
16 Hackeando
Plataformas móviles
Julio Javier Iglesias Pérez
C|EH Julio Iglesias Pérez

Introducción

En 2012 cerca de 17.676 programas malware para móviles fueron detectados durante la primera mitad.

Cerca de un cuarto de los malwares vinieron desde China, mientras que el 17% vinieron de Rusia y el 16.5% desde EEUU.

El surgimiento de malware para móviles ocurrió al mismo tiempo que China se convirtió en el mercado de smartphones más grande del mundo. Los móviles con Android lideran el mercado con un 68%, de acuerdo con la firma Canalys.

Terminologías

- **Stock ROM:** Es la ROM por defecto (Sistema Operativo) de un dispositivo Android provisto por el fabricante.
- **CyanogenMod:** Es un ROM modificado sin las restricciones impuestas por la ROM original.
- **Bricking el dispositivo Móvil:** Es la alteración del Sistema del dispositivo utilizando rooting o jailbreaking, de manera tal que causa que el dispositivo móvil se vuelva inestable o inoperable
- **Trae tu propio dispositivo (BYOD: Bring Your Own Device):** Es una política de negocios que permite a los empleados llevar sus dispositivos móviles a su trabajo.

Vectores de ataque

Exfiltración de Datos:
- Datos extraídos del FLUJO de Datos y de Correo electrónico.
- Pantalla y captura de imágenes Impresas.
- Copia de la clave USB y pérdida de la copia de seguridad.

Manipulación de datos:
- Modificación por otra aplicación.
- Intentos de sabotaje sin ser detectados.
- Jail-broken dispositivo.

La pérdida de datos:
- Vulnerabilidades de aplicaciones.
- Acceso físico no aprobado.
- Pérdida del dispositivo.

Malware:
- Virus Y Rootkits.
- Modificación de Aplicación.
- Modificación de Sistema Operativo.

Vulnerabilidades y Riesgos

- Las nuevas funcionalidades amplifican la atracción de las plataformas utilizadas en los dispositivos móviles, pues, proveen una fácil ruta para que los atacantes lancen ataques y explotaciones. Los atacantes utilizan distintas tecnologías como Android y otras instancias múltiples para insertar aplicaciones maliciosas con una funcionalidad oculta que puede obtener información sensible del usuario.

Vulnerabilidades y Riesgos

Las siguientes son algunos de los riesgos y vulnerabilidades asociadas con las plataformas móviles:

- Tiendas de aplicaciones (App Stores).
- Malware móvil.
- App Sandboxing.
- Cifrado de dispositivo y aplicaciones.
- Actualizaciones del Sistema y Alicaciones.
- Jailbreaking y Rooting.
- Vulnerabilidades de las aplicaciones móviles.
- Problemas de privacidad (Geolocación).
- Seguridad de Datos.
- Permisos Ejecutivos.
- Seguridad de las comunicaciones.
- Ataques físicos

Problemas de Seguridad en las App Stores

Cuando los usuarios descargan aplicaciones desde una App Store oficial, entonces la aplicación es segura ya que fue probada. El problema se suscita cuando los usuarios descargan aplicaciones desde App Stores de terceros, ya que existe una posibilidad de que la aplicación descargada contengan malware, ya que en estas App Stores no se realizan las pruebas que sí se realizan en las App Stores oficiales.

Problemas de Seguridad en las App Stores

Por ejemplo, un atacante descarga un juego legítimo y lo "reempaqueta" con un malware y lo sube a una App Store de terceros (no oficial). Cuando un usuario descarga este juego, el malware obtiene información y envía credenciales del usuario como logs/photo/videos/sensitive al atacante sin conocimiento del usuario. Con esta información, el atacante puede explotar el dispositivo utilizando muchos ataques, como también el atacante puede utilizar técnicas de ingeniería social para incitar a los usuarios a realizar descargas desde estas App Stores. Las aplicaciones pueden dañar otras aplicaciones y datos y enviar información sensible a los atacantes.

Amenazas de Malware Móvil

En los últimos años, muchos usuarios están cambiando el uso de equipos personales hacia los smartphones y tablets. Esto incrementó la adopción de dispositivos móviles por los usuarios para uso personal, lo que incitó a los atacantes a lanzar ataques a estos dispositivos móviles. Los atacantes lo hacen porque la información almacenada en estos es mucho más sensible. SMS poofing, fraude, etc. son ataques realizados por los atacantes en dispositivos móviles.

El malware incluido en móviles incluye virus, malware SMS, botnets móviles, spyware, troyanos destructivos, etc.

Para infectar los dispositivos móviles, el atacante que escribe un malware o crea una aplicación maliciosa y la publica en una Store y aguarda a que el usuario instale ésta. Cuando esto sucede, el atacante toma control sobre el dispositivo.

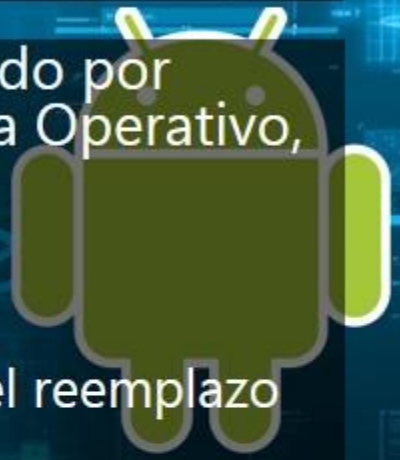
Problemas de Seguridad en App Sandboxing

Asegurar un ambiente sandbox: En un entorno de recinto seguro (sandbox), a cada aplicación se le da su propio entorno de trabajo. Como resultado, la aplicación está limitada a acceder a los otros datos de usuario y los recursos del sistema. Esto proporciona protección a los dispositivos móviles contra las amenazas de malware.

Ambiente sandbox vulnerable: En los entornos sandbox vulnerables, la aplicación maliciosa aprovecha las deficiencias y vulnerabilidades del sandbox y lo bypasea. Como resultado, la aplicación puede acceder a otros datos de usuario y los recursos del sistema que están restringidos.

Android

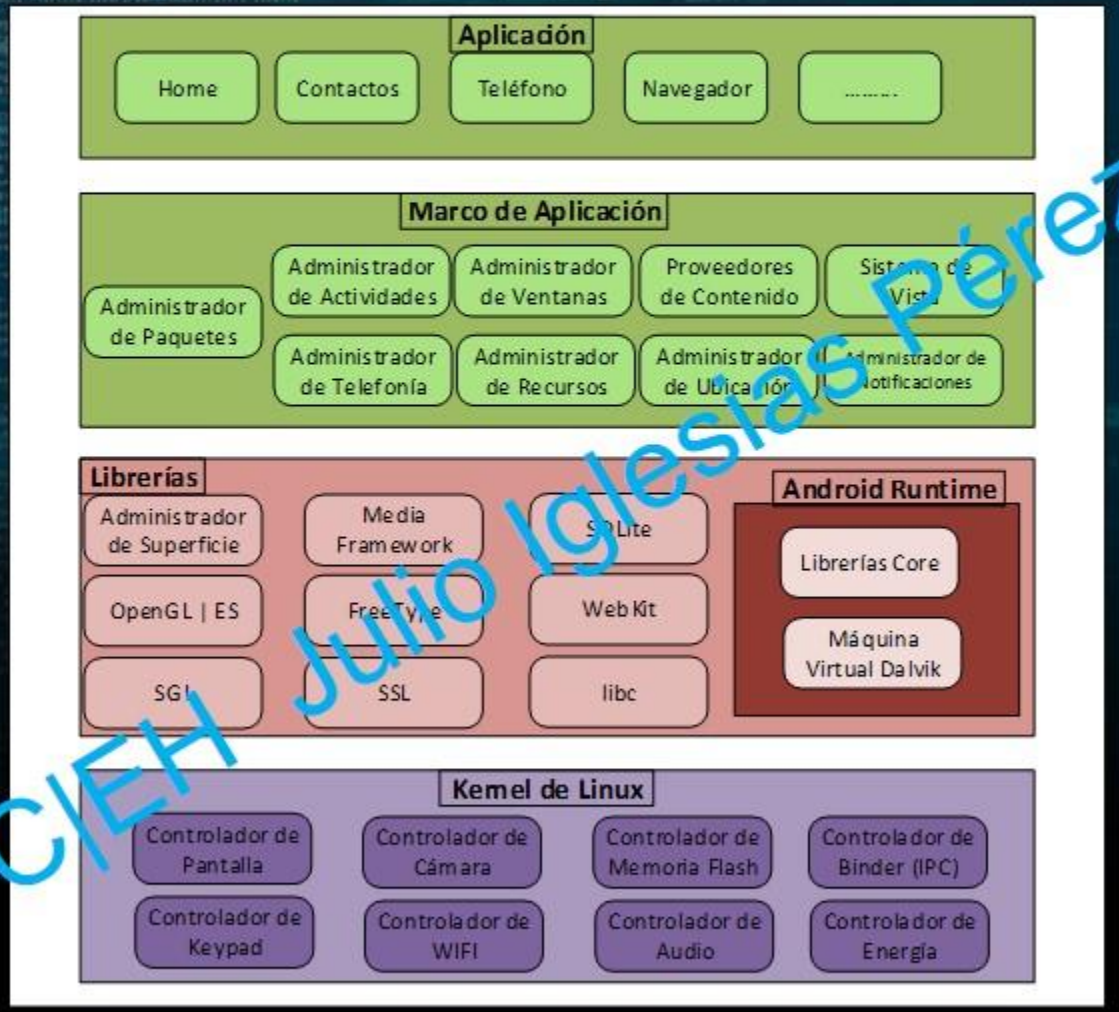
Android es el nombre del ambiente de software creado por Google para dispositivos móviles que incluye Sistema Operativo, software y aplicaciones claves.



Características

- Marco de aplicación que permite la reutilización y el reemplazo de componentes.
- Máquina virtual Dalvik optimizada para dispositivos móviles.
- Navegador integrado basado en el motor WebKit de código abierto.
- SQLite para almacenamiento de datos estructurados.
- Soporte multimedia para audio comunes, vídeo y formatos de imágenes fijas (MPEG4, H.264, MP3, AAC, AMR, JPG, PNG, GIF).
- Entorno de desarrollo incluyendo un emulador de dispositivos, herramientas para depuración, memoria y perfiles de rendimiento, y un plugin para el IDE Elipse.

Arquitectura de Android



Arquitectura de Android

Aplicación: Las aplicaciones provistas por Android incluyen: cliente de correo electrónico, SMS, calendario, mapas, navegador, contactos, etc. Estas aplicaciones están escritas en lenguaje Java

Marco de Aplicación

- Android al ser una plataforma abierta, los desarrolladores tienen acceso completo a la API que es utilizada por las aplicaciones básicas
- El Sistema de Vista puede ser utilizado para crear listas, grids, text boxes, botones, etc. en la aplicación
- El proveedor de contenidos permite a las aplicaciones acceder a los datos desde otras aplicaciones, con el fin de compartir sus propios datos
- El administrador de recursos aloja los recursos de no-código como cadenas, gráficos, etc.
- El administrador de notificaciones ayuda a las aplicaciones a mostrar mensajes personalizados en la barra de estado
- El administrador de actividades controla el ciclo de vida de las aplicaciones

Arquitectura de Android

Librerías: Comprenden cada código que proporciona las características principales de un sistema operativo Android. Por ejemplo, la base de datos de apoyo es proporcionada por la librería SQLite para que una aplicación pueda utilizar para el almacenamiento de datos y funcionalidades para el navegador web proporcionado por el Kit de Biblioteca Web.

La librería principal de Android incluye el Administrador de superficie, Media Framework, SQLite, OpenGL | ES, FreeType, WebKit, SGL, SSL, licb, SQLite (motor), y LibCoreWeb (motor de navegador web)

Arquitectura de Android

Librerías: Comprenden cada código que proporciona las características principales de un sistema operativo Android. Por ejemplo, la base de datos de apoyo es proporcionada por la librería SQLite para que una aplicación pueda utilizar para el almacenamiento de datos y funcionalidades para el navegador web proporcionado por el Kit de Biblioteca Web.

