The Advent of New Ransomware Targeting The Mac OS X

FFRI, Inc.
http://www.ffri.jp

Table of Contents

- Background

- KeRanger
  - Overview
  - Technical Information
  - Route of Infection
  - Correspondence situation of XProtect
  - Common point with Linux.Encoder

- Measures for Ransomware

- Conclusion/Wrapup

Background

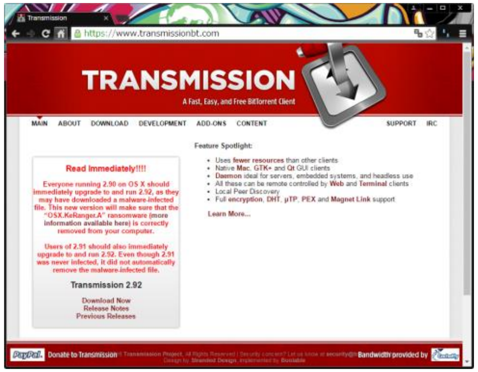
- In Japan, it has been reported many damage caused by ransomware such as TeslaCrypt 3.0 and Locky from the end of 2015.
- These malware are targeting a Windows PC primarily because it does not work with devices operating at the *nix based OS.
- However, ransomware which has targeted the Linux server has been discovered in October 2015. Furthermore, new ransomware which is working completely in Mac OS X has been discovered in March 2016.
- In this slide, we describe focused on KeRanger a ransomware of Mac OS X.

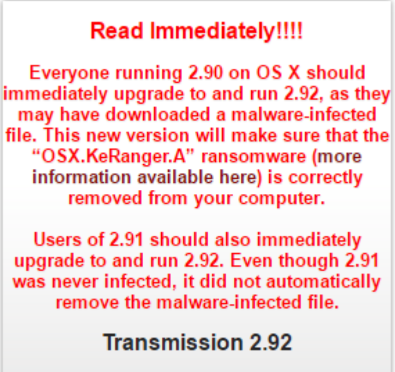
KeRanger: Overview

- A Ransomware which is working completely for the first time in Mac OS X that reported by Palo Alto Networks.

- Characteristics
  - Disguised in Transmission (BitTorrent client app).
  - To avoid the Gatekeeper by a valid code signing.
  - After infection, to encrypt a specific area through the hiding period of 3 days.

- Current Status
  - Apple
    - Revoked the certificate.
    - Added a signature to XProtect.
  - Client app
    - It has been replaced to legitimate app.





Read Immediately!!!!

Everyone running 2.90 on OS X should immediately upgrade to and run 2.92, as they may have downloaded a malware-infected file. This new version will make sure that the "OSX.KeRanger.A" ransomware (more information available here) is correctly removed from your computer.

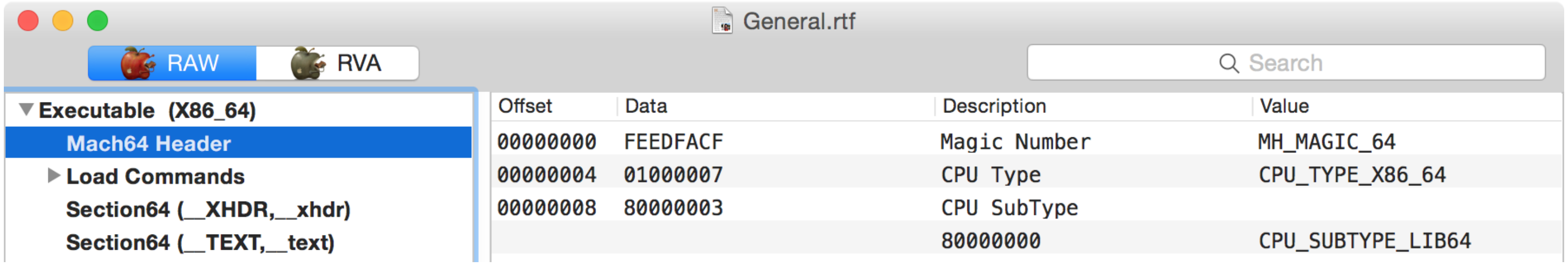
Users of 2.91 should also immediately upgrade to and run 2.92. Even though 2.91 was never infected, it did not automatically remove the malware-infected file.

