

ccn-cert

IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

Madrid, 10 y 11 de diciembre 2015

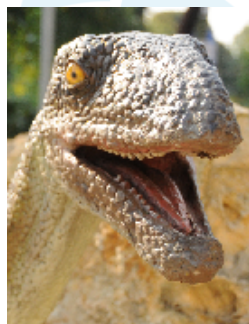
La cosecha de 2015 de Golden, Reineta y Gala



(Versión para publicar)

www.ccn-cert.cni.es

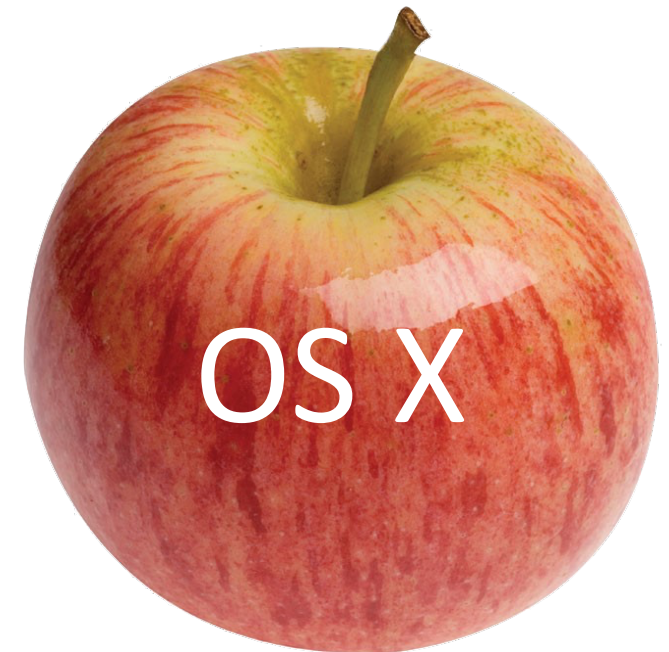
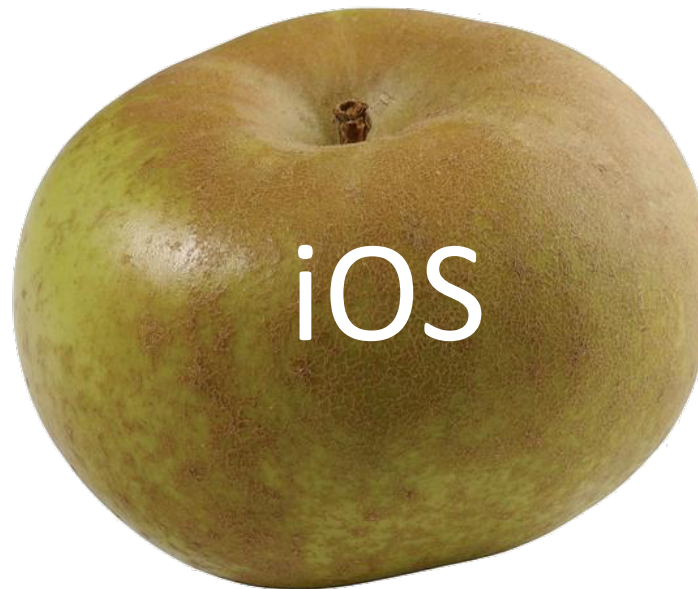




- Raúl Siles
- DinoSec (www.dinosec.com)
- raul@dinosec.com

\$ DinoSec

Golden, Reineta y Gala



Índice

- 1. La cosecha**
- 2. Golden**
- 3. Reineta**
 - Vulnerabilidades, jailbreak, tecnologías inalámbricas, apps (XcodeGhost, desarrolladores empresariales, APIs privadas)
- 4. Gala**
- 5. Conclusiones**





“La cosecha”

- La cosecha de este año ha sido muy fructífera, especialmente en algunas regiones del mundo (ej. China)
- Han surgido nuevas variedades inesperadas a lo largo de todo este año, fruto de diferentes investigaciones recientes
- Investigaciones centradas en analizar, profundizar y demostrar que estas no son tan saludables como se piensa



Vulnerabilidades comunes entre dispositivos Apple (SO)

Actualizaciones de seguridad de Apple

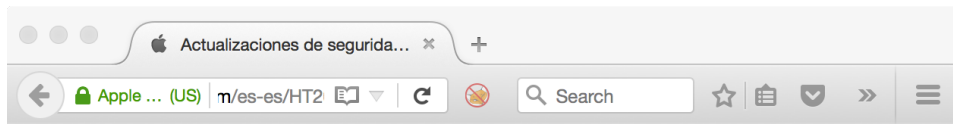
¡Qué bonito es saber idiomas!

¿HT1222?



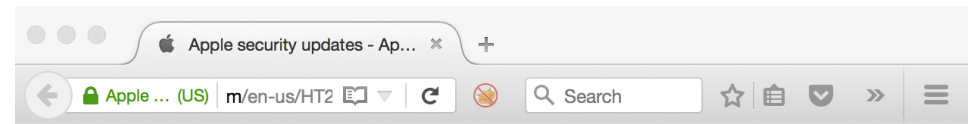
<https://support.apple.com/en-us/HT201222>

<https://support.apple.com/es-es/HT201222>



Actualizaciones de seguridad

Nombre y enlace a información	Disponible para	Fecha de publicación
OS X Server 5.0.15	OS X Yosemite v10.10.5, OS X El Capitan v10.11.1 o posterior	21 de octubre de 2015
Xcode 7.1	OS X Yosemite v10.10.5 o posterior	21 de octubre de 2015
Actualización de seguridad de EFI para Mac 2015-002	OS X Mavericks v10.9.5	21 de octubre de 2015
iTunes 12.3.1	Windows 7 y posterior	21 de octubre de 2015
OS X El Capitan 10.11.1 y Actualización de seguridad 2015-007	OS X Mavericks v10.9.5, OS X Yosemite v10.10.5 y OS X El Capitan v10.11	21 de octubre de 2015
Safari 9.0.1	OS X Mavericks v10.9.5, OS X Yosemite v10.10.5 y OS X El Capitan v10.11	21 de octubre de 2015
watchOS 2.0.1	Apple Watch Sport, Apple Watch, Apple Watch Edition y Apple Watch Hermes	21 de octubre de 2015
iOS 9.1	iPhone 4s y posterior, iPod touch (5.ª generación) y posterior, iPad 2 y posterior	21 de octubre de 2015



