de encriptación, Zerber crea 3 tipos de archivo diferentes (#DECRYPT MY FILES#.txt, #DECRYPT MY FILES#.html, #DECRYPT MY FILES#.vbs) con instrucciones paso a paso para realizar el pago en cada carpeta que contenga archivos encriptados. En el mensaje, se asegura que los usuarios solo podrán desencriptar los archivos si usan un desencriptador desarrollado por los ciberdelincuentes llamado 'Zerber Decryptor' (Fig. 1).

El archivo #DECRYPT MY FILES#.vbs contiene un VBScript que, cuando se ejecuta, reproduce por los altavoces del equipo el mensaje “Your documents, databases and other important files have been encrypted!” (en español, "sus documentos, bases de datos y otros archivos importantes han sido encriptados"). Para descargar el desencriptador, el usuario tiene que pagar un rescate de 1,24 BitCoins (en la fecha del análisis, equivalían a 546.72 $). Si no se paga el rescate en 7 días, el importe se duplica hasta los 2,48 BTC. También se indica a los usuarios que solo pueden realizar el pago desde el navegador TOR y tras seguir las instrucciones proporcionadas en el sitio web. Por desgracia, en la fecha del análisis no había ninguna herramienta capaz de desencriptar los archivos afectados por Cerber. Por tanto, la única solución a este problema sería restaurar el sistema a partir de una copia de seguridad.

La nota de rescate asociada con el Ransomware ZERBER contendrá la siguiente información: ¡Sus documentos, fotos, bases de datos y otros archivos importantes han sido cifrados! Un ejemplo de mensaje ofrecido al usuario por este Ransomware se muestra en la Figura 1. Para descifrar los archivos, siga las instrucciones:

1. Descargue e instale el "Tor Browser" de https://www.torproject.org/
2. Ejecútalo
3. En el sitio web abierto "Tor Browser": [expurgado]
4. Siga las instrucciones en este sitio web

Figura 1: Mensaje del Ransomware Zerber luego de encriptar los documentos de la PC.

Este programa maligno se introduce en el sistema a través de correos electrónicos de spam, archivos adjuntos de correo electrónico, intercambio de ficheros de Redes, ejecutables maliciosos en diversos sitios de Internet, etc.

Después de que el usuario abre el archivo adjunto malicioso, ZERBER comienza a trabajar y descarga uno de los siguientes archivos maliciosos detectados en infosec:

- 1.exe con 3e4798c2b808b7dbad7f80b397dc97df
- 124.exe con 9c73dfc02bf01fc1da8efc349d23646b
- read.php?f = 0.dat con d958463bf73128114b59c3f9a65bfc19
- 4DUi5.exe con 794a556c1a98f70673a5ba3ed791382f
- user.php?f = 1.dat con 8abc023a9ebb7188881fabb747b4f68d

Después de esos archivos se han descargado en el ordenador del usuario, el virus Ransomware comienza a prepararse para cifrar archivos. Para hacer esto, el código malicioso realiza las siguientes actividades [8]:

- Suelta ficheros que se asemejan a archivos limpios.
- Lee las configuraciones de seguridad en Windows.
- Analiza en busca de nombres y procesos y crea nuevos procesos.
- Modifica wscript.exe para modificar archivos en% System32% y% de Microsoft Directorios%. Entre los archivos modificados son - rsaenh.dll, WScript.exe, WScript.exe.mui, sortdefault.nls, wshom.ocx, stdole2.tlb, KERNELBASE.dll.mui, msxml3.dll

Como actuar ante una infección por Win32.ZERBER

El Ransomware ZERBER es muy similar a otros troyanos Ransomware, incluyendo CryptoWall y TeslaCrypt. Estos ataques son casi idénticos, sólo difieren en pequeños detalles, y es muy probable que compartan grandes porciones de su código. Los usuarios de computadoras deben evitar pagar el rescate de Zerber Ransomware por dos razones:

1. Los usuarios de las computadoras no tienen ninguna garantía de que los estafadores responsables del ataque de Ransomware ZERBER cumplirán su parte del trato y proporcionarán el descifrador después de que se haya hecho el pago.
2. El pago del rescate de Zerber Ransomware permite a los creadores de estos programas malignos fraudulentos seguir llevando a cabo estos ataques y financiar el desarrollo de nuevos Ransomware.