Transmission 2.92

Source: https://www.transmissionhttps://www.transmissionbt.com/bt.com/

KeRanger: Technical Information <Trojan>

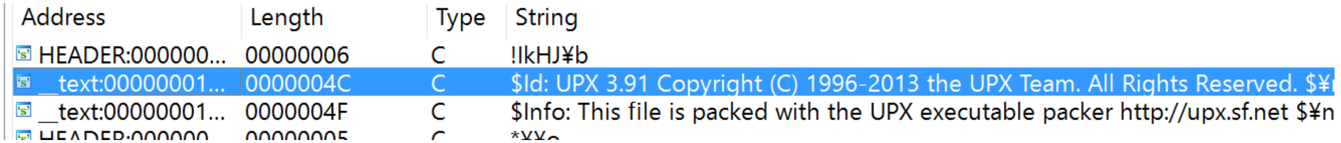
- Contamination of malware
  - The executable (Mach-O) file that disguised itself as an RTF file is included in disguised DMG file.



▼Executable (X86_64)
Mach64 Header
▶Load Commands
Section64 (__XHDR,__xhdr)
Section64 (__TEXT,__text)

Offset	Data	Description	Value
00000000	FEEDFACF	Magic Number	MH_MAGIC_64
00000004	01000007	CPU Type	CPU_TYPE_X86_64
00000008	80000003	CPU SubType	
		80000000	CPU_SUBTYPE_LIB64

  - The malicious file need to unpack before analysis because it is packed with UPX 3.91.



Address	Length	Type	String
HEADER:000000...	00000006	C	!lkHJ¥b
__text:00000001...	0000004C	C	$Id: UPX 3.91 Copyright (C) 1996-2013 the UPX Team. All Rights Reserved. $¥
__text:00000001...	0000004F	C	$Info: This file is packed with the UPX executable packer http://upx.sf.net $¥n
HEADER:000000	00000005	C	*¥¥o

KeRanger: Technical Information <Code signing>

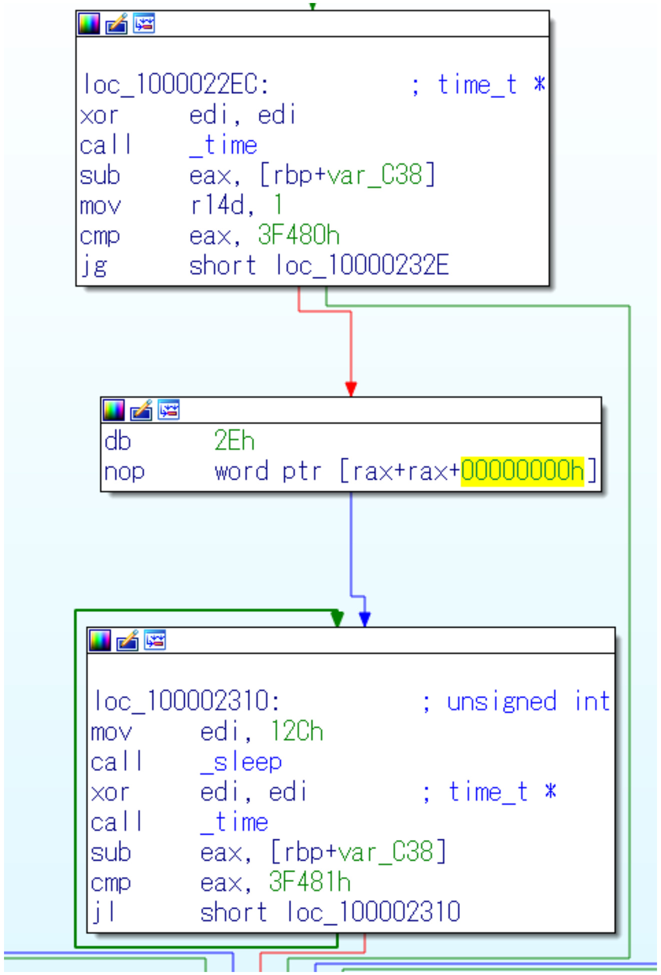
- Signature information
  - In OS X, it is possible to dump the signature information by using the “codesign” command.

```
$ codesign -d -vvvv Transmission.app
---- 省略 ----
Authority=Developer ID Application: POLISAN BOYA SANAYI VE TICARET ANONIM SIRKETI
(Z7276PX673)
Authority=Developer ID Certification Authority
Authority=Apple Root CA
Signed Time=2016/03/04 11:03:57
---- 省略 ----
```

  - From the above, it can be seen infected application is being signed on March 4, 2016 by using the official certificate by Apple.