Security updates

Name and information link	Available for	Release date
Xcode 7.2	OS X Yosemite v10.10.5 or later	8 Dec 2015
Safari 9.0.2	OS X Mavericks v10.9.5, OS X Yosemite v10.10.5, OS X El Capitan v10.11 and v10.11.1	8 Dec 2015
watchOS 2.1	Apple Watch Sport, Apple Watch, Apple Watch Edition, and Apple Watch Hermes	8 Dec 2015
OS X El Capitan 10.11.2 and Security Update 2015-008	OS X Mavericks v10.9.5, OS X Yosemite v10.10.5, OS X El Capitan v10.11 and v10.11.1	8 Dec 2015
tvOS 9.1	Apple TV (4th generation)	8 Dec 2015
iOS 9.2	iPhone 4s and later, iPod touch (5th generation) and later, iPad 2 and later	8 Dec 2015
OS X Server 5.0.15	OS X Yosemite v10.10.5, OS X El Capitan v10.11.1 or later	21 Oct 2015
Xcode 7.1	OS X Yosemite v10.10.5 or later	21 Oct 2015
Mac EFI Security Update 2015-002	OS X Mavericks v10.9.5	21 Oct 2015
iTunes 12.3.1	Windows 7 and later	21 Oct 2015
OS X El Capitan 10.11.1 and Security Update 2015-007	OS X Mavericks v10.9.5, OS X Yosemite v10.10.5, and OS X El Capitan v10.11	21 Oct 2015
Safari 9.0.1	OS X Mavericks v10.9.5, OS X Yosemite v10.10.5, and OS X El Capitan v10.11	21 Oct 2015



Recolectando la cosecha de años previos: 2013

¿Quién quiere que le asignen un CVE...? Sólo hay que escuchar con atención...

- VII Jornadas STIC CCN-CERT (10-11 DIC 2013)
 - “Vulnerabilidades Wi-Fi de dispositivos móviles en redes empresariales 802.1x/EAP” (Raúl Siles, DinoSec)
- iOS 8.3 (8 de abril de 2015)

- Wi-Fi

Impacto: La contraseña de un usuario podría enviarse a un punto de acceso Wi-Fi que no es de confianza

Descripción: La pantalla que informa de un certificado Wi-Fi que no es de confianza solo tenía un botón para confiar en el certificado. Un usuario que no deseara usar el punto de acceso Wi-Fi tendría que pulsar en los botones de inicio o bloqueo para salir de la pantalla. Este problema se ha solucionado añadiendo el botón "Cancelar".

ID CVE

CVE-2015-5762: Michael Santos

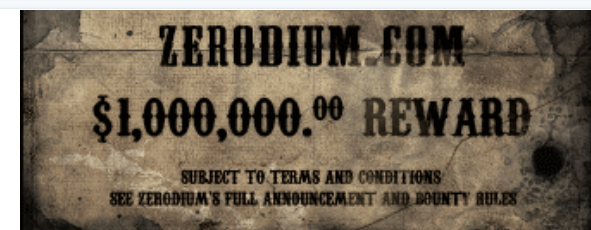


<https://support.apple.com/es-es/HT204661>

Precio de mercado de las manzanas

ZERODIUM - The Million Dollar iOS9 Bug Bounty

- \$ 1 millón de \$ (total: \$ 3M – agencias de 3...)
- Anunciado el 21/09/2015
 - Jailbreak *untethered* exclusivo, basado en web, para la última versión de Apple iOS 9
 - Vector de ataque inicial
 - Pagina web: navegador (Safari, Chrome o app)
 - Mensaje o fichero vía SMS/MMS
 - Ejecución de código remota (instalación de app)
 - Sin intervención adicional del usuario
- Ganadores anunciados el 01/11/2015



<https://www.zerodium.com/ios9.html>



OMG

“Oh My God!”

De forma detallada se recomienda:

- Trabajar como si se estuviera comprometido: suponer que los sistemas están y se comprometerían o lo estarán pronto y, por lo tanto, proteger los activos fundamentales en un medio comprometido.

Javier Candau @CCNCERT "Tenemos que trabajar como si estuviéramos infectados y con la Red comprometida" #ESADECiber

...SE DEBE TRABAJAR COMO SI SE ESTUVIERA COMPROMETIDO



www.ccn-cert.cni.es

A realistic yellow apple with a small brown stem is centered in the frame. The text "watchOS" is written in a bold, black, sans-serif font across the middle of the apple. In the background, there is a faint, light blue silhouette of the island of Taiwan and some large, semi-transparent blue letters that appear to be part of a watermark or logo.

watchOS

Evolución de la cosecha de este año

Apple Watch: ¿No aprendemos del pasado...?

- Watch OS 1.0 (24/04/2015)
- Watch OS 1.0.1 (19/05/2015)
 - <https://support.apple.com/en-us/HT204870>
 - Ej. Redirecciones ICMP
- watchOS 2 (21/09/2015)
 - <https://support.apple.com/en-us/HT205213>
- watchOS 2.0.1 (21/10/2015)
 - “Stop **arbitrary** code execution” (13 de 14)
 - <https://support.apple.com/en-us/HT205378>

Nº. oficial de vulnerabilidades:

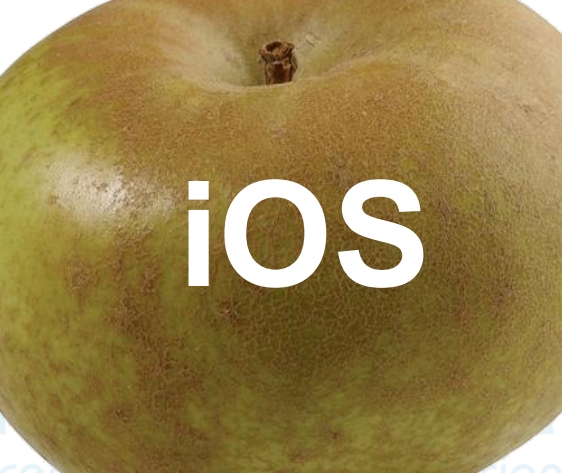
- wOS 1.0.1: 13
- wOS 2.0: 39
- wOS 2.0.1: 14
- wOS 2.1: 30

wOS x.y: 96

08/12/2015



"Invisible optical label for transmitting information between computing devices"

A close-up photograph of a single, ripe green apple. The apple has a smooth, slightly textured skin with some yellowish-green mottling. The word "iOS" is printed in a large, white, sans-serif font across the center of the apple. The background is a solid, light blue color.