La librería principal de Android incluye el Administrador de superficie, Media Framework, SQLite, OpenGL | ES, FreeType, WebKit, SGL, SSL, licb, SQLite (motor), y LibCoreWeb (motor de navegador web)

Android Runtime: Incluye librerías básicas y la máquina virtual de Dalvik. El conjunto de librerías básicas permite a los desarrolladores escribir aplicaciones Android utilizando el lenguaje de programación Java. La Máquina virtual Dalvik es de gran ayuda en la ejecución de aplicaciones de Android. Dalvik puede ejecutar múltiples máquinas virtuales de manera eficiente.

Arquitectura de Android

Kernel de Linux: El sistema operativo Android fue construido basado en el núcleo Linux. Esta capa está formada por todos los controladores de dispositivos de bajo nivel, controlador de pantalla, controlador de cámara, controlador de memoria Flash, controlador Binder (IPC), controlador de teclado, controlador WIFI, controlador de audio, y la administración de energía de varios componentes de hardware de un dispositivo Android .

Android Device Administration API

El Device Administration API fue introducido en Android 2.2 y provee características administrativas a nivel del Sistema. Estas APIs permiten a los desarrolladores crear aplicaciones seguras.

Sus características son: Contraseña habilitada, longitud mínima de contraseña, contraseñas alfanuméricas requeridas, contraseñas complejas requeridas en la contraseña, mínimo de letras requeridas en la contraseña, mínimo de letras minúsculas en la contraseña, mínimo de caracteres no-letras requeridas, mínimo de dígitos requeridos, mínimo de símbolos requeridos, mínimo de letras mayúsculas requeridas, tiempo de caducidad de la contraseña, restricción en el historial de las contraseñas, máximo de intentos en la contraseña, máximo de tiempo de inactividad antes de bloquear el dispositivo, requerir cifrado en el almacenamiento, deshabilitar cámara, bloquear dispositivo inmediatamente, limpiar los datos del dispositivo.

Android Device Administration API

C|EH Julio Iglesias Perez

Android Rooting

El Rooting permite a los usuarios de Android lograr control privilegiado (conocido como "acceso de superusuario") en el subsistema.

Este proceso involucra explotar vulnerabilidades en el firmware del dispositivo y copiar el binario SU a una ubicación (ej /system/xbin/su) y obtener acceso con el comando chmod.

El rooting permite a las aplicaciones ejecutar comandos con privilegios como:

Modificar o eliminar archivos del sistema, módulos, ROMs (stock firmware) y núcleos; quitar aplicaciones de fabricante (bloatware); acceso en bajo nivel al hardware que típicamente no está disponible en la configuración por defecto; rendimiento mejorado, tethering (atado) wifi y bluetooth; instalar aplicaciones en tarjetas SD; mejor interfaz y teclado.

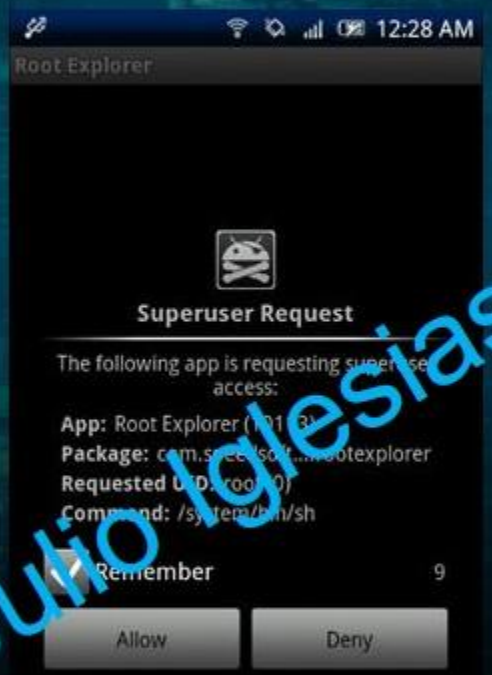
Los riesgos involucrados al Rooting:

Pierde garantía; rendimiento pobre; infección malware; brick.

Rooteando Teléfonos Android con SuperOneClick

- Conectar el dispositivo Android en el equipo vía USB.
- Instalar el controlador si es necesario.
- Desconectar y reconectar, pero esta vez seleccionar "change only" para asegurarse de que la tarjeta SD no sea montada.
- Ir a Settings, Applications, Develpment, y habilitar USB Debugging para configurar el Android en modo depuración.
- Ejecutar SuperOneClick.exe.
- Clic en el botón "Root".
- Esperar hasta que salga el mensaje "Running a Su test Success!"
- Ahora revisar las aplicaciones instaladas en el dispositivo.
- El ícono Superuser significa que tenemos acceso de superusuario (reiniciar el dispositivo si es que éste no aparece).

Rooteando Teléfonos Android con SuperOneClick



C|EH Julio Iglesias Pérez

Rooteando Teléfonos Android con Superboot

1. Descargar y extraer los archivos de Superboot.
2. Colocar el teléfono en modo bootloader
   - Apagar el dispositivo, quitar la batería, y colocar el cable USB.
   - Cuando el ícono de la batería aparezca en la pantalla, volver a colocar la batería.
   - Ahora presionar el botón encendido mientras manteiene pulsado el botón de la cámara
   - Para teléfonos Android que tienen el trackball, apagar el teléfono y mantener presionado el trackball, luego encender el teléfono.
3. Dependiendo del S.O. del equipo realizar:
   - Windows: Doble clic en "install-superboot-windows.bat".
   - Mac y Linux: Abrir una terminal en el directorio donde contenga los archivos y luego ejecutar: chmod +x install-superboot-mac.sh seguido de ./install-superboot-mac.sh
4. El dispositivo está rooteado.

Herramientas de Rooteo de Android

Además, existen otras herramientas que pueden ser utilizadas para rootear Android:

- Unrevoked: http://unrevoked.com
- Recovery Flasher: http://sites.google.com/site/adlxmod
- Universal Androot: http://forum.xda-developers.com
- Unlock Root: http://www.unlockroot.com

Session Hijacking utilizando DroidSheep

- Es una herramienta web para realizar session hijacking (sidejacking).
- Escucha paquetes HTTP enviados vía wifi (802.11) y extrae los IDs de las sesiones de estos paquetes.
- Puede capturar sesiones utilizando la librería libpcap y soporta: Redes abiertas, redes cifradas con WEP, cifradas con WPA y WPA2 (PSK solamente).

Session Hijacking utilizando DroidSheep

C|EH Julio Iglesias Pérez

Sniffer para Android: FaceNiff

FaceNiff es una aplicación para Android que permite realizar sniff e interceptar perfiles de sesiones Web solo cuando Wi-Fi no está utilizando EAP, pero debería trabajar sobre cualquier red privada (Open/WEP/WPA-PSK/WPA2-PSK).

Esta aplicación no funciona si el usuario web utiliza SSL.

Sniffer para Android: FaceNiff

C|EH Julio Iglesias Pérez

Troyano para Android: ZitMo (Zeus-in-the-Mobile)

Este Troyano malware fue diseñado para robar cuentas bancarias online. Este elude la aplicación segura bancaria o simplemente enviando SMS desde los teléfonos infectados a un móvil de comando y control de propiedad de los cibercriminales.

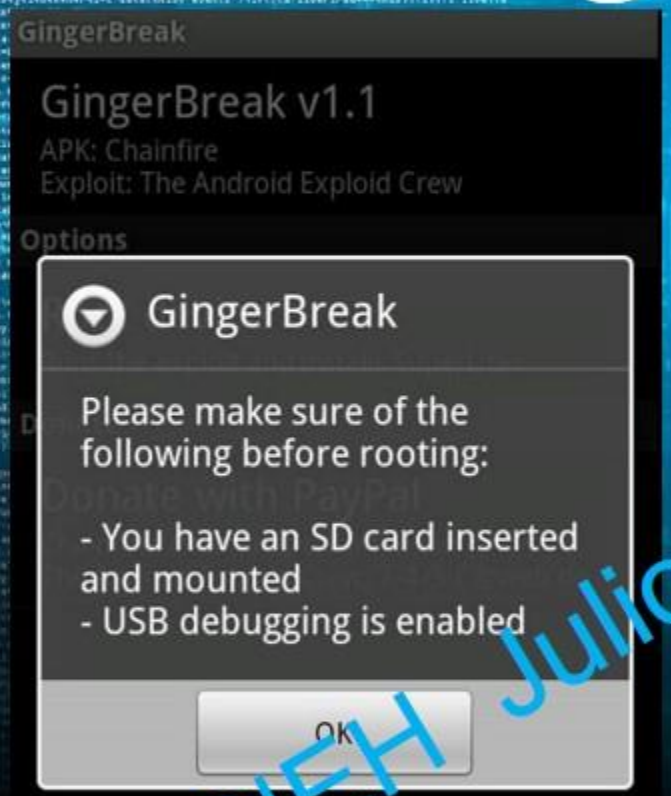
Troyano para Android: ZitMo (Zeus-in-the-Mobile)

C|EH Julio Iglesias Perez

Troyano para Android: GingerBreak

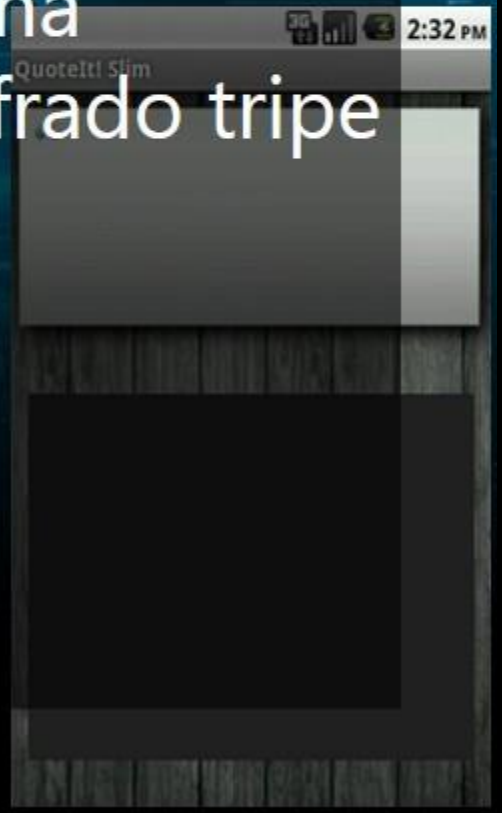
GingerBreak es un troyano que infecta los dispositivos móviles con Android. Cae y ejecuta otro Troyano detectado como Exploit: **"AndroidOS/CVE-2011-1823",** si éste se ejecuta satisfactoriamente, obtiene privilegios administrativos en el dispositivo.

Troyano para Android: GingerBreak



Troyano para Android: AcnetSteal

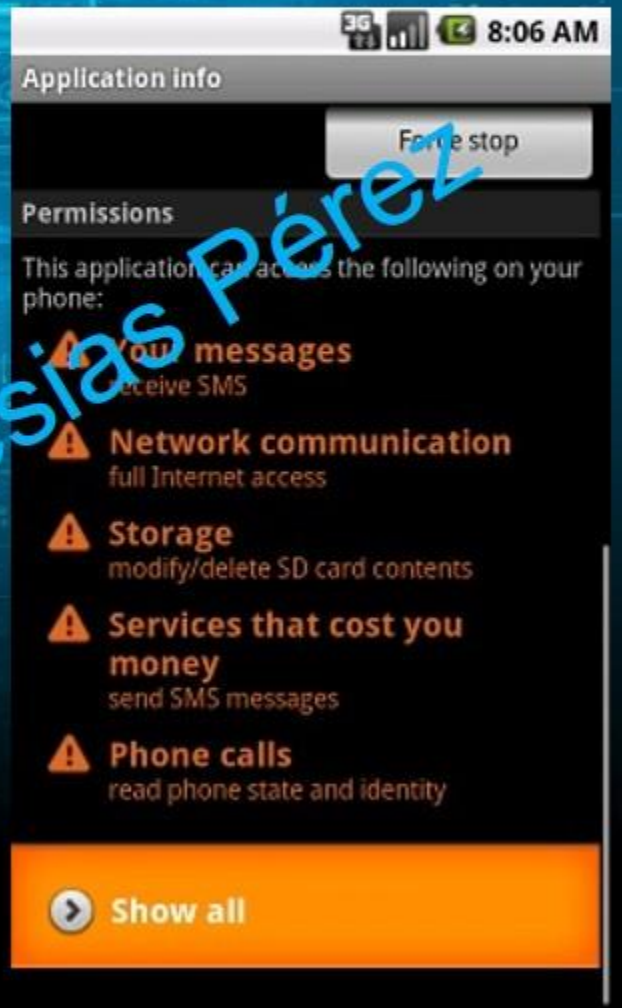
- AcnetSteal: Es un programa que recolecta datos e información del dispositivo. Envía información de los contactos a una ubicación remota utilizando el cifrado tripe DES.



