CHECK POINT
DESMITIFICANDO LOS ATAQUES A LA SEGURIDAD DE DISPOSITIVOS MÓVILES

Los ataques a sus dispositivos móviles y al tráfico de la red están evolucionando rápidamente. Los atacantes de dispositivos móviles están robando (eso es lo que hacen) a través de métodos probados y efectivos en el mundo "tradicional" (cableado) y aplicándolos al mundo móvil, mientras proponen nuevas tácticas nunca vistas y que verdaderamente aprovechan los nuevos caminos que ofrecen los dispositivos móviles para entrar en la red de una organización. Por tanto, necesita prevenir todas las formas en las que un atacante puede aprovechar los dispositivos móviles para:

ESPIAR Y ESCUCHAR

Tomar el control del micrófono y cámara de su dispositivo

RECOPILAR DATOS DE LA EMPRESA

Incluidos emails, mensajes de texto y registro de llamadas

PONER EN RIESGO LOS CONTENEDORES SEGUROS

Extraer datos de aplicaciones

A continuación se recoge una rápida presentación de los tipos más comunes de ataques a móviles y las formas que tiene de prepararse para evitarlos.

APLICACIONES MALWARE PARA ANDROID

QUÉ HACEN Y CÓMO FUNCIONAN	VECTORES DE INFECCIÓN (CÓMO ENTRAN)	DAÑO QUE PUEDEN CAUSAR	CÓMO DETECTARLOS Y EVITARLOS
Se trata de aplicaciones maliciosas que se instalan en un dispositivo usando el sistema operativo (SO) Android. El malware normalmente se camufla como una app inocente, como por ejemplo un juego, un visor de PDFs o sala de conferencia, y luego se ejecuta en segundo plano llevando a cabo toda su actividad maliciosa.	Las aplicaciones maliciosas pueden descargarse desde Google Play o desde otra tienda de apps, a través de un e-mail, o de un sitio Web infectado o incluso de una red de publicidad. Las aplicaciones maliciosas también pueden ser cargadas por un atacante que consiga acceso físico al dispositivo (algunas veces de forma accidental por sus hijos, sobrinos, nietos, etc.).	Las aplicaciones con malware pueden actuar como un troyano de acceso remoto, con un kit de vigilancia con el que el atacante puede robar contraseñas, datos corporativos y correos electrónicos, además de capturar la actividad del teclado (keylogging) y la información en pantalla (screen scraping). También pueden activar el micrófono para escuchar conversaciones y reuniones, actuar como un troyano para robar contactos o mensajes de texto (mensajes SMS), o hacer de botnet móvil para enviar mensajes SMS a números premium.	**DETECTAR**: Para poder detectar la amplia variedad de aplicaciones maliciosas que pueden penetrar en su entorno es necesario una combinación de antivirus, detector de anomalías de tráfico y un sistema de análisis del comportamiento de las aplicaciones (Sandboxing y análisis de tráfico y código avanzado). **PREVENIR**: Necesita disponer de una solución instalada en el dispositivo (On-Device) que permita a los usuarios eliminar el malware que ya está instalado en el mismo, y un sistema de mitigación basado en la red para bloquear cualquier actividad que intente filtrar datos al exterior.

