CryptoLocker Ransomware

secureworks.com/research/cryptolocker-ransomware

Keith Jarvis

Wednesday, December 18, 2013 *By: Keith Jarvis*

Background

In mid-September 2013, the SecureWorks® CTU™ security intelligence research team, a thought leader in IT Security services, observed a new ransomware malware family called CryptoLocker. Ransomware malware such as Reveton, Urausy, Tobfy, and Kovter has cost consumers considerable time and money over the past several years. Ransomware prevents victims from using their computer normally (e.g., by locking the screen) and uses social engineering to convince victims that failing to follow the malware authors' instructions will lead to real-world consequences. These consequences, such as owing a fine or facing arrest and prosecution, are presented as being the result of a fabricated indiscretion like pirating music or downloading illegal pornography. Victims of these traditional forms of ransomware could ignore the demands and use security software to unlock the system and remove the offending malware. CryptoLocker changes this dynamic by aggressively encrypting files on the victim's system and returning control of the files to the victim only after the ransom is paid.

Infection vector

The earliest CryptoLocker samples appear to have been released on the Internet on September 5, 2013. Details about this initial distribution phase are unclear, but it appears the samples were downloaded from a compromised website located in the United States, either by a version of CryptoLocker that has not been analyzed as of this publication, or by a custom downloader created by the same authors.

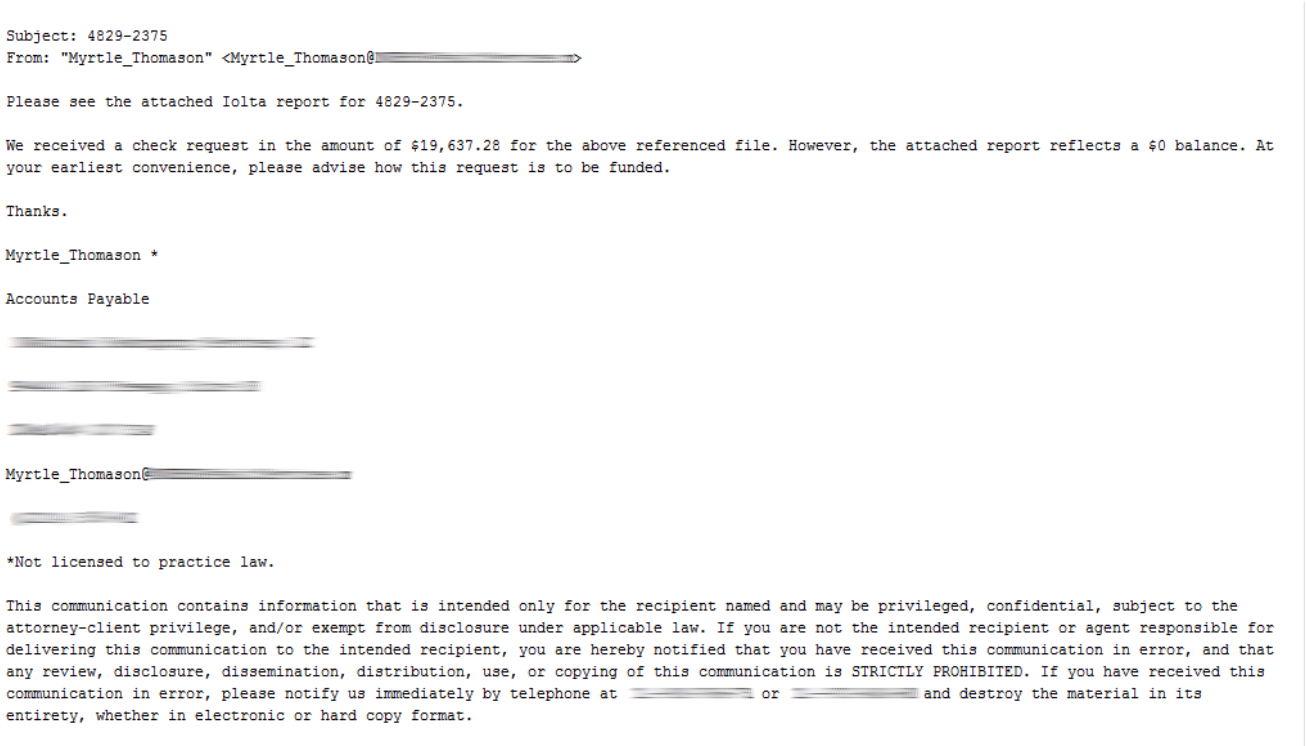
Early versions of CryptoLocker were distributed through spam emails targeting business professionals (as opposed to home Internet users). The lure was often a "consumer complaint" against the email recipient or their organization. Attached to these emails was a ZIP archive with a random alphabetical filename containing 13 to 17 characters. Only the first character of the filename is capitalized. The archive contained a single executable with the same filename as the ZIP archive but with an EXE extension. Table 1 lists several examples observed by CTU researchers.

Compressed archive	Included executable file
Jcgnbunudberrr.zip	Jcgnbunudberrr.exe

Lmpjxmvheortt.zip	Lmpjxmvheortt.exe
Icmcobxksjghdlnnt.zip	Icmcobxksjghdlnnt.exe
Gfaiqhgtqakbxlbf.zip	Gfaiqhgtqakbxlbf.exe

Table 1. Filenames of email-delivered malware samples.

On October 7, 2013, CTU researchers observed CryptoLocker being distributed by the peer-to-peer (P2P) Gameover Zeus malware in a typical pay-per-installation arrangement. In this case, Gameover Zeus was distributed by the Cutwail spam botnet using lures consistent with previous malware distribution campaigns. Figure 1 shows a phishing email delivered by Cutwail on October 7, 2013. Attached to the message is a ZIP archive containing a small (approximately 20KB) executable using a document extension in the filename and displaying an Adobe Reader icon. This Upatre malware downloads and executes Gameover Zeus, which in turn downloads and installs other malware families including CryptoLocker.



Subject: 4829-2375
From: "Myrtle_Thomason" <Myrtle_Thomason@[redacted]>

Please see the attached Iolta report for 4829-2375.

We received a check request in the amount of $19,637.28 for the above referenced file. However, the attached report reflects a $0 balance. At your earliest convenience, please advise how this request is to be funded.

Thanks.

Myrtle_Thomason *

Accounts Payable

[redacted]

Myrtle_Thomason@[redacted]

[redacted]

*Not licensed to practice law.

This communication contains information that is intended only for the recipient named and may be privileged, confidential, subject to the attorney-client privilege, and/or exempt from disclosure under applicable law. If you are not the intended recipient or agent responsible for delivering this communication to the intended recipient, you are hereby notified that you have received this communication in error, and that any review, disclosure, dissemination, distribution, use, or copying of this communication is STRICTLY PROHIBITED. If you have received this communication in error, please notify us immediately by telephone at [redacted] or [redacted] and destroy the material in its entirety, whether in electronic or hard copy format.

Figure 1. Spam email containing the Upatre downloader. (Source: Dell SecureWorks)

As of this publication, Gameover Zeus remains the primary method of distributing CryptoLocker. In addition to being distributed by Cutwail, Gameover Zeus has also been distributed by the Blackhole and Magnitude exploit kits.

Execution and persistence

CryptoLocker hides its presence from victims until it has successfully contacted a command and control (C2) server and encrypted the files located on connected drives. Prior to these actions, the malware ensures that it remains running on infected systems and that it persists across reboots. When first executed, the malware creates a copy of itself in either %AppData% or %LocalAppData%. CryptoLocker then deletes the original executable file.

CryptoLocker then creates an "autorun" registry key:

```
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "CryptoLocker":<random>.exe
```

Some versions of CryptoLocker create an additional registry entry:

```
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce "*CryptoLocker":<random>.exe
```

The asterisk at the beginning of the key name ensures that the malware executes even if the system is restarted in "safe mode."

Additional configuration data is stored in the following registry key:

```
HKCU\SOFTWARE\CryptoLocker or HKCU\SOFTWARE\CryptoLocker_0388
```

The VersionInfo value stored within this key contains configuration data encoded with the XOR key 0x819C33AE. The PublicKey value contains the RSA public key received from the C2 server during the initial network connection.

The executable files in early CryptoLocker samples used a random filename formatted like a GUID:

```
{71257279-042B-371D-A1D3-FBF8D2FADFFA}.exe
```

However, the executable files in recent samples use the naming pattern shown in the second column of Table 1.

Network

Several early versions of CryptoLocker, thought to be part of a beta testing phase, included code to connect to 184.164.136.134. This IP address is located in a PhoenixNAP datacenter in Arizona, but it was likely under the administrative control of Jolly Works Hosting. As of this publication, this IP address is no longer active, and CryptoLocker samples released since mid-September no longer reference it.

The malware's network communications use an internal domain generation algorithm (DGA) that produces 1,000 potential C2 domain addresses per day. The domain names contain 12 to 15 alphabetical characters and are within one of seven possible top-level domains (TLDs): com, net, org, info, biz, ru, and co.uk. An error in the algorithm prevents it from using 'z' in a generated domain name. The threat actors never registered a domain under the 'co.uk' TLD, and Nominet, the official registrar for the 'uk' ccTLD, began to sinkhole all potential addresses under this domain on October 18, 2013. As a result, the threat actors cannot use 'co.uk' domain names.

The threat actors have also used static C2 servers embedded inside the malware. On October 17, a sample was distributed that first connected to inworkforallthen . com before cycling through the domains created by the DGA. Several days later, another sample was hard-coded to connect to ovenbdjnihhdlb . net prior to attempting other generated domains. Since that time, new samples frequently contain static addresses taken from the pool of domain names created by the DGA.

CryptoLocker cycles indefinitely until it connects to a C2 server via HTTP. After connecting to an attacker-controlled C2 server, CryptoLocker sends a phone-home message encrypted with an RSA public key embedded within the malware (see Figure 2). Only servers with the corresponding RSA private key can decrypt this message and successfully communicate with an infected system.

```
POST /home/ HTTP/1.1
Accept: */*
Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: 184.164.136.134
Content-Length: 192
Cache-Control: no-cache
Pragma: no-cache

[raw binary data]
```

Figure 2. CryptoLocker's initial phone-home traffic. (Source: Dell SecureWorks)

Analysis of the IP addresses used by the threat actors reveals several patterns of behavior. The first is that the threat actors use virtual private servers (VPS) located at different ISPs throughout the Russian Federation and in former Eastern bloc countries. The extended use of some of these hosts, such as 93.189.44.187, 81.177.170.166, and 95.211.8.39, suggests that they are located at providers that are indifferent to criminal activity on their networks or are complicit in its execution (such as so-called "bulletproof" hosting providers). The remaining servers appear to be used for several days before disappearing. The threat actors could be strategically using this pattern to remain a moving target, or some ISPs could be terminating their service.