Troyano para Android: Cawitt

- Cawitt: Opera silenciosamente en segundo plano obteniendo información del dispositivo para luego enviarla a un servidor remoto. Recolecta información como ID del dispositivo, número IMEI (International Mobile Equipment Identity), número de teléfono, ID BOT, y módulos.

Troyano para Android: Cawitt



Troyano para Android: Frogonal

- Frogonal: Es una versión reempaquetada de una aplicación original donde sus funcionalidades extra son utilizadas para propósitos maliciosos. Extrae información como Identificación de la aplicación del troyano, número de teléfono, número IMEI, serial SIM, modelo del dispositivo, versión del Sistema Operativo, disponibilidad root.

Troyano para Android: Frogonal

Troyano para Android: Gamex

- Gamex: Esconde sus componentes maliciosos dentro del archivo empaquetado. Una vez que obtiene acceso root por parte del usuario, se conecta a un servidor de comando y control (C&C) para descargar mas aplicaciones y luego enviar los números IMEI e IMSI. También establece conexión a un vínculo externo que contiene un archivo APK reempaquetado, y procede a descargar e instalar el archivo.

Troyano para Android: Gamex

C|EH Julio Iglesias Pérez

Troyano para Android: KabStamper

- Kabstamper: Es un malware distribuido por aplicaciones con troyanos que entrega noticias y videos en el grupo AKB48. Su código es muy destructivo ya que destruye (valga la redundancia) imágenes encontradas en tarjetas SD, DCIM, carpeta de la cámara, etc. Cada cinco minutos, el malware revisa su carpeta y la modifica cada imagen encontrada sobrescribiéndola con una imagen predefinida.

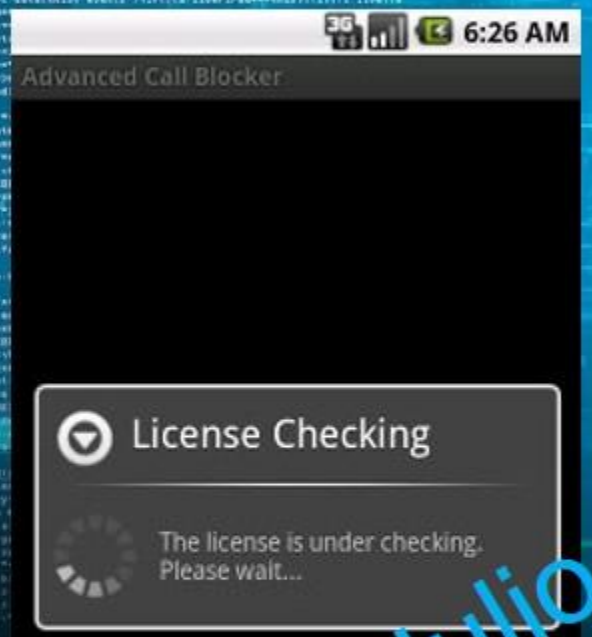
Troyano para Android: KabStamper

C|EH Julio Iglesias Pérez

Troyano para Android: Mania

- Mania: Es un malware que envía SMS con el contenido "tel" o "quiz" al número 84242. Cualquier respuesta a este número es redirigido a otro dispositivo para prevenir que el usuario sospeche. Es conocido por utilizar una técnica de "troyanización", donde es reempaquetado con otra aplicación original para engañar a las víctimas.

Troyano para Android: Mania



C|EH Julio Iglesias Pérez

Troyano para Android: PremiumSMS

- PremiumSMS: es un troyano que recoge beneficios de sus actividades de envío de SMS. Tiene un archivo de configuración que contiene datos sobre el contenido de los mensajes SMS y los numbres de sus receptores.
- Ejemplo:
- PremiumSMS:
  - 1. Número: 1151
  - Contenido: 692046 169 BG QCb5T3w
  - 2. Número: 1161
  - Contenido: 692046 169 BG QCb5T3w
  - 3. Número: 3381
  - Contenido: 692046 169 BG QCb5T3w

Troyano para Android: SMSSpy

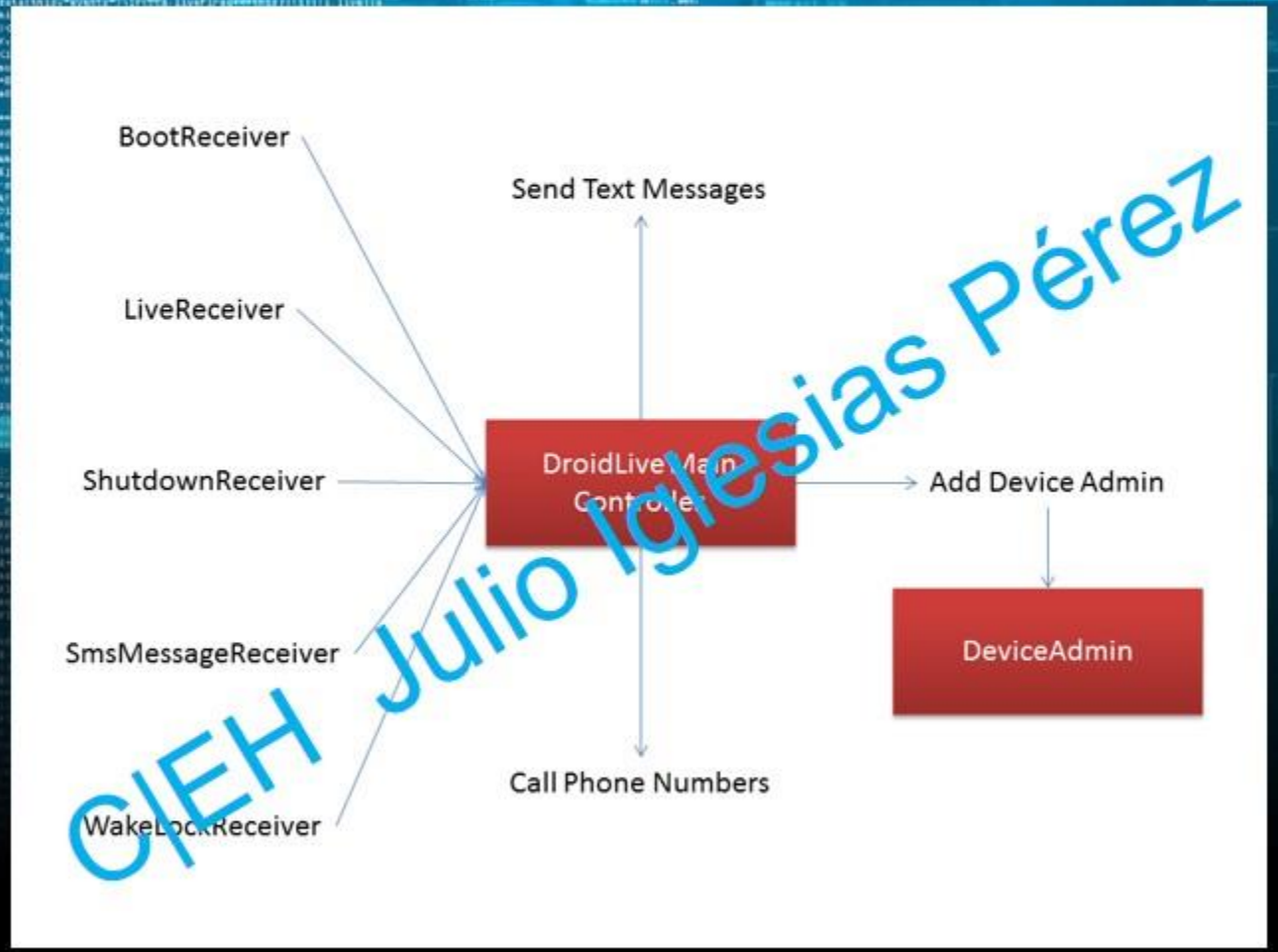
- SmsSpy. Posee una suite de aplicaciones de seguridad Android que registra todos los mensajes SMS recibidos dentro de una base de datos. Este malware apunta a clientes bancarios en España donde por spamm envía un mensaje de Protección de Seguridad Extra para el móvil.

Troyano para Android: SMSSpy

Troyano para Android: DroidLive SMS

- DroidLive se enmascara como una biblioteca de Google, intenta utilizar el API de Administración de Dispositivo. Intenta instalarse por si mismo como una aplicación de administración de dispositivo, y es capaz de aprovechar los datos personales y la realización de una mezcla de actividades nefastas en dispositivos móviles Android.

Troyano para Android: DroidLive SMS



Troyano para Android: UpdtKiller

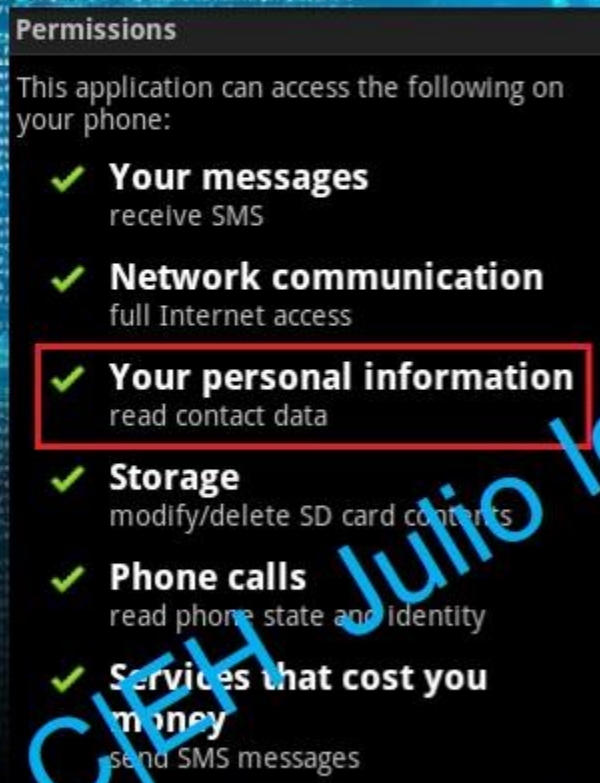
- UpdtKiller: Se conecta a un servidor de comando y control (C&C), desde donde recibe comandos y envía información del usuario. Este malware también es capaz de matar procesos de antivirus, y así evitar ser detectado.

Troyano para Android: UpdtKiller

Troyano para Android: FakeToken

- FakeToken roba factores de autenticación y banco (Contraseña de Internet y mTAN) directamente desde el dispositivo.
- A través de correos phishing, inyectando páginas web, e inyectando páginas web phishing, puede ser enviador por el banco, puede simular ser una aplicación segura, y puede redirigir a usuarios a un falso vendedor que ofrece "eBanking SMS Guard".

Troyano para Android: FakeToken



Asegurando dispositivos Android

- Habilitar el bloqueo de pantalla en su dispositivo Android.
- Nunca rootear el dispositivo.
- Descargar aplicaciones solo del market oficial.
- Mantener su dispositivo actualizado con un software de A.V. para Android.
- No descargar aplicaciones APK (Android Package Files) directamente.
- Mantener actualizado el Sistema.
- Utilizar Protectores Android gratuitos donde pueda asignar contraseñas a los mensajes de texto, cuentas de correos electrónicos, etc.
- Personalizar su pantalla bloqueada con información del usuario.

Política de Aplicaciones de Dispositivo Google

Esta política permite al administrador de Google Apps del dominio establecer políticas de seguridad para su dispositivo Android.

Se trata de una aplicación de administración de dispositivos de Google Apps para Negocios, Educación, y Gubernamentales que hacen de su dispositivo Android más seguro para el uso empresarial.

Esta aplicación permite a los administradores de TI hacer cumplir las políticas de seguridad y borrar de forma remota el dispositivo.

