McAfee Labs Threat Advisory

Ransom Cryptolocker

June 22, 2018

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics, and symptoms that may be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive "Malware and Threat Reports" at the following URL**:** https://sns.secure.mcafee.com/signup_login.

Summary

Ransom Cryptolocker is a ransomware that on execution locks the user's system, thereby leaving the system in an unusable state. It also encrypts the list of file types present in the user's system. The compromised user has to pay the attacker with a ransom to unlock the system and to get the files decrypted.

McAfee detects this threat under the following detection name[s]:

- Ransom-[Variant Name]!partialMD5

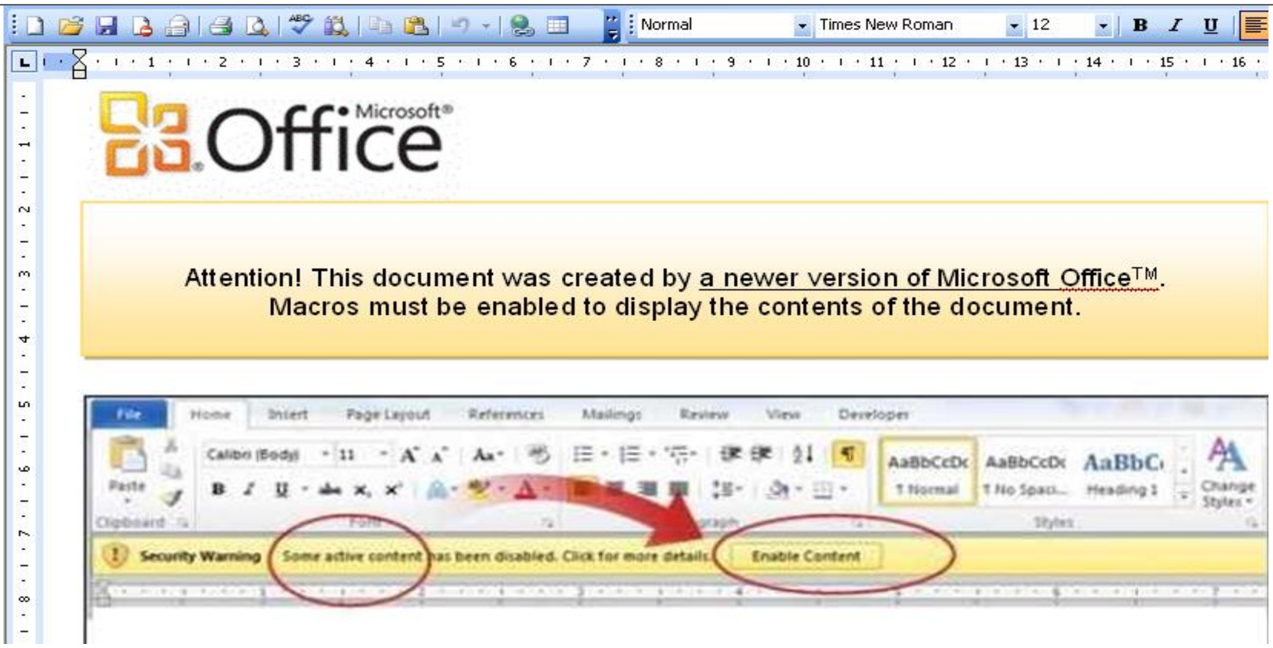
Detailed information about the threat, its propagation, characteristics, and mitigation are in the following sections:

Infection and Propagation Vectors

The malware is being propagated via malicious links in spam emails, which leads to pages exploiting common system vulnerabilities. These exploit pages will drop Ransom Cryptolocker and other malicious executable files on the affected machine.

A recent variant of the malware is still using spam as a propagation vector, but instead of links to exploit sites, it comes with an attachment in the form of a Word file. The Word document contains a VB macro that will download the malware directly to the user's machine.

