Mac OS X を狙う新たなランサムウェアの登場

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

目次

- 背景
- KeRanger
  - 概要
  - 特徴に関する技術情報
  - 感染経路
  - XProtect 対応状況確認
  - Linux.Encoderとの共通点
- ランサムウェア対策
- まとめ

背景

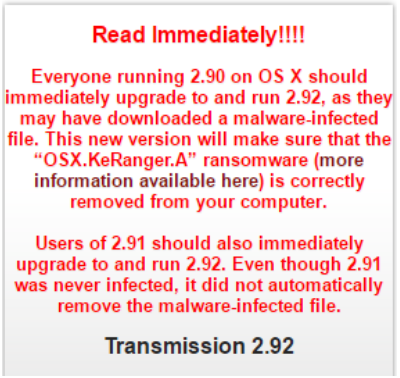
- 2015年末から vvvウイルスで知られる Teslacrypt 3.0 や Locky などのランサムウェアによる被害が国内で相次いでいる。
- これらは、主に Windows PC をターゲットにしており、スマートフォンをはじめ Windows OS 以外では動作しない。
- しかし、2015年10月頃に Linux サーバをターゲットにしたランサムウェア (Linux.Encoder) が発見され、2016年3月には OS X では初とされる完全に動作するランサムウェア (KeRanger) も確認されている。
- 本スライドでは、 OS X のランサムウェア KeRanger にフォーカスして解説をする。

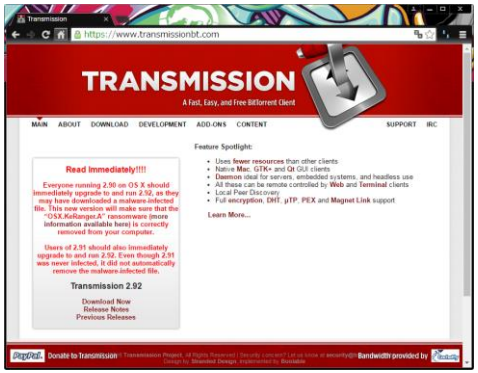
KeRanger 概要

- パロアルト社が発見した OS X で初めて完全に機能するランサムウェア

- 特徴
  - BitTorrent のクライアントアプリ（Transmission）に偽装（Trojan）
    - サイバー攻撃によって公式サイトのインストーラが上記差し替えられていた
  - 有効な証明書による署名が付与されていたことから、 OS X 標準のセキュリティ機能である GateKeeper を回避して実行される
  - 感染後、3日間の潜伏期間を経て特定領域の暗号化が行われる

- 現在の状況
  - Apple
    - 証明書の無効化
    - XProtect にシグネチャを追加
  - BitTorrent クライアントアプリ
    - 正規のアプリケーションに差し替え済み

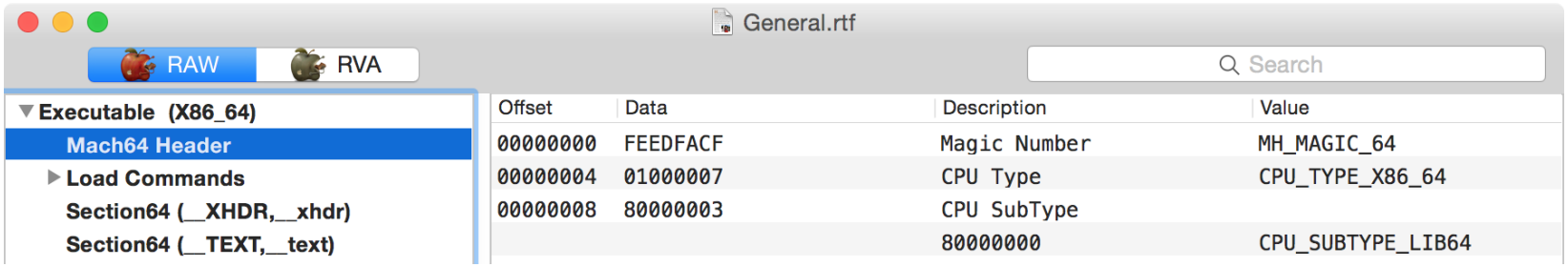




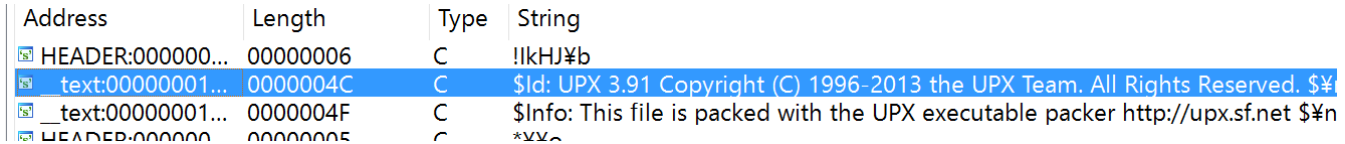
Source: https://www.transmissionhttps://www.transmissionbt.com/bt.com/