KeRanger: Technical Information <Hiding Period>

- About the hiding period
  - KeRanger encrypt some specific area through the hiding period of 3 days.
  - During the hiding period, KeRanger is checking the time every 5 minutes.
  - The encryption is executed to files which have specific extension in “/Users” and “/Volume”.
    - 300 kinds of extension has been registered in KeRanger.

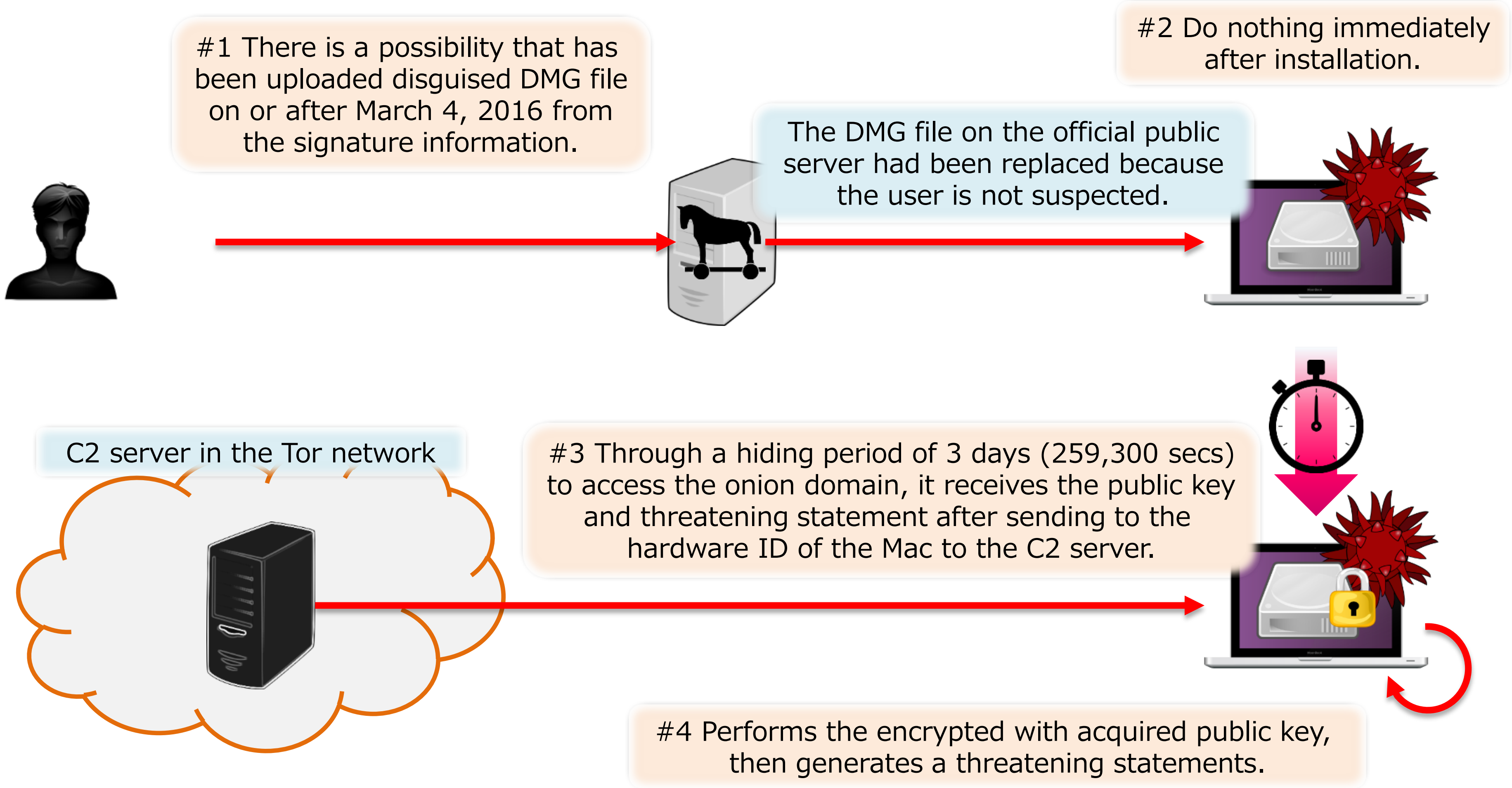


```
loc_1000022EC:                  ; time_t *
xor     edi, edi
call    _time
sub     eax, [rbp+var_C38]
mov     r14d, 1
cmp     eax, 3F480h
jg      short loc_10000232E
```

```
db      2Eh
nop     word ptr [rax+rax+00000000h]
```

```
loc_100002310:                  ; unsigned int
mov     edi, 12Ch
call    _sleep
xor     edi, edi                ; time_t *
call    _time
sub     eax, [rbp+var_C38]
cmp     eax, 3F481h
jl      short loc_100002310
```