When opened, the document will attempt to disguise as a valid Microsoft Office warning telling the user to enable Macros, like in the following example:



Attention! This document was created by a newer version of Microsoft Office™.
Macros must be enabled to display the contents of the document.

Security Warning Some active content has been disabled. Click for more details. Enable Content

Figure 1: Office document with Macro

The spam message is targeting mainly users in the Netherlands, even though infections can occur anywhere due to the methods used in propagation. The Subjects seen so far include these:

- Den Haag - Incassoburea Nederland.
- Den Haag - Intrum Justitia
- Den Haag - Intrum Incasso
- Den Haag Incasso Nederland.
- INCASSO NEDERLAND.
- *INCASSO* NEDERLAND.

The attachments are .doc or .zip files that may be named as one of the following examples:

- Order5611041101.doc
- Order561104146.doc
- Order561104112.zip
- Order561104133.zip
- Processing1011201435.doc
- Processing1011201435.zip

The malicious documents being used in these spam campaigns are detected by the following name[s]:

- W97M/Downloader.[variant name]

Coverage for the above mentioned detection names are available from the production DAT 7623.

Mitigation

Mitigating the threat at multiple levels such as file, registry, and URL could be achieved at various layers of McAfee products. Browse the product guidelines available here (click **Knowledge Center**, and select **Product Documentation** from the Content Source list) to mitigate the threats based on the behavior described below in the “Characteristics and symptoms” section.

Refer the following KB articles to configure Access Protection rules in VirusScan Enterprise:

- KB81095 - How to create a user-defined Access Protection Rule from a VSE 8.x or ePO 5.x console
- KB54812 - How to use wildcards when creating exclusions in VirusScan Enterprise 8.x

Ransom Cryptolocker usually installs itself into the Application Data folder. However, the new variant is installed in the C:\Windows folder with a random filename, like the following example:

- C:\WINDOWS\ixineden.exe

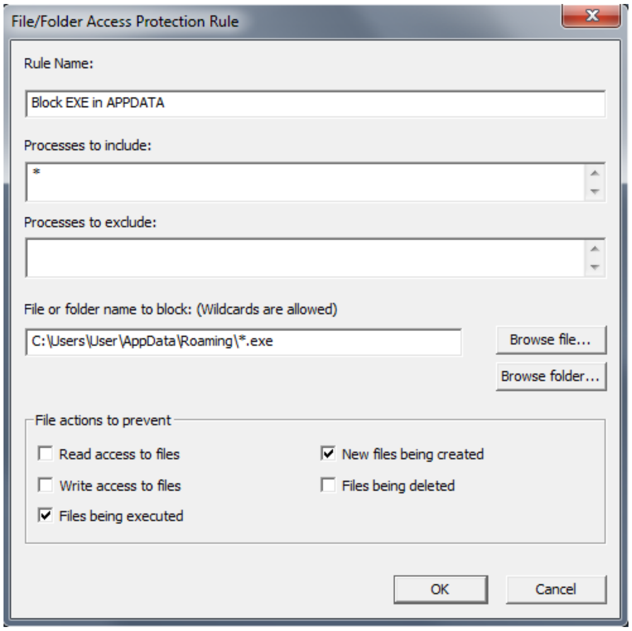
It also creates a folder in %APPDATA% to save its configuration files:

- C:\Documents and Settings\All Users\Application Data\oziqemegewypyvuh

Users can configure and test Access Protection Rules to restrict the creation of new files and folders when there are no other legitimate uses.

