Monthly Research

OS X のマルウェアとセキュリティ

株式会社ＦＦＲＩ
http://www.ffri.jp

Ver 1.00.02

アジェンダ

- 背景と目的
- OS X のマルウェアやサイバー攻撃の事例
- その他の OS X マルウェア
- OS X のマルウェア対策機能
- OS X に対するセキュリティの研究
- まとめ

背景と目的

- 2014 年 9 月末に OS X で動作する iWorm という新しいマルウェアが発見された
- 発見したセキュリティ企業 Dr.Web によると全世界で 17,000 以上の端末が感染しているという
- iWorm は、海賊版ソフトウェアに仕込まれており、それをインストールすると感染する
- iWorm はボット型マルウェアであり、攻撃者がソーシャルニュースサイト reditt.com に書き込む C&C サーバのアドレスとポートのリストを受信し、そこに接続して命令を受け取る仕組み
- 本調査では、上記背景をきっかけとし、これまでに発見されている OS X のマルウェアとマルウェアに対抗する OS X のセキュリティ機能について調査する

OS X のマルウェアとサイバー攻撃の事例

- 近年発生した代表的な OS X のマルウェアとサイバー攻撃
  - Flashback (2011)
    - OS X で最も感染拡大したマルウェア
    - 60万台以上に感染したと言われるボット
    - Adobe Flash のインストーラを偽装
    - 改ざんされ Blackhole Exploit Kit が設置された Web サイトを閲覧した場合に Java プラグインの脆弱性を攻撃して感染する亜種あり
  - Apple を含む複数の企業に対する水飲み場攻撃 (2013)
    - Apple, Facebook, Twitter, Microsoft を含む最低 40 社に被害
    - iPhoneデベロッパーフォーラム　iPhonedevSdk.com　が改ざんされた
    - Java プラグインの脆弱性を悪用

Web 経由の脆弱性攻撃によるマルウェア感染(Drive by Download) 、水飲み場攻撃が Windows と同様に行われている

その他の OS X マルウェア

- これまでに発見された OS X のマルウェアについて、
  ESET の Mac Malware Facts というサイトにまとまっている
  - http://www.eset.com/int/mac-malware-facts/
  - 2004 年から 2014 年の 10 年間でも 1 サイトに収まる数
  - しかし、2010 年以降は新種が増加傾向にある
  - OS X には既に様々なタイプのマルウェアが出現している
    - ワーム Leap
    - ボット Flashback, Tsunami
    - スケアウェア MacSweep, iMunizator, MacDefender
    - スパイウェア Hovdy, OpinionSpy
    - 遠隔操作(RAT) HellRTS, HellRTS, BlackHole, Sabpab

Windows と同様に様々なマルウェアが存在する

OS X のマルウェア対策機能（１）

- OS X にはマルウェア対策となるセキュリティ機能がいくつかある
  - OS X 10.10 Yosemite までに次の機能が実装されている
    - NX/W^X（10.5~）と ASLR（10.7~）
      - 脆弱性攻撃対策
    - Gatekeeper（10.7.5~）
      - 意図せずにマルウェアが実行されるのを防ぐ機能
      - アプリのデジタル署名とダウンロードファイルかどうかのチェック
    - App Sandbox（10.5~）
      - アプリが攻撃されても意図しない動作を防止する機能
        - » Adobe Flash Player、Silverlight、QuickTime、Oracle Java プラグイン、PDF ビューアなどの標準アプリが対象
        - » Windows 8 の App Container 類似機能
          - » FFRI Monthly Research 2012年10月 参照

OS X のマルウェア対策機能（２）

- XProtect（10.6~）
  - 標準搭載のパターンマッチング方式のウイルス対策ソフト
  - 2014 年10 月末時点で 41 種類のマルウェアが登録されている
  - パターンファイルは下記のパスにある
    - /System/Library/CoreServices/CoreTypes.bundle/Contents/Resources/XProtect.plist

