

#### Monthly Research A Survey of Threats in OS X and iOS

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

Ver 1.00.01



## **Overview/Background**

- Recently, business use of Mac and iPhone/iPad is increasing.
  - It is possible to coexist with Windows by virtual machine or Boot Camp.
  - BYOD(Bring Your Own Device) solution for iPhone is available.
    - iPhone is popular for general users in Japan, so it is often also used to BYOD.
  - It is believed no malware exists on iPhone.
- A security researcher showed that OS X's four security mechanisms(Gatekeeper, XProtect, App Sandbox, Code Signing) were avoidable easily at RSA Conference USA 2015.
  - He said that no security software for Mac detects his attack technique.
- Therefore, we surveyed threats of OS X and iOS





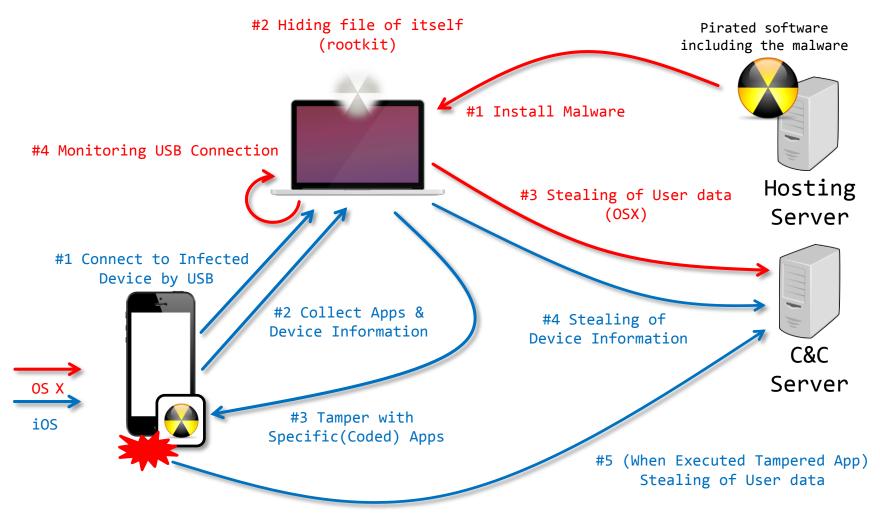
# Case Studies: OS X/iOS Malware

- [OS X/2014] iWorm
  - Infected via pirated software.
  - This bot gets C&C server address list which was written by the attacker on reditt.com.
- [iOS/2014] WireLurker
  - Infected to Windows and OS X via pirated software.
  - Infected iPhone App by abusing Sync function.
  - Send contacts list to C&C server.
- [iOS/2015] OneClick Fraud App
  - Attacker abuses "iOS Developer Enterprise Program" and distributes malware any place other than AppStore.
  - This malware displays fraud contents on the Web server side.\*

\* The malware to use such a technique is generally in Android.