27 de mayo de 2015

ROOTKITS PARA ANDROID

QUÉ HACEN Y CÓMO FUNCIONAN	VECTORES DE INFECCIÓN (CÓMO ENTRAN)	DAÑO QUE PUEDEN CAUSAR	CÓMO DETECTARLOS Y EVITARLOS
Los Rootkits para Android son programas maliciosos diseñados para habilitar accesos con privilegios (root) en un dispositivo aprovechando vulnerabilidades del SO Android, y sin ser detectados. Una vez implementados en el dispositivo tienen el aspecto de un archivo del sistema operativo Android (normalmente se cargan a sí mismos en el directorio System) y no pueden eliminarse sin llevar a cabo una restauración de los ajustes de fábrica. Esto les hace invisibles para las soluciones Antivirus porque se requiere acceso con privilegios para analizar las ubicaciones donde se instala el rootkit.	Los rootkits pueden incrustarse en apps descargadas desde Google Play o desde otra tienda de apps, a través de un e-mail, o de un sitio Web o red infectada. Los rootkits también pueden preinstalarse en un dispositivo o ser cargados por un atacante que consiga acceso físico al dispositivo. Una vez en el dispositivo, los rootkits usan un exploit para romper el sandbox de aplicaciones del sistema operativo e instalarse profundamente en el sistema operativo.	Los rootkits pueden actuar como un troyano de acceso remoto, con un kit de vigilancia que el atacante puede usar para robar contraseñas, datos corporativos y correos electrónicos, además de capturar la actividad del teclado (keylogging) y la información en pantalla (screen scraping). También pueden activar el micrófono para escuchar conversaciones y reuniones, o actuar como un botnet para robar contactos o mensajes de texto (mensajes SMS).	**DETECTAR**: Para detectar actividad anormal en un dispositivo, incluyendo comunicaciones establecidas por binarios que no son aplicaciones, es necesaria tener la capacidad de realizar detección de anomalías de eventos y red, además de un análisis del comportamiento de las aplicaciones en el dispositivo que permita detectar actividad anormal en el mismo. **PREVENIR**: Para contener la amenaza es necesario poder bloquear las comunicaciones del malware que no provienen de aplicaciones.

EXPLOITS

QUÉ HACEN Y CÓMO FUNCIONAN	VECTORES DE INFECCIÓN (CÓMO ENTRAN)	DAÑO QUE PUEDEN CAUSAR	CÓMO DETECTARLOS Y EVITARLOS
Estos abarcan un gran número de ataques que utilizan vulnerabilidades del sistema operativo (SO) para permitir a los atacantes conseguir privilegios de acceso más altos (root) y romper el Sandbox del sistema operativo.	Los exploits pueden disfrazarse de aplicaciones descargadas de Google Play o desde otra tienda de apps, a través de un e-mail, o de un sitio Web infectado o una red publicitaria. Los exploits también pueden ser cargados por un atacante que consiga acceso físico al dispositivo.	Una vez que se ejecuta el exploit, el atacante puede espiar el almacenamiento de otras aplicaciones, memoria y recursos, obteniendo así acceso al contenido empresarial cifrado dentro de las soluciones Mobile Device Management (MDM), Contenedores y Wrappers. Básicamente tienen acceso a toda la información almacenada o que pasa a través del dispositivo móvil.	**DETECTAR**: Se necesita un análisis de comportamiento de aplicaciones y un análisis en Sandbox de las descargas (payloads). El sandbox necesita ser capaz de comportarse solamente como el dispositivo atacado para sí evitar que el malware detecte que se ejecutará en una máquina virtual. **PREVENIR**: Se necesita una solución On-Device que permita a los usuarios eliminar el malware que ya existe en el dispositivo y bloquear cualquier actividad de filtración de datos al exterior. Puede usar la solución basada en la red para bloquear el tráfico exploit y contener el ataque.

MALWARE IOS DISTRIBUIDO USANDO CERTIFICADOS DE EMPRESA O DE DESARROLADORES FALSOS

QUÉ HACEN Y CÓMO FUNCIONAN	VECTORES DE INFECCIÓN (CÓMO ENTRAN)	DAÑO QUE PUEDEN CAUSAR	CÓMO DETECTARLOS Y EVITARLOS
El malware para iOS suministrado mediante el uso de certificados falsos es un software malicioso que se instala en un dispositivo con sistema operativo iOS de Apple, acompañado de certificados validados por Apple que en realidad representan a una organización de confianza que ha sido puesta en riesgo. ¿Ha oído alguna vez hablar de los ataques Stuxnet, Flame y Bit9? – Todos ellos usaron un método parecido a este.	Apple otorga dos tipos de certificados para aquellas organizaciones que se comprometen a cumplir las directrices de Apple. Estos son: 1. Certificados de desarrollador (Developer), que permiten a los desarrolladores probar sus apps antes de que salgan al público en la App Store de Apple. 2. Certificados de empresa (Enterprise), que proporcionan a las organizaciones la oportunidad de establecer su propio mercado interno para apps dedicadas. Apple valida que las aplicaciones son firmadas por un certificado válido antes de que sean cargadas (lo que significa que no es instalada desde la App Store) en el dispositivo. Si un atacante es capaz de obtener un certificado, puede usarlo para validar su malware e instalarlo en cualquier dispositivo iOS sin pasar a través del proceso de investigación del App Store. Un usuario puede ser engañado entonces para descargar lo que en principio parece una app inofensiva. (Hay que tener en cuenta que dado el gran número de apps que existe, es muy difícil para Apple monitorizar el uso de certificados, y como resultado, han empezado a aparecer ataques, como FinFisher mRAT que usa este tipo de certificados).	Este malware puede usarse para hacer prácticamente de todo. Puede actuar como troyano de acceso remoto, con un toolkit de vigilancia que permite al atacante robar contraseñas, emails, registros del calendario y geolocalizar al usuario en tiempo real. Incluso puede activar el micrófono para escuchar las conversaciones y reuniones.	**DETECTAR**: Se necesita un sistema de evaluación de riesgo del dispositivo que pueda detectar en el dispositivo apps iOS que estén utilizando certificados Enterprise/Developer robados o fraudulentos. **PREVENIR**: Se necesita un sistema de eliminación On-Device que pueda bloquear o eliminar certificados fraudulentos para erradicar el ataque.