Vulnerabilidades

centro criptológico nacional

Evolución de la cosecha en los últimos años

Estadísticas

- iOS: 9 años

- 2007: iPhone 2G (iOS 1)
- 2008: iPhone 3G (iOS 2)
- 2009: iPhone 3GS (iOS 3)
- 2010: iPhone 4 (iOS 4) + iPad 1
- 2011: iPhone 4S (iOS 5) + iPad 2
- 2012: iPhone 5 (iOS 6) + iPad 3 & 4 & mini
- 2013: iPhone 5c & 5s (iOS 7) + iPad air & mini 2
- 2014: iPhone 6 & 6+ (iOS 8) + iPad air 2 & mini 3
- 2015: Apple Watch (1 & 2) & iOS 9



08/12/2015 iOS 9.x: 201

Nº. oficial de vulnerabilidades:

- iOS 9: 101
- iOS 9.0.1: -
- iOS 9.0.2: 1
- iOS 9.1: 49
- iOS 9.2: 50

Nº. oficial de vulnerabilidades:

- iOS 6: 197
- iOS 7: 80
- iOS 7.1: 41

Nº. oficial de vulnerabilidades:

- iOS 8: 56
- iOS 8.1: 5
- iOS 8.1.1: 9
- iOS 8.1.2: -
- iOS 8.1.3: 34
- iOS 8.2: 6
- iOS 8.3: 58
- iOS 8.4: 33
- iOS 8.4.1: 71

iOS 8.x: 272



Vulnerabilidades en la pantalla de desbloqueo de iOS

Hasta iOS 9.2 (Dec 2015)

- iOS 5.x: 4
- iOS 6.x: 8
- iOS 7.x: 12
- iOS 8.x: 11
- iOS 9.x: 5...

iOS 9.0.2

- Pantalla bloqueada

Disponible para: iPhone 4s y posterior, iPod touch (5.ª generación) y posterior, iPad 2 y posterior

Impacto: Una persona con acceso físico a un dispositivo iOS podría acceder a las fotos y los contactos desde la pantalla bloqueada

Descripción: Un problema de la pantalla bloqueada permitía acceder a las fotos y los contactos en un dispositivo bloqueado. Este problema se ha solucionado restringiendo las opciones ofrecidas en un dispositivo bloqueado.

ID CVE

CVE-2015-5923

Nº. oficial de
vulnerabilidades:

- iOS 9.0.2: 1

<http://blog.dinosec.com/2014/09/bypassing-ios-lock-screens.html>



Jailbreaks

La industria (China) del jailbreak

- Pangu8 (<http://en.8.pangu.io>)
 - 8.0 – 8.1 (Oct'14)
- TaiG (<http://www.taig.com/en/>)
 - iOS 8.0 – 8.1.1 (Nov'14)
 - iOS 8.1.2 (Dic'14)
- TaiG 2
 - iOS 8.1.3 – 8.3 (Jun'15)
 - iOS 8.4 (Jul'15)
 - PP Assistant (25pp – Alibaba: iOS 8.4 – plagiarism)
- Pangu9 (<http://en.pangu.io>)
 - iOS 9.0 – 9.0.2 (Oct'15)



太极起

(evad3rs)
(i0nic)
TaiG
3K Assistant
PP Assistant
(Pangu)
Cydia



Download



Download



PANGU JAILBREAK

<http://www.forbes.com/sites/thomasbrewster/2015/06/26/china-iphone-jailbreak-industry/>



CCN-cert
centro criptológico nacional



Bluetooth

Vulnerabilidades recientes de Bluetooth en OS X

- OS X 10.10.5 (<https://support.apple.com/es-es/HT205031>)
 - BT LCE: CVE-2015-3779
 - Revela diseño memoria kernel: CVE-2015-3780
 - Acceso a notificaciones de otros disp. iCloud: CVE-2015-3786
 - DoS: CVE-2015-3787
 - DoS o LCE: CVE-2015-3777
- OS X 10.10.4 (<https://support.apple.com/es-es/HT204942>)
 - BT LCE: CVE-2015-3683
- OS X 10.10.2 (<https://support.apple.com/es-es/HT204244>)
 - BT RCE (Mountain Lion y Mavericks): CVE-2014-4497
 - BT RCE: CVE-2014-8836
 - BT RCE: CVE-2014-8837



Bluetooth

Vulnerabilidades recientes de Bluetooth en iOS (& OS X)

- Arreglado en iOS 9.0 & OS X 10.11 (pero sin CVE)
 - Desplazamiento por directorios en AirDrop
 - AirDrop está disponible desde la pantalla de desbloqueo (Centro de control)
 - Modificación de ficheros de configuración para permitir cualquier app firmada con un certificado de desarrollador empresarial
 - Instalación de apps maliciosas (sin jailbreak) + "Masque attacks(s)"
 - Instalación de un perfil de configuración
 - Modificación de Springboard para confiar en el certificado empresarial
 - Sin la intervención del usuario
 - Sustitución de apps legítimas
 - Vídeo: <https://youtu.be/j3JODDmk2Hs>

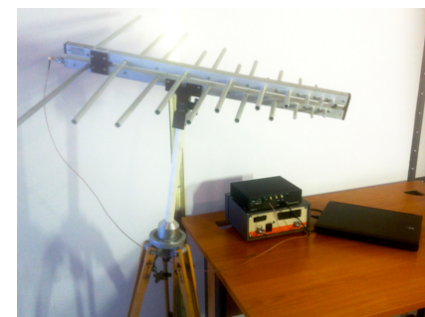
<http://www.forbes.com/sites/thomasbrewster/2015/09/16/airdrop-ios-vulnerability/>



Controlando Siri remotamente

Voice Hacking

- Siri: Asistente personal digital de Apple
- Investigadores franceses (Oct 2015)
 - ANSSI: Agencia gubernamental dedicada a la seguridad
- Transmisión silenciosa de comandos remota hacia Siri (2-5 metros)
 - Ondas de radio (electromagnéticas) convertidas a señales eléctricas
 - Parece audio que proviene del micrófono del usuario: "Hey, Siri..."
 - GNU Radio & USRP
- iPhone con auriculares y micrófono actuando de antena
 - Interacción completa con Siri: iniciar llamadas, enviar SMS, e-mails, navegar a sitios web, etc.



<http://www.wired.com/2015/10/this-radio-trick-silently-hacks-siri-from-16-feet-away/>



Apps

(Aplicaciones móviles)

centro criptológico nacional

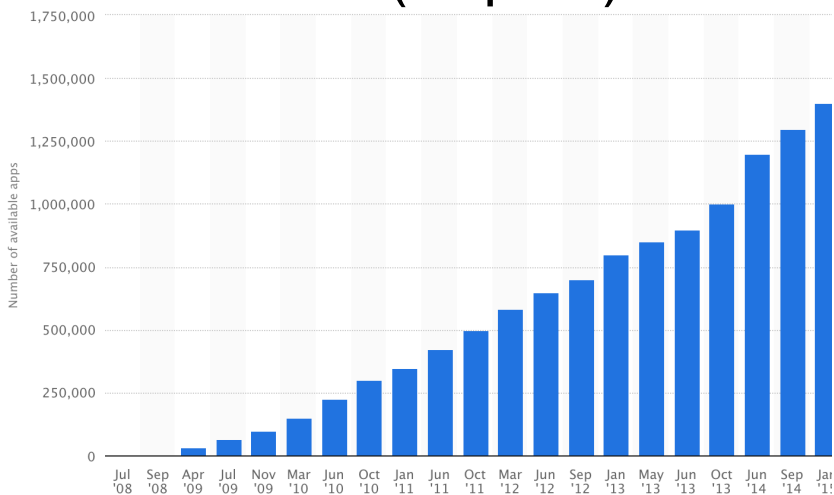


Available on the
App Store

App Store

¿Qué son estos números?