KeRanger 特徴に関する技術情報 <Trojan>

- 不正ファイルの混入
  - マルウェアが混入された Transmission.app のパッケージ内容を観察すると、/Contents/Resources の中にリッチテキストファイル (*.rtf) に偽装した Mach-O ファイルが存在する



  - ファイルは UPX 3.91 でパックされているため解析するには事前にアンパック処理を行う必要がある



KeRanger 特徴に関する技術情報 <署名>

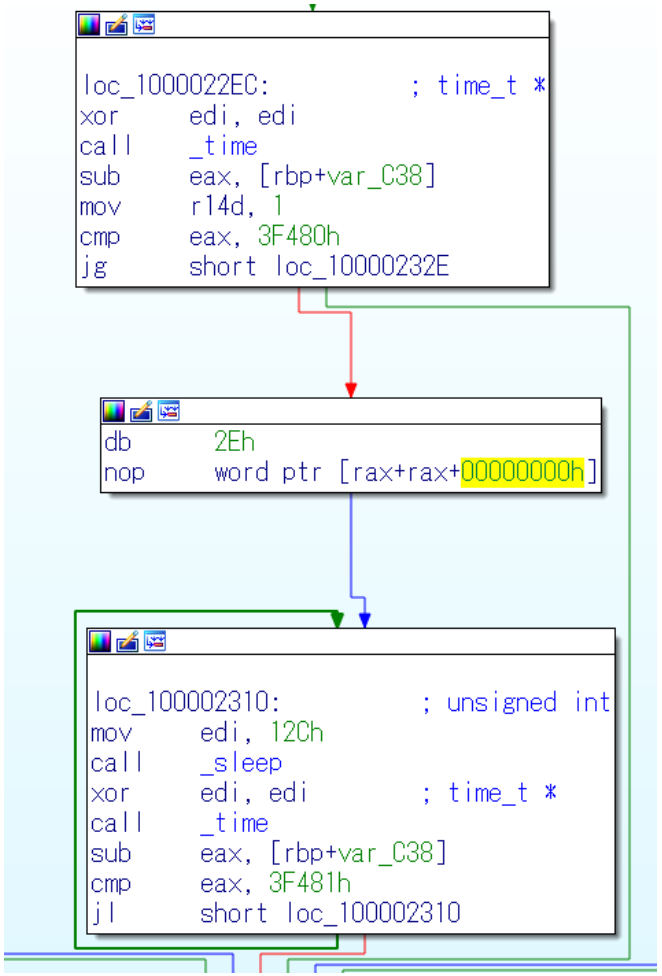
- 署名情報
  - OS Xでは、codesign コマンドを使用することで署名情報をダンプする事が可能

```
$ 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 ----
```

  - 上記から、マルウェアが混入されたパッケージはAppleによる正式な証明書を使用して2016年3月4日に署名されている事が分かる

KeRanger 特徴に関する技術情報 <潜伏期間>

- 潜伏期間について
  - KeRanger は Windows PC で
    よく見られるランサムウェアとは異なり、
    実行直後に暗号化は行わずに3日間の
    潜伏期間を経て活動を始める
  - 潜伏期間中は、 5分間隔で実行される
    time 関数で取得した時間の差分チェック
    が行われる
  - 暗号化は /Users と /Volume 以下の
    ファイルを対象に行われる
    - 登録されている拡張子は300個

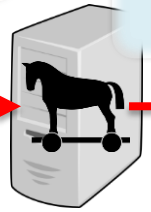


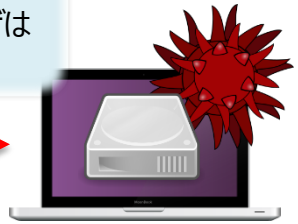
KeRanger 感染経路

(1)署名情報から2016年3月4日以降に
不正なDMGファイルがアップロード
された可能性がある

(2)インストール直後は、何もしない
（潜伏期間）

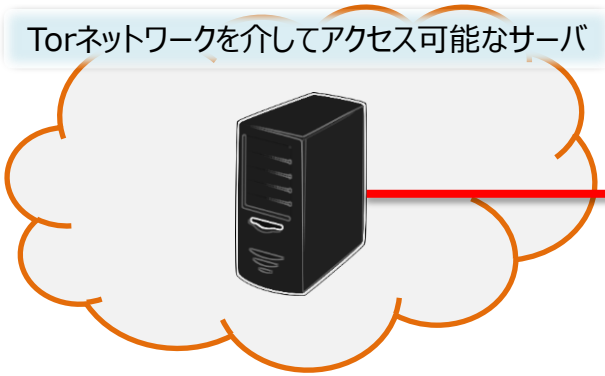
海賊版等ではなく、正規の公開サーバ上の
ファイルが置き換えられていたため、ユーザは
気付く事が出来ない