Además, esta aplicación permite sonar, bloquear o localizar los dispositivos Android a través de la página de Mis dispositivos: http://www.google.com/apps/mydevices

Política de Aplicaciones de Dispositivo Google

Limpieza remota de servicios

- Si los usuarios tienen instalado Google Sync en un dispositivo móvil soportado o con la Política de Aplicaciones de Dispositivo Google, se puede utilizar el panel de control de Google Apps para limpiar remotamente el dispositivo.
- Para limpiar remotamente un dispositivo perdido o robado:
  - Iniciar sesión en el panel de control de Google Apps.
  - Clic en Settings, Mobile
  - En la pestaña Devices, llevar el cursor sobre el dipositivo que se quiere limpiar.
  - Clic en Remote Wipe.
  - Aparecerá un diálogo de confirmación. Si estamos seguros de realizar la limpieza, hacer clic en Wipe Device.

Herramienta de Seguridad Android: DroidSheep Guard

- Esta herramienta monitorea la tabla ARP y las ventanas emergentes, en caso de detectar entradas sospechosas en las tablas APR.
- Puede deshabilitar la conexión WIFI inmediatamente para proteger las cuentas.
- Trabaja con ataques basados en ARP como DroidSheep y Faceniff

Herramienta de Seguridad Android: DroidSheep Guard

C|EH Julio Iglesias Pérez

Escaner de Vulnerabilidades para Android: X-Ray

- X-Ray escanea el dipositivo Android para determinar si hay vulnerabilidades o falta de parches en el Sistema.
- Presenta la lista de vulnerabilidades que permiten identificar y revisar la presencia de cada vulnerabilidad en el dispositivo.
- X-Ray es automáticamente actualizado para permanecer escaneando las nuevas vulnerabilidades descubiertas.

Escaner de Vulnerabilidades para Android: X-Ray

C|EH Julio Iglesias Pérez

Herramienta de Test de Intrusión para Android: Android Network Toolkit - Anti

- En cada ejecución, Anti va a mapear la red, escanear por dispositivos activos y vulnerabilidades y mostrará la información según lo siguiente: led verde indica dispositivo activo, led amarillo indica puertos disponibles, y led rojos indica que se encontró una vulnerabilidad.
- Cada dispositivo será representando el tipo de dispositivo.
- Cuando termina el escaneo, Anti producirá un reporte automático especificando qué vulnerabilidades están presentes en el dispositivo, mejores prácticas y cómo corregir cada una.

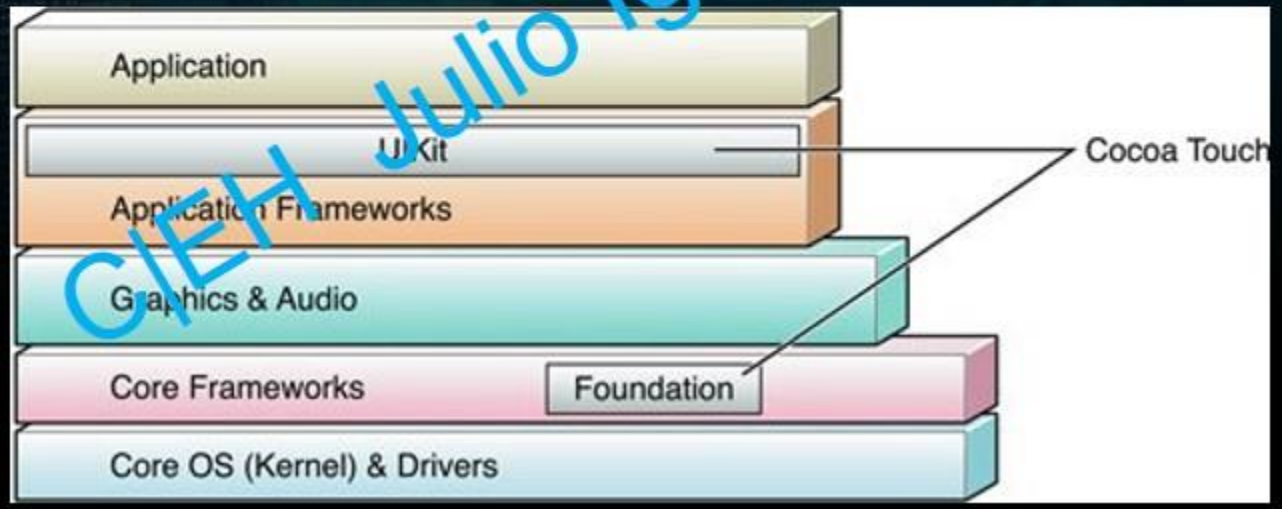
Herramienta de Test de Intrusión para Android: Android Network Toolkit - Anti

Herramientas de rastreo Android

- Herramientas de rastreo Androd
- Find my Phone: http://findmyphone.mangobird.com
- Prey Anti-Theft: http://preyproject.com
- Android Anti Theft Security: http://www.snuko.com
- Where is my Droid: http://whereismydroid.com
- iHound: http://www.ihoundsoftware.com
- GadgetTrak Mobile Security: http://www.gadgettrack.com
- Total Equipment Protection App: http://protection.sprint.com
- AndroidLost.com http://www.androidlost.com

Hackeando IOS

- El Sistema Operativo móvil de Apple soporta dispositivos Apple como iPhone, iPod touch, iPad y Apple TV
- La interfaz del usuario está basada en el concepto de manipulación directa utilizando gestos multitáctiles



Jailbreaking iOS

- Jailbreaking es definido como el proceso de instalar un conjunto de parches del núcleo que permite a los usuarios ejecutar aplicaciones de terceros no firmados por el vendedor del S.O.
- Jailbreaking provee acceso root al Sistema y permite descargar aplicaciones de terceros, temas, extensiones en los dispositivos iOS
- Jailbreaking quita las restricciones sandbox, que habilita a las aplicaciones acceder a recursos e información del dispositivo restringida.

Tipos de Jailbreaking

- Userland Exploit: Permite acceso a nivel de usuario pero no permite acceso a nivel iboot.
- iBoot Exploit: Permite acceso a nivel de usuario e iboot. Utilizado generalmente para reducir los controles iOS de bajo nivel.
- Bootrom Exploit: Permite acceso a nivel de usuario e iboot. Este proceso encuentra un agujero en la aplicación para descartar revisión de firmas.

Técnicas Jailbreaking

- Jailbreaking atado: Si los dispositivos inician una copia de seguridad en sí mismo, ya no tener un núcleo parchado, y puede quedar atrapado una parte del Estado en Iniciado, con el fin de que se inicie completamente con un núcleo parchado, que, esencialmente, debe ser "re jailbrokeado "con una computadora (usando la" función de arranque atada" de una herramienta de jailbreak) cada vez que se encienda

Técnicas Jailbreaking

- Jailbreaking no atado: Tiene la propiedad de que si el usuario enciende y apaga el dispositivo, éste iniciará completamente y el núcleo será parchado sin ayuda de una computadora, en otras palabras se aplicará un jailbreak cada vez que reinicie

Aplicación para dispositivos Jailbreakeados: Cydia

- Cydia es una aplicación para iOS que permite al usuario encontrar e instalar paquetes de software (incluyendo aplicaciones, interfaces personalizadas, y extensiones del sistema) en un Sistema Jailbreakeado iPhone, iPod Touch o iPad.
- Es una Herramienta de Empaquetamiento Avanzada (APT: Advanced Packaging Tool) y un sistema de administración de paquetes dpgk, eso significa que los paquetes disponibles en Cydia son provistos por un sistema descentralizado de repositorios (también llamadas fuentes) que listan estos paquetes.

Aplicación para dispositivos Jailbreakeados: Cydia

C|EH Julio Iglesias Pérez

Herramientas Jailbreaking: RedSn0w y Absinthe

- RedSn0w: Permite realizar jailbreak al iPhone, iPod Touch y iPad corriendo una variedad de versiones firmware.
- Absinthe: Es una solución jailbreak para iPhone, iPad y AppleTV disponible gracias a Chronic Dev Team

Herramientas Jailbreaking: RedSn0w y Absinthe

Jailbreak iOS 6 atado utilizando RedSn0w

- Paso 1. Descargar RedSn0w y abrirlo
- Paso 2. Ingresar el iOS en modo DFU presionando Home y Power por 10 segundos y luego soltando Power mientras se sigue presionando Home por 10 segundos más
- Paso 3. Clic en Jailbreak
- Paso 4. Seleccionar Instalar Cydia y hacer clic en Next en la opción "Please select your options"
- Paso 5. Esperar aproximadamente 5 minutos hasta que el proceso de Jailbreak esté completo y sea redireccionado a la pantalla Home
- Paso 6. Volver a colocar el dispositivo en Modo DFU
- Paso 7. Volver a la página principal de RedSn0w y seleccionar Extras, Just boot
- Paso 8. Ahora se verá a Cydia en la pantalla Home una vez que el dispositivo inicie

Herramienta Jailbreaking: Sn0wbreeze

- Sn0wBreeze es una herramienta Jailbreak para Sistemas Windows que permiten crear un archivo Pre-Jailbroken personalizado del firmware iOS que debe ser restaurado en el iPhone, iPod Touch, o iPad para que esté jailbreakeado. Permite a los iPhones desbloquear la actualización a la última firmware sin actualizar su baseband en el proceso. Ofrece un full control sobre el jailbreak, permitiendo personalizar opciones avanzadas como el tamaño de la partición raíz.

Herramienta Jailbreaking: Sn0wbreeze

Herramienta Jailbreaking: PwnageTool

- PwnageTool es una herramienta jailbreaking que permite desbloquear y crear un IPSW personalizado, permitiendo actualizar el firmware mientras se preserva el baseband.

Herramienta Jailbreaking: PwnageTool

Herramienta Jailbreaking: LimeRa1n

- LimeRa1n es una herramienta jailbreaking inventada por GeoHot (hacker profesional) para detener que Chronic Dev libere un exploit bootROM llamado SHAtter. Una de las características de esta herramienta permite cambiar entre los métodos de jailbreaking y soporta Sistemas Windows y Mac OS X.
- http://www.limera1n.com

Herramienta Jailbreaking: LimeRa1n

C|EH Julio Iglesias Pérez

Herramienta Jailbreak: Jailbreakme

- Jailbreakme es una herramienta que permite realizar jailbreak a iPhones, iPod Touch, o iPad a través de servicios en línea. Es utilizado para proveer jailbreak no atado a iPad 2.
- http://www.jailbreakme.com

Herramienta Jailbreak: Jailbreakme

Herramienta Jailbreak: Blackra1n

- Blackra1n es una herramienta Jailbreak para firmwares iPhone, iPod o iPad. Puede trabajar en todos los dispositivo sin tener que realizar ajustes avanzados en el software. Trabaja tanto en Sistemas Windows como en Mac OS. Diseñado por Geohot.
- http://blackra1n.com

Herramienta Jailbreak: Blackra1n

C|EH Julio Iglesias Perez

Herramienta Jailbreak: Spirit

- Spirit es una herramienta jailbreak que permite realizar jailbreak no atado. Sirve para iPad, iPhone e iPhone Touch en ciertas versiones de firmware.

Guía para asegurar iOS

1. Utilizar el bloqueo con contraseña.
2. Deshabilitar Javascript y los addons web.
3. Utilizar los dispositivos iOS en redes WIFI seguras y protegidas.
4. No almacenar información sensible en la base de datos del lado del cliente.
5. No acceder a servicios web en una red comprometida.
6. No abrir vínculos o archivos adjuntos desde fuentes desconocidas.
7. Utilizar herramientas de terceros confiables.
8. Cambiar la contraseña por defecto (alpine) del root.

Guía para asegurar iOS

9. NO realizar jailbreak o rootear el dispositivo si es utilizado en ambientes empresariales.
10. Configurar "Find My iPhone" para limpiar los dispositivos robados.
11. Habilitar la detección Jailbreak y proteger el acceso a las cuentas de iTunes (AppleID) y Google.
12. Deshabilitar los servicios iCloud para que la información empresarial sensible no sea respaldada en la nube.

