McAfee Labs Threat Advisory

Ransomware-Locky

October 13, 2016

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.snssecure.mcafee.com/content/signup_login.

Summary

Ransomware-Locky is a ransomware, which upon execution, encrypts certain file types present in the user's system. The compromised user has to pay 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

The malware is being propagated via spam emails that come with an attachment in the form of a malicious Microsoft Office document file or a Java Script file disguised as documents. The malicious Office file contains a macro with the malicious code and the Java Script file contains the malicious code itself. In both cases the code is highly obfuscated and allows the malware to download and execute second-stage Ransomware-Locky files.

The malicious Office file or Java Script file usually arrives on the victim's machine as an attachment as part of spam or phish emails. The document files can be a Word document (.doc file or .docx file) or an Excel workbook (.xls file or .xlsx file). The files can arrive attached as a ZIP archive or directly attached to the email pretending to be legitimate documents.

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

- invoice_J-12345678.doc
- Rechnung-54-110090.xls
- paychecks exported 4D8A52B1.js
- FedEx_0000717240.doc.js
- Refund_Payment_Details_0000679553.doc.js
- Cancellation Form 6328B32E.js
- DOC-20161005-WA0002715.wsf
- paperwork scan ~1EB91.wsf

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

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 actually 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.

Intel Security 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 the 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. The recommended setting is to select the option "Disable all macros with notification" in "Macro Settings."

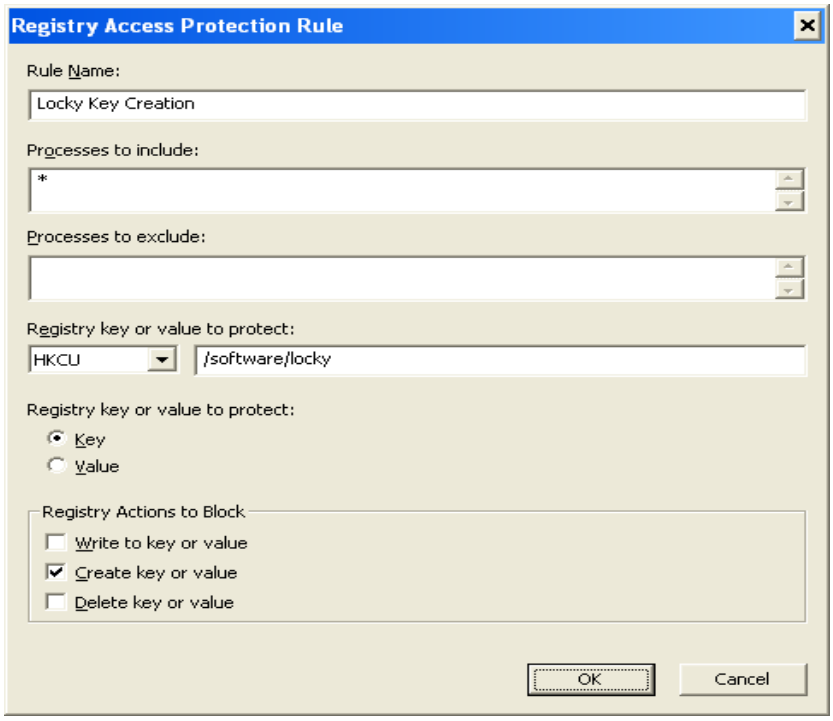
- **End users should back up business data to the organization's shared folders**. Data residing on user devices may be permanently lost in the event of a ransomware infection.