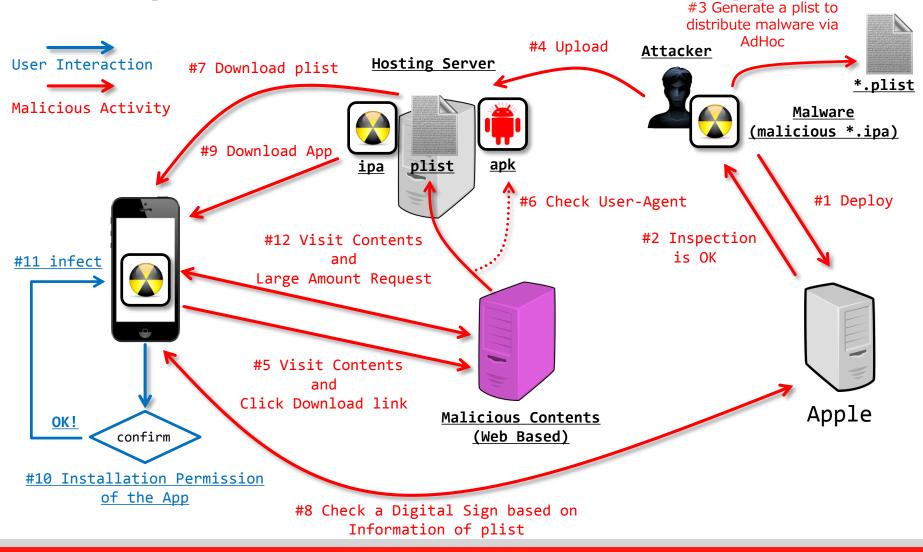


#### **Activity Overview: WireLurker**





#### **Activity Overview: OneClick Fraud App**







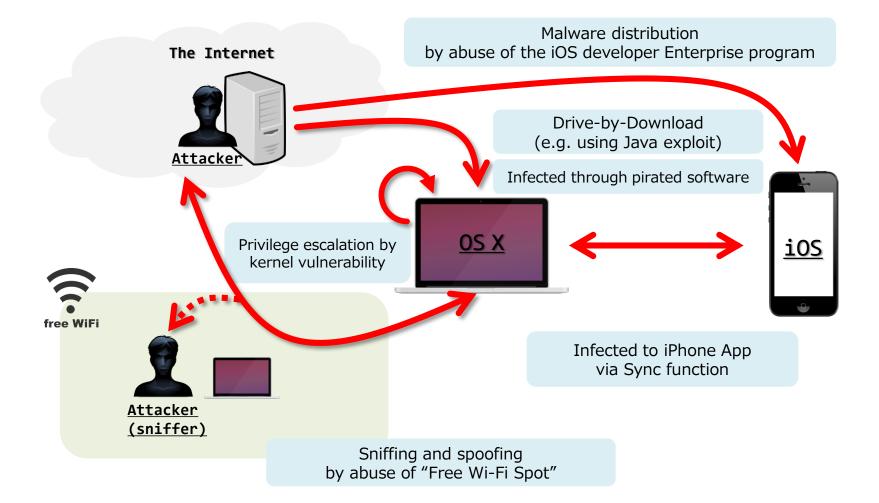
# Case Studies: OS X/iOS Vulnerability

- [OS X/iOS] Denial of Service via crafted Unicode text
  - CVE-2015-1157
  - OS/app crashes or reboots when it received crafted message.
  - Reported in May 2015.
  - Fixed at iOS 8.4 and OS X 10.10.4.
- [OS X/iOS] Cross Application Resource Access (XARA)
  - Vulnerability caused by authentication between application.
  - Various passwords might be stolen if the vulnerability is exploited.
  - Reported in June 2015.
  - Apple officials released the following statement:
     *"we implemented a server-side app security update that secures app data and blocks apps with sandbox configuration issues from the Mac App Store."*





#### **Routes of Infection and Cyber Attacks**





### Conclusion

- Recently, OS X and iOS are becoming target of cyber attacks.
  - As a result, attack technique peculiar to OS X and iOS comes up.
     (e.g. Abuse of sync function, malware distribution by AdHoc etc.)
- We recommend some security settings for Mac and iPhone based on current state of threats.
  - Target system is OS X 10.10.x (Yosemite) and iOS 8.x.
  - These settings are only minimal measures.
  - These are not always preventing any attacks.







- 1. Install security update automatically
  - Keep latest software version for vulnerability fix.

••• <		App Store	Q 検索	
	最新の状態に保て	目すると、OS X、および App St っことができます。	tore からのアプリケーションを	
	<ul> <li>✓ アップデートを自動的に確認</li> <li>✓ 新しいアップデートをバックグラウンドでダウンロード アップデートをインストールする準備ができたら通知されます</li> <li>✓ アプリケーションアップデートをインストール</li> <li>✓ OS X アップデートをインストール</li> <li>✓ システムデータファイルとセキュリティアップデートをインストール</li> </ul>			
		<b>で購入したアプリケーションを自</b> -research@ffri.jp でサインインしてい		
	ソフトウェア・フ	<b>アップデートがあります</b> アッ	プデートを表示	
				?