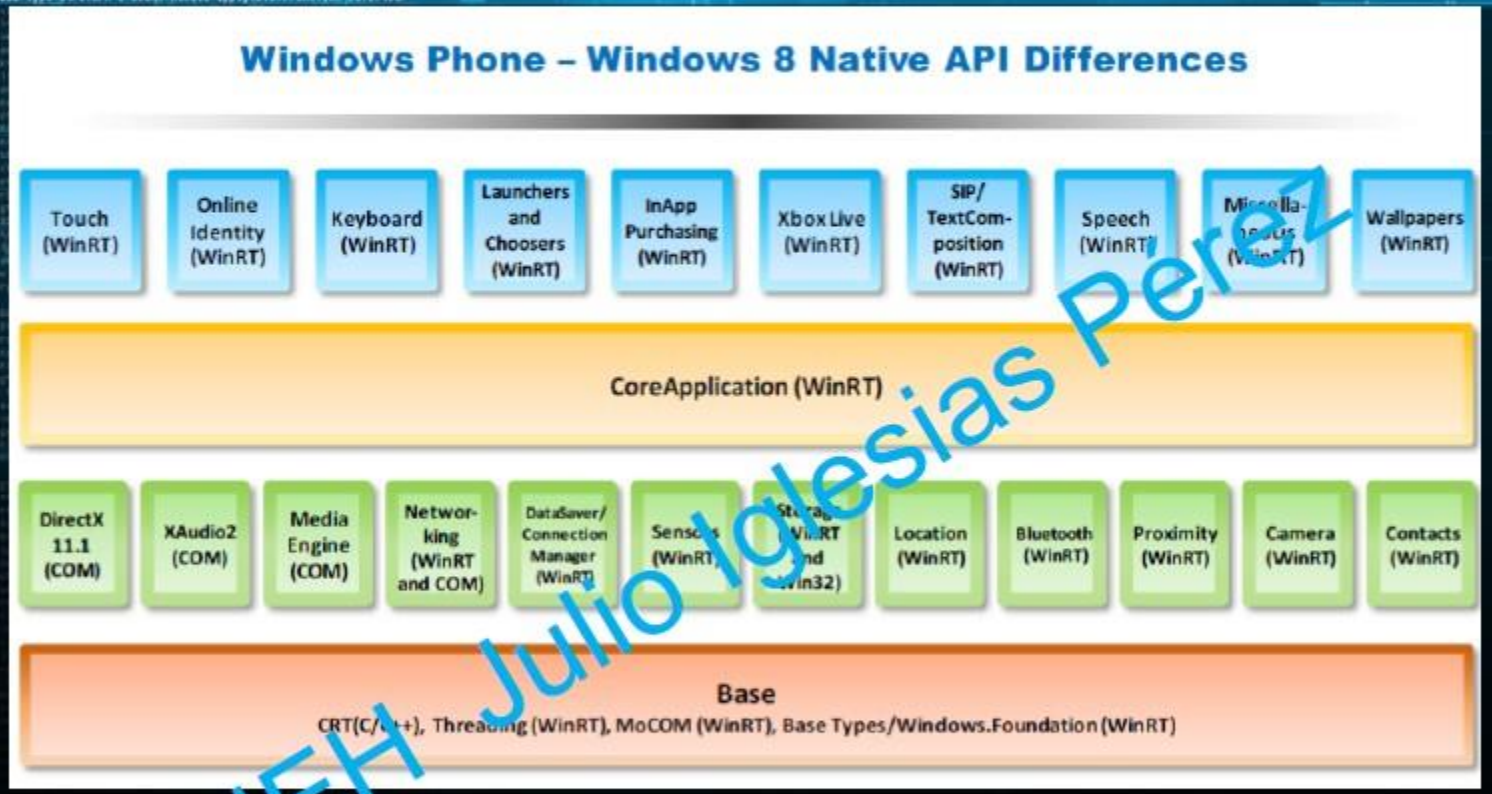
Herramientas de Seguimiento iOS

- Find my iPhone: https://itunes.apple.com
- iHound: https://www.ihoundsoftware.com
- GadgetTrak iOS Security: http://www.gadgettrak.com
- iLocalis: http://ilocalis.com

Hackeando Windows Phone

- Se permite que los dispositivos con pantallas más grandes y procesadores multi-core de hasta 64 núcleos
- Núcleo y soporte Windows mejorados para el almacenamiento extraíble.
- Los componentes básicos de Windows 8, incluyendo el núcleo, sistema de archivos, drivers, pila de red, componentes de seguridad, medios de comunicación y soporte gráfico.
- Internet Explorer 10, tecnologías de mapas de Nokia, y multitarea.
- Compatible con Near Field Communication (NFC), incluyendo el pago y el intercambio de contenidos con Windows Phone y equipos con Windows 8.
- Compatibilidad con código nativo (C y C + +), portabilidad simplificada de plataformas como Android, Symbian e iOS.
- Control de transporte y la marca del elemento "wallet" es posible a través de la tarjeta SIM o hardware del teléfono.
- Bitlocker Nativo de 128 bits cifrado y gestión remota de dispositivos de Windows Phone.
- Protocolo de arranque seguro United Extensible Firmware Interface (UEFI) y firmware sobre el aire de las actualizaciones de Windows Phone.
- Características mejoradas aplicación sandboxing y VoIP y video chat en la integración de VoIP para cualquier aplicación de chat y vídeo.

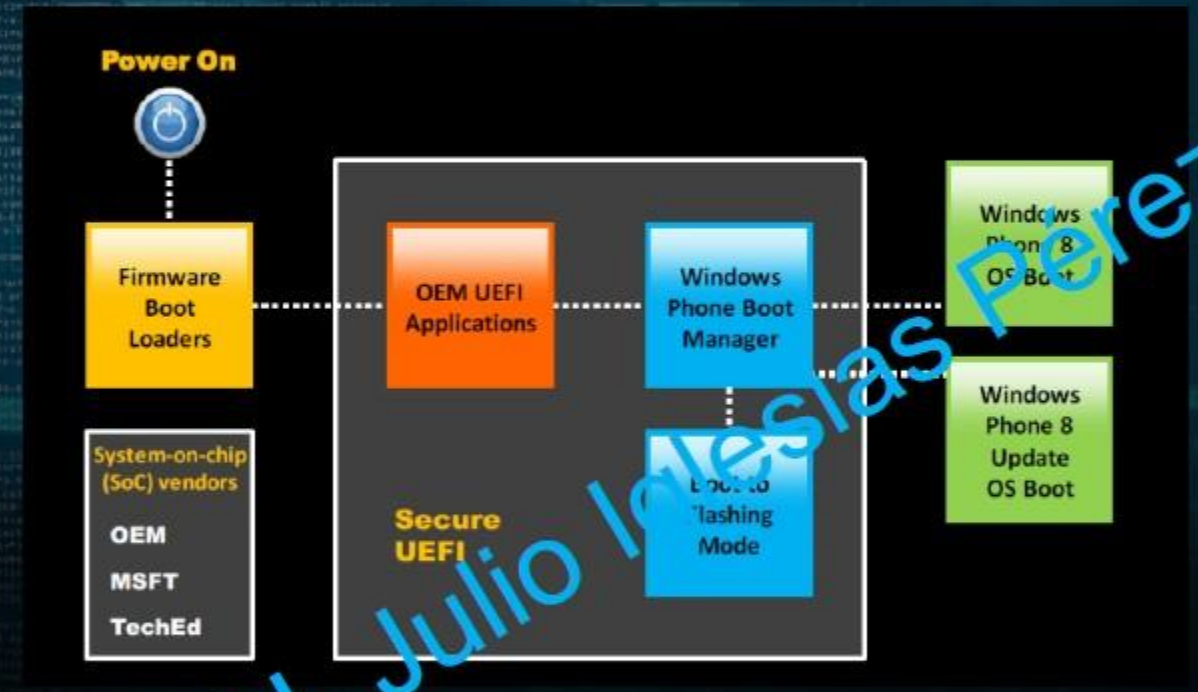
Arquitectura Windows Phone



Proceso de Arranque Seguro

- La meta de la característica de arranque seguro de Windows Phone 8 es diseñar un proceso de arranque que permita correr el Sistema para garantizar que solo los componentes confiables sean cargados.
- Cuando se enciende por primera vez el firmware inicia una Firmware Interface Extensible Unified (UEFI) en segundo plano que valide el HASH de estas firmas en comparación con las firmas de los gestores de arranque inicial para confirmar el ambiente del Sistema. En esta etapa las firmas se comparan en el Administrador de arranque de Windows Phone para permitir que solo las aplicaciones originales y de confianza.

Proceso de Arranque Seguro



C|EH Julio Ieslas Perez

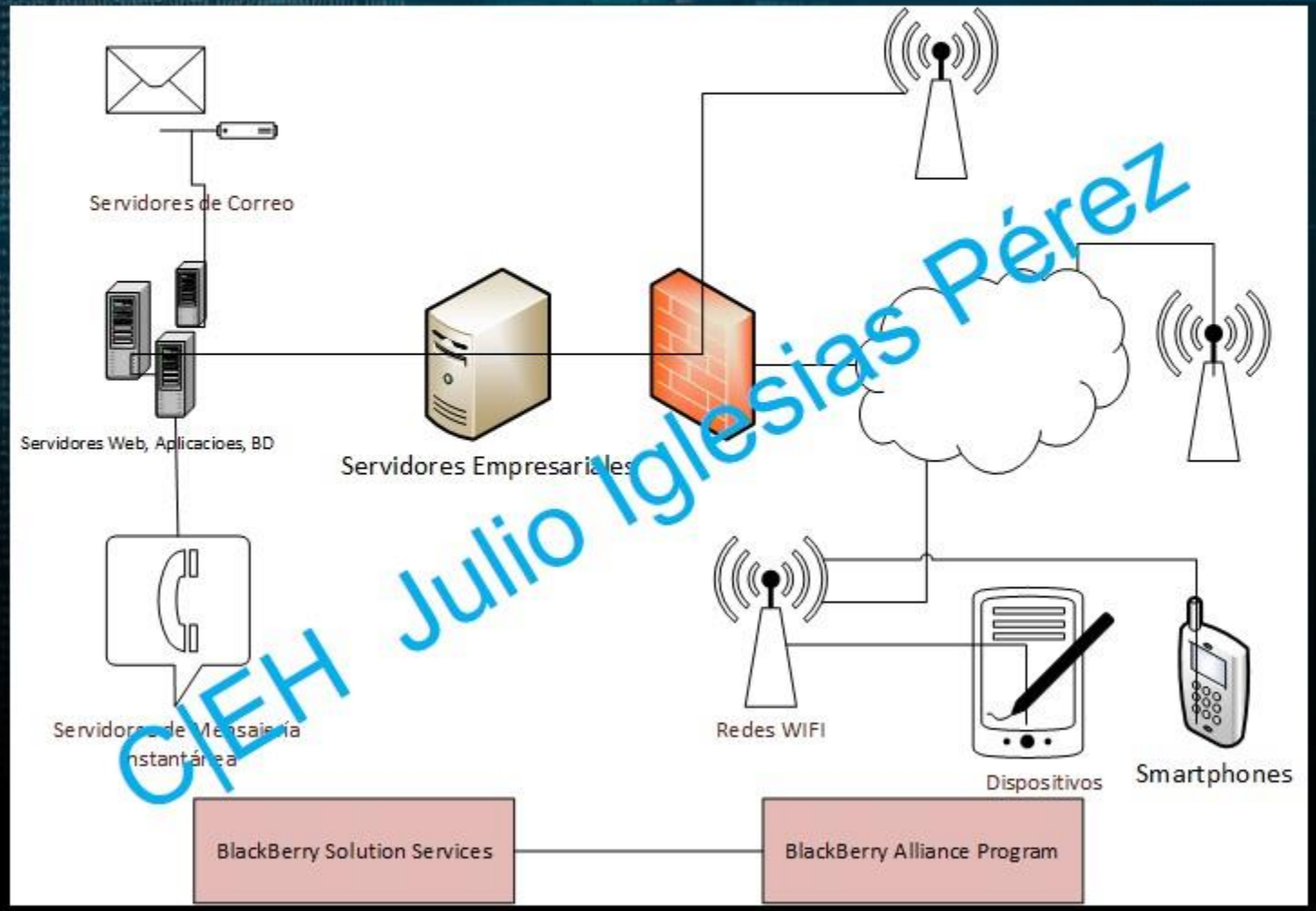
Guía para asegurar sistemas con Windows Phone

- Descargar aplicaciones solo del Zune Marketplace.
- Mantener el dispositivo actualizado.
- Limpiar el historial de navegación.
- Utilizar Zune desktop para respaldar información.
- Evitar acceder a sitios web protegidos por contraseña en redes WIFI no seguras.
- Configurar bloqueo de pantalla con contraseña.
- Proteger la SIM (Suscriber Identify Module) con un PIN (Personal Identification Number)

Hackeando Blackberry

- El Sistema Operativo BlackBerry fue desarrollado por Research in Motion (RIM) para su linea de smartphones y handheld.
- Incluye un framework basado en Java que implementa J2ME Mobine Information Device Profile v2 (MIDP2) y Connected Limited Device Configuration (CLDC).
  - Soporte nativo para correos corporativos.
  - BlackBerry Enterprise Server.
  - BlackBerry Messenger.
  - BlackBerry Internet Service.
  - Cliente de correo BlackBerry .