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

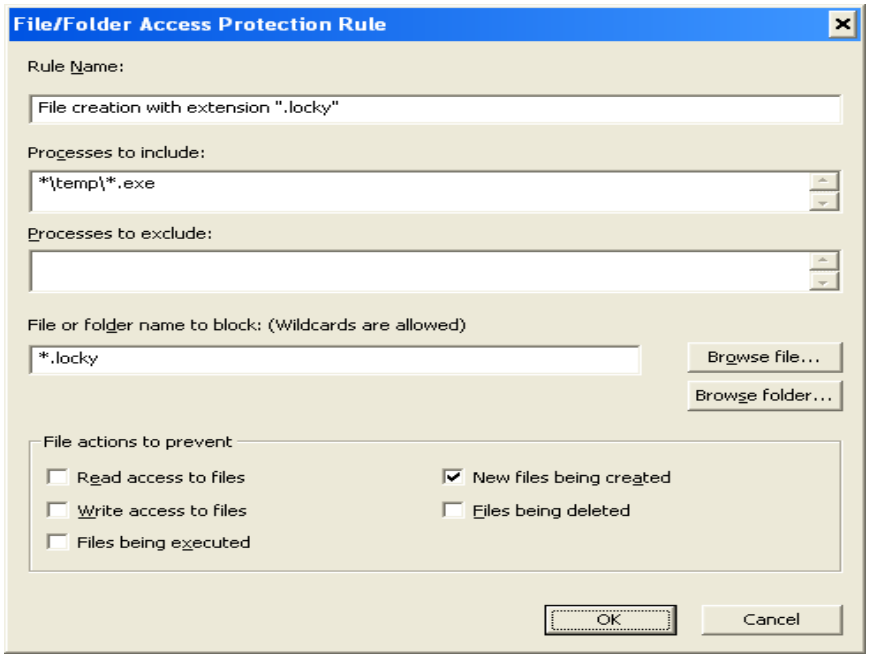
Users can configure and test Access Protection Rules to restrict the creation of new files and folders when there are no other legitimate uses.

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.

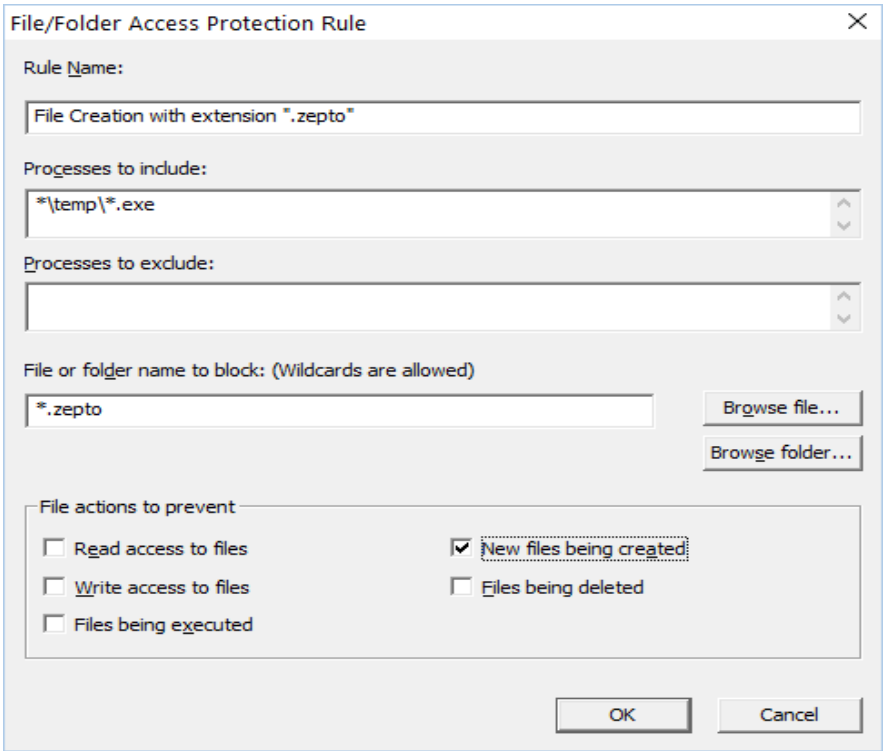
- Block registry key/value creation under "HKCU\Software\locky":