Select **New files being created** and add the following file location in **File or folder name to block**:

- [OS installed drive]\Documents and Settings\[logged in user]\ Application Data*.exe [For windows XP]
- [OS installed drive]\Users\[logged in user]\AppData\Roaming *.exe [For Windows 7]



File/Folder Access Protection Rule

Rule Name:

Block EXE in APPDATA

Processes to include:

*

Processes to exclude:

File or folder name to block: (Wildcards are allowed)

C:\Users\User\AppData\Roaming\*.exe

File actions to prevent

□ Read access to files ☑ New files being created

□ Write access to files □ Files being deleted

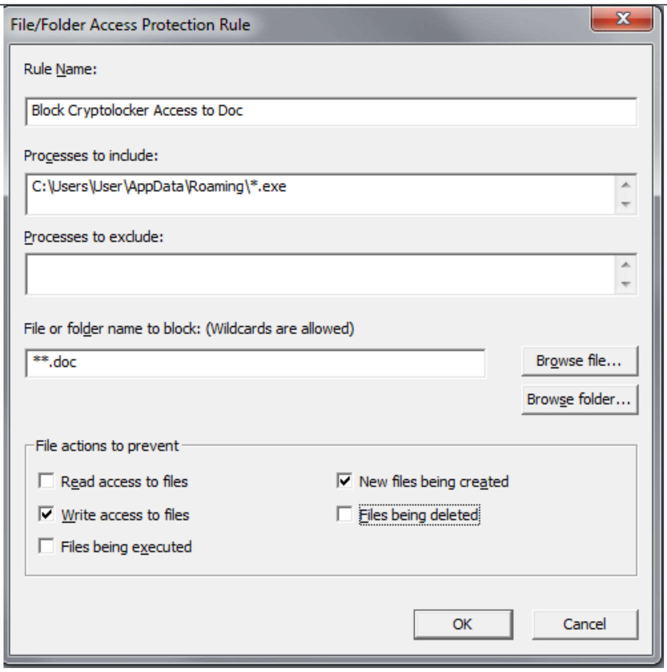
☑ Files being executed

It is also recommended that you select and test the **Files being executed** option for the above folders, and add only known legitimate programs under the Application Data folder to **Processes to exclude**.

Also, users can configure Access Protection Rules to prevent the files from being encrypted by the Cryptolocker.

Select **Write access to files** and **New files being created**. Include the following file location in **Processes to include**:

- [OS installed drive]\Documents and Settings\[logged in user]\ Application Data*.exe [For windows XP]
- [OS installed drive]\Users\[logged in user]\AppData\Roaming *.exe [For Windows 7]



Rule Name: Block Cryptolocker Access to Doc

Processes to include: C:\Users\User\AppData\Roaming\*.exe

Processes to exclude:

File or folder name to block: (Wildcards are allowed) **.doc

File actions to prevent

- ☐ Read access to files
- ☑ Write access to files
- ☐ Files being executed
- ☑ New files being created
- ☐ Files being deleted

Similarly, add the file type in **File or folder name to block** to prevent the encryption. Users can configure similar rules for all other file types that are encrypted by Cryptolocker.

For blocking all types of files being modified by Cryptolocker, use:

- [OS installed drive]\Documents and Settings\[logged in user]\ Application Data*.* [For windows XP]***
- [OS installed drive]\Users\[logged in user]\AppData\Roaming *.* [For Windows 7]***

HIPS
To blacklist applications using a Host Intrusion Prevention custom signature, refer to KB71329.
To create an application blocking rules policies to prevent the binary from running, refer to KB71794.
To create an application blocking rules policies that prevents a specific executable from hooking any other executable, refer to KB71794.

***** Disclaimer:** Use of ***.*** in an access protection rule would prevent all types of files from running and being accessed from that specific location. If specifying a process path under **Processes to Include**, the use of wildcards for Folder Names may lead to unexpected behavior. Users are requested to make this rule as specific as possible.

New Variant (November 2014)

Because the new variant uses spam attachments to spread, users may want to follow some other mitigation procedures to avoid this threat:

- Instruct users to not open unknown or unsolicited attachments.
- Ensure Microsoft Office Security policies for macros are set to High or Very High.
- Ensure GTI is enabled on gateway devices and endpoints.
- Ensure there are no allow list policies that exempt .doc/.docx attachments from spam/AV scanning.