KeRanger: Route of Infection



#1 There is a possibility that has been uploaded disguised DMG file on or after March 4, 2016 from the signature information.

#2 Do nothing immediately after installation.

The DMG file on the official public server had been replaced because the user is not suspected.

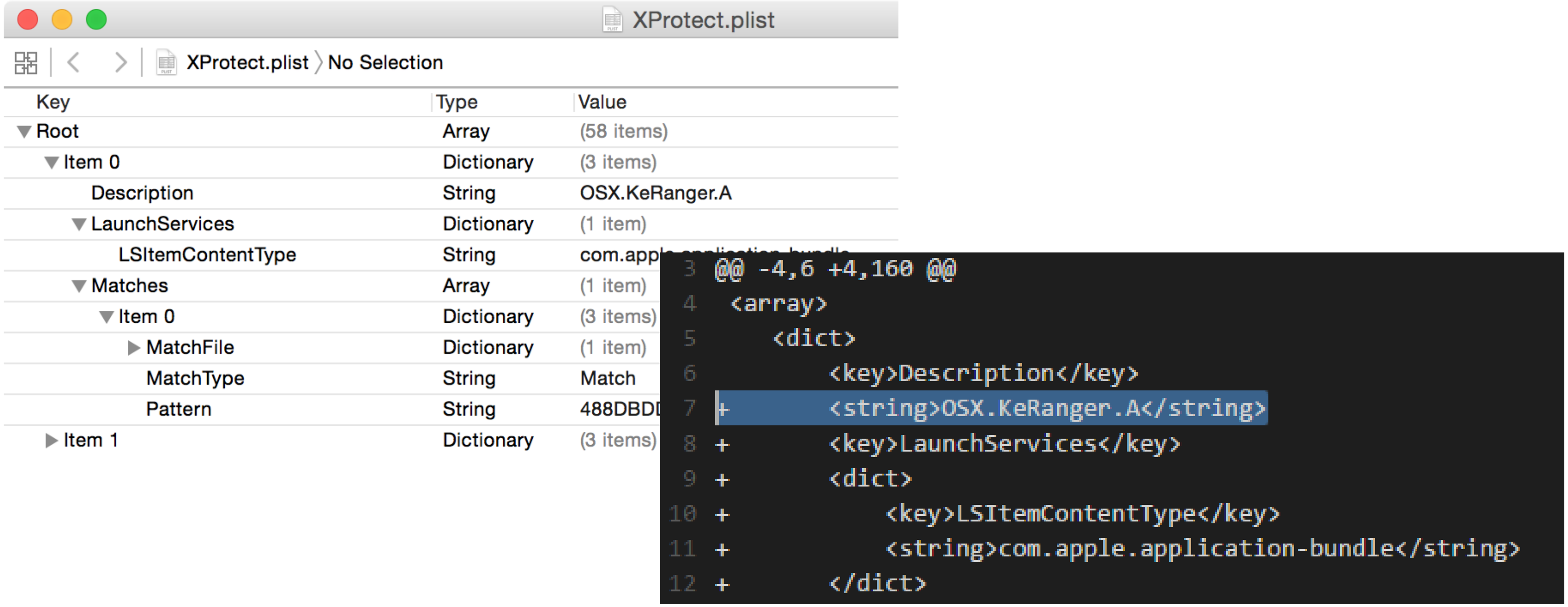
C2 server in the Tor network

#3 Through a hiding period of 3 days (259,300 secs) to access the onion domain, it receives the public key and threatening statement after sending to the hardware ID of the Mac to the C2 server.

#4 Performs the encrypted with acquired public key, then generates a threatening statements.

Correspondence Situation of XProtect

- As a result of KeRanger discovery, Apple invalidated the certificate and added new signature to XProtect with update.



Key	Type	Value
▼Root	Array	(58 items)
▼Item 0	Dictionary	(3 items)
Description	String	OSX.KeRanger.A
▼LaunchServices	Dictionary	(1 item)
LSItemContentType	String	com.app
▼Matches	Array	(1 item)
▼Item 0	Dictionary	(3 items)
▶MatchFile	Dictionary	(1 item)
MatchType	String	Match
Pattern	String	488DBDD
▶Item 1	Dictionary	(3 items)

```
@@ -4,6 +4,160 @@
 <array>
    <dict>
        <key>Description</key>
+       <string>OSX.KeRanger.A</string>
+       <key>LaunchServices</key>
+       <dict>
+           <key>LSItemContentType</key>
+           <string>com.apple.application-bundle</string>
+       </dict>
```

Common point with Linux.Encoder

- KeRanger is pointed out that a rewrite of the ransomware for Linux server that was discovered in October 2015.

- For example:
  - Libraries used for encryption with high probability the same.
    - The function symbol names used also encrypt both malware begins with “mbedtls_” because it is possibility of using PolarSSL known as lightweight libraries.

  - Almost the same threatening statements file.
    - Both malware generate README_FOR_DECRYPT.txt because details (e.g. payment procedures, etc.) are described in this file.

Measures for Ransomware

- If you’ve been infected with ransomware, we do not recommend that you pay to the attacker because recovery of damage is not the trustworthy promise.