- 100.000 millones (Jul'08-Jun'15)- Descargas totales
- 1,5 millones (Jun'15)- Número total de apps
- 10.000 (Sep'15) - Número de apps para Apple Watch



Referencias: <http://ipod.about.com/od/iphonesoftwareterms/qt/apps-in-app-store.htm> & <http://www.statista.com/statistics/263794/number-of-downloads-from-the-apple-app-store/> & <http://www.statista.com/statistics/263795/number-of-available-apps-in-the-apple-app-store/>



Apps (XcodeGhost)

centro criptológico nacional



XcodeGhost (1/3)

¿Buenas prácticas de la industria? (verificar firmas del software)

- ¿De dónde descargan los desarrolladores sus herramientas?
 - Velocidad de descarga de los servidores de Apple: 3 GB
 - Fuentes no oficiales, colegas, Baidu (compartición de ficheros), etc
- Versión de Xcode troyanizada que infecta apps de iOS & OS X
 - Objeto Mach-O malicioso distribuido junto al compilador (LLVM linker)
 - CoreServices: Clases UIWindow & UIDevice
 - <https://github.com/XcodeGhostSource/XcodeGhost>
 - Apps del mercado chino y... ¡otras 39 apps legítimas! (al menos...)
 - Malware en la AppStore (¿revisión de código de Apple?)
 - Sexta vez: LBTM, InstaStock, FindAndCall, Jekyll & FakeTor

<http://researchcenter.paloaltonetworks.com/2015/09/novel-malware-xcodeghost-modifies-xcode-infects-apple-ios-apps-and-hits-app-store/>

XcodeGhost (2/3)

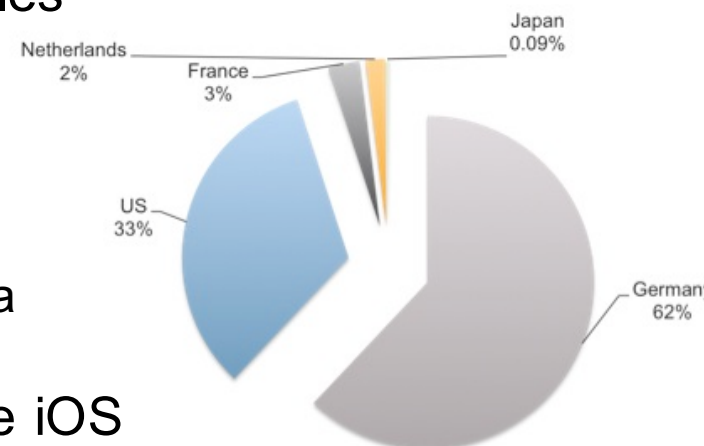
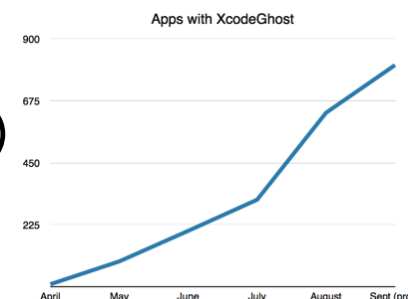
Extrapolar el mismo escenario fuera de China... (realidad)

- Potencialmente, cientos de millones de usuarios afectados
- 39 apps: WeChat, Didi (Uber chino), app oficial para la compra de billetes de tren, app principal Telco, app principal de bolsa...
- Muchas otras apps: WinZip, PDFReader, CamScanner...
 - Fox-IT (+50 apps), Qihoo 360 (344 apps), Pangu Team (3.418 apps)...
- Recolecta información y la envía cifrada a servidores C&C (Amazon AWS)
- Recibe comandos de los servidores C&C y puede:
 - Generar ventanas de diálogo falsas ("phishing", ej. iCloud), abrir URLs de esquemas específicos (ataques entre apps), leer/escribir del/al portapapeles (ej. gestor de contraseñas)...
- Desde marzo 2015 (Xcode falsos) hasta mediados de septiembre 2015
 - Validando la versión de Xcode: <https://developer.apple.com/news/?id=09222015a>
 - Gatekeeper: `$ spctl --assess --verbose /Applications/Xcode.app`

XcodeGhost (3/3)

Los especímenes de malware también evolucionan

- Variantes (XcodeGhost S) un mes y medio después (Nov 2015)
 - Actualizado para iOS 9 y ATS (Apple Transport Security)
 - Lista de excepciones para los servidores C&C que usan HTTP
- Entornos de distribución de apps iOS empresariales
 - 210 empresas afectadas en varios países
- La manipulación del tráfico C&C permitiría:
 - Distribuir apps fuera de la App Store
 - Forzar la navegación a URLs específicas
 - Lanzar la página de descarga de una app concreta
 - Generar ventanas de diálogo falsas (phishing)
- Aún hay muchas versiones antiguas de apps y de iOS
 - <https://sourcedna.com/blog/20150922/xcodeghost-lifecycle-in-app-store.html>



https://www.fireeye.com/blog/threat-research/2015/11/xcodeghost_s_a_new.html



Apps **("Desarrolladores" empresariales)**

ccv-cent

centro criptológico nacional

Distribución de apps fuera de la AppStore

- Apple Developer Enterprise Program (vs Apple Developer Program)
 - <https://developer.apple.com/programs/enterprise/> (\$299/año)
- Provisionamiento de apps iOS para distribución interna
 - Supuestamente sólo pueden ser empleadas para distribución interna
 - Técnicamente se pueden usar para instalar cualquier app en cualquier dispositivo 😊 (violación de los términos de uso del programa)
 - No pasa por los mecanismos de revisión de Apple (AppStore)
 - Permite el uso de APIs privadas de Apple (operaciones sensibles)
- El usuario debe aceptar su instalación (dos pulsaciones)
 - En iOS 9 se debe confiar en el perfil de provisionamiento (manualmente)

<http://johannesluderschmidt.de/provision-ios-ipa-app-for-in-house-enterprise-distribution/>