5. RETO PARA LOS ANALISTAS DE PROGRAMAS MALIGNOS Y DESARROLLADORES DE PRODUCTOS DE SOFTWARE ANTIVIRUS

Las diferentes variantes de las familias de los programas malignos Win32.Locky, Win32.Wanna y Win32.Zerber representan un gran reto para los analistas de programas malignos y desarrolladores de productos de software antivirus. El análisis de códigos malignos es una labor imprescindible en un Laboratorio Antivirus. Su trabajo fundamental se basa en hacer ingeniería inversa del código ejecutable de estos programas.

La labor comienza con el análisis del código hexadecimal de los ficheros infectados con ayuda de herramientas de software desensambladores y debuggers, prestando especial atención a los ciclos de descifrado y el analista también debe ser capaz de reconocer las instrucciones “garbage” dentro del código maligno y debe detectar las trampas antidebuggers y antiemuladores utilizadas por los creadores de estos programas malignos y lograr traspasarlas con el objetivo de poder realizar un estudio detallado del código malicioso. Para llevar a cabo este estudio el analista debe dominar además, entre otros aspectos, las estructuras lógicas de los diferentes formatos de los archivos, así como las funciones internas de los Sistemas Operativos.

6. CONCLUSIONES

Después de algunos años de investigación y desarrollo acerca de este complejo tema podemos se puede asegurar que la detección de Ransomware sigue siendo una tarea difícil. Es necesario implementar un conjunto de mecanismos y herramientas de seguridad para poder alcanzar un nivel de protección aceptable [9].

El análisis de las famílias de programas malignos Win32.Locky, Win32.Wanna y Win32.Zerber es de gran interés por el uso de la técnica de Ransomware. En el presente artículo no se ha agotado toda la información técnica acerca de esta familia de códigos malignos, nos hemos enfocado básicamente en los principales mecanismos de su funcionamiento, así como en la forma de detectarlo y cómo prevenir a los usuarios finales de ser contaminados. Una forma de evitar esto último es tener siempre el antivirus actualizado y activada la Protección Permanente.

La Empresa de Consultoría y Seguridad Informática (Segurmática) ha desarrollado productos de software antivirus de diferentes tipos como identificadores, descontaminadores, preventores, detectores genéricos, recuperadores, filtros de correo electrónico y otros para diversos sistemas operativos, los cuales identifican y descontaminan estas familias de programas malignos de tipo Ransomware como Win32.Locky, Win32.Wanna y Win32.Zerber, así como los restantes programas malignos que han sido detectados en el país hasta la fecha [10].

La aparición de programas malignos que utilizan técnicas de alta complejidad es cada vez más frecuente. En la actualidad existen muchos de ellos que combinan varias de estas técnicas, los cuales representan un gran reto para los analistas de programas malignos y desarrolladores de productos de software antivirus. Estos desarrolladores deben tener en cuenta cada uno de los aspectos analizados en este artículo con el objetivo de ofrecer a los usuarios finales una respuesta rápida y eficiente que pueda satisfacer sus necesidades en el enfrentamiento diario a los ataques producidos por los códigos malignos [11].

4. REFERENCIAS BIBLIOGRÁFICAS

[1] R. S. Sajjan y V. R. Ghorpade, «Ransomware attacks: Radical menace for cloud computing», en 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2017, pp. 1640-1646.
[2] https://www.malwaretips.com/blogs/remove-ransom-win32-locky-a
[3] https://www.microsoft.com/malware-encyclopedia-description
[4] S. Saxena y H. K. Soni, «Strategies for Ransomware Removal and Prevention», en 2018 Fourth International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), 2018, pp. 1-4.
[5] http://www.4threatsremoval.com/es/como-eliminar-trojan-ransom-win32-wanna-m
[6] https://es.howtouninstall.guide/solucion-a-desinstalar-trojan-ransom-win32-wanna-m-de-windows-8
[7] http://www.4threatsremoval.com/es/como-eliminar-trojan-ransom-win32-zerber-ejma
[8] https://www.eliminarspyware.scanforvirus.org/deshacerse-de-trojan-ransom-win32-zerber-ejma-facilmente
[9] A. El-Kosairy y M. A. Azer, «Intrusion and ransomware detection system», en 2018 1st International Conference on Computer Applications Information Security (ICCAIS), 2018, pp. 1-7.
[10] http://www.segurmatica.cu
[11] Peter Szor, "*The Art* of Computer Virus Research and Defense".