McAfee Labs Threat Advisory

Ransomware-Locky

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

Ransomware-Locky is a ransomware that encrypts certain file types present on the user's system upon execution. The compromised user must pay a ransom to the attacker to get the files decrypted.

McAfee detects this threat under the following detection name:

- Ransomware-Locky

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

- Infection and Propagation Vectors
- Mitigation
- Characteristics and Symptoms
- Restart Mechanism
- Indicators of Compromise (IOC)
- McAfee Foundstone Services

Infection and Propagation Vectors

Ransomware-Locky has primarily used spam emails in the past for its propagation. These spam emails can contain two types of attachments: an archive consisting of either:

1. Malicious JavaScript/VBScript or
2. Malicious Microsoft Office documents (MS Word or Excel file) or PDF documents.

The purpose of both types of malicious attachments is to download and execute Ransomware-Locky files on the target system.

The attachments in the spam emails are Office document files or Archives, some of which may be named, but are not limited, to one of the following:

- invoice_J-12345678.doc
- 724971.docm
- 413941.docm
- 672082.docm
- 490481.docm
- Rechnung-54-110090.xls
- paychecks exported 4D8A52B1.js
- FedEx_0000717240.doc.js
- Refund_Payment_Details_0000679553.doc.js
- Cancellation Form 6328B32E.js
- 0000e06b.js
- 0000f3dd.js

- 0000e073.js
- 0000f3fb.js
- DOC-20161005-WA0002715.wsf
- paperwork scan ~1EB91.wsf
- 7076430404.vbs
- 344412006.vbs
- 399621003.vbs
- 2863692201.vbs
- 13599503451008_5542894_841496.vbs
- 9667031904.vbs
- 013599385938287_3498504_974746.vbs
- 9040111301.vbs
- 6790591602.vbs
- 66287850.pdf
- a54ff3d6f.pdf
- a7a867810.pdf
- 03131169.pdf
- 84358917.pdf
- 4d7ab6179.pdf
- 93633060.pdf
- 26363e501.pdf
- 6b5827b76.pdf
- 9b4a9bbea.pdf
- 7df75af76.pdf
- c8d4fe8f9.pdf
- JPG_4115.7z
- JPG_0425.7z
- Scan_008_2162750514.rar
- noreply@narit.or.th_20170731_853997.rar
- Scan_0070_5784071340.rar
- Scan_009_3228955730.rar
- 13599789783241_4680873_675421.rar
- noreply@iwatani.co.jp_20170731_222426.rar
- 013599317033166_4490029_950073.rar
- noreply@surfsponge.com_20170731_808835.rar
- Scan_005_1206610482.rar
- July-August2017.rar

The subjects used in the spam campaign may be named, but are not limited to, one of the following:

- ATTN: Invoice J-12345678
- Per E-Mail senden: Rechnung-54-110090.xls
- Invoice IN00000160V00008647772
- Your Order
- Document from Paige
- Please sign
- 03131169.pdf
- Paper
- Scanned image from MX-2600N
- Voice Message Attached from 01317033166 - name unavailable
- JPG_0425
- Outstanding invoices email 1 of 2
- < No Subject > (Some malspam is also sent without a Subject)

Mitigation

Mitigating the threat at multiple levels, such as file, registry, and URL, can 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 to the following Knowledge Base 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

Emails from unknown senders should be treated with caution. If an email looks strange, do the following: ignore it, delete it, and never open attachments or click on URLs. Opening file attachments, especially from unknown senders, harbors risks. Attachments should first be scanned with an antivirus program and, if necessary, deleted without being opened.

Never click links in emails without checking the URL. Many email programs permit the actual target of the link to be seen by hovering the mouse over the visible link without clicking on it (called the mouse-over function).

Macros can run in an Office application only if Macro Settings are set to "Enable all macros" or if the user manually enables a macro. By default, it will be in a disabled state.