Distribución de apps fuera de la AppStore

O... cómo hackear el ecosistema de Apple por \$299/año + certificado HTTPS

"Dos pulsaciones para gobernarlos a todos"



Distribución “benigna”: Beta Testers (1/2)

España (y China): Mayo 2015 – Curso SANS SEC575 en Madrid

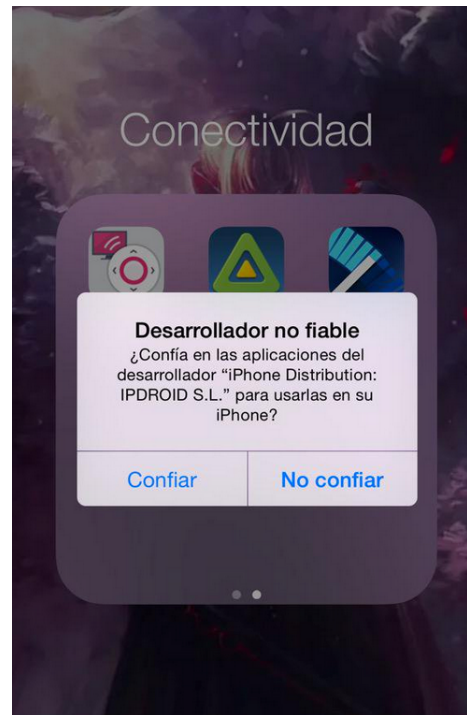
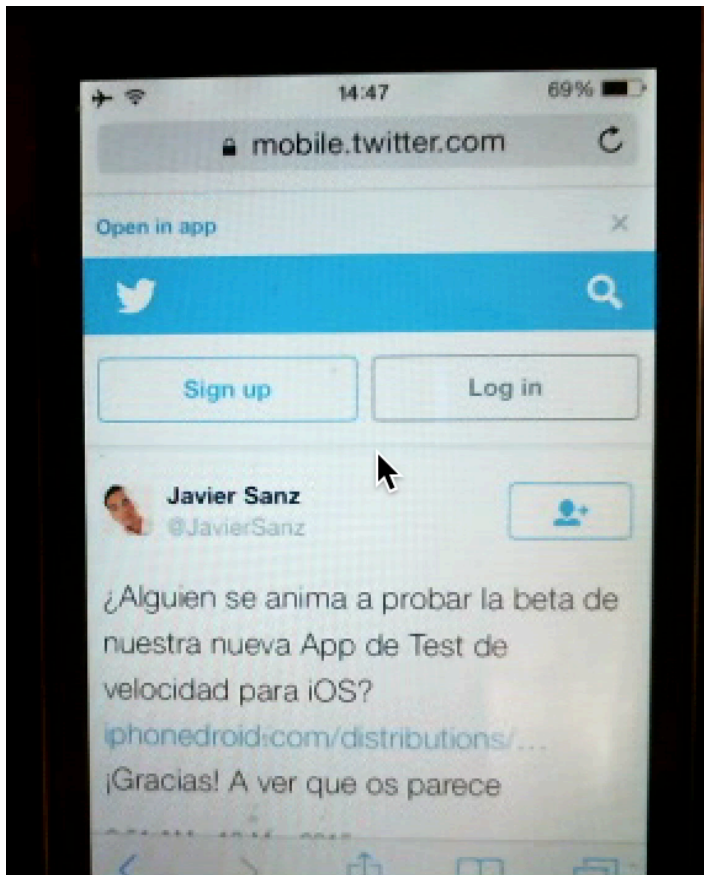


- Requisitos para el "desarrollador" empresarial (\$299/año)
 - Certificado para la distribución de la app
 - Perfil de aprovisionamiento
 - Crear el fichero IPA y el Manifest asociado (fichero PLIST)
 - Enlace web "itms-services" al fichero de Manifest
 - El Manifest referencia al fichero IPA (app)
 - Disponer de un servidor web con un certificado HTTPS válido
- Ejemplo: Tweet, página web, etc
 - Google dork...

```
<a href="itms-services://?action=download-manifest&url=https://www.dinosec.com/dist/app/manifest.plist">¡Instalar app!</a>
```

(2/2)