Hackeando Blackberry



Vectores de ataque BlackBerry

- Firma de Código maliciosa.
- Exploits archivos JAD.
- Manipulación de memoria y procesos.
- Exploits SMS (Short Message Service).
- Exploits de correo electrónico.
- Ataques a datos PIM.
- Vulnerabilidades de conexiones TCP/IP.
- Ataques telefónicos.
- Malwares BlackBerry.

Firma de código malicioso

- Las aplicaciones BlackBerry deben estar firmadas por RIM para obtener full acceso a las APIs del Sistema.
- Si una firma no se encuentra en la aplicación o si está alterada, el JVM restringirá o rechazará el acceso a API a la aplicación.
- Los atacantes pueden obtener firmas de código anónimas utilizando tarjetas de crédito pre-pagadas y detalles falsos, firmar la aplicación y publicarla dentro del BlackBerry App World.
- Los atacantes también pueden comprometer el sistema de un desarrollador para robar las firmas de código y sus contraseñas para descifrar las firmas cifradas.

Exploits de archivos JAD y Manipulación de Procesos de memoria

- Exploits de archivos JAD
  - Los archivos .jad (Java Application Descriptors) incljyen los atributos de una aplicación java, como descripción de la aplicación, detalles del vendedor y tamaño, y provee la URL donde la aplicación puede ser descargada.
  - Es utilizado como una manera de proveer una instalación Over The Air (OTA) de aplicaciones java en dispositivos J2ME.
  - Los atacantes pueden especialmente los archivos .jad elaboradas con información suplantada y engañar a los usuarios a instalar aplicaciones maliciosas.
- Manipulaciones de Procesos/Memoria
  - Los atacantes pueden crear aplicaciones maliciosas creando bucles infinitos, con una condición de ruptura en el medio que siempre será falsa para saltar la verificación de compilador.
  - Causará un ataque DoS cuando la aplicación maliciosa se ejecute causando que el dispositivo no responda.

Exploits SMS

- Intercepción SMS
  - El envío y recepción de mensajes pueden ser realizados fácilmente utilizando aplicaciones sin firmar. Los mensajes desde un BlackBerry comprometido puede ser enviado y recibido por terceros fácilmente utilizando una aplicación maliciosa.

Exploits de correos electrónicos

- En móviles BlackBerry, todos los correos son enviados, recibidos y leídos a través del paquete net.rim.blackberry.api.mail y éste puede ser utilizado solo en aplicaciones firmadas.
- El servicio de archivos adjuntos de BlackBerry solo soporta archivos como .doc, .pdf, .txt, .wpd, .xls, y .ppt, pero puede enviar cualquier archivo vía correo. Un adjunto con tipo de archivo .doc no es soportado vía BlackBerry.

Ataques a datos PIM y vulnerabilidades de conexiones TCP/IP

- Ataques a datos PIM
  - Los datos PIM (Personal Information Management) en la base de datos PIM de un dispositivo BlackBerri incluye libreta de direcciones, calendarios, tareas e información memopads.
  - Los atacantes pueden crear aplicaciones maliciosas firmadas que leen los datos PIM y los envían a un atacante utilizando distintos mecanismos de transporte.
  - Las aplicaciones maliciosas también pueden eliminar o modificar datos PIM

- Vulnerabilidades de conexiones TCP/IP
  - Si el firewall del dispositivo está apagado, las aplicaciones firmadas pueden abrir conexiones TCP sin que el usuario lo note.
  - Las aplicaciones maliciosas instaladas pueden crear una conexión reversa con el atacante habilitándolo a utilizar el dispositivo infectado como un proxy TCP y obtener acceso a los recursos internos de la organización.
  - Los atacantes también pueden explotar la conexión TCP reversa para backdoors y realizar varios ataques de obtención de información.

Spyware Blackberry: FindSpy Mobile

- Permite al atacante a:
  - Grabar comunicaciones comunes como llamadas de voz, SMS/MMS y correos.
  - Vigilancia en vivo a través de llamadas silenciosas.
  - Descarga de archivos (contactos, calendario, fotos, archivos).
  - Rastreo (GPS y Cell ID).
  - Registro de comunicaciones de BlackBerry Messenger.
  - Afectar las comunicaciones con la central.

Spyware Blackberry: FindSpy Mobile

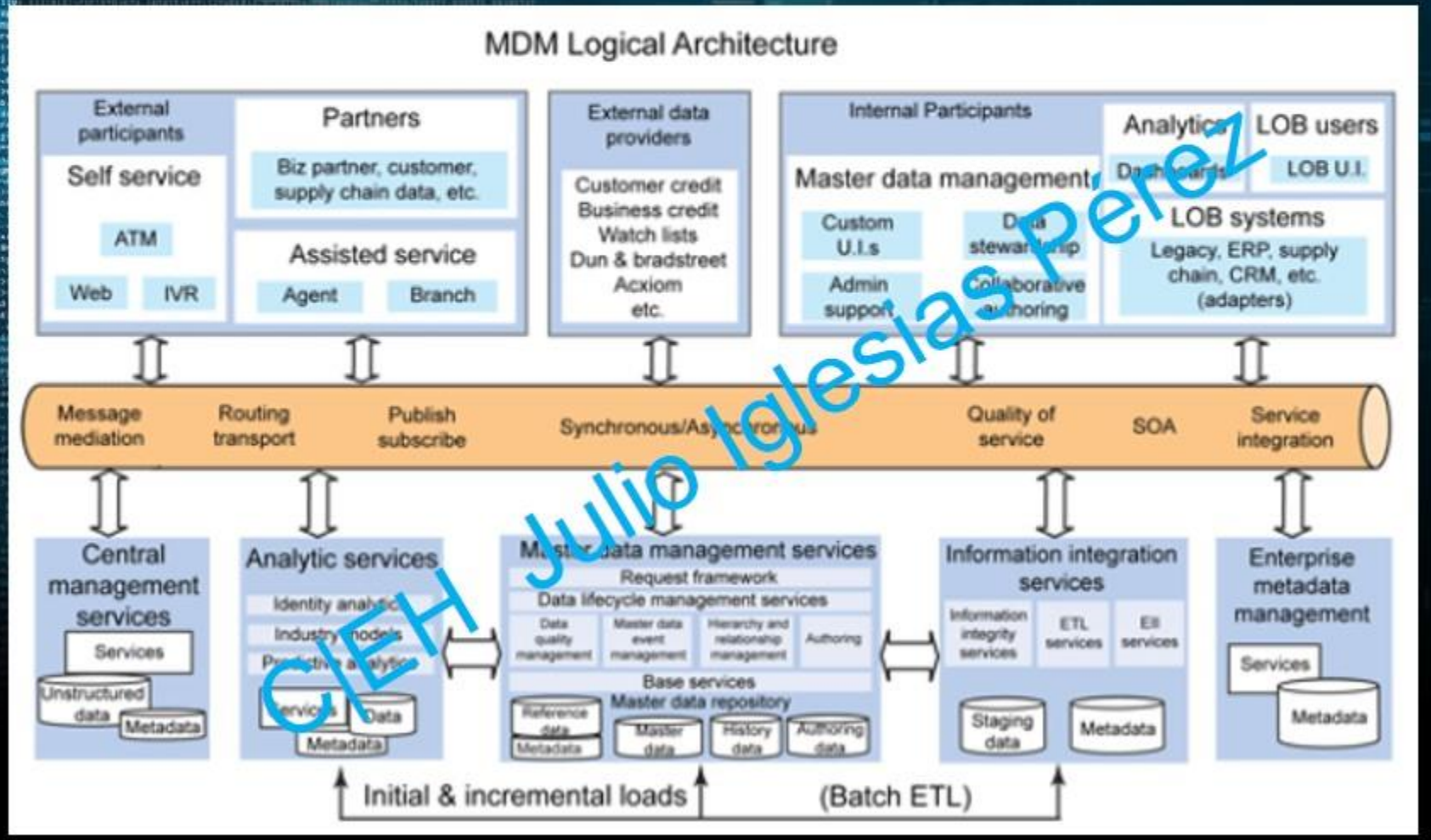
Guía para asegurar dispositivos BlackBerry

- Utilizar la característica protección de contenido para proteger los datos en una red organizativa BlackBerry.
- Utilizar cifrado de contraseñas para proteger archivos en dispisitivos BlackBerry.
- Utilizar BlackBerry Protect u otra aplicación de seguridad para asegurar datos confidenciales.
- Habilitar el cifrado de tarjetas y dispositivos SD para proteger los datos.
- Las organizaciones deben seguir una política de seguridad para administrar los dispositivos BlackBerry.
- Mantener un mecanismo de monitoreo para la infraestructura de red en las redes organizativas BlackBerry.
- Deshabilitar aplicaciones innecesarias desde las redes organizativas BlackBerry.
- Proveer capacitación en seguridad y ataques en dispositivos sobre redes organizativas BlackBerry.

Administración de Dispositivos Móviles (MDM)

- MDM provee plataformas para distribuciones por cable o por el aire, opciones de configuración y datso para todos los tipos de dispositivos móviles incluyendo teléfonos móviles, smartphones, tablets, etc.
- MDM ayuda a implementar directivas en toda la empresa para reducir costos de soporte, discontinuidad del negocio y riesgos de seguridad.
- Ayuda a los administradores de sistema a implementar y administrar aplicaciones de software por todos los dispositivos de la empresa para asegurar, monitorear, administrar y soportar dispositivos móviles.
- Puede ser utilizado para administrar dispositivos de la organización y personales a través de la empresa.

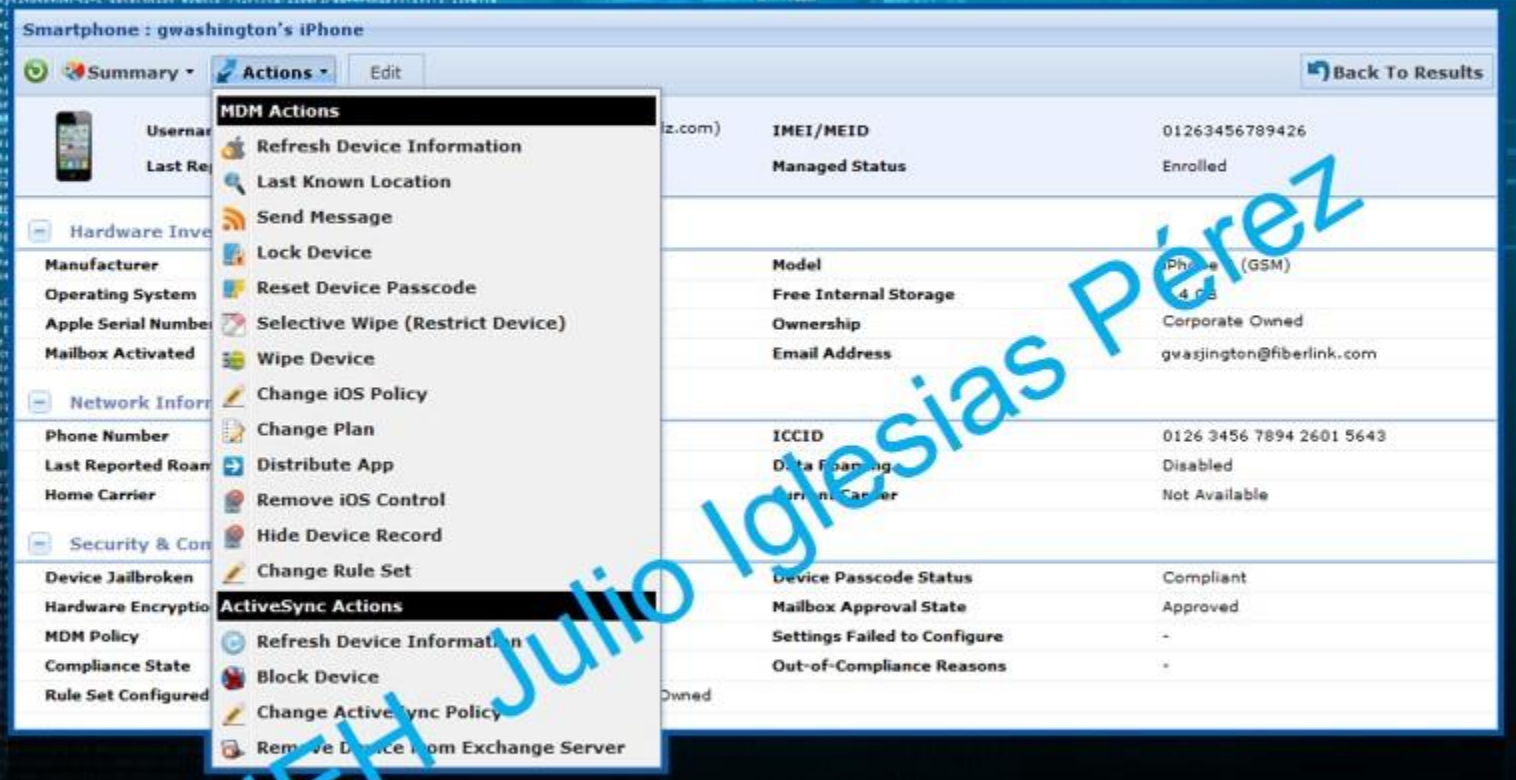
Arquitectura MDM



Solución MDM: MaaS360 Mobile Device Management

- MaaS360 soporta el ciclo de vida completo MDM para smartphones y tablets incluyendo iPhone, iPad, Windows Phone, Android, BlackBerry y Kindle Fire.
- Como plataforma cloud integrada, MaaS360 simplifica MDM con implementación rápida y comprensiva visibilidad y control que se extiende a través de los dispositivos móviles, aplicaciones y documentos.