Deny messages with the following subjects:

- Den Haag - Incassoburea Nederland.
- Den Haag - Intrum Justitia
- Den Haag - Intrum Incasso
- Den Haag Incasso Nederland.
- INCASSO NEDERLAND.
- *INCASSO* NEDERLAND.

Users of the following products may want to check if GTI is enabled in order to block the IP addresses being used to send spam:

- SaaS
- Email & Web Security 5.6
- Email Gateway (7.x or later) 7.5
- Email Gateway (7.x or later) 7.0
- GroupShield for Microsoft Exchange 7.0.x

Desktop users need to enable the Outlook plugin and also install the Site Advisor browser plugin to detect the spam attachment before it is opened and block access to the malicious domains.

Characteristics and Symptoms

Description

Ransom Cryptolocker belongs to a family of malware that encrypts the compromised user files available in the system and demands the user to pay a ransom to retrieve the files. The contents of the original files are encrypted using AES Algorithm with a randomly generated key.

Once the system is infected, the malware binary first tries to connect to a hard coded command and control server with IP address 184.164.136.134. If this attempt fails, it generates a domain name using random domain name algorithm and appends it with one among the following domain names:

- .org
- .net
- .co.uk
- .info
- .com
- .biz
- .ru

Once the system initiates the communication with the remote C&C server, the malware binary proceeds to the next step, which is to encrypt the compromised user files in the system. After generating the AES encryption key and submitting it to the C&C server, the malware binary searches for the below mentioned file types in the user system fixed and removable devices.

List of file types the malware encrypts:

*.odt	*.xls	*.pst	img_*.jpg	*.mrf	*.cer
*.ods	*.xlsx	*.dwg	*.dng	*.nef	*.crt
*.odp	*.xlsm	*.dxf	*.arw	*.nrw	*.pem
*.odm	*.xlsb	*.dxg	*.srf	*.orf	*.pfx
*.odc	*.xlk	*.wpd	*.bay	*.raf	*.eps
*.odb	*.ppt	*.rtf	*.crw	*.raw	*.indd
*.doc	*.pptx	*.mdf	*.dcr	*.ptx	*.cdr
*.docx	*.pptm	*.dbf	*.kdc	*.pef	????????.jpg
*.docm	*.mdb	*.psd	*.erf	*.srw	????????.jpe
*.wps	*.accdb	*.pdd	*.mef	*.der	

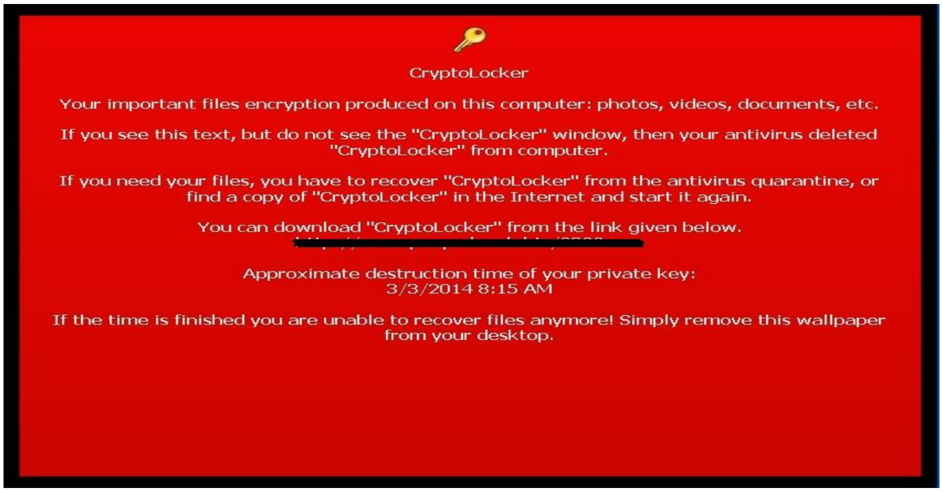
Encryption Technique

The malware uses an AES algorithm to encrypt the files. The malware first generates a 256-bit AES key and this will be used to encrypt the files. In order to be able to decrypt the files, the malware author needs to know that key. To avoid transmitting the key in clear text, the malware will encrypt it using an asymmetric key algorithm, namely the RSA public/private key pair.