iOS 7 & 8: Una vez al ejecutar la 1ª vez... vs. iOS9



www.ccn-cert.cni.es



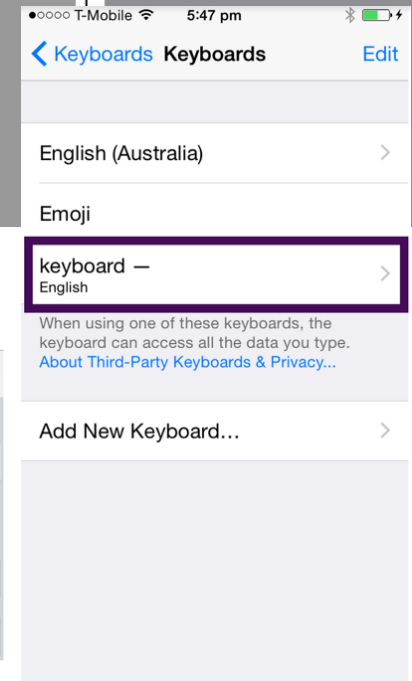
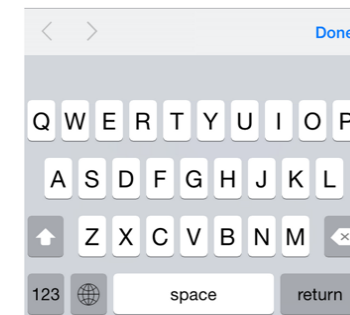
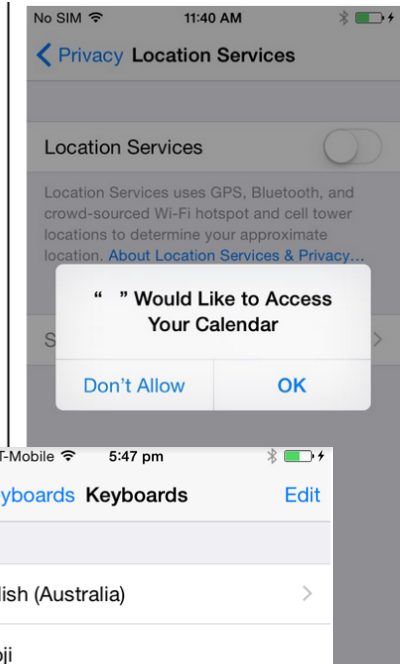
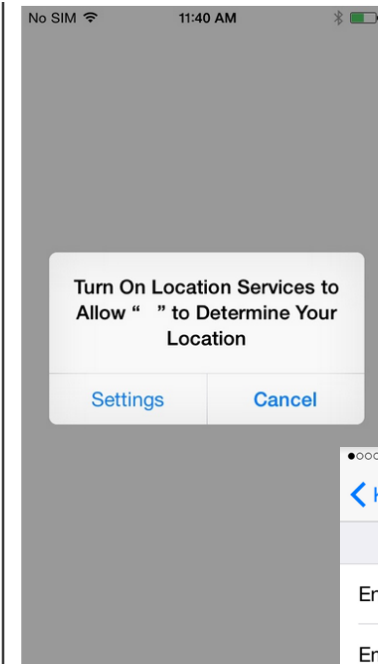
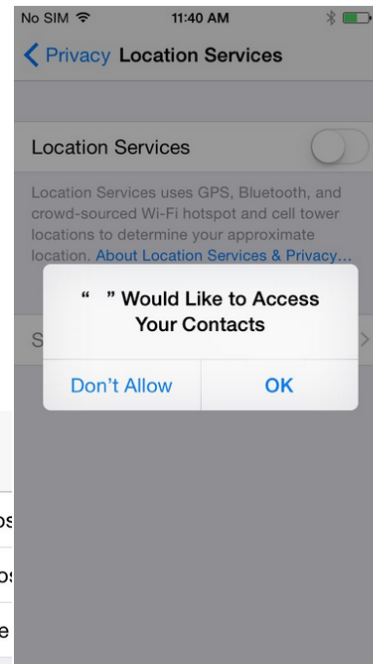
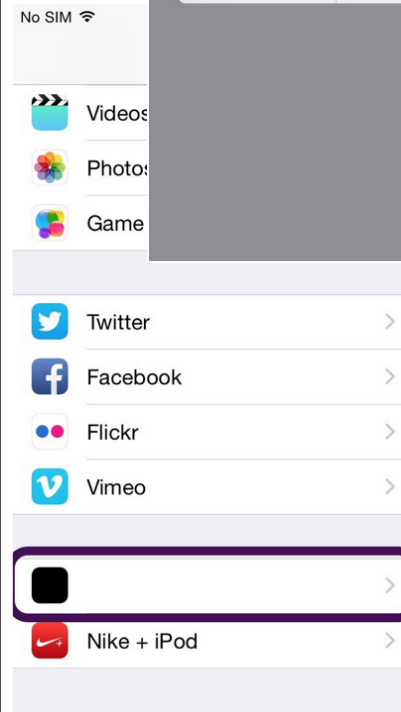
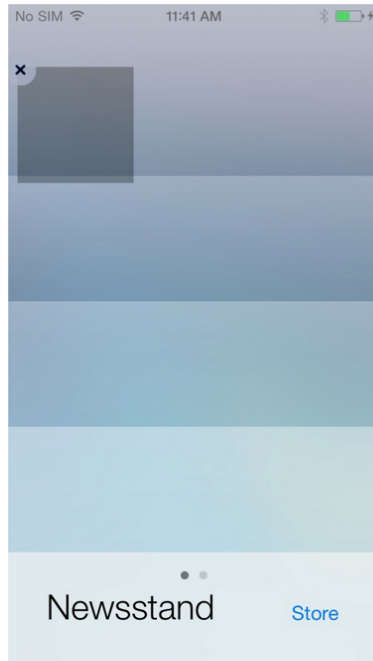
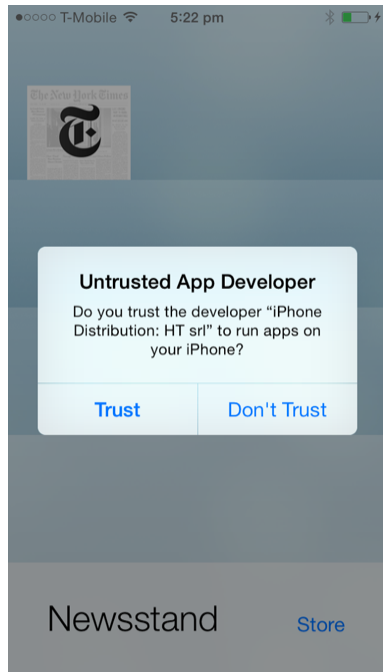
Distribución “maligna”: Hacking Team (1/2)

Italia: Julio 2015

- Malware para dispositivos iOS sin el jailbreak (App: Newsstand)
 - Además de 11 apps usadas en "Masque Attacks"
 - WhatsApp, Twitter, Facebook, Facebook Messenger, WeChat, Google Chrome, Viber, Blackberry Messenger, Skype, Telegram, y VK
- Infección desde la web o por USB (malware OS X o Windows)
- Obtener información de contactos, calendario, localización...
- Instalación de un teclado personalizado (keylogger de todas las apps)
 - Similar al teclado por defecto de iOS
 - Debe ser seleccionado manualmente por el usuario (o un tercero)

<https://blog.lookout.com/blog/2015/07/10/hacking-team/>

Distribución “maligna”: Hacking Team (2/2)





Apps

(APIs privadas de Apple)

ccv-cert

centro criptológico nacional

APIs privadas de Apple (1/2)

- Objective-C
 - Mecanismo de envío de mensajes para la llamada a métodos
 - `objc_msgSend` (parámetros de tipo String)
 - Nombre de clase y nombre de método
 - No resueltos estáticamente, sino en tiempo de ejecución
 - Ofuscación y/o cifrado
 - Cargar una librería (`dlopen`) y acceder a una función (`dlsym`)
 - En tiempo de ejecución (o `NSStringFromClassString/NSStringSelectorFromString`)
- Apple AppStore App Review (escrutinio)
 - APIs privadas que acceden a información sensible del usuario

APIs privadas de Apple (2/2)

- "iRiS: Vetting Private API Abuse in iOS Applications" (Oct 2015)
 - Análisis dinámico de llamadas a APIs que no pueden resolverse estáticamente ("sospechosas")
 - Analizaron 2.019 apps: 146 (7%) usan 150 APIs privadas (25 críticas)
- SourceDNA (Oct 2015) – métodos descritos previamente –
 - 256 apps afectadas (+1 millón de descargas)
 - Youmi's Ad SDK (librería binaria ofuscada para anuncios)
 - Envía la info del usuario a un servidor en China
 - Lista de apps instaladas, app en ejecución actualmente (desde hace 2 años), nº. serie, componentes hardware (periféricos), "e-mail" Apple ID...

