McAfee Labs Threat Advisory

Ransomware-Locky

February 19, 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 that upon execution encrypts certain file types present in the user's system. The compromised user has to pay the attacker to get the files decrypted.

This threat is detected 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. The malicious Office files contain a macro to download Ransomware-Locky files.

The malicious Office file usually arrives on a vitamin machine as an attachment as part of spam or phish emails. The file can be a Word document (.doc file and .docx file) or an Excel workbook (.xls file and .xlsx file).

Email 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.

Please refer to the following URL to learn more about malicious Office files:
https://kc.mcafee.com/corporate/index?page=content&id=PD25689

The attachments in the spam emails are Office document files, some of which may be named as one of the following:

- invoice_J-12345678.doc
- Rechnung-54-110090.xls

The subjects used in the spam campaign may be named as one of the following:

- ATTN: Invoice J-12345678
- Per E-Mail senden: Rechnung-54-110090.xls

Coverage for the above-mentioned detection name is available from the production DAT version 8080.

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 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

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 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".

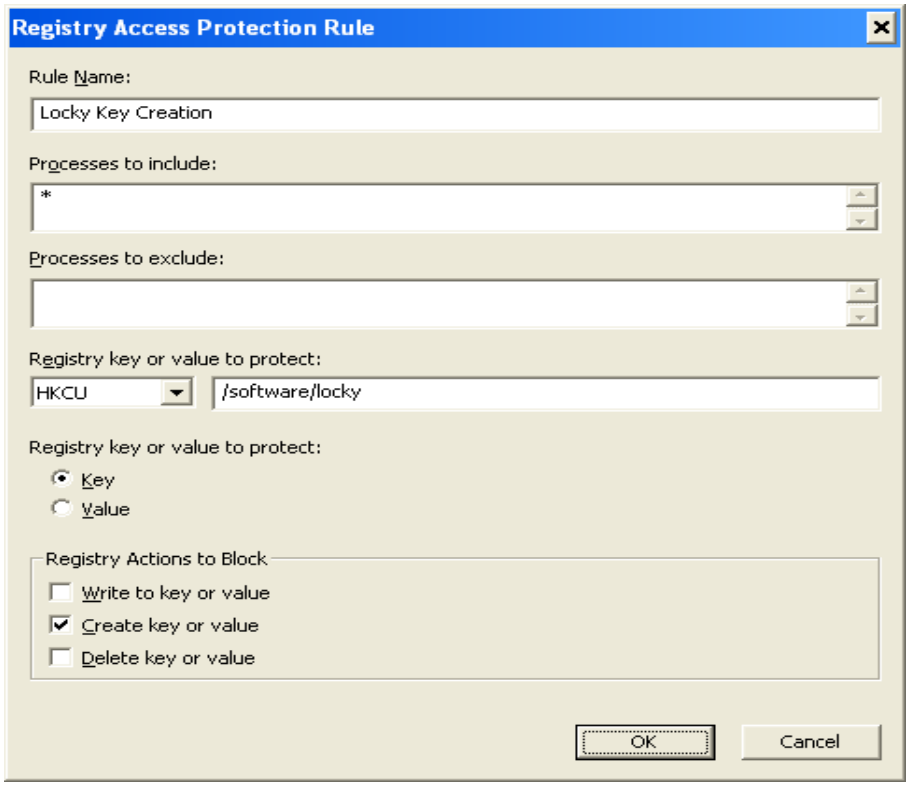
- **End users should back up business data to the organization's shared folders**. Data residing on user devices may be permanently lost in the event of a ransomware infection.

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

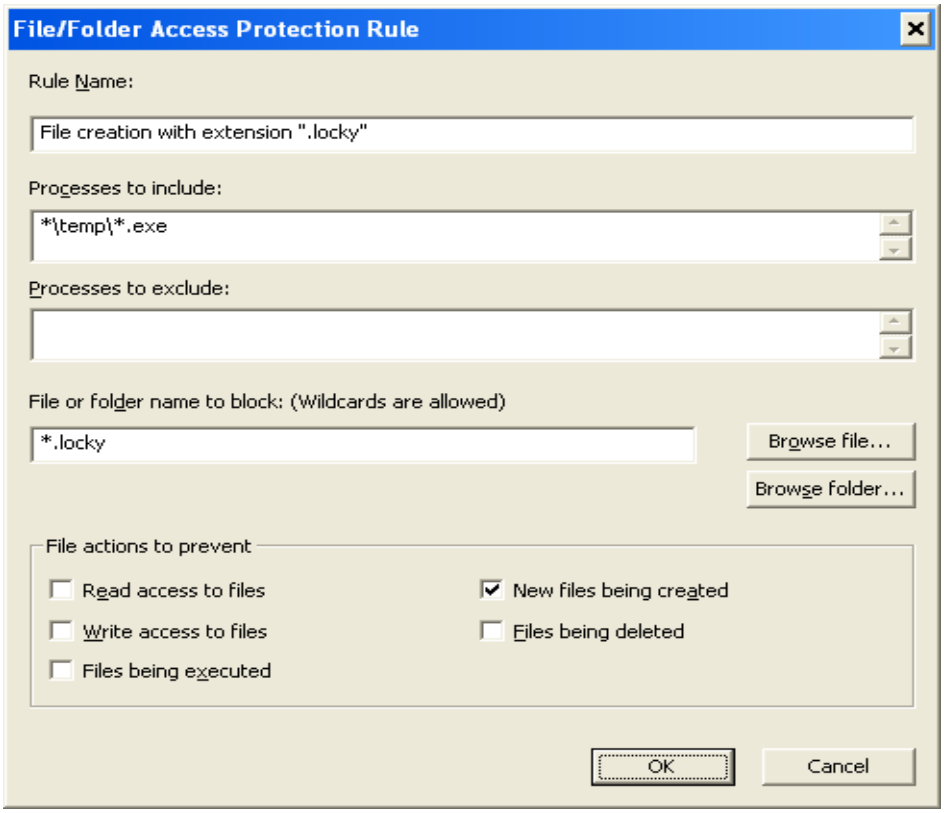
Users can configure and test Access Protection Rules to restrict the creation of new files and folders when there are no other legitimate uses.