A complete list of network indicators is included in the Threat indicators section.

Encryption

Instead of using a custom cryptographic implementation like many other malware families, CryptoLocker uses strong third-party certified cryptography offered by Microsoft's CryptoAPI. By using a sound implementation and following best practices, the malware authors have created a robust program that is difficult to circumvent. The malware uses the "Microsoft Enhanced RSA and AES Cryptographic Provider" (MS_ENH_RSA_AES_PROV) to create keys and to encrypt data with the RSA (CALG_RSA_KEYX) and AES (CALG_AES_256) algorithms.

The encryption process begins after CryptoLocker has established its presence on the system and successfully located, connected to, and communicated with an attacker-controlled C2 server. This communication provides the malware with the threat actors' RSA public key, which is used throughout the encryption process.

The malware begins the encryption process by using the GetLogicalDrives() API call to enumerate the disks on the system that have been assigned a drive letter (e.g., C:). In early CryptoLocker samples, the GetDriveType() API call then determines if the drives are local fixed disks or network drives (DRIVE_FIXED and DRIVE_REMOTE, respectively). Only those two types of drives are selected for file encryption in early samples. Samples since late September also select removable drives (DRIVE_REMOVABLE), which can include USB thumb drives and external hard disks.

After selecting a list of disks to attack, the malware lists all files on those disks that match the 72 file patterns shown in Table 2. Over time, the threat actors adjusted which types of files are selected for encryption; for example, PDF files were not encrypted in very early samples but were added in mid-September. As a result, the list in Table 2 is subject to change.

*.odt	*.ods	*.odp	*.odm	*.odb	*.doc	*.docx	*.docm
*.wps	*.xls	*.xlsx	*.xlsm	*.xlsb	*.xlk	*.ppt	*.pptx
*.pptm	*.mdb	*.accdb	*.pst	*.dwg	*.dxf	*.dxg	*.wpd
*.rtf	*.wb2	*.mdf	*.dbf	*.psd	*.pdd	*.eps	*.ai
*.indd	*.cdr	????????.jpg	????????.jpe	img_*.jpg	*.dng	*.3fr	*.arw
*.srf	*.sr2	*.bay	*.crw	*.cr2	*.dcr	*.kdc	*.erf
*.mef	*.mrw	*.nef	*.nrw	*.orf	*.raf	*.raw	*.rwl
*.rw2	*.r3d	*.ptx	*.pef	*.srw	*.x3f	*.der	*.cer
*.crt	*.pem	*.pfx	*.p12	*.p7b	*.p7c	*.pdf	*.odc

Table 2. File patterns selected for encryption.

Each file is encrypted with a unique AES key, which in turn is encrypted with the RSA public key received from the C2 server. The encrypted key, a small amount of metadata, and the encrypted file contents are then written back to disk, replacing the original file. Encrypted files can only be recovered by obtaining the RSA private key held exclusively by the threat actors.

As a form of bookkeeping, the malware stores the location of every encrypted file in the Files subkey of the HKCU\SOFTWARE\CryptoLocker (or CryptoLocker_0388) registry key (see Figure 3).

Имя	Тип	Значение
(По умолчанию)	REG_SZ	(значение не присвоено)
C:?Documents and Settings?Default User?Шаблоны?excel.xls	REG_DWORD	0x0188537c (25711484)
C:?Documents and Settings?Default User?Шаблоны?excel4.xls	REG_DWORD	0x0188537c (25711484)
C:?Documents and Settings?Default User?Шаблоны?powerpnt.ppt	REG_DWORD	0x0188538c (25711500)
C:?Documents and Settings?Default User?Шаблоны?quattro.wb2	REG_DWORD	0x0188538c (25711500)
C:?Documents and Settings?Default User?Шаблоны?winword.doc	REG_DWORD	0x0188539b (25711515)
C:?Documents and Settings?Default User?Шаблоны?winword2.doc	REG_DWORD	0x0188539b (25711515)

Figure 3. List of encrypted files stored by CryptoLocker. (Source: Dell SecureWorks)

After finishing the file encryption process, CryptoLocker periodically rescans the system for new drives and files to encrypt.

The malware does not reveal its presence to the victim until all targeted files have been encrypted. The victim is presented with a splash screen containing instructions and an ominous countdown timer (see Figure 4).

Figure 4. Splashscreen presented to victims. (Source: Dell SecureWorks)

Payment

The ransom amount varied in very early samples (see Table 3), but settled at $300 USD or 2 BTC (Bitcoins) within the few weeks after CryptoLocker's introduction. Dramatic Bitcoin price inflation in the latter months of 2013 prompted the threat actors to reduce the ransom to 1 BTC, 0.5 BTC, and then again to 0.3 BTC, where it remains as of this publication.

Amount	Currency (abbreviation)
100	U.S. Dollar (USD)
100	Euro (EUR)
100	Australian Dollar (AUD)
200	Brazilian Real (BRL)
100	Canadian Dollar (CAD)
2000	Czech Koruna (CZK)
1000	Danish Krone (DKK)

100	British Pound Sterling (GBP)
1000	Mexican Peso (MXN)
1500	Norwegian Krone (NOK)
200	New Zealand Dollar (NZD)
500	Polish Zloty (PLN)
200	Romanian Leu (RON)
1500	Swedish Krona (SEK)

Table 3. Original ransom amounts in various denominations. (Source: Dell SecureWorks)

The threat actors have offered various payment methods to victims since the inception of CryptoLocker. The methods are all anonymous or pseudo-anonymous, making it difficult to track the origin and final destination of payments.

cashU

Figure 5. Payment options using the cashU service. (Source: Dell SecureWorks)

The description of cashU shown in Figure 5 is taken directly from the Wikipedia entry about the method:

cashU is a prepaid online and mobile payment method available in the Middle East and North Africa, a region with a large and young population with very limited access to credit cards. Because of this, cashU has become one of the most popular alternative payment option for young Arabic online gamers and e-commerce buyers.

Ukash

Figure 6. Payment options using the Ukash service. (Source: Dell SecureWorks)

The description of Ukash shown in Figure 6 is largely taken from a Facebook post about the product:

Ukash is electronic cash and e-commerce brand. Based on a prepaid system, Ukash allows users to purchase and then spend money online.

Money can be purchased from one of the reported 420,000 participating retail locations worldwide, or by using the company's website. This electronic money can then be used to pay online, or loaded on to a prepaid card or eWallet.

*You can **combine multiple values** of your Ukash into a single amount and have your new Ukash Code and value emailed to you if you want. You will need to register at Ukash.com, login and then go to the Manage Ukash area to use the Combine tool.*

Paysafecard

A screenshot of the Paysafecard dialog was not immediately available for this publication, but the description states:

Paysafecard is an electronic payment method for predominantly online shopping and is based on a pre-pay system. Paying with paysafecard does not require sharing sensitive bank account or credit card details. Using paysafecard is comparable to paying with cash in a shop and it is currently available in over 30 countries.

Paysafecard works by purchasing a PIN code printed on a card, and entering this code at webshops.

Paysafecard is available from many supermarkets, petrol stations, tobacconists and newsagents.

Bitcoin

Figure 7. Payment options using the Bitcoin service. (Source: Dell SecureWorks)

The description of Bitcoin shown in Figure 7 is copied almost verbatim from several online resources:

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

Green Dot MoneyPak

Figure 8. Payment options using the MoneyPak service. (Source: Dell SecureWorks)

The description of MoneyPak shown in Figure 8 is copied directly from the MoneyPak website:

MoneyPak is an easy and convenient way to send money to where you need it. The MoneyPak works as a 'cash top-up card'.

Where can I purchase a MoneyPak?

MoneyPak can be purchased at thousands of stores nationwide, including major retailers such as Walmart, Walgreens, CVS/pharmacy, Rite Aid, Kmart and Kroger. Click here to find a store near you.

How do I buy a MoneyPak at the store?

Pick up a MoneyPak from the Prepaid Product Section or Green Dot display and take it to the register. The cashier will collect your cash and load it onto the MoneyPak.

Current payment options

Although early versions of CryptoLocker included numerous payment options, the threat actors now only accept MoneyPak and Bitcoin. The Bitcoin option was originally marketed as the "most cheap option" [sic] for ransom payment based on the difference between the $300 USD ransom and the market rate of Bitcoins. From August to December 2013, the Bitcoin market experienced major volatility and dramatically increased in price, negating any monetary benefits for victims to choose this payment method.

The variety of payment options and currency choices in early CryptoLocker versions suggests the threat actors originally anticipated a global infection pattern. For reasons unknown to CTU researchers, the threat actors elected to focus exclusively on English-speaking countries and removed the payment options less popular in these countries.

Anecdotal reports from victims who elected to pay the ransom indicate that the CryptoLocker threat actors honor payments by instructing infected computers to decrypt files and uninstall the malware. Victims who submit payments are presented with the payment activation screen shown in Figure 9 until the threat actors validate the payment. During this payment validation phase, the malware connects to the C2 server every fifteen minutes to determine if the payment has been accepted. According to reports from victims, payments may be accepted within minutes or may take several weeks to process.