<http://www.cse.buffalo.edu/~mohaisen/classes/fall2015/cse709/docs/deng-ccs15.pdf>

<https://sourcedna.com/blog/20151018/ios-apps-using-private-apis.html>

Abusando las APIs privadas de Apple

- YiSpecter (Oct 5, 2015)
 - Certificado de desarrollador empresarial (evitar la AppStore)
 - APIs privadas (evitar App Review)
 - MobileInstallation: instalación de apps locales (fichero .ipa) & desinstalación
 - Reclama el derecho empleado por apps de sistema
 - `com.apple.private.mobileinstall.allowedSPI`
 - Monitorizar la app abierta actualmente y mostrar una pantalla con anuncios
 - SpringBoardServices: `SBSCopyFrontmostApplicationDisplayIdentifier`
 - SpringBoardServices: `SBSLaunchApplicationWithIdentifier`
 - Lista de apps instaladas: `MobileInstallationLookup`
 - Manipulación de Mobile Safari: buscador por defecto, favoritos, etc.

<http://researchcenter.paloaltonetworks.com/2015/10/yispecter-first-ios-malware-attacks-non-jailbroken-ios-devices-by-abusing-private-apis/>



Escalada de privilegios (1/4)

rootpipe

- *Apple OS X Admin framework*
 - *Hidden backdoor API to root privileges (XPC)*
 - Desde 2011 (OS X 10.7.x)
- Emil Kvarnhammar
 - 09/04/2015
- Fix: OS X 10.10.3 (CVE-2015-1130)
 - Apple decidió no parchear versiones previas de OS X 10.9.x...
- Metasploit: exploit/osx/local/rootpipe



Raul Siles
@raulsiles

Seguir

OS X < 10.10.3:

```
$ vi run.c
...
$ gcc run.c -o run
$ rootpipe.py run run-root
$ ./run-root
sh-3.2# id
uid=0(root) ...
```

truesecdev.wordpress.com/2015/04/09/hid

Ver traducción

```
Settings myIsAuthenticated
rsp, rsp
jne_stubs__getuid
eax, eax
al, al
eax, al
rsp
```

<https://truesecdev.wordpress.com/2015/04/09/hidden-backdoor-api-to-root-privileges-in-apple-os-x/>

Escalada de privilegios (2/4)

DYLD_PRINT_TO_FILE

- *Dynamic linker (dyld) error logging to an arbitrary file, as root*
- Steffan Esser
 - 07/07/2015
- Fix: OS X 10.10.5 (CVE-2015-3760) – Desde OS X 10.10
- Protección
 - <https://www.suidguard.com> (<https://github.com/sektioneins/SUIDGuard>)
- Ataques reales:
 - https://blog.malwarebytes.org/mac/2015/08/dyld_print_to_file-exploit-found-in-the-wild/

https://www.sektioneins.de/en/blog/15-07-07-dyld_print_to_file_lpe.html

Escalada de privilegios (3/4)

tpwn

- *XNU LPE (NULL Pointer Deference)*
- Luca Todesco
 - 15/08/2015
- Fix: OS X 10.11 (CVE-2015-5847 & 5864) – Desde OS X 10.6.8
 - Fixed in 10.11.1 (CVE-2015-5932)
- Protección
 - <https://github.com/kpwn/NULLGuard>

<https://github.com/kpwn/tpwn>

Escalada de privilegios (4/4)

npwn

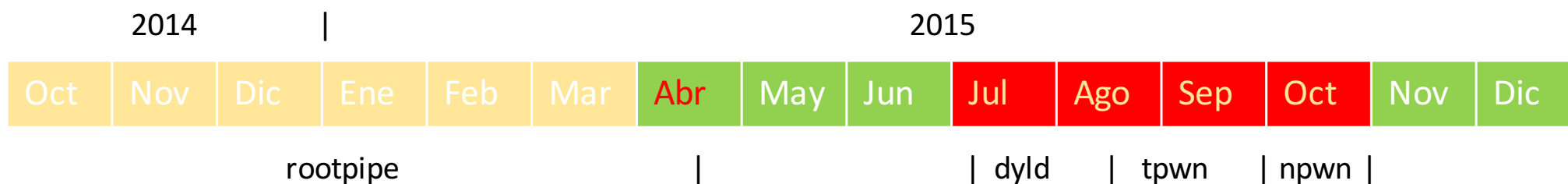
- Kernel exploit
 - Permite evitar System Integrity Protection (SIP o rootless)
 - *"[any] piece of malware is one password or vulnerability away from taking full control of the device"*
- Luca Todesco
 - 11/09/2015 (Desde 07/2015 - tweet)
- Fix: OS X 10.11.1 (CVE-2015-6974) – Desde OS X 10.11

<https://www.blackhat.com/docs/eu-15/materials/eu-15-Todesco-Attacking-The-XNU-Kernal-In-El-Capitain.pdf>
<https://ghostbin.com/paste/ckeu8>

Escalada de privilegios: Resumen

¿Cuánto tiempo hemos sido vulnerables...?

- rootpipe: 09/04/2015 (08/04/2015 – OS X 10.10.3) - responsable
 - Conocido desde 03/10/2014 – 7 meses
- DYLD_PRINT_TO_FILE: 07/07/2015 (13/08/2015 – OS X 10.10.5) – 1 mes y 1 semana
- tpwn: 15/08/2015 (30/09/2015 – OS X 10.11) – 1 mes y medio
- npwn: 11/09/2015 (21/10/2015 – OS X 10.11.1) – 1 mes y medio
 - Conocido desde 07/2015 – 4 meses



Amarillo: Vulnerabilidad conocida privadamente

Rojo: Vulnerabilidad conocida públicamente

iCloud Remote Lock Bug

Guía CCN-STIC de OS X



Raul Siles
@raulsiles

+ Seguir

(1/2) Interesting OS X (DoS) bug when a lock PIN code is remotely set via iCloud. After 5 failed attempts, the anti-brute force timeout...

Ver traducción

RETWEETS
3



6:42 - 7 sept. 2015

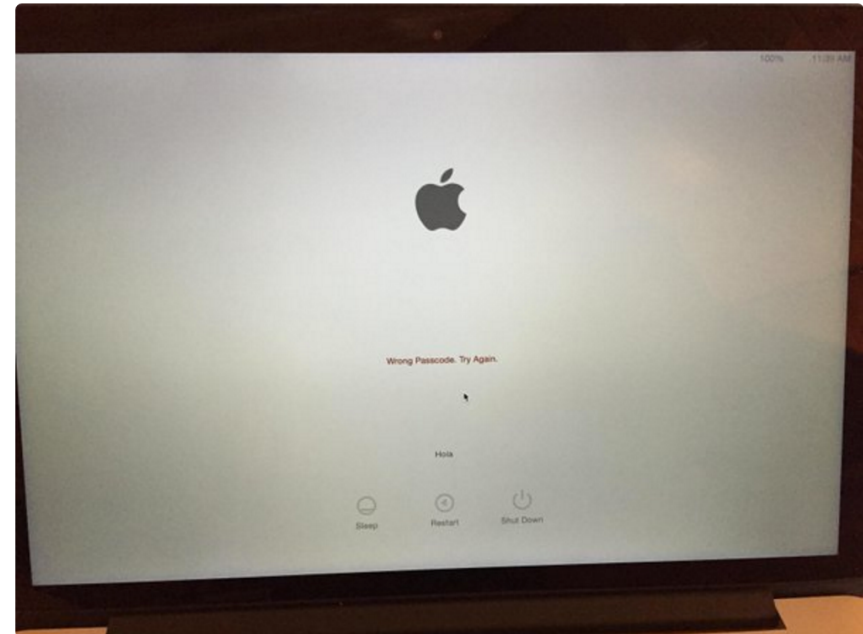


Raul Siles
@raulsiles

+ Seguir

(2/2) ...appears (1-5-15-60 mins), but there is no input field to enter the system lock PIN code to unlock the Mac!