- 2. Disable Java plug-in on browser
  - Java vulnerabilities are exploited for a lot of malware infection on Mac.

	セキュリティ Q 枚 # セキュリティ ブライバシー 通知 機能拡張 詳細	
Java パージョン Java 8 Update 51 QuickTime パージョン 7.7.3	Java Web サイトでのこのブラグインの実行許可を設定してください:	
	ー ほかの Web サイトにアクセスしたとき: 開かない 📀	
	完了	





- 3. Enable Firewall
  - Firewall is blocking untrusted inbound communication.







- 4. Finder settings
  - Finder does not display file extension by default
  - We recommend "Show all filename extensions" to detect malware disguised as harmless file.







- 5. Encryption setting of disk (FileVault)
  - It is possible to prevent info leakage when your mac was lost or stolen.

••• < >		セキュリティとプライバジ	シー Q 検索	8
	一般 F	FileVault ファイアウォール	プライバシー	
		スクの内容を自動的に暗号化す - タを保護します。	す FileVault を入にする	
		して自動的に生成されます。パスワ	₹たは復旧キーが必要です。復旧キー フードと復旧キーを両方とも忘れる	
	ディスク"Macin	tosh HD"の FileVault は切にな	なっています。	





- 6. Screen lock with password
  - It is possible to prevent info leakage when your mac was lost or stolen.

	セキュリティとプライバシー	Q ロック
一般	FileVault ファイアウォール プライル	バシー
このユーザのログイン	パスワードが設定されています パスワー	ードを変更
🔽 スリープとスク	フリーンセーバの解除にパスワードを要求	開始後: 5 分後に ᅌ
	されているときにメッセージを表示 ロック	クのメッセージを設定
✓ 自動ログインを	を使用不可にする	





- 7. Disable built-in guest user
  - It is possible to reduce attack surface.







- 8. Use strong encryption method for Wi-Fi
  - Do not connect to non-encrypted access point
  - Do not use WEP and WPA-PSK (TKIP)
  - Use WPA2 or WPA-PSK (AES)

	Wi-Fi ネットワーク"testWEP"には WEP パスワート が必要です。
	パスワード:
	<ul> <li>─ パスワードを表示</li> <li>✓ このネットワークを記憶</li> </ul>
?	キャンセル 接続





- 9. Enable "Find my Mac"
  - It is possible to trace location when your mac was lost or stolen

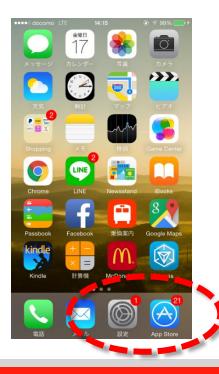






#### 1. Install Software update

- iOS update is included security updates
- Keep latest iOS version for vulnerability fix.











2. Screen lock with Touch ID/Passcode

- It is possible to prevent info leakage when lost or stolen

•••• docomo LTE 14:19	# 99% +	••••• docomo LTE 14:20
設定		設定 Touch IDとパスコ
AA 画面表示と明るさ	>	TOUCH IDを使用:
● 壁紙	>	iPhoneのロックを解除
◀ サウンド	>	iTunes & App Store
Mon IDとパスコード		iTunes Store/App Storeでのコンテン IDパスワードを入力する代わりに指紋 す。
プライバシー	>	指紋
		指紋1
iCloud	>	
iTunes & App Store	>	指紋を追加
		パスコードをオフにする
🖂 メール/連絡先/カレンダー	- >	
	>	パスコードを変更
リマインダー	>	パスコードを要求
こ 電話	>	バスコードを安求 
◯ メッセージ	>	
		簡単なパスコードは4桁の数字です。