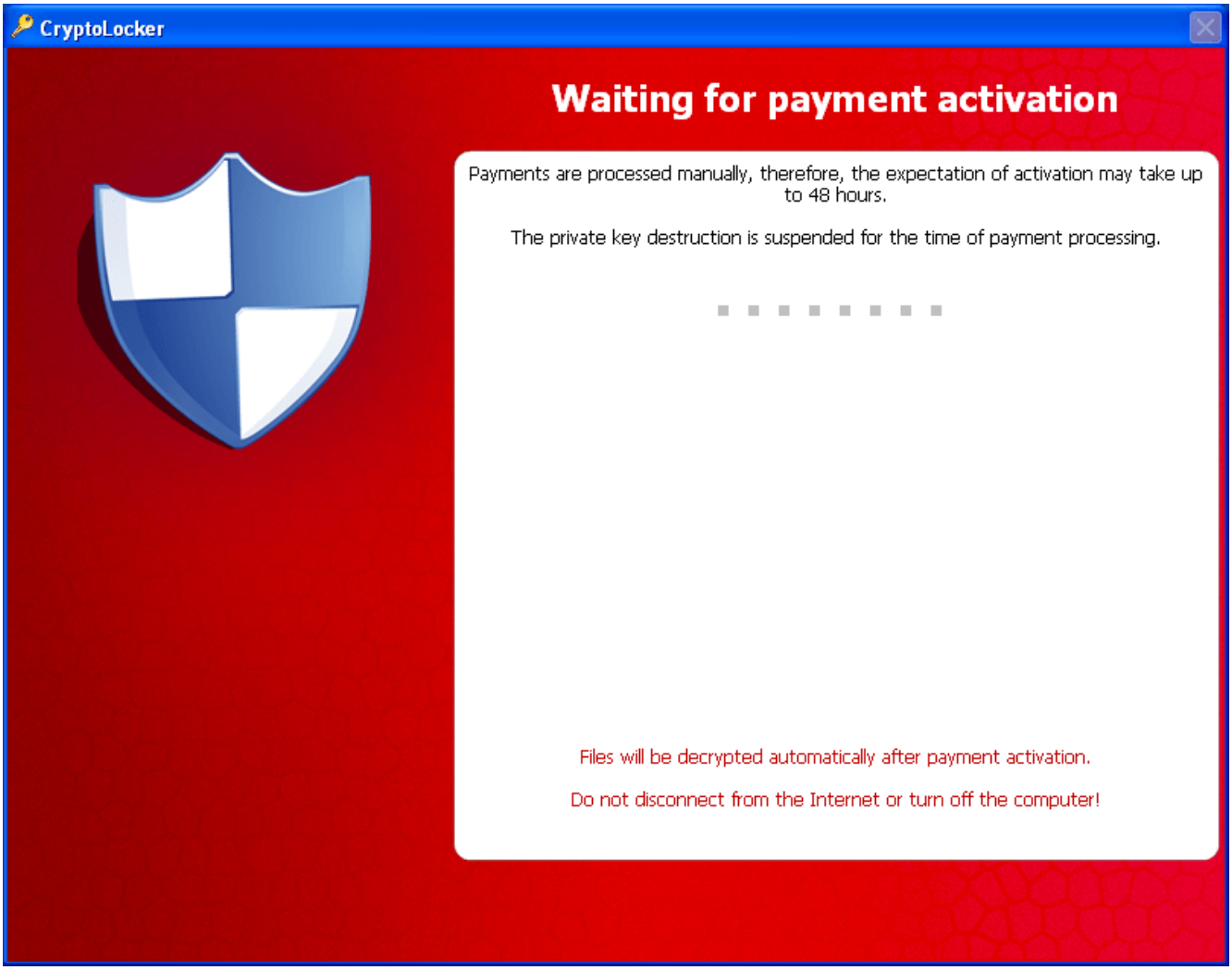


Figure 9. Payment activation screen. (Source: Dell SecureWorks)

Late payment

In early November 2013, the threat actors introduced the "CryptoLocker Decryption Service" (see Figure 10). This service gives victims who failed to pay the ransom before the timer expired a way to retrieve the encrypted files from their infected system.

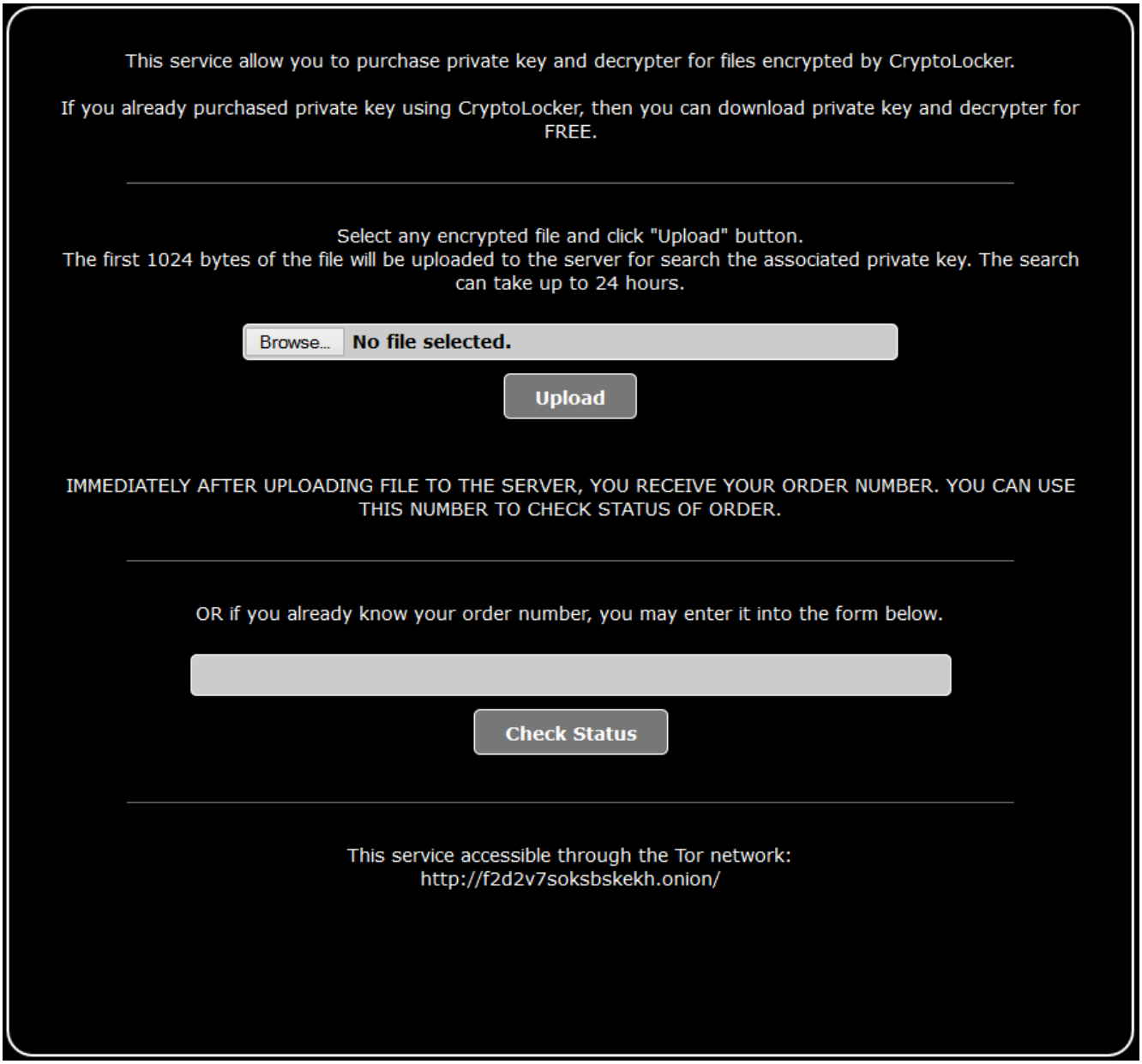


Figure 10. The "CryptoLocker Decryption Service" landing page. (Source: Dell SecureWorks)

The service uploads the first kilobyte of an encrypted file, which contains the header prepended by the malware. The threat actors use that data to query their database for the RSA private key that matches the RSA public key used during file encryption. If the private key is located, the threat actors present the victim with the page shown in Figure 11. The victim is given the option of sending payment to a randomly generated Bitcoin wallet. Early versions of this service charged 10 BTC, but the price was quickly reduced to 2 BTC. After receiving the payment, the threat actors redirect victims to a page that includes instructions on how to decrypt files.

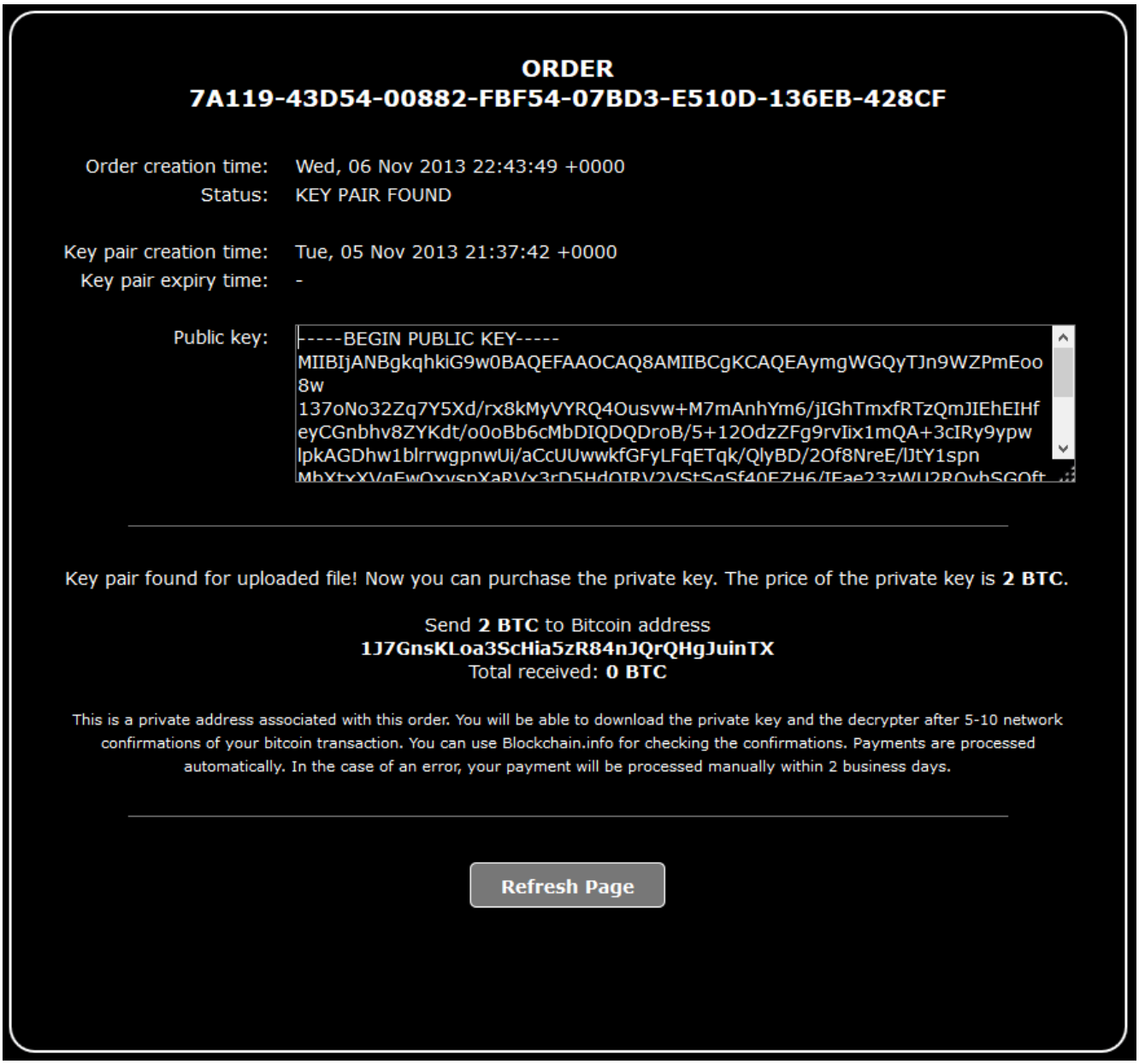


Figure 11. Page displayed when the private key is successfully located. (Source: Dell SecureWorks)

Collected ransoms

In December 2013, Michele Spagnuolo published a thesis discussing a Bitcoin forensics framework called Bitlodine. He discusses identifying Bitcoin addresses controlled by the CryptoLocker threat actors and tracing potential ransom payments made to those addresses. Figure 12 graphs the total number of ransoms paid per day (in gray) along with the total value of those payments in U.S. dollars on the day they were received (in blue).

