Análisis del *malware CTB-Locker*

Ignacio Ballesteros González
w140062
05448027V

22 de octubre de 2017

Índice

Resumen

Primera práctica de la asignatura de *Seguridad de las Tecnologías de la Información*. Se realizará el estudio de una muestra del código malicioso *CTB-Locker*. Se ha elegido la opción *(a)* de estudio en base a las normas establecidas.

$$((5448027 * 485750) \ mod \ 331) = 73$$

1. Introducción

CTB-Locker es un malware que cifra los ficheros de la víctima y pide una compesación económica para recuperer los archivos cifrados. [2]

Código malicioso *CTB-Locker*

Tipo Toyano

Familia Secuestrador/Rescatador *(ramsonware)*

2. Ficha resumen

Denominación *CTB-Locker*

Origen/autor Tapkin. [1]

Destinatario Usuarios comunes. Empresas. Países de habla inglesa. [5]

Fecha de lazamiento Publicado en foros rusos el 10 de junio de 2014 [1]

Fecha de descubrimiento 4 de febrero de 2015 [1]

Tipo de código malicioso *Ramsonware*

Funcionamiento general

Modo de infección Campañas de Spam en fichero infectados. [1]

Modo de replicación No aplica.

Modo de propagación Campañas de *phising*.

Modo de ocultación No aplica.

Ejecución de la carga Ficheros infectados.

Tiempo de vulnerabilidad relacionada

Las infecciones se han producido en periodo que abarca desde finales de enero de 2015 a mediados de febrero de 2015. [3]

Modo de desinfección

La compañía F-Secure ha incluido el mecanismo de desinfección en su herramienta general.

Ejemplo de ataque donde se ha empleado

Ver Figura 1 y 2

Medidas de seguridad tomadas tras su descubrimiento

1. Uso de herramientas de detección del *malware*.
2. Educación en la prevención de campañas de *phising*.

Resto de miembros de su familia

Asociado a *CTB-Locker* Kaspersky designa a la familia de *malware* como *Trojan-Ransom.Win32.Onion*.

A veces se le conoce también como *Dalexis* [3]

Relacionado con la familia *Cryptolocker* [2]

Por otro lado, se han creado imitaciones del *malware* como *Poliglot* [4, p. 11]

Otra información relevante

CTB-Locker comprimía los archivos con una herramienta propia antes de cifrarlos. [1]

Figura 1: Ejemplo de correo de Spam con infección

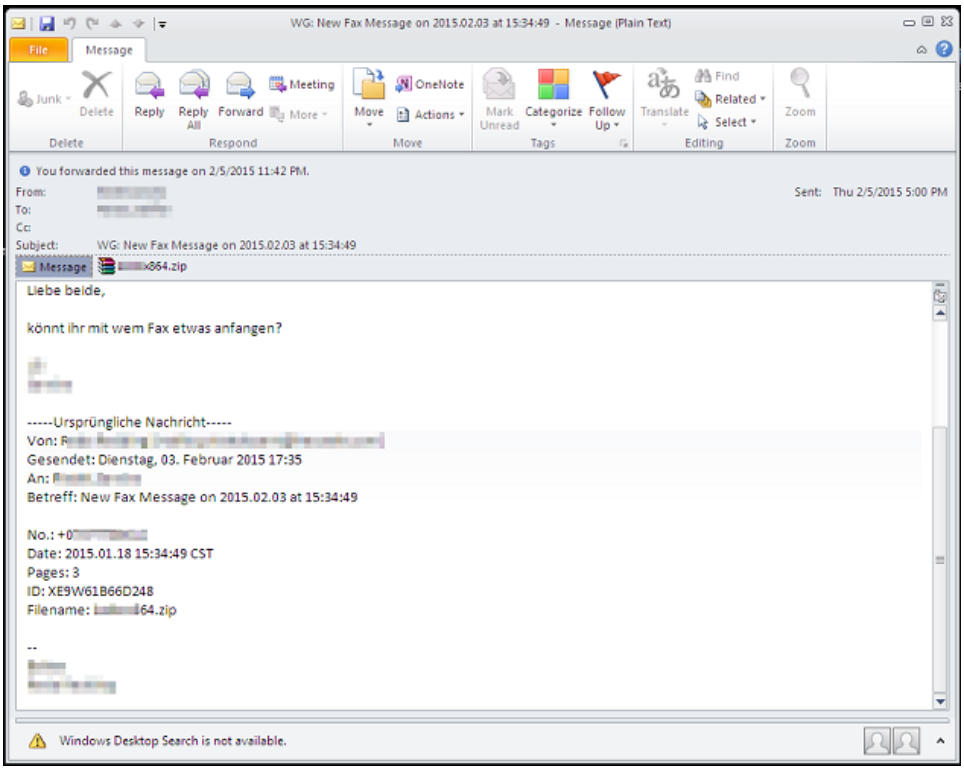

Figura 2: Pantalla una vez están los archivos cifrados.

3. Conclusiones

El *malware CTB-Locker* tuvo una fugaz aparición enmarcada en la ola de ramsonware de 2015. Cotenía mecanismos novedosos para el cifrado de los ficheros y a su vez la calidad de desarrollo era elevada.

Referencias

[1] CheckPoint. Malware analysis ctb locker, 2015. https://blog.checkpoint.com/2015/02/19/malware-analysis-ctb-locker/.

[2] F-Secure. Ctb-locker threat description. Technical report, F-Secure, 2014.

[3] F-Secure. Ctb-locker infections on the rise. Technical report, F-Secure, 2015.

[4] Kaspersky. Historia del año: la revolución del ramsonware, 2016.

[5] Sophos. The current state of ramsonware, ctb-locker, 2015. https://news.sophos.com/en-us/2015/12/31/the-current-state-of-ransomware-ctb-locker/.