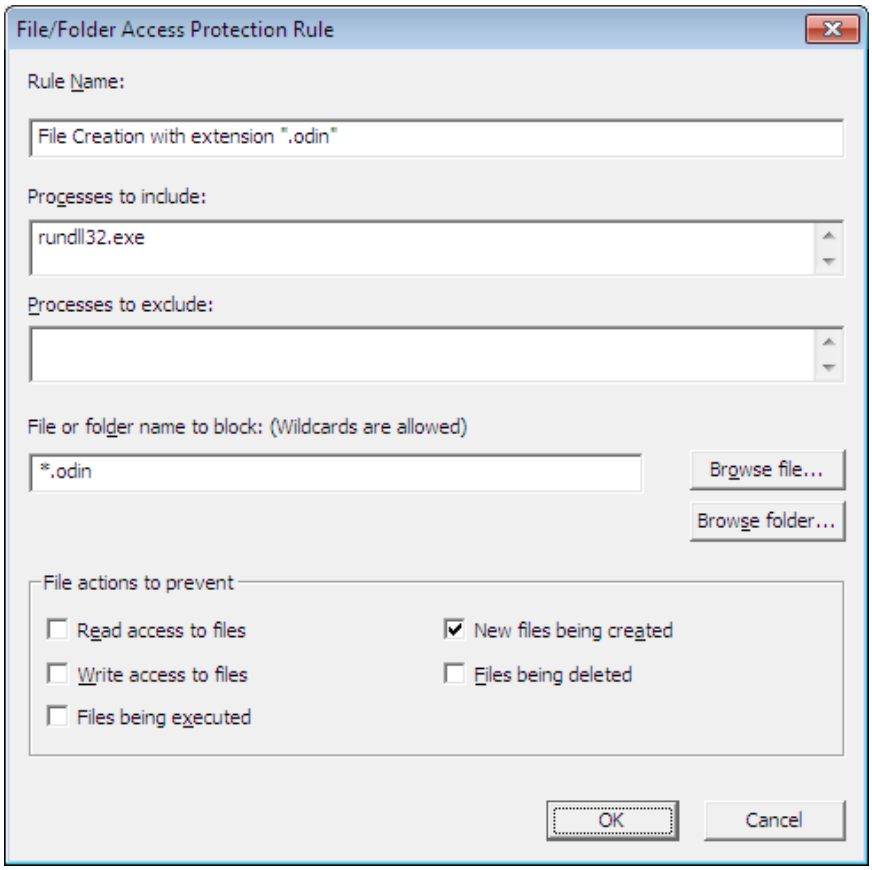
- Block a new file creation with the extension ".locky" by a process running from the %temp% location:



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



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



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 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

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 latest version, 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{a7c7a6b1-2d27-11e0-aaa3-806d6172696f}\\

- Calculate MD5 of the GUID
  Only GUID with braces considered for MD5 calculation
  "{a7c7a6b1-2d27-11e0-aaa3-806d6172696f}"
  MD5 of above GUID string: 50DA5BC8E75B1354C350BCACA54E3AFC

- First 16 characters considered as Personal Identification ID
  Personal Identification ID: 50DA5BC8E75B1354

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 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={personal_identifier}&act=getkey&affid={affiliate_id}&lang={language_code}&corp={is_enterprise_user}&serv={is_running_server_OS}&os={OS_name}&sp={servicepack_version}&x64={is_OS_64bit}

POST request to get recovery instructions:

- id={personal_identifier}&act=gettext&lang={language_code}

NOTE: Malware encrypts the above POST request before posting it.

Ransomware-Locky encrypts the files with the following extensions:

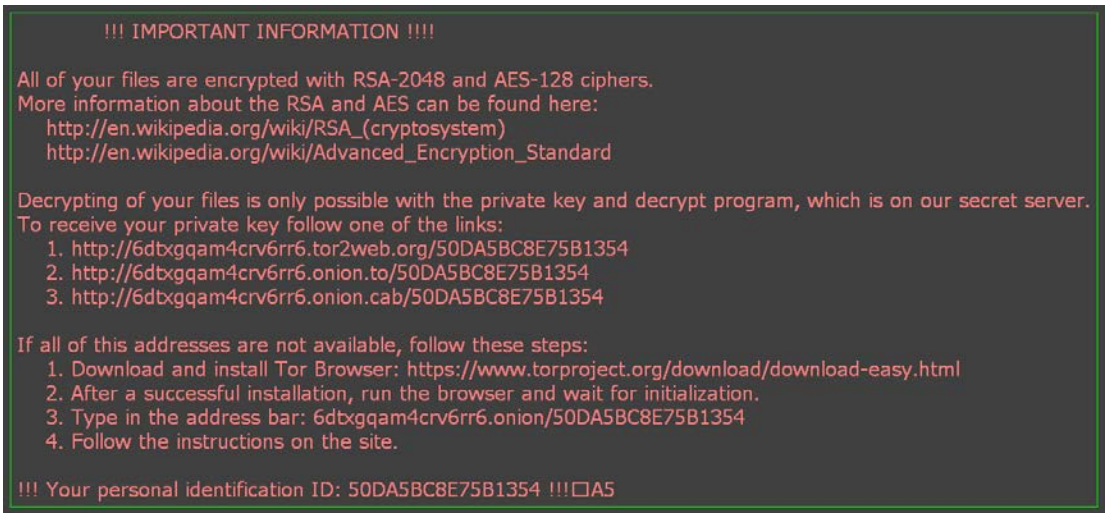
.asm, .c, .cpp, .h, .png, txt, .cs, .gif, .jpg, .rtf, .xml, .zip, .asc, .pdf, .rar, .bat, .mpeg, .qcow2, .vmdk .tar.bz2, .djvu, .jpeg, .tiff, .class, .java, .SQLITEDB, .SQLITE3, .lay6, .ms11, .sldm, .sldx, .ppsm, .ppsx, .ppam, .docb, .potx, .potm, .pptx, .pptm, .xltx, .xltm, .xlsx, .xlsm, .xlsb, .dotm, .dotx, .docm, .docx, wallet.dat and etc,.