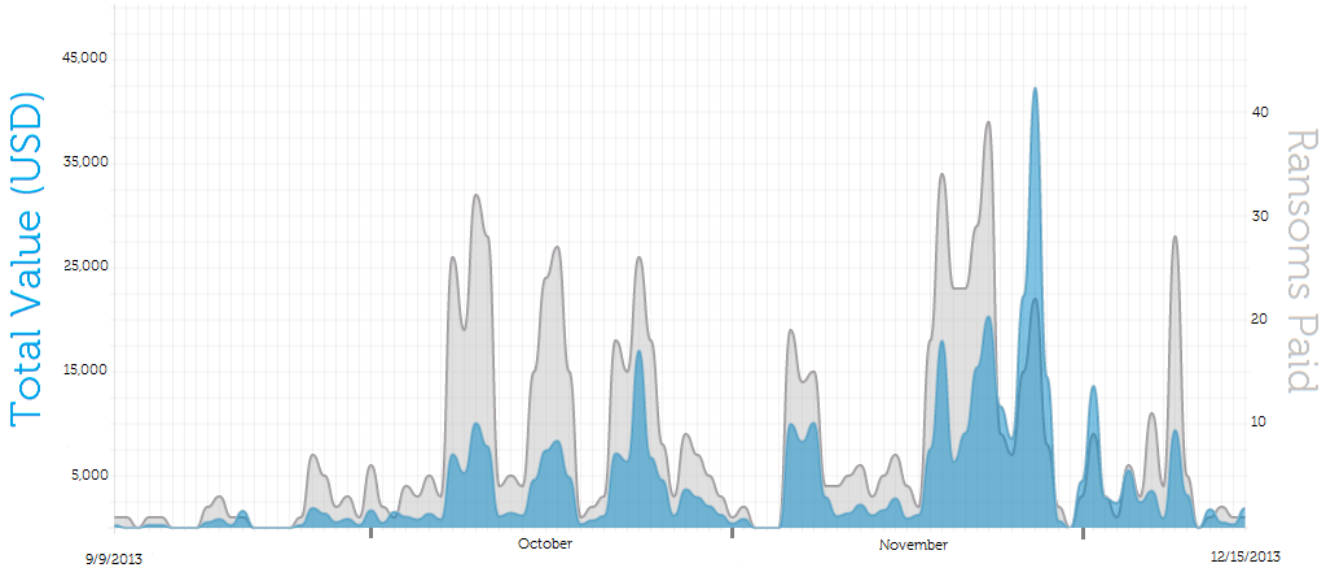


Figure 12. Ransoms paid through Bitcoin. (Source: Dell SecureWorks)

Using the daily weighted BTC price, if the threat actors had sold the 1,216 total BTC collected over the period shown in Figure 12 immediately upon receiving them, they would have earned nearly $380,000. If they elected to hold these ransoms, they would be worth nearly $980,000 as of this publication based on the current weighted price of $804/BTC.

These figures represent a conservative estimate of the number of ransoms collected by the CryptoLocker gang. Based on conversations with U.S.-based victims, the ease of payment with MoneyPak and the numerous technical barriers to obtaining Bitcoins led to most payments being made through the former method. CTU researchers suspect that a significant portion of Bitcoin payments are being made by individuals outside of the U.S., where MoneyPak is not available and Bitcoin is the only option. Based on this information and measurements of infection rates, CTU researchers estimate a minimum of 0.4%, and very likely many times that, of CryptoLocker victims are electing to pay the ransom.

Victims

Based on its design, deployment method, and empirical observations of its distribution, CryptoLocker appears to target English-speakers, specifically those located in the United States. Malware authors from Russia and Eastern Europe, where the CryptoLocker authors are thought to originate, commonly target victims in North America and Western Europe. Law enforcement cooperation between these regions is complicated by numerous factors, which often results in threat actors believing that they can operate with impunity.

CTU researchers observed early infections occurring disproportionately at financial institutions, but anecdotal reports suggest that early victims were in verticals as diverse as hospitality and public utilities. As of this publication, there is no evidence the actors are targeting specific industries. The threat actors have also broadened their attacks to include home Internet users in addition to professionals.

CTU researchers began actively monitoring the CryptoLocker botnet on September 18, 2013 and analyzed various data sources, including DNS requests, sinkhole data, and client telemetry, to build the approximate daily infection rates shown in Figure 13. Spikes coinciding with Cutwail spam campaigns

that resulted in increased CryptoLocker infections are clearly indicated, including the period of high activity from October through mid-November. Likewise, periodic lulls in activity have occurred frequently, including a span from late November through mid-December.

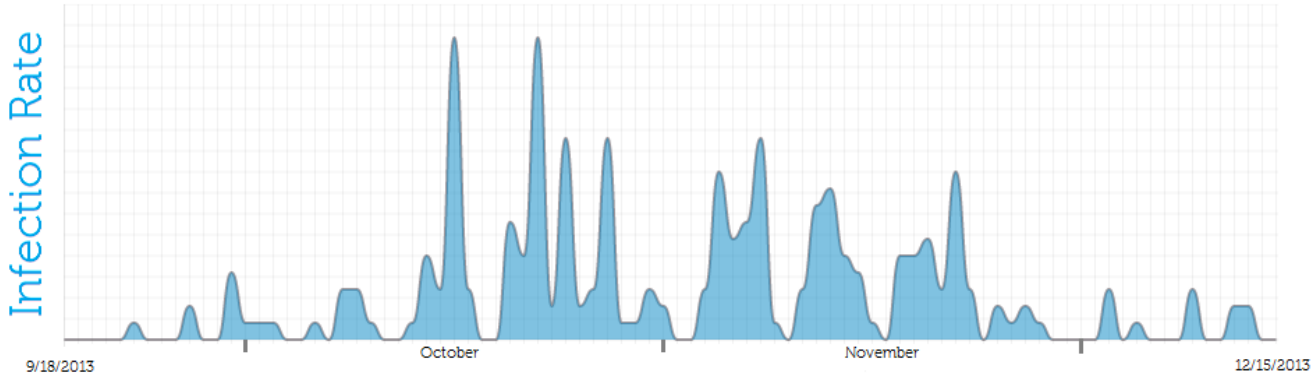


Figure 13. Approximated infection rates. (Source: Dell SecureWorks)

The CTU research team registered multiple domains from the pool used by CryptoLocker to construct a sinkhole infrastructure and assess the malware's global impact. Between October 22 and November 1, 2013, 31,866 unique IP addresses contacted CTU sinkhole servers. Figure 14 shows the geographic distribution of these IP addresses.

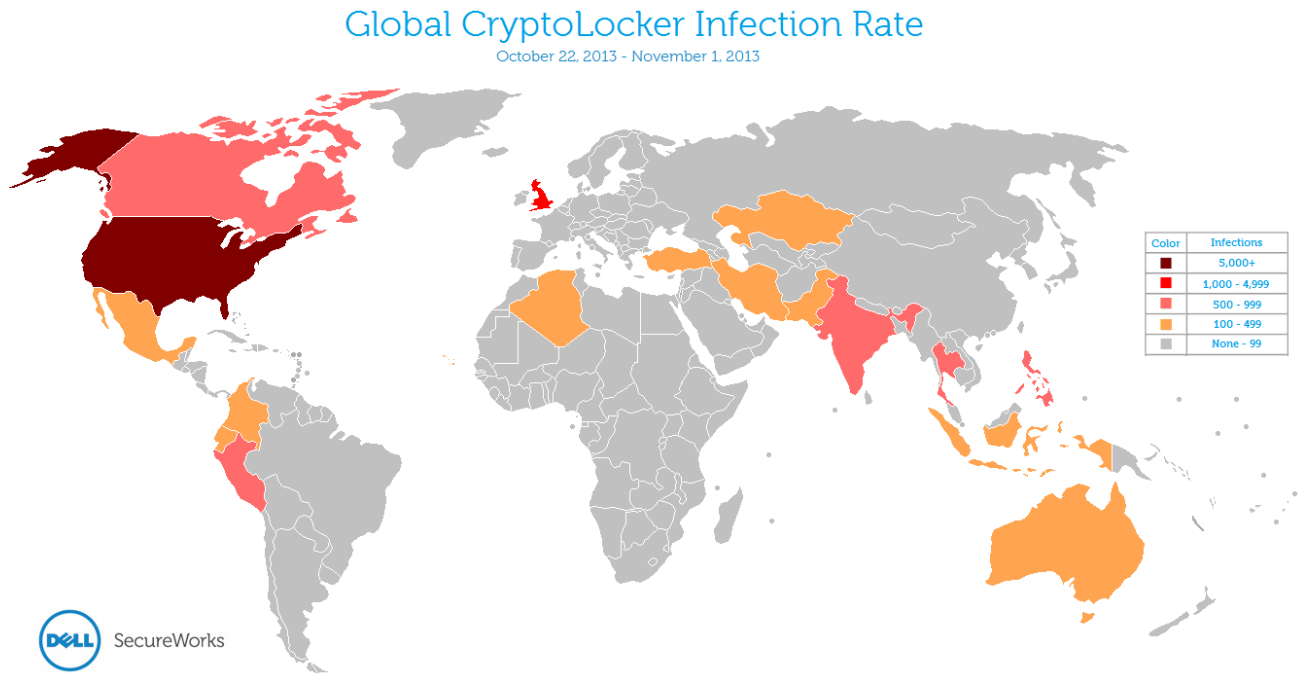


Figure 14. Global distribution of CryptoLocker infections between October 22 and November 1, 2013. (Source: Dell SecureWorks)

The United States was disproportionately represented among countries with measurable infection rates. Table 4 lists countries with the top ten infection rates.