This newly generated AES key is encrypted using the unique RSA public key created by the malware author and present in the malicious executable. This encrypted key is then submitted to the C&C server. The only way to recover the key after the malware finishes executing is by having the RSA private key associated with the public key used.

This key is only known to the malware author, and is never transmitted via the network or present in the infected machine. Hence, it's impossible to recover the user's encrypted files without that key after they have been infected.

Once the system is compromised, the malware displays the below mentioned warning to the user and demand ransom to decrypt the files.



CryptoLocker

Your important files encryption produced on this computer: photos, videos, documents, etc.

If you see this text, but do not see the "CryptoLocker" window, then your antivirus deleted "CryptoLocker" from computer.

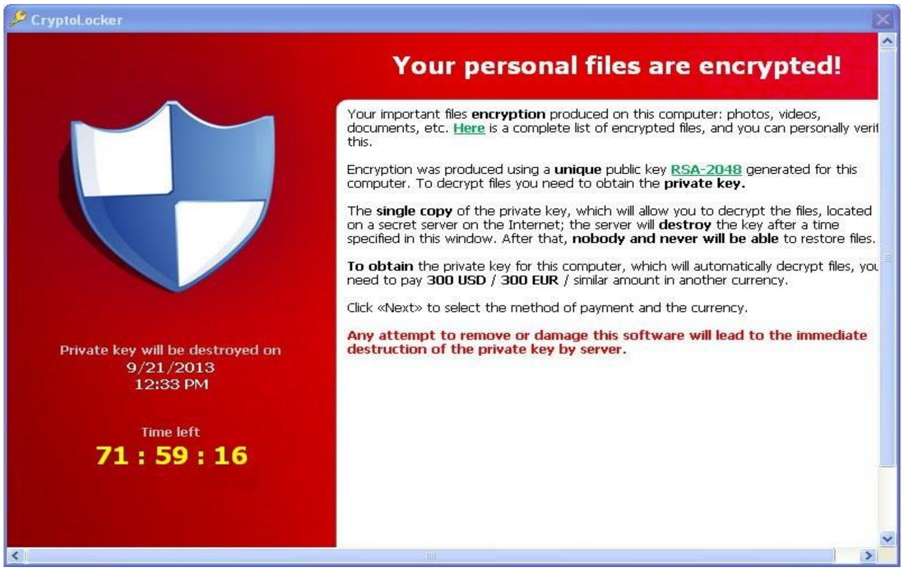
If you need your files, you have to recover "CryptoLocker" from the antivirus quarantine, or find a copy of "CryptoLocker" in the Internet and start it again.

You can download "CryptoLocker" from the link given below.
[redacted]

Approximate destruction time of your private key:
3/3/2014 8:15 AM

If the time is finished you are unable to recover files anymore! Simply remove this wallpaper from your desktop.

Figure 2: Ransom Cryptolocker Desktop wallpaper



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verit this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files.