Solución MDM: MaaS360 Mobile Device Management



Soluciones MDM

- Citrix XenMobile MDM: http://www.zenprise.com
- Absolute Manage MDM: http://www.absolute.com
- SAP Afaria: http://www.sybase.com
- Device Management Centre: http://www.sicap.com
- AirWatch: http://www.air-watch.com
- Good Mobile Manager: http://www1.good.com
- MobileIron: http://www.mobileiron.com
- Rule Mobility: http://www.tangoe.com
- TARMAC: http://www.tarmac-mdm.com
- MediaContact: http://www.device-mangement-software.com

Guía General para Seguridad en Plataformas Móviles

- No cargar muchas aplicaciones y evitar subir automáticamente fotos a las redes sociales.
- Realizar una valoración de riesgos de la arquitectura de aplicación.
- Mantener un control de configuración y administración.
- Instalar aplicaciones de tiendas confiables.
- No agregar aplicaciones basadas en ubicación como Google Maps salvo que haya un radio GPS que soporte la aplicación.
- Asegurar que el Bluetooth esté apagado por defecto.
- No compartir información entre aplicaciones con GPS habilitado, salvo que sea necesario.
- Nunca conectar dos redes separadas como WIFI y Bluetooth de manera simultanea.

Guía General para Seguridad en Plataformas Móviles

- Utilizar código de acceso
  - Configurar un código de acceso utilizando preferentemente la longitud máxima para obtener acceso al dispositivo móvil.
  - Configurar auto bloqueo para que éste se bloquee cuando no esté en uso.
  - Habilitar limpiar luego de ciertos intentos fallidos de desbloqueo.
- Actualizar el Sistema y Aplicaciones
- Habilitar la administración remota
- En ambientes empresariales utilizar un software MDM para asegurar, monitorear y dar soporte a dispositivos móviles implementados a través de la organización
- No permitir Rooting oi Jailbreak.
  - Asegurar que la solución MDM prevenga el uso de éstos.
  - Incluir esta cláusula en la política de seguridad móvil.
- Utilizar Servicios de limpiado remoto como Remote Wipe (Android) y Find My iPhone o FindMyPhone (Apple iOS) para localizar el móvil perdido o robado.
- Si está soportado, configurar el dispositivo para cifrar el almacenamiento con cifrado de hardware.

Guía General para Seguridad en Plataformas Móviles

- Realizar respaldo y sincronización periódicos
- Filtrar barrearas de reenvío de correo.
- Configurar reglas de certificación de aplicaciones.
- Asegurar las reglas de los permisos del navegador.
- Diseñar e implementar políticas de dispositivos móviles.

Guía General para Seguridad en Plataformas Móviles

- Deshabilitar la colección de diagnósticos y uso de datos en Settings/General/About
- Aplicar actualizaciones de software cuando estén disponibles.
- Limitar registro de datos almacenados en el dispositivo.
- Utilizar cifrado del dispositivo y parche en las aplicaciones.
- Prohibir llaves USB.
- Cifrar backups.
- Prevenir caché de correos.
- Verificar la ubicación de las impresoras antes de imprimir documents sensibles.
- Presionar el botón de encendido para bloquear el dispositivo cuando no esté en uso.
- Reportar dispositivo perdido o robado a la organización.

Guía para el Administrador de Seguridad en Plataformas Móviles

1. Publicar una política empresarial que especifique el uso aceptable de dispositivos externos en la organización.
2. Publicar una política para la nube.
3. Habilitar medidas de seguridad como antivirus, para proteger los datos en el datacenter.
4. Implementar una política que especifique los niveles de acceso a datos y aplicación permitida, grado de uso de dispositivos, y qué está prohibido.
5. Especificar un tiempo de espera para cierre de sesión.
6. Especificar si la contraseña del dominio será almacenada en el dispositivo o si los usuarios deben ingresarla cada vez que se les requiera acceso.
7. Determinar los métodos de autenticación de acceso al Gateway:
   - Sin autenticación
   - Dominio + RSA SecurID
   - Solo dominio
   - Autenticación SMS
   - Solo RSA SecurID

Herramienta de Protección Móvil: BullGuard Mobile Security

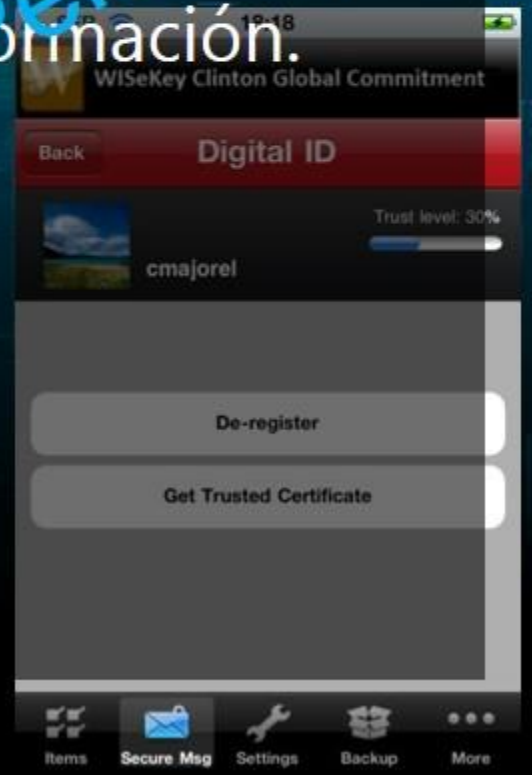
- Tiene un antivirus completo para móviles.
- Hace un seguimiento del móvil si es robado o perdido vía GPS, bloquea o limpia la información de él.

Herramienta de Protección Móvil: Lookout

- Esta herramienta protege al móvil de amenazas en la seguridad y privacidad, realizar respaldos, ayuda a encontrar dispositivos perdidos y permite administrar el móvil remotamente.

Herramienta de Protección Móvil: WISeID

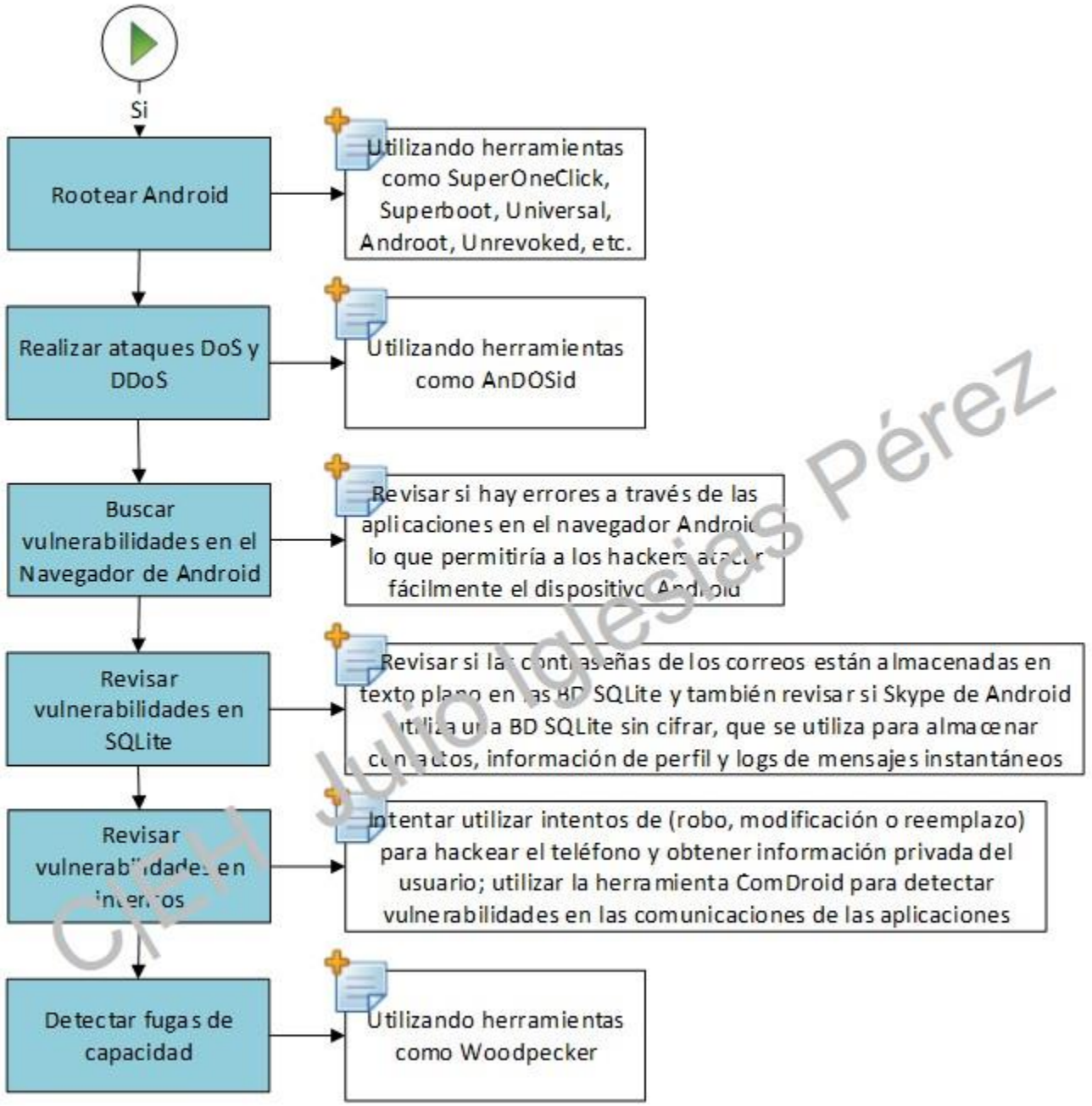
- Se utiliza para cifrar información personal almacenada, Información Personal Identificable (PII: Personally Identifiable Information), PINs, tarjetas de crédito, notas y otra información.