McAfee recommends that users use the default macro setting in Office applications to avoid further infection. Also, users should be warned to be cautious with documents requesting to activate macros by clicking "Enable Content" or "Enable Macros" buttons in Microsoft Office. These days, most malicious documents contain a message requesting the user to click on the mentioned buttons.

Furthermore, Microsoft has released a new feature in Microsoft Office 2016, which can help enterprise administrators configure proper group policies to prevent users from activating macros in high-risk scenarios. More information and a guide of how to enable this feature is available at the official Microsoft TechNet blog site: https://blogs.technet.microsoft.com/mmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/.

Microsoft also recommends the following:
"If your enterprise does not have any workflows that involve the use of macros, disable them completely. This is the most comprehensive mitigation that you can implement today."

Please refer to the following URL to learn more about malicious Office files:

https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25689/en_US/McAfee_Labs_Threat_Advisory-W97MDownloader_X97MDownloader.pdf

Additional End User Recommendations

- **Do NOT open Office document file attachments unless specifically requested from the sender**. View the email header or send a separate email to validate the sender before opening attachments.

- **Disable Macro in Microsoft Office applications**. Macros can run in Office applications only if the Macro Settings are set to "Enable all macros" or if the user manually enables a macro. By default, it will be in a disabled state. The recommended setting is to select the option "Disable all macros with notification" in "Macro Settings."

- **End users should back up business data to the organization's shared folders**. Data residing on user devices may be permanently lost in the event of a ransomware infection.

- **Report suspect email to the organization's Security Operations Center**. Remind your employees how and where to submit suspicious email safely.

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

Disclaimer: This option is dangerous and needs to be tested before deployment because it can block legitimate applications, but it is effective against an infection scenario.

- Block registry key/value creation under "HKCU\Software\locky":

Registry Access Protection Rule ✕

Rule Name:

Locky Key Creation

Processes to include:

*

Processes to exclude:

Registry key or value to protect:

HKCU ▼   /software/locky

Registry key or value to protect:

- ⦿ Key
- ○ Value

Registry Actions to Block
- ☐ Write to key or value
- ☑ Create key or value
- ☐ Delete key or value

OK   Cancel

- Block a new file creation with the extension ".locky" by a process running from %temp% location:

File/Folder Access Protection Rule ✕

Rule Name:

File creation with extension ".locky"

Processes to include:

\temp.exe

Processes to exclude:

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

*.locky   Browse file...

Browse folder...

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

OK   Cancel

- Block a new file creation with extension ".zepto" by a process running from %temp% location:

File/Folder Access Protection Rule ✕

Rule Name:

```
File Creation with extension ".zepto"
```

Processes to include:

```
*\temp\*.exe
```

Processes to exclude:

```

```

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

```
*.zepto
```

[Browse file...]
[Browse folder...]

File actions to prevent

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

[OK] [Cancel]

As in the examples above, the same rule can be used to prevent new encrypted files from being created by the malware, but the "File or Folder name to block" option should be changed to match the new file extension. Different variants of locky have been known to create the following file extensions on disk:

- .locky
- .zepto
- .thor
- .odin
- .aesir
- . zzzzz
- .osiris
- .diablo6
- .lukitus
- .ykcol
- .asasin

- Block a new file creation with the extension ".odin" by the rundll32.exe process:

File/Folder Access Protection Rule

Rule Name:

File Creation with extension ".odin"

Processes to include:

rundll32.exe

Processes to exclude:

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

*.odin   Browse file...
           Browse folder...

File actions to prevent
☐ Read access to files   ☑ New files being created
☐ Write access to files   ☐ Files being deleted
☐ Files being executed

OK   Cancel

- Block a new file creation with extension ".diablo6" by a process running from %temp% location:

File/Folder Access Protection Rule   ✕

Rule Name:

Block file creation with extension ".diablo6"

Processes to include:

\temp.exe

Processes to exclude:

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

*.diablo6   Browse file...
              Browse folder...

File actions to prevent
☐ Read access to files   ☑ New files being created
☐ Write access to files   ☐ Files being deleted
☐ Files being executed

OK   Cancel

- Block a new file creation with extension ".lukitus" by a process running from %temp% location:

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.