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

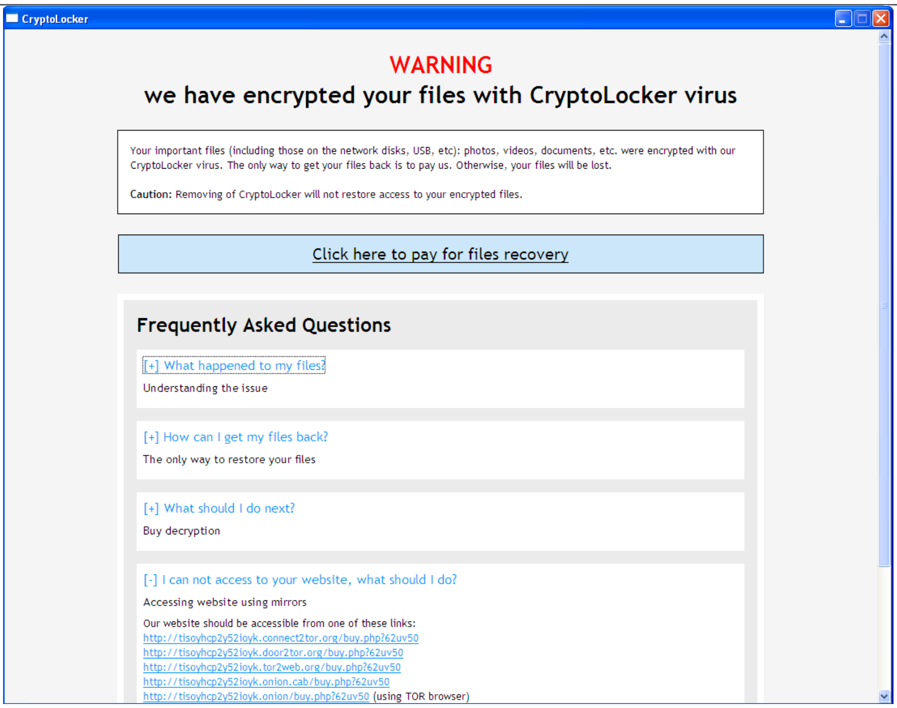
Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
9/21/2013
12:33 PM

Time left
71 : 59 : 16

Figure 3: Ransom Cryptolocker Warning Message



WARNING

we have encrypted your files with CryptoLocker virus

Your important files (including those on the network disks, USB, etc): photos, videos, documents, etc. were encrypted with our CryptoLocker virus. The only way to get your files back is to pay us. Otherwise, your files will be lost.

Caution: Removing of CryptoLocker will not restore access to your encrypted files.

Click here to pay for files recovery

Frequently Asked Questions

[+] What happened to my files?

Understanding the issue

[+] How can I get my files back?

The only way to restore your files

[+] What should I do next?

Buy decryption

[-] I can not access to your website, what should I do?

Accessing website using mirrors

Our website should be accessible from one of these links:
http://tisoyhcp2y52ioyk.connect2tor.org/buy.php?62uv50
http://tisoyhcp2y52ioyk.door2tor.org/buy.php?62uv50
http://tisoyhcp2y52ioyk.tor2web.org/buy.php?62uv50
http://tisoyhcp2y52ioyk.onion.cab/buy.php?62uv50
http://tisoyhcp2y52ioyk.onion/buy.php?62uv50 (using TOR browser)

Figure 4: New variant of Cryptolocker targeting Dutch users.

It maintains the list of files that were encrypted by this malware under the following registry entry:

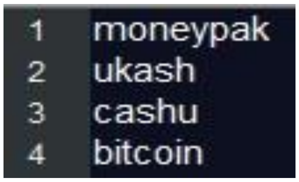
- HKEY_CURRENT_USER\Software\CryptoLocker\Files

On execution, this malware binary copies itself to %AppData% location and deletes itself using a batch file:

- %AppData%\{2E376276-3A5A-0712-2BE2-FBF2CFF7ECD5}.exe

NOTE: %AppData% refers to the current user's Application data location.

The malware author receives the ransom amount from the compromised user from one among the following payment methods:



1 moneypak
2 ukash
3 cashu
4 bitcoin

Figure 4. Payment methods used by the attackers

Network Connections
Cryptolocker uses the DGA (Domain Generation Algorithm) to generate the Random Domain names hourly based.