Country	Number of infected systems	Percentage of total
United States	22,360	70.2%
Great Britain	1,767	5.5%

India	818	2.6%
Thailand	691	2.2%
Peru	688	2.2%
Canada	658	2.1%
Philippines	645	2.0%
Indonesia	427	1.3%
Iran	333	1.0%
Ecuador	264	0.8%

Table 4. Geographic breakdown of infection counts. (Source: Dell SecureWorks)

The CTU research team implemented a similar sinkhole infrastructure between December 9 and December 16, which was during a period of limited malware activity. Additionally, recent samples use hard-coded C2 domains, which limits the conclusions that can be drawn from information gathered from sinkhole domains. During this observation period, 6,459 unique IP addresses contacted the CTU sinkhole servers. Figure 15 shows the geographic distribution of these IP addresses.

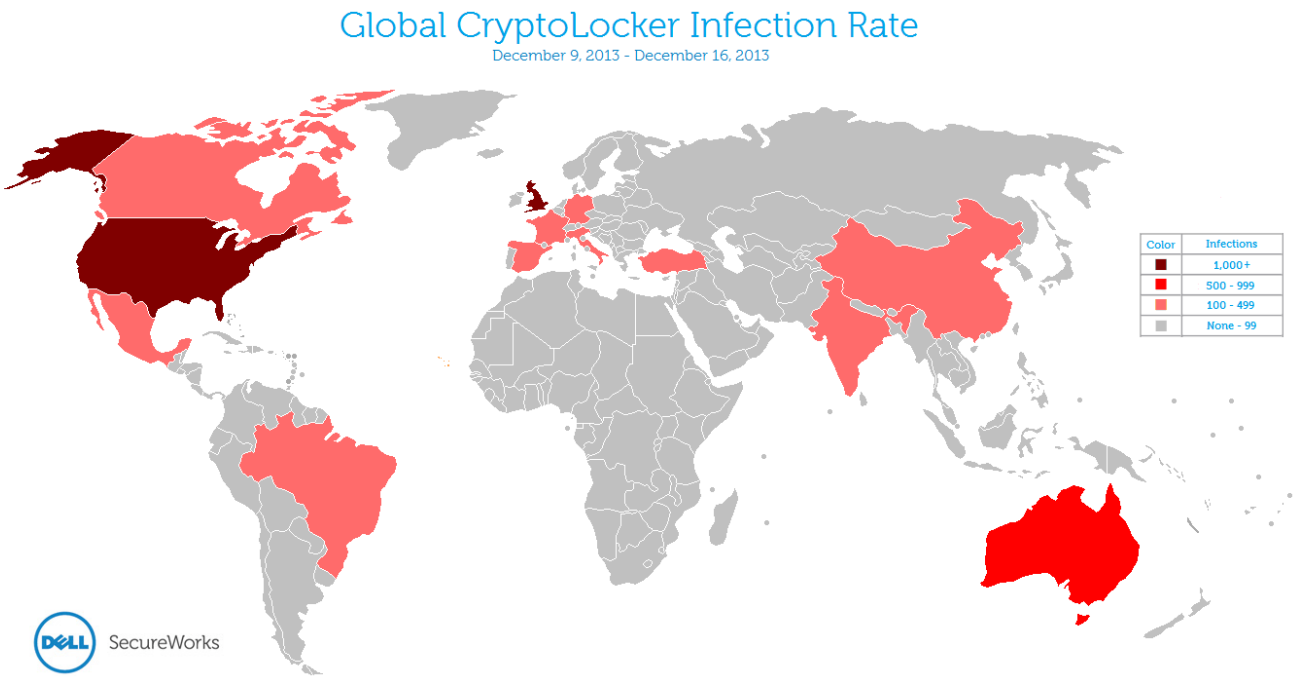


Figure 15. Global distribution of CryptoLocker infections between December 9 and December 16, 2013. (Source: Dell SecureWorks)

In the samples gathered by the December sinkhole, the United Kingdom and Australia approached the absolute infection numbers of the U.S, despite having much smaller populations. CTU researchers are unsure whether this change is an anomaly or represents a change in the threat actors' strategy.

Table 5 lists countries with the top ten infection rates.

Country	Number of infected systems	Percentage of total
United States	1,540	23.8%
Great Britain	1,228	19.0%
Australia	836	12.9%
France	372	5.8%
Brazil	309	4.8%
Italy	204	3.2%
Turkey	182	2.8%
Spain	145	2.2%
China	138	2.1%
Canada	135	2.1%

Table 5. Geographic breakdown of infection counts. (Source: Dell SecureWorks)

Based on the presented evidence, CTU researchers estimate that 200,000 to 250,000 systems were infected globally in the first 100 days of the CryptoLocker threat.

Mitigation

By incorporating the following components in a defense-in-depth strategy, organizations may be able to mitigate the CryptoLocker threat:

- Block executable files and compressed archives containing executable files before they reach a victim's inbox. Email remains a top infection vector for malware in general and this threat in particular.
- Consider aggressively blocking known indicators (see Table 6) from communicating with your network to temporarily neuter the malware until it can be discovered and removed. CryptoLocker does not encrypt files until it has successfully contacted an active C2 server.
- Reevaluate permissions on shared network drives to prevent unprivileged users from modifying files.
- Regularly back up data with so-called "cold," offline backup media. Backups to locally connected, network-attached, or cloud-based storage are not sufficient because CryptoLocker encrypts these files in the same manner as those found on the system drive.
- Implement Software Restriction Policies (SRPs) to prevent programs like CryptoLocker from executing in common directories such as %AppData% or %LocalAppData%.
- Use Group Policy Objects (GPOs) to create and restrict permissions on registry keys used by CryptoLocker, such as HKCU\SOFTWARE\CryptoLocker (and variants). If the malware cannot open and write to these keys, it terminates before encrypting any files.

Conclusion

CryptoLocker is neither the first ransomware nor the first destructive malware to wreak havoc on infected systems. However, the malware authors appear to have made sound design decisions that complicate efforts to mitigate this threat and have demonstrated a capable distribution system based on the Cutwail and Gameover Zeus botnets. Evidence collected by CTU researchers confirms the threat actors have previous experience in malware development and distribution, especially of ransomware. Based on the duration and scale of attacks, they also appear to have the established and substantial "real world" infrastructure necessary to "cash out" ransoms and launder the proceeds.

Threat indicators

To mitigate exposure to the CryptoLocker malware, CTU researchers recommend that clients use available controls to restrict access using the indicators in Table 6. The domains listed in the indicators table may contain malicious content, so consider the risks before opening them in a browser. CTU researchers have attempted to remove IP addresses and domain names operated by security vendors and private researchers, but some non-malicious infrastructure may be included. Date gaps in domain name information represent periods when the threat actors elected not to register malicious domains or when CTU researchers had insufficient data to determine those domain names.

Indicator	Type	Context
qwlpubwopsyj.org	Domain name	C2 domain, September 9, 2013
sypdwysctilgr.net	Domain name	C2 domain, September 9, 2013
txeuntcemcwj.biz	Domain name	C2 domain, September 10, 2013
qqkoluhwexlr.biz	Domain name	C2 domain, September 10, 2013
xeogrhxquuubt.com	Domain name	C2 domain, September 10, 2013
qaaepodedahnslq.org	Domain name	C2 domain, September 10, 2013
vbitnxdgsiwg.biz	Domain name	C2 domain, September 11, 2013
sbfuwsxasjkp.net	Domain name	C2 domain, September 11, 2013

afmkdchedjkcai.org	Domain name	C2 domain, September 11, 2013
jxjyndpaoofctm.com	Domain name	C2 domain, September 11, 2013
ueymssvirqnwqqs.net	Domain name	C2 domain, September 11, 2013
wojscmlfgvhw.net	Domain name	C2 domain, September 12, 2013
dakpicuylsrfcl.biz	Domain name	C2 domain, September 12, 2013
nuafhowbvpmgbn.net	Domain name	C2 domain, September 13, 2013
uoerpkaffwnds.org	Domain name	C2 domain, September 13, 2013
aycysyspcpvwgtw.biz	Domain name	C2 domain, September 16, 2013
qhqmhxuhapgkaq.biz	Domain name	C2 domain, September 16, 2013
wnoctmckyrtbou.org	Domain name	C2 domain, September 16, 2013
pahwvolnihur.biz	Domain name	C2 domain, September 16, 2013
rtqajjkivmltosy.org	Domain name	C2 domain, September 17, 2013
jyyfmnefedjogsh.biz	Domain name	C2 domain, September 17, 2013
qjtwguxajaqqhu.org	Domain name	C2 domain, September 17, 2013

lrexdcwwpyny.biz	Domain name	C2 domain, September 17, 2013
nnpiceisyfgiprh.org	Domain name	C2 domain, September 18, 2013
xtagmlgwrrqsto.biz	Domain name	C2 domain, September 18, 2013
fyflgkbdydnf.biz	Domain name	C2 domain, September 19, 2013
jebounnlykpt.org	Domain name	C2 domain, September 19, 2013
dookhuvnmgamvgr.net	Domain name	C2 domain, September 20, 2013
vahroshwfnih.org	Domain name	C2 domain, September 20, 2013
rcoxshllfoldxie.org	Domain name	C2 domain, September 23, 2013
kdsdsapurvgf.biz	Domain name	C2 domain, September 23, 2013
phiiykytxrlfjx.info	Domain name	C2 domain, September 24, 2013
ubnxaasfigrbhj.biz	Domain name	C2 domain, September 24, 2013
lwxmytwfuwuk.net	Domain name	C2 domain, September 24, 2013
hefjkoscpbof.org	Domain name	C2 domain, September 24, 2013
wypqdsmpfvuq.org	Domain name	C2 domain, September 25, 2013