- 3. Use strong encryption method for Wi-Fi
  - Do not connect to non-encrypted access point
  - Do not use WEP and WPA-TKIP
  - Use WPA2 or WPA-PSK(AES)



Do not connect to nonencrypted access point





- 4-1. Do not "trust" PC unnecessarily
  - WireLurker infects to iPhone via infected PC
- 4-2. Do not install apps provided by untrusted developer
  - Confirm app developer identity when iOS demands your permission







5. Enable "Find my iPhone" and "Backup"

- It is possible to trace your iPhone location when lost or stolen.
- Even if iPhone breaks down, you can restore data from backup.









#### 6. Check privacy settings

- iOS can control core functions(camera, location service, etc.) for each apps.
- Check your needs and app permissions.



••••• de 設知		0% 🛑 +
1	位置情報サービス フ	†ン >
	連絡先	>
	カレンダー	>
	リマインダー	>
*	写真	>
*	Bluetooth共有	>
<b>!</b>	マイク	>
Ó	カメラ	>
	ヘルスケア	>
	HomeKit	>
<b>=</b>	モーションアクティビティ	>
データ されま	へのアクセスを要求したAppが上のカテゴリ す。	に表示
y	Twitter	>

	ocomo LTE 14:49 ライバシー 位置情報	® ∜ 100% <del>■</del> *
$\bigcirc$	App Store	使用中のみ >
0	Chrome	┩使用中のみ >
f	Facebook	┩使用中のみ >
8	Google Maps	使用中のみ >
<b></b>	Ingress	┩ 常に許可 >
<b>1</b>	iOBD2	常に許可 >
	LINE	使用中のみ >
M.	McDonald's	┩使用中のみ >
	Siriと音声入力	┩使用中のみ >
ð	カメラ	┩使用中のみ >
	カレンダー	許可しない >
<b>.</b>	マップ	使用中のみ >
	天気	┩常に許可 >
	システムサービス	>





#### 7. Check profile settings

- Do not install suspicious profile
- Delete suspicious profile
- Malicious profile allow sniffing of your traffic by attacker





### References

- Malware Persistence on OS X Yosemite
  - <u>https://www.rsaconference.com/writable/presentations/file\_upload/ht-r03-malware-persistence-on-os-x-yosemite\_final.pdf</u>
- WIRELURKER: A New Era in iOS and OS X Malware
  - <u>https://www.paloaltonetworks.com/content/dam/paloaltonetworks-</u> <u>com/en\_US/assets/pdf/reports/Unit\_42/unit42-wirelurker.pdf</u>
- Japanese one-click fraudsters target iOS users with malicious app delivered over the air
  - <u>http://www.symantec.com/connect/blogs/japanese-one-click-fraudsters-target-ios-users-malicious-app-delivered-over-air</u>
- Unauthorized Cross-App Resource Access on MAC OS X and iOS
  - <u>https://drive.google.com/file/d/0BxxXk1d3yyuZOFlsdkNMSGswSGs/view?pli=1</u>
- Serious OS X and iOS flaws let hackers steal keychain, 1Password contents
  - <u>http://arstechnica.com/security/2015/06/serious-os-x-and-ios-flaws-let-hackers-steal-keychain-1password-contents/</u>
- iPhone text message bug can crash Apple Watch, iPad and Mac too
  - <u>http://www.theguardian.com/technology/2015/may/28/iphone-text-message-bug-crash-apple-watch-ipad-mac</u>
- Malicious Profiles The Sleeping Giant of iOS Security
  - <u>https://www.skycure.com/blog/malicious-profiles-the-sleeping-giant-of-ios-security/</u>
- NETMARKETSHARE
  - <u>http://www.netmarketshare.com/</u>
- openclipart
  - <u>https://openclipart.org/share</u>



## **Contact Information**

E-Mail : <u>research—feedback@ffri.jp</u> Twitter: <u>@FFRI\_Research</u>