The following are some of the observed domains of the C&C servers:

soudpmiyvxmd.org	wxfaxwfotkcp.co.uk	avlpfgiqwdudk.info	irvggrirvsqqy.com
gbpboroxfiep.co.uk	xvaqocjidsht.info	ngmneoxxoisqk.com	jnwsjavtnkvmh.net
ofoauksakmgs.info	soywduppiyvf.com	udsmjlwhfkmeg.net	dyddkwwieairg.biz
crjxtpyytwxf.com	tmtntatjrhbj.net	intkitmowpkrw.biz	euepnfkkvrnnf.ru
qgyvutxttqaj.net	upjsdeujrdpv.biz	vlqtsbjlaojjg.ru	ehbktmjmyefwg.org
estttyesdbrv.biz	vnejtjydblua.ru	jvrrrjysrthwg.org	fdcwwuwoqvkso.co.uk

uwuexnaukgiy.ru	ynnivqvmcyxxr.org	hjxywcvnbotlg.co.uk	fxcyhrpfigvcu.info
vupuoseotond.org	mxoguylttevli.co.uk	ifylakjpsgyhf.info	sidwgwvsyqlxu.com
hdauthcpbwblw.net	oxibtrwnccaej.org	ntmpidpuhvjxm.com	pykluscfamoho.biz
unbssmidrhqhn.biz	dsfyhcdkeiprs.co.uk	opnclitaxswlu.net	qulxxxgkqjcun.ru
bnhdumqalrkij.ru	qdgwghjxusfnj.info	igemsolqdaotb.org	jjrtvxqpkhxem.org
loppindadxdnv.info	mkqclshftuqbu.com	tnfhkwqywydsb.net	hxgfjfggoebgr.biz
uvdotgvjluqgb.ru			

New Variant (November 2014)

As of November 2014 a new variant of Cryptolocker was found targeting users in the Netherlands. This new variant performs basically the same actions as previous ones, but with some important differences.

The threat is now using VB macros in .doc files attached to email to spread. The documents need to be opened by the user, and macros must be active for the download to occur.

Once the macro is enabled, the following domain will be contacted to download the actual Cryptolocker sample:

- Hxxp : // imagecenterdown.ru / info.png
- Hxxp : // officeimage.ru / a.png
- Hxxp : // officeimage.ru / b.png
- Hxxp : // officeimage.ru / image.png

The sample will be executed and will inject itself into Explorer before executing the malicious functions.

The first action after running is to contact the following site to post the generated key and receive information about the infection:

- Deadwalk32.ru

It also tries to delete any information about Shadow Copy to avoid files being recovered by the user:

- vssadmin.exe Delete Shadows /All /Quiet

Another change from the previous version is that this one seems to be capable of stealing contacts from local email clients to send spam. The malware will scan the system for the following files and registry keys to collect email addresses:

- eabook.mab
- history.mab
- Thunderbird\Profiles\

- HKCU\Software\Microsoft\Internet Account Manager\Accounts\00000001
- HKCU\Software\Microsoft\Internet Account Manager
- HKCU\Software\Microsoft\Office\Outlook\OMI Account Manager\Accounts
- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Microsoft Outlook Internet Settings
- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook

After that, as in previous variants, the malware will start encrypting all files with specific extensions on the machine, adding the extension .encrypted to them.

Restart Mechanism

The following registry entry would enable the Trojan to execute every time when Windows starts:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\
    - CryptoLocker "%AppData%\{2E376276-3A5A-0712-2BE2-FBF2CFF7ECD5}.exe"

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
    - ywupytit: "C:\WINDOWS\ufivehen.exe"

Getting Help from the McAfee Foundstone Services team

This document is intended to provide a summary of current intelligence and best practices to ensure the highest level of protection from your McAfee security solution. The McAfee Foundstone Services team offers a full range of strategic and technical consulting services that can further help to ensure you identify security risk and build effective solutions to remediate security vulnerabilities.

You can reach them here: https://secure.mcafee.com/apps/services/services-contact.aspx

This Advisory is for the education and convenience of McAfee customers. We try to ensure the accuracy, relevance, and timeliness of the information and events described; they are subject to change without notice.

Together is power.