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

Characteristics and Symptoms

Ransomware-Locky belongs to a family of Ransomware malware that encrypts the compromised user's files available in the system and demands the user to pay a ransom amount to retrieve the files. The contents of the original files are encrypted using an RSA-2048 and AES-1024 algorithm.

On execution, Ransomware-Locky usually copies itself into the %temp% folder with a randomly named ".exe" or ".dll" file:

- %temp%\<random name>.exe
- %temp%\<random name>.dll

For the .exe version, the malware will add the "Run" registry entry with a value name "Locky" with data pointing to the dropped file in the %temp% directory. The main malicious file will be deleted after it copies itself to the %temp% directory and executes the copied file.

In the ".odin" variant, Locky will download an encrypted DLL instead of the .exe file, which will then be decrypted and executed by using the legitimate Microsoft tool rundll32.exe by a command similar to the following:

- rundll32.exe %temp%\<random_filename>.dll, qwerty 323

The new process started from the %temp% directory generates a unique ID (Personal Identification ID) using following mechanism:

- Get volume GUID (windows drive) path.
    Ex: \\\\?\\Volume{a7c7xxxx-xxxx-11e0-aaa3-xxxxxx72696f}\\

- Calculate MD5 of the GUID
    Only GUID with braces considered for MD5 calculation
    "{a7c7xxxx-xxxx-11e0-aaa3-xxxxxx72696f}"
    MD5 of above GUID string: 50xx5BxxE7xx13xxC3xx0BxxCAxxE3xFC

- First 16 characters considered as Personal Identification ID
    Personal Identification ID: 50xx5BxxE7xx13xx
   xx – Redacted bytes

Ransomware-Locky also removes the volume shadow copies from the compromised system, thereby preventing the user from restoring the encrypted files. (Shadow copy is a Windows feature that helps users make backup copies—snapshots—of computer files or volumes.) Ransomware-Locky uses the following command to delete all the shadow volume copies on the computer:

    "vssadmin.exe Delete Shadows /All /Quiet"

Ransomware-Locky contacts the Command and Control (CnC) server to get the Public Key as well as recovery instruction text, and stores them in the registry.

POST request to get public key:
    id={machine-id}&act=getkey&affid={affiliate-id}&lang=en&corp={corporate-machine}&serv={is-server}&os={operating-system-name}&sp={service-pack-version}&x64={is-64-bit-system}

POST request to get recovery instructions:
    id={machine-id}&act=gettext&lang=en