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 %temp% location:



Host IPS

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.
To block attacks from a specific IP address through McAfee Nitrosecurity IPS, refer to KB74650.

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.

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

- SaaS
- Email and 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

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" file:

- C:\Users\<UserProfile>\AppData\Local\Temp\<random name>.exe

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.

The new process started from the %temp% directory generates a unique ID (Personal Identification ID) using the 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 the public key and recovery instruction text in the registry.

POST request to get public key:

> id=50DA5BC8E75B1354&act=getkey&affid=1&lang=en&corp=0&serv=0&os=Windows+XP&sp=3&x64=0

POST request to get recovery instructions:

> id=50DA5BC8E75B1354&act=gettext&lang=en

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

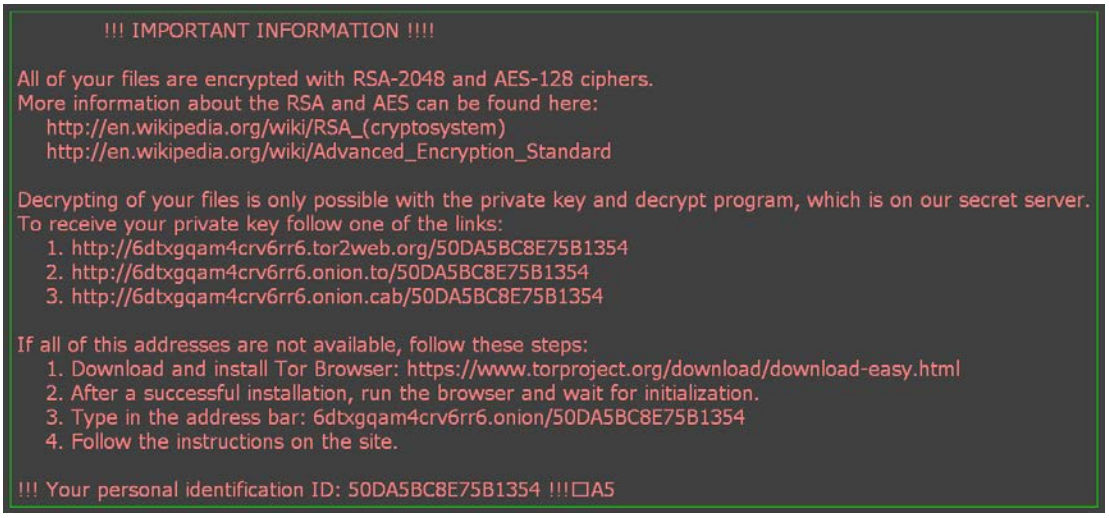
Ransomware-Locky encrypts the files with following extensions:

> .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,.

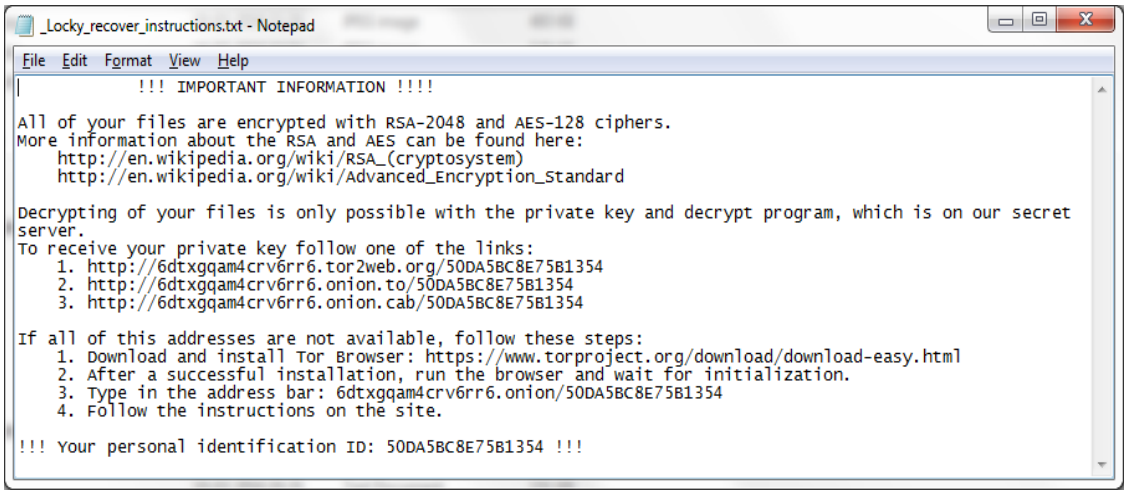
After files are successfully encrypted, malware opens the recovery instructions image and text file. Malware also changes the desktop background with the recovery instruction image file:

- _Locky_recover_instructions.bmp
- _Locky_recover_instructions.txt

_Locky_recover_instructions.bmp:



_Locky_recover_instructions.txt:



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 comprised 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 in an automated way.

We assume the user's machine to be infected:

If the following registry key has been added to the system:

- 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]

If there is any network traffic to the IP addresses mentioned below:

- 95.181.171.58
- 185.14.30.97
- 195.22.28.196
- 195.22.28.198
- pvwinlrmwvccuo.eu
- cgavqeodnop.it
- kqlxtqptsmys.in
- wblejsfob.pw

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.