OSX.Abk.A	OSX.FlashBack.A	OSX.LaoShu.A	OSX.QHost.WB.A
OSX.AdPlugin.i	OSX.FlashBack.B	OSX.Leverage.a	OSX.Revir.A
OSX.AdPlugin2.i	OSX.FlashBack.C	OSX.MacDefender.A	OSX.Revir.ii
OSX.CoinThief.A	OSX.GetShell.A	OSX.MacDefender.B	OSX.Revir.iii
OSX.CoinThief.B	OSX.HellRTS	OSX.Machook.A	OSX.Revir.iv
OSX.CoinThief.C	OSX.HellRTS	OSX.MaControl.i	OSX.RSPlug.A
OSX.DevilRobber.A	OSX.Iservice.A	OSX.Mdropper.i	OSX.SMSSend.i
OSX.DevilRobber.B	OSX.Iservice.B	OSX.NetWeird.i	OSX.SMSSend.ii
OSX.FileSteal.i	OSX.iWorm.A	OSX.NetWeird.ii	
OSX.FileSteal.ii	OSX.iWorm.B	OSX.OpinionSpy	
OSX.FkCodec.i	OSX.iWorm.C	OSX.Prxl.2	

OS X に対するセキュリティの研究

- OS X に対する新しい攻撃手法が日々研究され、発表されている
- Black Hat Europe 2014 (2014.10) では下記の発表があった
  - EXPLORING YOSEMITE: ABUSING MAC OS X 10.10
    - マルウェアプロセスを隠蔽する Rootkit 技術の発表
    - OS X 10.10 上で動作するカーネルモードとユーザーモードそれぞれにおける新しい Rootkit 手法
    - ドライバロード時に行われる検証のバイパス手法

まとめ

- OS X が対象となったWeb 経由の脆弱性攻撃によるマルウェア感染や水飲み場攻撃の事例がある
- OS X のマルウェアは近年増加傾向にあり、種類も多様化してきている
- OS X には標準でいくつかのマルウェア対策機能が搭載されている
- OS X に対するセキュリティ研究は日々行われており、新しい脆弱性や攻撃手法が発見される可能性がある

参考情報 1

- エンジニアが知っておくべき”iWorm”
  - http://dev.classmethod.jp/security/understanding-iworm/
- New OS X botnet discovered
  - http://news.drweb.com/show/?i=5976&lng=en
- OSX/Flashback
  - http://go.eset.com/us/resources/white-papers/osx_flashback.pdf
- アップルに関連したハッキングのタイムライン
  - http://blog.f-secure.jp/archives/50694622.html
- Malware Attack on Apple Said to Come From Eastern Europe
  - http://www.bloomberg.com/news/2013-02-19/apple-says-a-small-number-of-mac-computers-infected-by-malware.html
- これがアップルのハック感染元。水飲み場攻撃でフェイスブック、ツイッターなど40社に被害？
  - http://www.gizmodo.jp/2013/02/_1_1.html
- 10 years of OS X malware
  - http://www.welivesecurity.com/2014/03/21/10-years-of-mac-os-x-malware/
- Mac Malware Facts
  - http://www.eset.com/int/mac-malware-facts/

参考情報 2

- Apple Mac List of Spyware, Keystroke Loggers, Trojan Horses, Backdoors and Malware for Mac OS X
  - http://macscan.securemac.com/spyware-list
- Mac Internet Security Threats
  - http://usa.kaspersky.com/internet-security-center/threats/mac
- Apple - OS X Yosemite - あなたのMacを守るように作られています。
  - https://www.apple.com/jp/osx/what-is/security/
- App Sandbox Design Guide: About App Sandbox
  - https://developer.apple.com/library/mac/documentation/Security/Conceptual/AppSandboxDesignGuide/AboutAppSandbox/AboutAppSandbox.html
- OS Xの「マルウェア」対策を知る
  - http://news.mynavi.jp/column/osxhack/081/
- EXPLORING YOSEMITE: ABUSING MAC OS X 10.10
  - https://www.blackhat.com/docs/eu-14/materials/eu-14-Tsai-Exploring-Yosemite-Abusing-Mac-OS-X-10-10.pdf

Contact Information

E-Mail ： research—feedback@ffri.jp
Twitter： @FFRI_Research