- There are example of countermeasures and mitigations below.
  - Security updates of the OS and apps will be conducted regularly.
  - Not to install or run apps that are signed by an untrusted publisher.
    - In the case of KeRanger, above-mentioned measure is not enough because it is signed by official certificate which was issued by Apple.
    - On the other hand, it can be determined that it is suspicious app by checking the difference of the signature because the developer ID is different from the previous version.
  - Increase the recoverable point by regularly conducts the backup.
    - We recommend to consider combination of the file server for backup because we found the code that KeRanger developer also tried to encrypt the Time Machine files for backup.

Conclusion/Wrapup

- Recently, most of ransomware had targeted a Windows PC. However, it has been clearly that OS X and Linux have been also targeted from ransomware by the discovery of KeRanger and Linux.Encoder.

- Considering the similarity of KeRanger and Linux.Encoder, it is possibility the code is leaked to the black market or have been created by the same developer.

- Some researchers have pointed out that the legitimate certificate is sold on the black market. Therefore, a malware which is possible to bypass Gatekeeper is likely to emerge again.

- Ransomware will easy to monetize for the attacker. Care must be taken because it is assumed to increase damage in the future.

References

- TRANSMISSION – A Fast, Easy, and Free BitTorrent Client
  - https://www.transmissionbt.com/
- NEW OS X RANSOMEWARE KERANGER INFECTED TRANSMISSION BITTORRENT CLIENT INSTALLER
  - http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/
- Mac上で完全に動作するランサムウェア「KeRanger」を実行させてみた。
  - http://applech2.com/archives/48035822.html
- KeRanger Is Actually A Rewrite of Linux.Encoder
  - https://labs.bitdefender.com/2016/03/keranger-is-actually-a-rewrite-of-linux-encoder/
- サイバー犯罪者に人気の商品「コード証明書」
  - http://asmarterplanet.com/jp-security/blog/2015/10/97.html