Monthly Research

OS X Malware and Security

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

Ver 1.00.02

Agenda

- Background
- Case Study: OS X malware and cyber attack
- Other OS X malware
- OS X anti-malware functions
- Security Research for OS X
- Summary

Background

- New OSX malware “iWorm” was discovered in the end of Sep 2014
- Dr.Web reported that it was infected more than 17,000 machines
- iWorm was infected through pirated software
- iWorm is bot and it receives list of C&C server addresses which attacker writes at reditt.com
- We investigate OS X malware and anti-malware functions in the wake of the above

Case Study: OS X malware and cyber attack

- OS X Malware and cyber attack of recent years
  - Flashback (2011)
    - Most infected enlarged malware on OS X
    - It is a bot that was infected to more than 600,000 machines
    - It had been disguised as Adobe Flash installer
    - Subspecies to infection by Drive-by Download using the Blackhole Exploit kit
  - Watering Hole attack targeted Apple and others (2013)
    - Damage occurs in at least 40 companies including Apple, Facebook, Twitter and Microsoft
    - iPhone developer Forum “iPhonedevSdk.com” was compromised
    - Java plug-in vulnerability was exploited

Drive-by Download and Watering Hole attack has been performed in a manner similar to Windows

Other OS X malware

- About discovered OS X malware to date,
  ESET reported it as "Mac Malware Facts"
  - http://www.eset.com/int/mac-malware-facts/
  - It's 10 years worth, but the amount that fits on a single page
  - However, a new kind is a tendency to increase after 2010
  - Various types of malware has already appeared on OS X
    - Worm: Leap
    - Bot: Flashback, Tsunami
    - Scareware: MacSweep, iMunizator, MacDefender
    - Spyware: Hovdy, OpinionSpy
    - RAT: HellRTS, HellRTS, BlackHole, Sabpab

Various malware is present as well as Windows

OS X anti-malware functions

- OS X has some anti-malware functions
  - The following features have been implemented by OS X 10.10 Yosemite
  - NX/W^X(10.5~) and ASLR(10.7~)
    - Vulnerability measures
      - Gatekeeper(10.7.5~)
        - Function of preventing unintended execution of malware
        - Verification of digital signature and app source
      - App Sandbox(10.5~)
        - Function to prevent unintended behavior if app will be exploited
        - Adobe Flash Player, Silverlight, QuickTime, Oracle Java plug-in, standard apps like PDF viewer
          - » Similar function to App Container of Windows 8
            - » Refer FFRI Monthly Research Oct 2012

OS X anti-malware functions(cont'd)

- XProtect(10.6~)
  - Anti-virus software as standard feature
  - It uses pattern matching method
  - 41 malware has been registered at the end of Oct 2014
  - The pattern file exists on the following path
    - /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	

Security Research for OS X

- New attack techniques for OS X are studied every day
- EXPLORING YOSEMITE: ABUSING MAC OS X 10.10
  (Black Hat Europe 2014)
  - New rootkit techniques for hiding a process on OS X 10.10
  - New ways in each of kernel mode and user mode
  - Bypassing Driver Loading Verification

Summary

- OS X has become a target of Drive-by Download and Watering Hole attack
- OS X malware is recently increasing and its kinds have been diversified
- OS X has some anti-malware features in standard
- Because security research for OS X is active, new vulnerabilities and attack methods will be discovered in the future

References 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/

References 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