Ver traducción



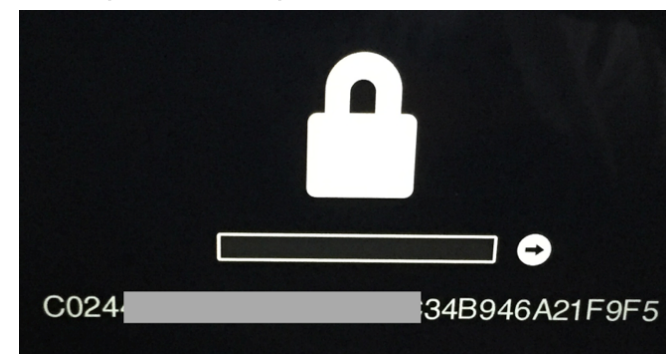
RETWEETS
3



6:43 - 7 sept. 2015

Acceso físico a OS X

- Establecer la contraseña en el firmware (o EFI) del equipo
 - PIN de bloqueo remoto desde iCloud: "Buscar mi Mac"
- Solicitada al arrancar en cualquier modo especial (por defecto)
- Si se "olvida", aún hay una opción...
 - Apple o Apple Authorized Service Provider o terceros (Internet)
 - Verificación del propietario
 - Acceso físico al equipo o hash
- Pantalla que solicita la contraseña del firmware
 - Ctrl+Alt+Cmd+Shift+S
 - Hash de 33 caracteres (17+16)
- Apple genera un código de respuesta en forma de fichero (keyfile), denominado "SCBO", que puede ser cargado en el arranque (memoria USB)





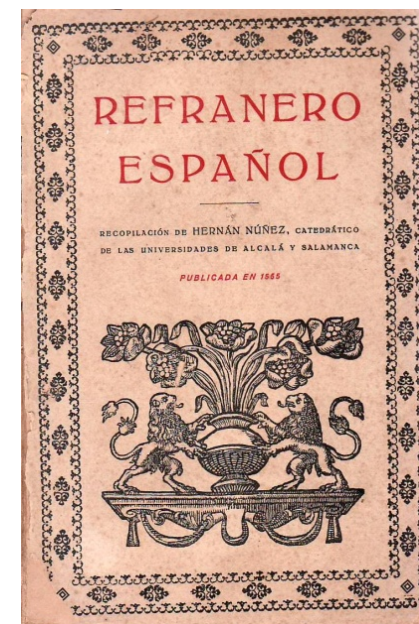
Low Hanging Fruit

El refranero español

Las manzanas... ¿pueden ser perjudiciales para la salud?

“Una manzana al día...
mantiene al intruso en
la lejanía”

(“An apple a day keeps the intruder away”)



Guías CCN-STIC: iOS & OS X

¡Muchas gracias!

¿Preguntas?



Raúl Siles

Fundador & Analista de Seguridad

raul@dinosec.com



www.dinosec.com

[@dinosec](https://twitter.com/dinosec)



Otra “perlas” de la cosecha de 2015 (1/2)

- AFNetworking (March 2015 - Abril 20 & 24, 2015)
 - <http://blog.mindedsecurity.com/2015/03/ssl-mitm-attack-in-afnetworking-251-do.html>
 - <https://sourcedna.com/blog/20150420/afnetworking-vulnerability.html> (+1,500 apps)
 - <https://sourcedna.com/blog/20150424/afnetworking-strikes-back.html> (25,000 apps)
- Darwin Nuke (DoS) 10/04/2015 – IP options (iOS 8 & OS X 10.10)
 - <https://securelist.com/blog/research/69462/darwin-nuke/>
- “No iOS Zone” (DoS) 22/04/2015 – Malicious SSL certificates (iOS < 8.3)
 - <https://www.skycure.com/blog/ios-shield-allows-dos-attacks-on-ios-devices/>
 - WiFiGate: <https://www.skycure.com/blog/wifigate-how-mobile-carriers-expose-us-to-wi-fi-attacks/>
- Apple Watch Exploit: Steal a Passcode-Protected Watch & Use Apple Pay to Buy Things
 - <https://youtu.be/2blTo-Ej6mo>
- XARA: Unauthorized Cross-App Resource Access on MAC OS X and iOS (Junio 2015)
 - <https://drive.google.com/file/d/0BxxXk1d3yyuZOFIsdkNMSGswSGs/view?pli=1>
 - <http://www.imore.com/depth-look-ios-os-x-xara-vulnerabilities>
- iOS Mail.app content injection (Junio 2015)
 - <https://github.com/jansoucek/iOS-Mail.app-inject-kit> (<https://www.youtube.com/watch?v=9wiMG-oqKf0>)
- KeyRaider: iOS Malware Steals Over 225,000 Apple Accounts (30/08/2015)
 - <http://researchcenter.paloaltonetworks.com/2015/08/keyraider-ios-malware-steals-over-225000-apple-accounts-to-create-free-app-utopia/> (for jailbroken devices)

Otra “perlas” de la cosecha de 2015 (2/2)

Masque Attack(S):

- "Masque Attack: All Your iOS Apps Belong to Us" (Nov'14)
 - <https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html>
 - Wirelurker:
 - <http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/>
- "iOS Masque Attack Revived: Bypassing Prompt for Trust and App URL Scheme Hijacking" (Feb'15)
 - https://www.fireeye.com/blog/threat-research/2015/02/ios_masque_attackre.html
- "Three New Masque Attacks against iOS: Demolishing, Breaking and Hijacking" (Jun'15)
 - https://www.fireeye.com/blog/threat-research/2015/06/three_new_masqueatt.html
- "iOS Masque Attack Weaponized: A Real World Look" (Aug'15)
 - https://www.fireeye.com/blog/threat-research/2015/08/ios_masque_attackwe.html

➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sondas@ccn-cert.cni.es
- redsara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es



Síguenos en Linked in