kermcmfomqdnaw.biz	Domain name	C2 domain, September 25, 2013
fukpbxfgejfllr.biz	Domain name	C2 domain, September 25, 2013
jvpopwqdmhahho.info	Domain name	C2 domain, September 25, 2013
fsihpjionkbb.net	Domain name	C2 domain, September 25, 2013
lcvvmgpdfbty.biz	Domain name	C2 domain, September 25, 2013
ewkovrirsprw.org	Domain name	C2 domain, September 25, 2013
bkfekyhvftxkwd.biz	Domain name	C2 domain, September 26, 2013
nxosmtaifwud.org	Domain name	C2 domain, September 26, 2013
emrsmpipfrtu.biz	Domain name	C2 domain, September 27, 2013
qdbvwfnyurewx.com	Domain name	C2 domain, September 27, 2013
gaeaglgxkkws.biz	Domain name	C2 domain, September 28, 2013
jpkpiichjjdm.org	Domain name	C2 domain, September 29, 2013
cmjbewheycxmr.net	Domain name	C2 domain, September 29, 2013
rvkpjfyxpsocbsn.org	Domain name	C2 domain, September 30, 2013

pwssoabbqtfs.net	Domain name	C2 domain, September 30, 2013
flavquyaoisq.info	Domain name	C2 domain, September 30, 2013
inveinqskeriapb.biz	Domain name	C2 domain, September 30, 2013
yoifiwpqreitpus.com	Domain name	C2 domain, September 30, 2013
vmkstanptubqm.net	Domain name	C2 domain, September 20, 2013
gkmlecoeshjxd.net	Domain name	C2 domain, October 1, 2013
gawpiclfrmnkb.org	Domain name	C2 domain, October 1, 2013
vvpbfbqpnaqq.net	Domain name	C2 domain, October 1, 2013
voafsbnewuxl.org	Domain name	C2 domain, October 1, 2013
tsgmgrofgsbqtuw.com	Domain name	C2 domain, October 1, 2013
myourlqubgdxles.org	Domain name	C2 domain, October 2, 2013
oxwqodvowcgr.biz	Domain name	C2 domain, October 3, 2013
suanecwngxhufr.biz	Domain name	C2 domain, October 3, 2013
axugjsdemnjuso.org	Domain name	C2 domain, October 3, 2013

klnvbfainjtibmn.org	Domain name	C2 domain, October 4, 2013
oamurnwjrrap.net	Domain name	C2 domain, October 4, 2013
ueygwkeaamxvpc.com	Domain name	C2 domain, October 5, 2013
ybmdqshtbarpvxx.net	Domain name	C2 domain, October 5, 2013
jnnkdjixngmjtrk.org	Domain name	C2 domain, October 5, 2013
mydqpbcaqlppiqn.biz	Domain name	C2 domain, October 5, 2013
gykcghilthjy.com	Domain name	C2 domain, October 6, 2013
rntkondhjwybkja.com	Domain name	C2 domain, October 6, 2013
fycuscwcjmaqkl.org	Domain name	C2 domain, October 6, 2013
uobuwcfaoerojos.net	Domain name	C2 domain, October 7, 2013
odxrjkgnahebp.biz	Domain name	C2 domain, October 7, 2013
udvdjsdnmnisj.biz	Domain name	C2 domain, October 10, 2013
afuxiuwttqpk.net	Domain name	C2 domain, October 10, 2013
kdcvlslmyurory.biz	Domain name	C2 domain, October 10, 2013

gktibioivpqbot.net	Domain name	C2 domain, October 10, 2013
vccpdadcaygc.biz	Domain name	C2 domain, October 11, 2013
dywpplmanlmsu.org	Domain name	C2 domain, October 14, 2013
rwyngtbvunfpk.org	Domain name	C2 domain, October 15, 2013
vaategmcgbpimoa.net	Domain name	C2 domain, October 15, 2013
cjlvuuhphnwbr.info	Domain name	C2 domain, October 15, 2013
cjlvuuhphnwbr.info	Domain name	C2 domain, October 16, 2013
wshufkvuruwxsua.com	Domain name	C2 domain, October 16, 2013
qvvmhsxxidvjmil.biz	Domain name	C2 domain, October 17, 2013
jcxyensduaeed.info	Domain name	C2 domain, October 17, 2013
ypvcyhohthmmm.info	Domain name	C2 domain, October 18, 2013
oobdujltidljprw.com	Domain name	C2 domain, October 18, 2013
ejelwtqlibhdof.org	Domain name	C2 domain, October 18, 2013
dfvoglnegikqvk.org	Domain name	C2 domain, October 18, 2013

qtcexpbgcusfp.com	Domain name	C2 domain, October 18, 2013
bhxytqseirfat.net	Domain name	C2 domain, October 18, 2013
pksjdseiarkf.net	Domain name	C2 domain, October 18, 2013
ldtbbqvouqnn.com	Domain name	C2 domain, October 18, 2013
clpgukoesqcuvp.biz	Domain name	C2 domain, October 19, 2013
utjpwmskhwqk.com	Domain name	C2 domain, October 19, 2013
impkyvkcbfps.info	Domain name	C2 domain, October 20, 2013
mcbksstivjvn.org	Domain name	C2 domain, October 20, 2013
ovenbdjnihhdlb.net	Domain name	C2 domain, October 21, 2013
ctexrkpwsdnepo.org	Domain name	C2 domain, October 21, 2013
vhohfvimhpsqn.info	Domain name	C2 domain, October 21, 2013
qikshmnujoitxe.com	Domain name	C2 domain, October 21, 2013
lsjpkatguitaohx.biz	Domain name	C2 domain, October 22, 2013
fefanfdwdpeevoe.info	Domain name	C2 domain, October 22, 2013

ciecxcsbdldwx.net	Domain name	C2 domain, October 22, 2013
pbxksllrmivxhjc.org	Domain name	C2 domain, October 23, 2013
cfuwtrfmyinvuo.org	Domain name	C2 domain, October 23, 2013
sptqapwrwcpclts.org	Domain name	C2 domain, October 24, 2013
qntptjfabhra.biz	Domain name	C2 domain, October 24, 2013
uoqkpgiygtmgi.net	Domain name	C2 domain, October 24, 2013
shryjqiaceibck.biz	Domain name	C2 domain, October 25, 2013
iimkdpysckqmot.org	Domain name	C2 domain, October 25, 2013
dmvhawouahhfsmj.org	Domain name	C2 domain, October 27, 2013
ariqhgoxrewhr.biz	Domain name	C2 domain, October 27, 2013
ofcxlybtofglm.org	Domain name	C2 domain, October 28, 2013
kwajtnjddqetolh.biz	Domain name	C2 domain, October 29, 2013
wifgslrwgvxwsy.com	Domain name	C2 domain, October 31, 2013
uvpevldfpfhoipn.info	Domain name	C2 domain, November 1, 2013

ywculygjuxhxtsh.net	Domain name	C2 domain, November 1, 2013
byoluqqhvjsbnqa.org	Domain name	C2 domain, November 1, 2013
dilkqddvhstlnwe.net	Domain name	C2 domain, November 2, 2013
tyqhngggjijlpxh.info	Domain name	C2 domain, November 2, 2013
qgugwncykxuuiid.info	Domain name	C2 domain, November 3, 2013
xvaxsxbptmerjb.com	Domain name	C2 domain, November 4, 2013
wikjpwxhskgoc.ru	Domain name	C2 domain, November 4, 2013
tlsylihoxxmvc.org	Domain name	C2 domain, November 5, 2013
tbmeoaosvbwe.biz	Domain name	C2 domain, November 6, 2013
vqojwwmocssqa.org	Domain name	C2 domain, November 6, 2013
lwvpgiabehxt.org	Domain name	C2 domain, November 8, 2013
stmdjbsbhojxp.net	Domain name	C2 domain, November 8, 2013
prwxcrswstle.org	Domain name	C2 domain, November 12, 2013
cutwdfsdcbfco.biz	Domain name	C2 domain, November 12, 2013

xqmrainncxrwho.net	Domain name	C2 domain, November 12, 2013
pasnepjktwbcmwo.org	Domain name	C2 domain, November 12, 2013
tquttkwcuemnpp.org	Domain name	C2 domain, November 13, 2013
qhanpujcdytu.biz	Domain name	C2 domain, November 13, 2013
mteyowfgnrbhgnm.org	Domain name	C2 domain, November 14, 2013
quykengjhtob.biz	Domain name	C2 domain, November 14, 2013
wbwcajwlqksl.org	Domain name	C2 domain, November 14, 2013
dltlqtwlioauuj.biz	Domain name	C2 domain, November 15, 2013
axxehlphcdss.org	Domain name	C2 domain, November 15, 2013
lhkbianumwfs.biz	Domain name	C2 domain, November 16, 2013
kqnvwyqyqqmkab.biz	Domain name	C2 domain, November 16, 2013
nqktirfigqfyow.org	Domain name	C2 domain, November 17, 2013
hwuiingqeuubi.org	Domain name	C2 domain, November 18, 2013
dclffueprfhkgf.biz	Domain name	C2 domain, November 19, 2013

gtdipovkdxricgl.biz	Domain name	C2 domain, November 19, 2013
gtdipovkdxricgl.biz	Domain name	C2 domain, November 20, 2013
boexeicnsbbxbg.org	Domain name	C2 domain, November 20, 2013
fksuksvrqqdetlp.org	Domain name	C2 domain, November 20, 2013
qnprseyycdot.biz	Domain name	C2 domain, November 20, 2013
vtcyrmxkkxvrick.biz	Domain name	C2 domain, November 21, 2013
tpsjegnvxqmtk.biz	Domain name	C2 domain, November 21, 2013
ftltwlsqhegsnav.org	Domain name	C2 domain, November 22, 2013
pvfvmuveigjhmjc.biz	Domain name	C2 domain, November 22, 2013
xqjafpdyjcvjwp.biz	Domain name	C2 domain, November 23, 2013
ftltwlsqhegsnav.org	Domain name	C2 domain, November 23, 2013
nqygxdafeivtgb.org	Domain name	C2 domain, November 23, 2013
hntfarwlevtcxm.org	Domain name	C2 domain, November 24, 2013
axqrgervreovhhc.biz	Domain name	C2 domain, November 25, 2013