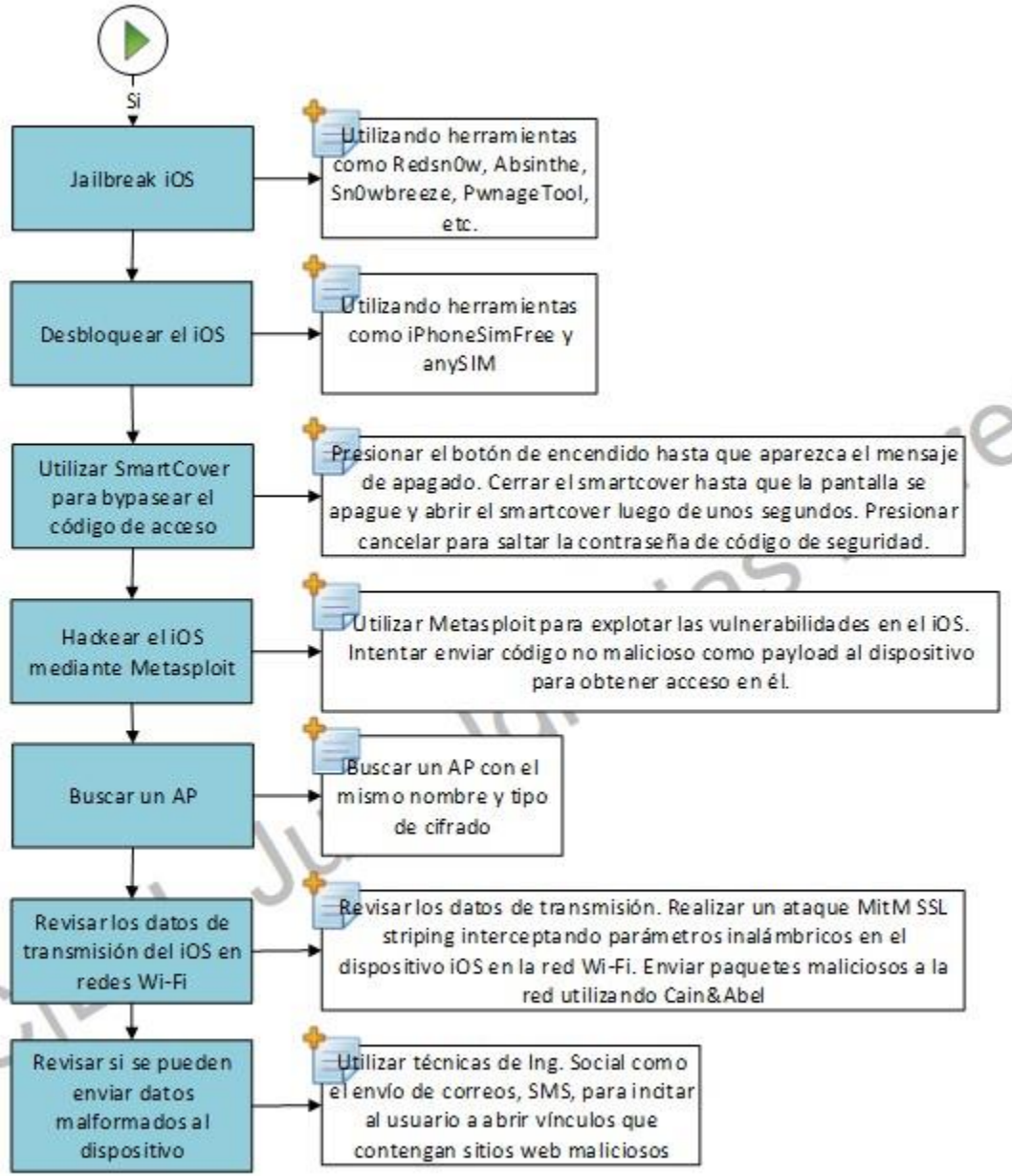
Herramientas de Protección Móvil

- McAfee Mobile Security: https://www.mcafeemobilesecurity.com
- AVG AntiVirus Pro for Android: http://www.avg.com
- avast! Mobile Security: http://www.avast.com
- Norton Mobile Security: http://us.norton.com
- ESET Mobile Security: http://www.eset.com
- Kaspersky Mobile Security: http://www.kaspersky.com
- F-Secure Mobile Security: http://www.f-secure.com
- Trend Micro Mobite Security: http://www.trendmicro.com
- Webroot Secure Anywhere Mobile: http://www.webroot.com
- NetQin Mobile Security: http://www.netqin.com

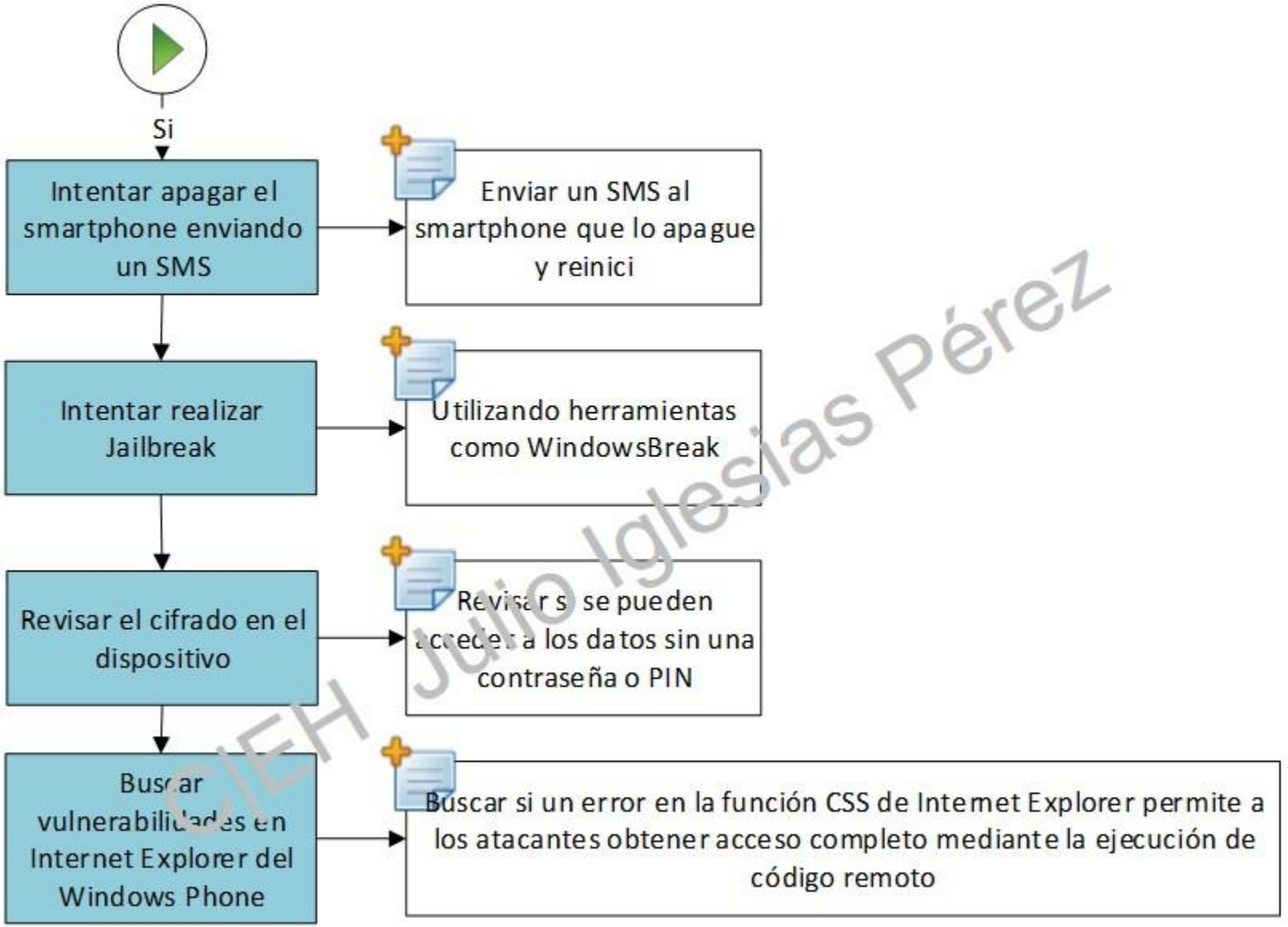

Test de Intrusión para Android
C|EH
Julio Iglesias Pérez



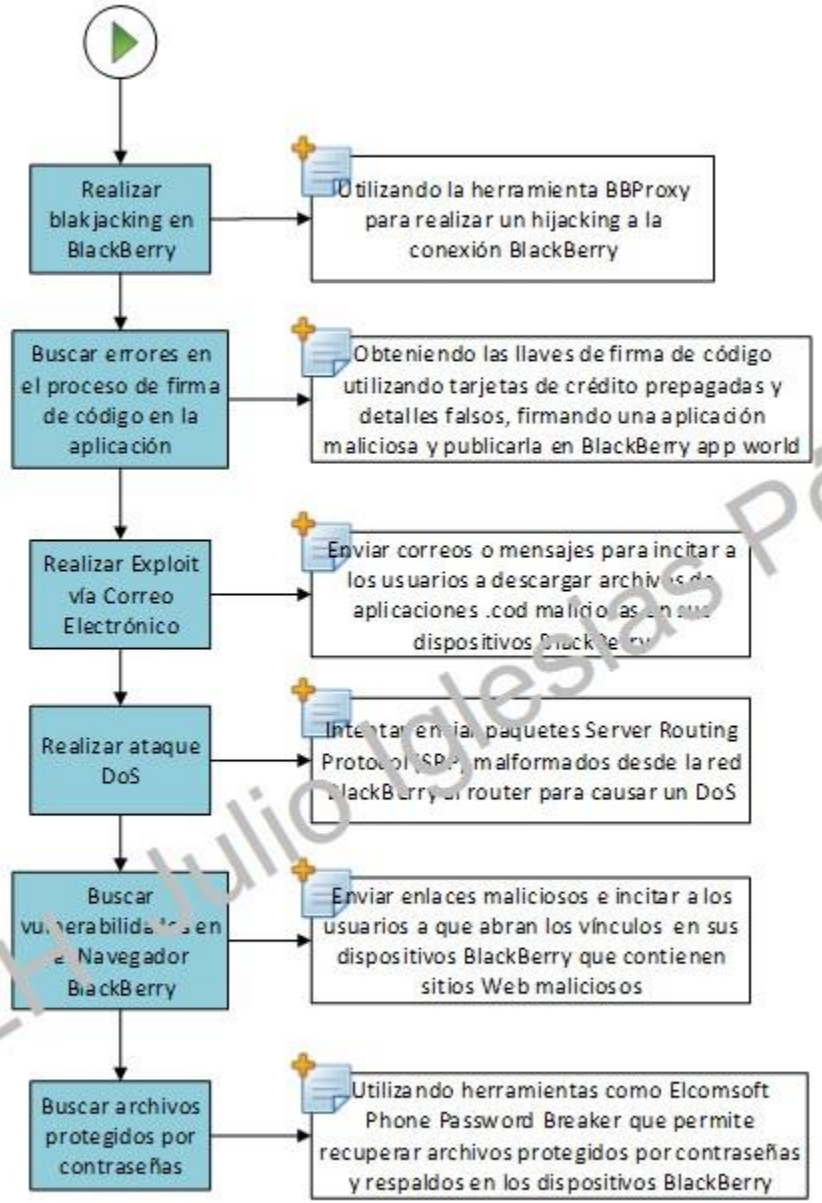

Test de Intrusión para iOS
C|EH
Julio Iglesias Pérez


Si
Jailbreak iOS
Utilizando herramientas como Redsn0w, Absinthe, Sn0wbreeze, PwnageTool, etc.
Desbloquear el iOS
Utilizando herramientas como iPhoneSimFree y anySIM
Utilizar SmartCover para bypasear el código de acceso
Presionar el botón de encendido hasta que aparezca el mensaje de apagado. Cerrar el smartcover hasta que la pantalla se apague y abrir el smartcover luego de unos segundos. Presionar cancelar para saltar la contraseña de código de seguridad.
Hackear el iOS mediante Metasploit
Utilizar Metasploit para explotar las vulnerabilidades en el iOS. Intentar enviar código no malicioso como payload al dispositivo para obtener acceso en él.
Buscar un AP
Buscar un AP con el mismo nombre y tipo de cifrado
Revisar los datos de transmisión del iOS en redes Wi-Fi
Revisar los datos de transmisión. Realizar un ataque MitM SSL striping interceptando parámetros inalámbricos en el dispositivo iOS en la red Wi-Fi. Enviar paquetes maliciosos a la red utilizando Cain&Abel
Revisar si se pueden enviar datos malformados al dispositivo
Utilizar técnicas de Ing. Social como el envío de correos, SMS, para incitar al usuario a abrir vínculos que contengan sitios web maliciosos


Test de Intrusión para Windows Phone
C|EH Julio Iglesias Pérez




Test de Intrusión para BlackBerry




¡Muchas Gracias!
C|EH Julio Iglesias Perez