NOTE: Malware encrypts the above POST request before posting it.
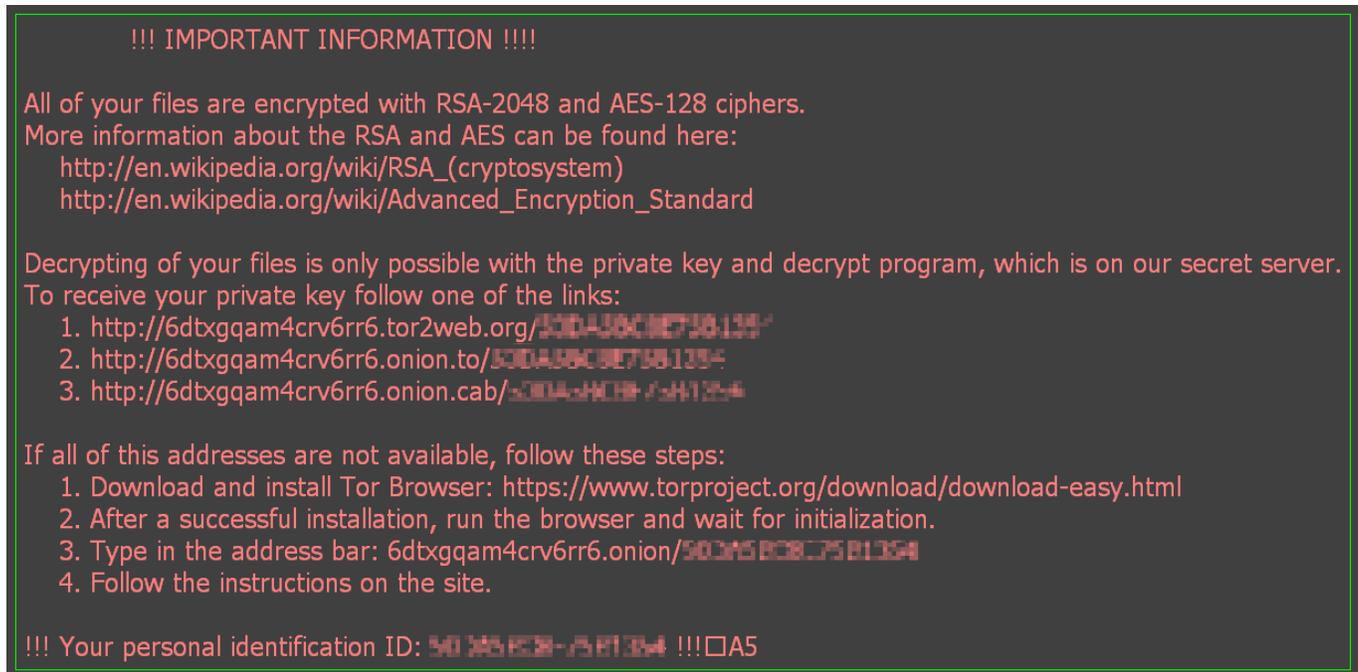
Ransomware-Locky encrypts the files with the following extensions:

    .asm, .c, .cpp, .h, .png, txt, .cs, .gif, .jpg, .rtf, .xml, .zip, .asc, .pdf, .rar, .bat, .mpeg, .qcow2, .vmdk .tar.bz2, .djvu, .jpeg, .tiff, .class, .java, .SQLITEDB, .SQLITE3, .lay6, .ms11, .sldm, .sldx, .ppsm, .ppsx, .ppam, .docb, .potx, .potm, .pptx, .pptm, .xltx, .xltm, .xlsx, .xlsm, .xlsb, .dotm, .dotx, .docm, .docx, wallet.dat etc.
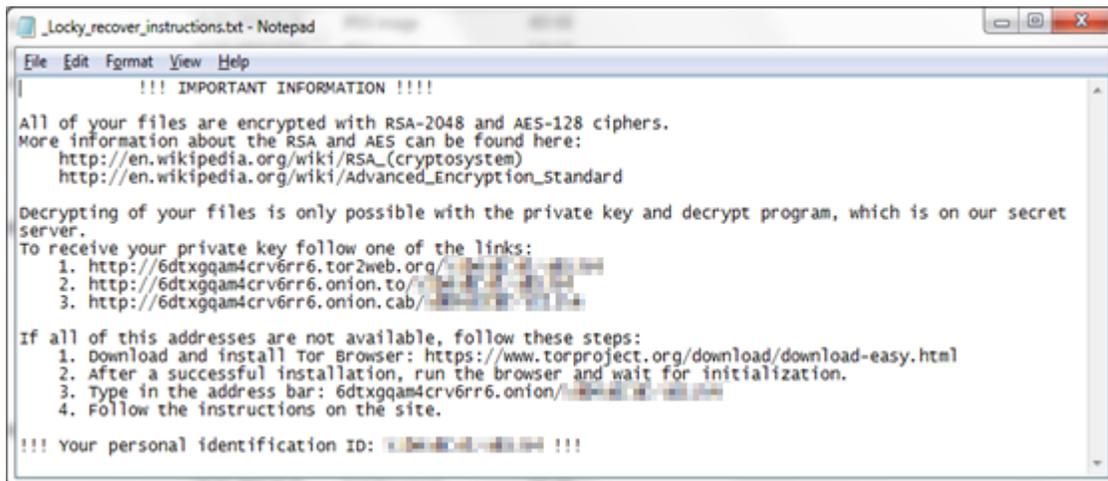
After encrypting the files, malware changes the desktop background with the recovery instruction image file and opens the text as well:

- _Locky_recover_instructions.bmp
- _Locky_recover_instructions.txt

_Locky_recover_instructions.bmp:

```
        !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
    http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
    1. http://6dtxgqam4crv6rr6.tor2web.org/████████████
    2. http://6dtxgqam4crv6rr6.onion.to/████████████
    3. http://6dtxgqam4crv6rr6.onion.cab/████████████

If all of this addresses are not available, follow these steps:
    1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
    2. After a successful installation, run the browser and wait for initialization.
    3. Type in the address bar: 6dtxgqam4crv6rr6.onion/████████████
    4. Follow the instructions on the site.

!!! Your personal identification ID: ████████████ !!!□A5
```

_Locky_recover_instructions.txt:

A new version of Locky creates recovery instructions in the following file names in desktop:

_HELP_instructions.bmp, _HOWDO_text.bmp
_HELP_instructions.html, _HOWDO_text.html

In other directories, the format changes as follows:

_{count maintained by malware}_HELP_instructions.html

_HELP_instructions.bmp, _HOWDO_text.bmp

_HELP_instructions.html, _HOWDO_text.html

Newer versions of Locky using the extensions ".diablo6" and ".lukitus" create a ransom note on the infected user's desktop named:

- Diablo6.htm, diablo6.bmp, diablo6-<random characters>.htm
- Lukitus.htm, lukitus.bmp

Although the file names for the ransom note differ, the content of the ransom notes are exactly the same as that of previous versions of Locky.

Onion site hosting Instructions on obtaining the Decryptor:

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
  "Locky" = "%TEMP%\<random name>.exe"

After the malware successfully completes encryption of the compromised system, it deletes itself from the %temp% directory and removes the "Run" registry entry.

Newer Versions of Locky (diablo6/lukitus variants) do not seem to have a restart mechanism. The intention is to encrypt the files on the target and display the ransom note to the target user (in the form of the htm, bmp file, or the desktop wallpaper) as soon as the ransomware is run by the infection vector.

Indicators of Compromise (IOC)

The following indicators can be used to identify potentially infected machines.

Registry keys added/modified by the malware:
- HKEY_CURRENT_USER\ Software\Microsoft\Windows\CurrentVersion\Run
  "Locky" = "%TEMP%\<random name>.exe"

- HKEY_CURRENT_USER\Software\Locky
  "id" = < Personal Identification ID>
  "pubkey" = <RSA public key received from the CnC Server>
  "paytext" = <Content of "Locky_recover_instructions.txt">
  "completed" = "0x1" [This value will be added after completion of encryption]

Presence of the following files on the system:
- _HELP_instructions.bmp
- _HOWDO_text.bmp
- _Locky_recover_instructions.bmp
- _HELP_instructions.html
- _HOWDO_text.html
- _Locky_recover_instructions.txt
- diablo6-<random characters>.htm, diablo6.bmp, diablo6.htm
- lukitus.htm
- lukitus.bmp

Attempted connection to the any of the following IP addresses:
- 95.181.171.58
- 185.14.30.97
- 195.22.28.196
- 195.22.28.198
- 31.210.120.156
- 182.92.220.92
- 109.237.111.179
- 109.237.111.179
- 109.237.111.179
- 185.17.120.130
- 185.17.120.130
- 185.75.46.220
- 185.75.46.220
- 185.80.148.137
- 185.80.148.137
- 192.162.103.213
- 192.162.103.213
- 192.162.103.213
- 31.202.128.249
- 31.202.128.249
- 78.108.93.185
- 78.108.93.185
- 78.108.93.185
- 91.228.239.216
- 91.228.239.216
- 78.155.205.46
- 119.28.100.249
- 212.109.220.109
- rtozottosdossder.net
- pvwinlrmwvccuo.eu
- cgavqeodnop.it
- kqlxtqptsmys.in
- wblejsfob.pw
- aboeon.net
- bdfxb.com

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.