axqrgervreovhhc.biz	Domain name	C2 domain, November 26, 2013
tnaujeuilsia.org	Domain name	C2 domain, November 26, 2013
vexnudbnovttaj.org	Domain name	C2 domain, November 27, 2013
rttvxygkmwlqmq.net	Domain name	C2 domain, November 29, 2013
jknuotworuebip.org	Domain name	C2 domain, December 1, 2013
cajqhxcwxbaap.biz	Domain name	C2 domain, December 1, 2013
lbmuvpwgcmquc.org	Domain name	C2 domain, December 1, 2013
wwfcogdgntlxw.biz	Domain name	C2 domain, December 2, 2013
usyusdoctfpnee.org	Domain name	C2 domain, December 3, 2013
swmbolrxyflhwm.biz	Domain name	C2 domain, December 3, 2013
yebdbfsomgdbqu.biz	Domain name	C2 domain, December 4, 2013
usyusdoctfpnee.org	Domain name	C2 domain, December 4, 2013
msncwipuqpxxoqa.org	Domain name	C2 domain, December 4, 2013
dhjicdgfykqoq.org	Domain name	C2 domain, December 5, 2013

pkakvsexbmxpwxw.org	Domain name	C2 domain, December 5, 2013
ghvoersorwsrgef.org	Domain name	C2 domain, December 6, 2013
dhjicdgfykqoq.org	Domain name	C2 domain, December 6, 2013
wjbodchhlgidofm.org	Domain name	C2 domain, December 6, 2013
bsngfunwcpkjt.org	Domain name	C2 domain, December 6, 2013
tmphandchtcnffy.org	Domain name	C2 domain, December 6, 2013
qnsoiclrikwj.org	Domain name	C2 domain, December 7, 2013
agwwcjhinwyl.org	Domain name	C2 domain, December 7, 2013
osmhvqijsiedt.org	Domain name	C2 domain, December 7, 2013
nfnfskbniyajd.org	Domain name	C2 domain, December 7, 2013
cmidahhutlcx.org	Domain name	C2 domain, December 8, 2013
emttankkwhqsoe.org	Domain name	C2 domain, December 8, 2013
ypxnqheckgjkbu.org	Domain name	C2 domain, December 9, 2013
ormyfnlykajkdr.org	Domain name	C2 domain, December 9, 2013

vsjotulrsjhyf.org	Domain name	C2 domain, December 10, 2013
cpapfioutwypmh.org	Domain name	C2 domain, December 10, 2013
kmjqcsfxnyeuo.org	Domain name	C2 domain, December 10, 2013
xivexnrjahpfk.org	Domain name	C2 domain, December 10, 2013
gavhopncgfmdq.org	Domain name	C2 domain, December 11, 2013
ykmccdhpgavm.org	Domain name	C2 domain, December 11, 2013
slbugcihgrgny.org	Domain name	C2 domain, December 11, 2013
wpowcdntgoye.org	Domain name	C2 domain, December 11, 2013
rkmmrxbpafgnplt.org	Domain name	C2 domain, December 12, 2013
fpvpnoqmgntmc.org	Domain name	C2 domain, December 12, 2013
ahqnsclgckkpho.org	Domain name	C2 domain, December 13, 2013
mqagyenfbebsau.org	Domain name	C2 domain, December 13, 2013
gavhopncgfmdq.org	Domain name	C2 domain, December 13, 2013
urkitujgkhsjl.org	Domain name	C2 domain, December 14, 2013

kgvmmylyflrqml.org	Domain name	C2 domain, December 14, 2013
93.189.44.187	IP address	C2 server, Russia
81.177.170.166	IP address	C2 server, Russia
95.211.8.39	IP address	C2 server, Netherlands
188.93.210.164	IP address	C2 server, Russia
91.218.121.139	IP address	C2 server, United States
173.246.105.23	IP address	C2 server, United States
217.12.219.32	IP address	C2 server, Ukraine
109.120.150.95	IP address	C2 server, Russia
194.28.174.119	IP address	C2 server, Ukraine
91.203.145.13	IP address	C2 server, Ukraine
46.254.16.22	IP address	C2 server, Russia
91.234.33.198	IP address	C2 server, Ukraine
134.0.118.114	IP address	C2 server, Russia
91.226.213.198	IP address	C2 server, Ukraine
91.226.212.198	IP address	C2 server, Ukraine
176.123.0.54	IP address	C2 server, Moldova
176.119.0.216	IP address	C2 server, Ukraine

188.65.211.137	IP address	C2 server, Russia
31.131.18.101	IP address	C2 server, Ukraine
185.22.64.72	IP address	C2 server, Kazakhstan
195.2.77.48	IP address	C2 server, Russia
188.190.101.82	IP address	C2 server, Ukraine
62.76.191.48	IP address	C2 server, Russia
95.59.26.43	IP address	C2 server, Kazakhstan
144.76.192.130	IP address	C2 server, Germany
194.28.174.119	IP address	C2 server, Ukraine
46.149.111.28	IP address	C2 server, Ukraine
83.69.233.25	IP address	C2 server, Russia
91.213.233.189	IP address	C2 server, Kyrgyzstan
109.234.154.254	IP address	C2 server, Russia
bc11c93f1b6dc74bf4804a35b34d9267	MD5 hash	Malware sample
a2bc3059283d7cc7bc574ce32cb6b8bfd27e02ac3810a21bd3a9b84c17f18a72	SHA256 hash	Malware sample
b17603f401719f1d99ad6472f8d6682a	MD5 hash	Malware sample
0be1f445537f124b5175e1f2d1da87e2e57aa4ba09ea5fe72b7bafaf0b8f9ad2	SHA256 hash	Malware sample
f1e2de2a9135138ef5b15093612dd813	MD5 hash	Malware sample
136e8991816b958bb76aaf22fefd18194cf78a80e95d572754f95e1f86149a65	SHA256 hash	Malware sample

a93d75cb6f72c1847c3f5afc9c94bbbb	MD5 hash	Malware sample
724799e37d6b47dc099caea7aabb0c1246a5041537d425601639d551e42bd425	SHA256 hash	Malware sample
df06f3263088fc9f7fde03fc8d2969fc	MD5 hash	Malware sample
39fd73f1d19201497233bbb320c1d7a63e33748c94d94653c3b5e64c0ef6b8b0	SHA256 hash	Malware sample
de400607d06b41a6f8b0935c3607541d	MD5 hash	Malware sample
9ec4697891cc6c9add803044a29bdd9d05701509b9eddc370d4caf00c15ef734	SHA256 hash	Malware sample
012d9088558072bc3103ab5da39ddd54	MD5 hash	Malware sample
0dd7f3dffe8c6e69df6137cb413ad25c474d73a86f1d46d52846990aa66e6f43	SHA256 hash	Malware sample
8acecb8a6ccec5631e990273ee1c96bb	MD5 hash	Malware sample
c5fdc30a67fbba53b710e6ff8d8e38ed4fb5e44eeced2efc370f906710602840	SHA256 hash	Malware sample
ccc9e5f7e53eaf6124df45bb14eccf8f	MD5 hash	Malware sample
d4adf29d2b50945896734bafb66ada120b53f5dd98f1a8ad3d30dcf69a98325e	SHA256 hash	Malware sample
16f0e31ac53b98411dd6719ff995872f	MD5 hash	Malware sample
3df9806a5cc986619f96755151cdbc23e1943280c1874c58b2758da2d7be6e64	SHA256 hash	Malware sample
04fb36199787f2e3e2135611a38321eb	MD5 hash	Malware sample
d765e722e295969c0a5c2d90f549db8b89ab617900bf4698db41c7cdad993bb9	SHA256 hash	Malware sample
57ae3d79ee697d2c382fdea56827e65f	MD5 hash	Malware sample
31327f225492ee58d7b47889e619d36cd380a908c1761fe376a185877f813894	SHA256 hash	Malware sample
180753f31b8295751aa3d5906a297511	MD5 hash	Malware sample

b264f35ff932fc5a100f7c2b4bd4888fe61db9878ef149279c3ad4bef2bdd8ed	SHA256 hash	Malware sample
551e4c94cd17860a7f49db5ec65ba58c	MD5 hash	Malware sample
d73d6964d2b1e3e466436fb981b6658d8e1fb5d0ddc43e7f24365cad2339842d	SHA256 hash	Malware sample
60ce367abdf38a35bb304253dd03da5d	MD5 hash	Malware sample
e0702fdeef58461133ef70efa25d258b1eaa089b26d57485106d0fea671e3afb	SHA256 hash	Malware sample
9cbb128e8211a7cd00729c159815cb1c	MD5 hash	Malware sample
bb12757c6a14207d8a9cd4d42ff93747795f8a09186752b1c94b5b373abbaf11	SHA256 hash	Malware sample
d2b1dc9cae99cd4c511a0df9af948639	MD5 hash	Malware sample
e38edbea38a47560bff7f48e23ba9eb7c872e180f16abb3482c021cac3cbfaed	SHA256 hash	Malware sample
04fc7ffc8439e27a51b5241e8bd00e75	MD5 hash	Malware sample
8bfe5d3d7e089cecb0238da7ae7d456702508003a91a417e5069b86592bc03e8	SHA256 hash	Malware sample
374f74def24ea6afad4e5f4b15dcd263	MD5 hash	Malware sample
f2181881d6ab133323dba5fecbf0cc4236f794ed1261406712b13307e98b90a1	SHA256 hash	Malware sample
444c339f422420bc317711dac06f3545	MD5 hash	Malware sample
cb7ce90b9de59004b2177e7a912c324ef4cec0262e181c83fff866113356e607	SHA256 hash	Malware sample
fec5a0d4dea87955c124f2eaa1f759f5	MD5 hash	Malware sample
4f3220da017e7be3e0b168a958134aae6dc96458cb12118e849465e2af752629	SHA256 hash	Malware sample
a5d1e987629cf939121f3bfb202c7d6a	MD5 hash	Malware sample
cc4350d0919d192bdad9ae262fc524d9d230b11dfc8d3c5886147caa0fdda465	SHA256 hash	Malware sample