(3)3日間(259,200秒)の潜伏期間を経て
onionドメインにアクセスし、C2サーバにMacの
ハードウェアIDなどを送信し、公開鍵や脅迫状を
受け取る

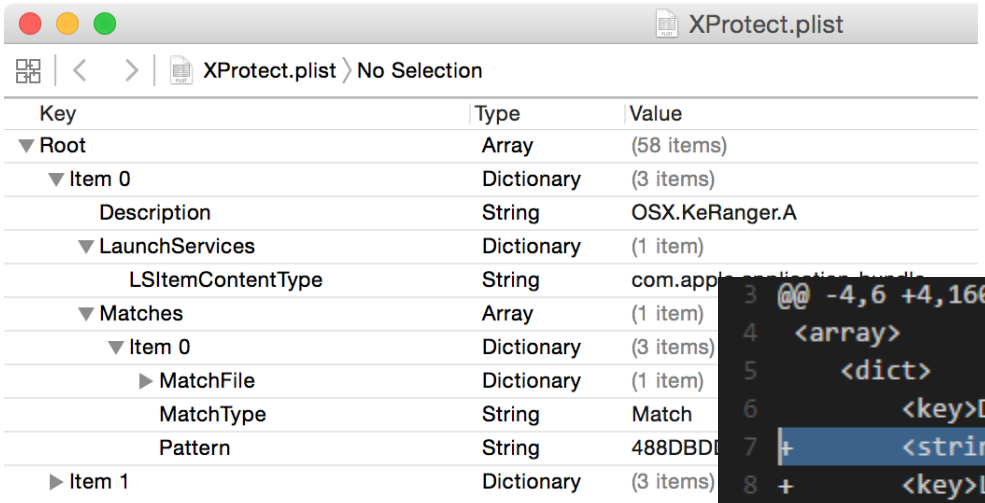
Torネットワークを介してアクセス可能なサーバ



(4)取得した公開鍵による暗号化や脅迫状
（README_FOR_DECRYPT.txt）の生成を行う

XProtect 対応状況の確認

- 今回のマルウェア発見を受けて、Appleでは既に該当の証明書を失効させたほか、アップデートによる XProtect のシグネチャ追加も行っている。




```
@@ -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>
```

Linux.Encoder との共通点

- KeRanger は 2015年10月に発見された Linux サーバ向けのランサムウェアである Linux.Encoder との類似性が指摘されている

- 例えば、以下の通りである
  - 暗号化に使用しているライブラリが同じ
    - 関数シンボル名が mbedtls_ となっていることから、どちらのマルウェアも軽量ライブラリとして知られている PolarSSL を使用している可能性
  - 暗号化を行うロジックが類似している
  - 脅迫状のテキストファイルがほぼ同一

ランサムウェア対策

- ランサムウェアに感染してしまった場合、要求に従うことで復号する旨の脅迫文が生成されるが、確実な復旧が保証されていないことから従うべきではない

- 上記を踏まえ、まずは感染しないための対策と感染してしまった後の被害を最小限に抑えるための対策の一例を以下に挙げる
  - OS やアプリの **セキュリティアップデートは定期的に実施** する
  - Apple が発行していない等、 **信頼されない発行元の証明書によって署名されているアプリをインストール、実行しない**
    - 今回の KeRanger は Apple が正式に発行した証明書による署名が行われたため、上記の対策だけでは不十分といえる。
    - 一方で、Developer ID が以前の版と異なっていた事から、署名の差分チェックを行うことで正式な証明書を使用していたとしても不審アプリとして判断する事ができる
  - TimeMachine 等による **バックアップを定期的に実施** し、リカバリー可能なポイントを増やす
    - KeRanger は TimeMachine のバックアップファイルに対しても暗号化試みる動きがあるとの事なので、TimeMachine だけでなくファイルサーバなども活用を検討する

まとめ

- 近年、猛威を振るっているランサムウェアのほとんどは Windows PC をターゲットにしていたが、今回紹介した KeRanger や Linux.Encoder の発見によって、OS X や Linux もランサムウェアの脅威に晒されている事が明らかとなった

- KeRanger と Linux.Encoder の類似性を踏まえると、コードがブラックマーケット等に流出もしくは同じ開発者によるものと考えられる

- 署名に使われる正規の発行元による証明書もブラックマーケット上で販売されている事を指摘している研究者もいることから、今後も GateKeeper を回避する OS X マルウェアが登場する可能性がある

- マルウェアの中でも、ランサムウェアはその性質上マネタイズしやすいといえることから、今後も様々な形で被害が増加することが想定されるため注意が必要である

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