NOTE: The latest version of Ransomware-Locky is able to encrypt files present on mapped drives, which are hard drives present on the network that have a drive letter assigned on the current system.

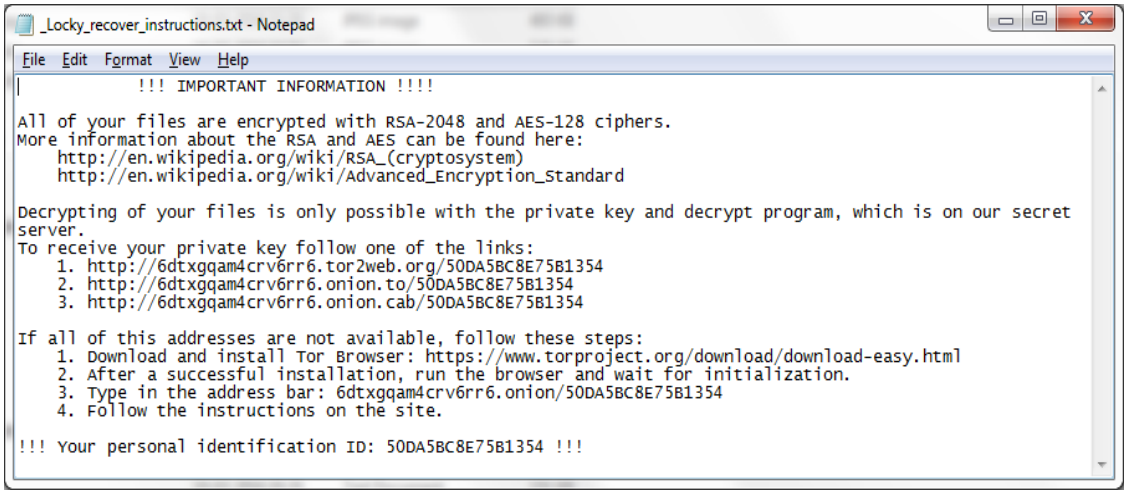
After encrypting the files, malware changes the desktop background with the recovery instruction image file and opens the text as well:

- _Locky_recover_instructions.bmp
- _Locky_recover_instructions.txt

_Locky_recover_instructions.bmp:



_Locky_recover_instructions.txt:

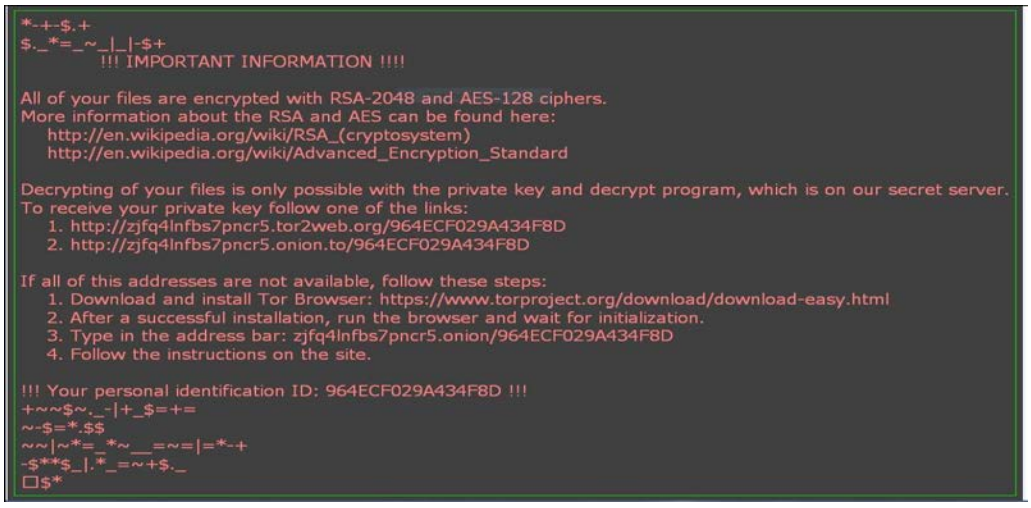


A new version of Locky creates recovery instructions in the following file names in desktop:

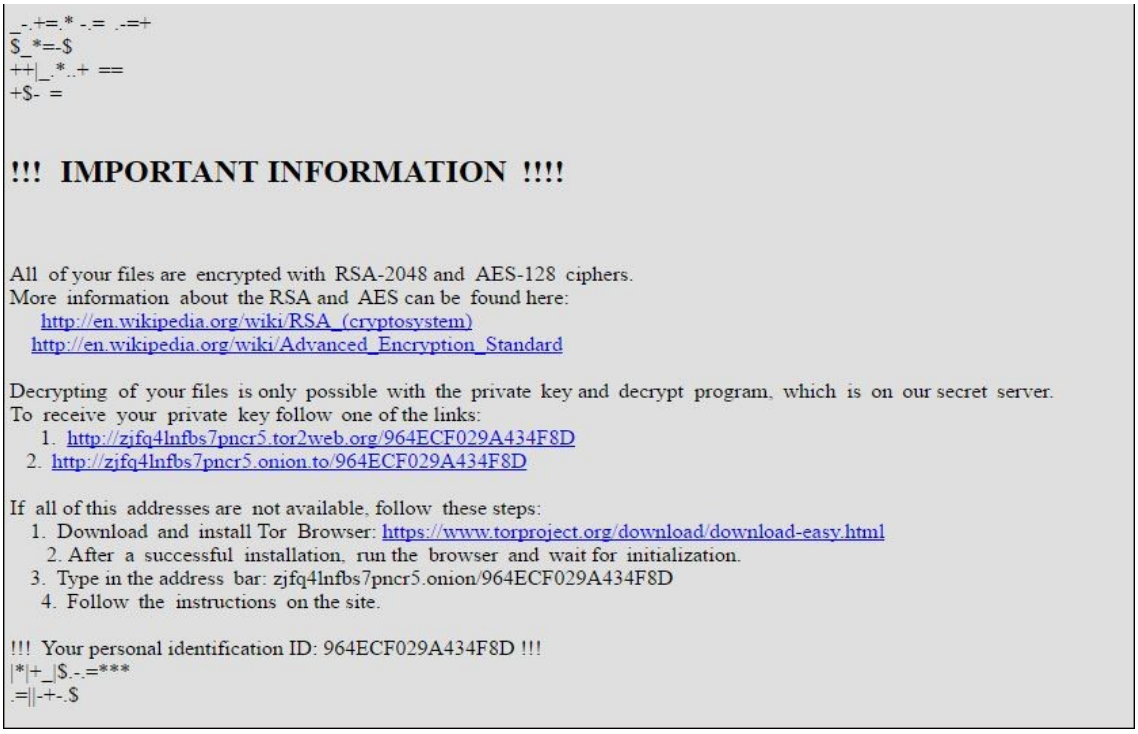
_HELP_instructions.bmp / _HOWDO_text.bmp
_HELP_instructions.html / _HOWDO_text.html

In other directories the format changes like this:

_{count maintained by malware}_HELP_instructions.html
_HELP_instructions.bmp / _HOWDO_text.bmp



_HELP_instructions.html / _HOWDO_text.html



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 also removes the “Run” registry entry.

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

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
- 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.