0204332754da5975b6947294b2d64c92	MD5 hash	Malware sample
2163570f047cefc466c0ca370e56b6fbb770c4f71603b2353c1b6fd8e482ced8	SHA256 hash	Malware sample
7ea2c970326af64b1b196c4dd12e61dc	MD5 hash	Malware sample
651f451aaf9a9694884322d91a225294af145006219c346d1a9b50a2d92db6d9	SHA256 hash	Malware sample
e1f6706fe8bdd3c63fc15cdfe3fdf723	MD5 hash	Malware sample
826fb87209f4538ff9a0d11c8a21d6df738956ab7ba8d6965cb8f46021013ae4	SHA256 hash	Malware sample
1eac61ee26db9242ba47437a027c47d4	MD5 hash	Malware sample
876511719fda2fab0438ad29f9cc2f8fd684c1897a88d433f7e9c3f2e85eac0b	SHA256 hash	Malware sample
0a6bd33f3d37809e92f272eaf304eab3	MD5 hash	Malware sample
58def7649806f63ce1dbd9d886ce200716209240b90b57dccf3941012c438784	SHA256 hash	Malware sample
e9cd494b249cea7b968fa89f1e7d40de	MD5 hash	Malware sample
76487462acfa06bc90bda7d72bee7f88ea2e70d838a50d9012362958ad93f02a	SHA256 hash	Malware sample
31a09770fea2d2ad58709b9a2f0e78c1	MD5 hash	Malware sample
931708bffa6eed76585c166a080ea6b544f32951cb5dbc2d2065088ee9ebad95	SHA256 hash	Malware sample
a8e0d4771c1f71709ddb63d9a75dc895	MD5 hash	Malware sample
b3530b7519660996d28eb31a8d5b585ec60601843c77dd9f2b712812c99843e4	SHA256 hash	Malware sample
dae2d96628ff94e65a35ae9a929ad7ba	MD5 hash	Malware sample
21c7a8f2ffdd80834fb9b82df5c02748ca08c48583b903d584c124b916d17a37	SHA256 hash	Malware sample
bbb445901d3ec280951ac12132afd87c	MD5 hash	Malware sample

ed95b1a888710f3ca4acacb49250fb6c21722e2882e31784bd2049d15f97d4de	SHA256 hash	Malware sample
62808c6de7ee1e9bb3e1aedf543a5549	MD5 hash	Malware sample
2f89ebdcc33bc0ec253e9d1bb9a5b252cc8dc0e90b78d7c464a487dab3b387a6	SHA256 hash	Malware sample
53a93128e59385dba9301a2a3d636899	MD5 hash	Malware sample
7925550392f06655abbc9ed66fa37e1754bf6612439cc7a6332db28fd8878b42	SHA256 hash	Malware sample
4cd6c47bfdfd5f3b6aba203326f9c615	MD5 hash	Malware sample
f26bc4c0e23430c444214bd32e5ae0dacee93c4409fa574e91f4204e691c5799	SHA256 hash	Malware sample
354f7ec15741db7fcdfe7b158c14dfaa	MD5 hash	Malware sample
6af16a07d19bcb99eed8b440d7a110ee1bad1dd95eaeda2302c423ab9a5a146c	SHA256 hash	Malware sample
9acf753845e32f40631a51fa53746766	MD5 hash	Malware sample
433717fd1916ba3ae569d9334c400ac8740fe7870e05bf57d2b05fd4023b2451	SHA256 hash	Malware sample
9605ca26b5f27f04c7a91fda86b3c489	MD5 hash	Malware sample
003c64fa11ea18a00c3e0bf2adf1a2b80287fb072d1f8108d1d55cbda17e60cb	SHA256 hash	Malware sample
aa6425695964d9c39a6adce54899abf3	MD5 hash	Malware sample
b2e6ba8776232da078e4d7648525b5dc97e70744ffbcae871048306f7fe9aba1	SHA256 hash	Malware sample
d81a9ebae58461f13404e4434be9a567	MD5 hash	Malware sample
c37dd01eaac834a0f2618e54e3f67b03484b3e36d491011334f3646b66fe0e56	SHA256 hash	Malware sample
2dfddacd5394e6994067c06075353c1b	MD5 hash	Malware sample
36ec7a5bcdd2685af78cdef0868758419254534835 5a6510132644541f4c4749	SHA256 hash	Malware sample

038e049f03ee9e2e0f424a3848d0acbb	MD5 hash	Malware sample
2ff9b57a16c7da6699be588b6239296576b6b5805db7a27e5f2dec243e0da75b	SHA256 hash	Malware sample
e0863465caf7d670a3385614290f27b2	MD5 hash	Malware sample
684051fd30d38f3d03c65e80087183ea1cbe1fc8f5dc03ebf7269498e9bffb98	SHA256 hash	Malware sample
cbd77dca77917bc800a8438b3e82f7e2	MD5 hash	Malware sample
44f62555fdfd1067de4ef55a8deb916e24832a80a28b91ba59b0aad527b565a4	SHA256 hash	Malware sample
5df84af6d39442e1b72dcc62f64e6cd0	MD5 hash	Malware sample
9f6443788563472c0280ad5b16ae7c1a918f1f2ce6e44d4d1a09a87a1f3412a8	SHA256 hash	Malware sample
81c8c8ccf5c493863832d5813d6036f4	MD5 hash	Malware sample
248e0103a5027800d92d517d4d6721c4b6dc0b533ee22f8452c79d5f48128fdc	SHA256 hash	Malware sample
8bcc561ef4d0ceaed3cdc3ae0c77575a	MD5 hash	Malware sample
1dec40385522800dfed483b645da71c1ee3afbbdec27e567662972d59c5cbf25	SHA256 hash	Malware sample
05a70f12f819c746bdc23791bc821346	MD5 hash	Malware sample
201131fb20d85b71765e5634821a2b35303643212c36023843485c56f47ac400	SHA256 hash	Malware sample
ab789367cc97965b7c4024040ff8a5f8	MD5 hash	Malware sample
cc4c212dcfe4bf82e60eaa0d220444f0f6dbf22c5f7a79be83fe28f2f00b89b5	SHA256 hash	Malware sample
4c23cabcb529721e349568581f730586	MD5 hash	Malware sample
2bff9d483420df2f41c7eba232c6d90853df6acfe9f9b163af5d3495ea082229	SHA256 hash	Malware sample
7c68b89340b21aed5a708cc9e9c3b392	MD5 hash	Malware sample

d4062e34b2ebd654b3dca215ec740c6f1a305ea567f6d65ddee58f540ec5beea	SHA256 hash	Malware sample
66e6f022ac8f3cdce9128aa0c5bbbbd2	MD5 hash	Malware sample
530fe2e0f839c4b601627a1100e38708ff95a69d8382b11cefce45149c30ddef	SHA256 hash	Malware sample
58e947d184f23bd86fba141fe64f5fc2	MD5 hash	Malware sample
59f0e747d6241c1013526c7e76ecd95ab2a22aaced595cd65c5ef3955a63bf92	SHA256 hash	Malware sample
758ed8f5044feeb7caeed96cfa4a929b	MD5 hash	Malware sample
3e42ded1cd2447b921b41afa53f36bf645a21193ed24e3adeaef1a7217210545	SHA256 hash	Malware sample
0a92daa19f2cc77a21cdbf8db6d8bb68	MD5 hash	Malware sample
ab097e8b19ec166a2ff65d10ab06a8d572216cee2b0c44ebe183a8cb60b2bae7	SHA256 hash	Malware sample
504beaa3730a60f65a4c55c5d0fd0f8d	MD5 hash	Malware sample
b1ea7524a80b9740df7e51c1010ba1a04f11c15d6392f5054dc40c8952290474	SHA256 hash	Malware sample
f549afdef741a0d6b2090c1192ab7a6c	MD5 hash	Malware sample
602da3639eeb39cdbc657aa5e75eba74735314e8a54727697abcd3884c8b6d8c	SHA256 hash	Malware sample
804cab7d5c46d27529b2af821d16564b	MD5 hash	Malware sample
c820fc37abaf946804b09033f51216a28cdefe17020722d2fc2f1f74b4963ef5	SHA256 hash	Malware sample
07b04f23fa69d5043cc9b082430cacc4	MD5 hash	Malware sample
683b7b2abf9dc1e9fdf04e33570f5d8bfbb465dac613570200c2ec92201cc85d	SHA256 hash	Malware sample
80dd41609ba3c3a43babe9fbd5d7480e	MD5 hash	Malware sample
04d2326212724fdfa41c8e7ee64e32b60ba5e058e54d3fa0cf756b1378e948b9	SHA256 hash	Malware sample

0e0e9422103858d89f4b49d66f32e29a	MD5 hash	Malware sample
9f8db7e1320389297c451ca762edc8b8c990cab86f1c976b63e8312408e2a554	SHA256 hash	Malware sample
7991ecbd1e532f67c2e9139097eb41f4	MD5 hash	Malware sample
821bb1dcc6c7c529f3865f7c3e3b45ef058e32723d8300adea743d39864b3d9c	SHA256 hash	Malware sample
7f9c454a2e016e533e181d53eba113bc	MD5 hash	Malware sample
c7dc529d8aae76b4e797e4e9e3ea7cd69669e6c3bb3f94d80f1974d1b9f69378	SHA256 hash	Malware sample
879a7a2069bd5764704c72c3ee974cd8	MD5 hash	Malware sample
b24ea7ef47994c2ee340e1bc971eaa9e1992f0d2aaece99f3a9381655509047b	SHA256 hash	Malware sample
69d514f0609e232044794a84f4dd51d9	MD5 hash	Malware sample
23c41bbb1055ba7b15dcb1d1ba9bf426ef73f57641b47865c656b9338181e67b	SHA256 hash	Malware sample
d6443e691b7608eae245943e3535fc25	MD5 hash	Malware sample
4287592dc66083613b642bd04b1c8c49df56edc7691d79de0bca645d3af0d5c3	SHA256 hash	Malware sample
7a502a032b0e56e2190752e50102c8cf	MD5 hash	Malware sample
7ff292c689c421394483c7bc4c0b6620b8cedd4fd70f8f8ef1f4fa334d418be8	SHA256 hash	Malware sample
7f3cc059ffc6c11fe42695e5f19553ab	MD5 hash	Malware sample
b4c05e0e065058ae79d3ce9d51a470946aae036d2b163f85adcef10a6343246a	SHA256 hash	Malware sample
5f876124a2f53c93eff9509d36a936b2	MD5 hash	Malware sample
e4febefe210e39c3570ac71e41b66557c257713d386acd7898af195a1bacf83d	SHA256 hash	Malware sample
1856df9370ada9569a1afb6b52863d6d	MD5 hash	Malware sample

77ea107525233afa3f43b8695b39bfc41919f026ab3526bb3b9841737bbb20c7	SHA256 hash	Malware sample
2a1609ef72f07abc97092cb456998e43	MD5 hash	Malware sample
038d31670f03d386e6f3affe331bf76cb894d695b0f9012d828db9413c223a07	SHA256 hash	Malware sample
2271eeaeeebfb638f74c5b60c32fc98b	MD5 hash	Malware sample
4da7781d443ffde85e0aaf3d6e8effb6fc8cdffeead56b5ba3183472c40bf6ff	SHA256 hash	Malware sample

Table 6. Indicators for the CryptoLocker malware.