PERFILES IOS MALICIOSOS

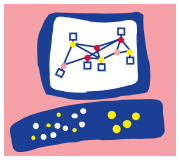
QUÉ HACEN Y CÓMO FUNCIONAN	VECTORES DE INFECCIÓN – CÓMO ENTRAN	DAÑO QUE PUEDEN CAUSAR	CÓMO DETECTARLOS Y EVITARLOS
Un ataque que use un archivo de configuración para iOS puede redefinir los parámetros de funcionalidad del sistema, como los ajustes de dispositivo, operador, mobile device management (MDM) y red. Un perfil puede saltarse los mecanismos de seguridad del dispositivo o la aplicación, por lo que resulta un objetivo muy atractivo para los atacantes.	El usuario puede ser engañado para descargar un perfil malicioso, y al hacerlo, proporcionar de forma inadvertida a la configuración fraudulenta la capacidad de redirigir todo el tráfico desde el dispositivo móvil a un servidor controlado por el atacante, e instalar más adelante apps falsas o incluso descifrar las comunicaciones. El perfil también puede cargarlo un atacante que consiga acceso físico al dispositivo.	Un perfil malicioso se salta los mecanismos de seguridad, así que puede usarse prácticamente para cualquier cosa. Puede permitir al atacante el robar contraseñas, emails, todos los datos almacenados o que pasen por el teléfono, los registros del calendario y datos de geolocalización, en tiempo real.	**DETECTAR**: Se necesita una evaluación de riesgo del dispositivo para detectar perfiles fraudulentos del iOS o perfiles que hayan sido alterados en el dispositivo. El análisis de comportamientos de aplicaciones puede usarse también para identificar perfiles que muestren una actividad sospechosa o anormal. **PREVENIR**: Se necesita un sistema de remediación On-Device que pueda bloquear o eliminar certificados fraudulentos para erradicar el ataque.

TROYANOS DE VIGILANCIA DE IOS Y DE ACCESO REMOTO MÓVIL (MRATS)

QUÉ HACEN Y CÓMO FUNCIONAN	VECTORES DE INFECCIÓN – CÓMO ENTRAN	DAÑO QUE PUEDEN CAUSAR	CÓMO DETECTARLOS Y EVITARLOS
iOS mRATs son programas maliciosos que se instalan en un dispositivo usando el sistema operativo Apple iOS y que dan al atacante la posibilidad de obtener acceso remoto a toda la información almacenada y que pase a través del dispositivo.	Estos ataques normalmente aprovechan dispositivos con jailbreak, lo que significa que se han eliminado previamente todos los mecanismos de seguridad de iOS. No es muy raro que los usuarios de iOS hagan jailbreak de sus propios dispositivos, para poder instalar cualquier app iOS que deseen, y no solo las de la tienda de Apple. Los atacantes también pueden hacer un jailbreak de un dispositivo iOS, bien obteniendo acceso físico al mismo o bien a través del clabe USB de un equipo comprometido. Una vez que el dispositivo tiene jailbreak, los atacantes pueden instalar la aplicación espía o de vigilancia de su elección, o disfrazarla en una aplicación de otra tienda de apps para que la descargue un usuario de forma inocente.	Los mRATs pueden actuar como un troyano de acceso remoto, con un toolkit de vigilancia con el que el atacante puede robar contraseñas, datos corporativos y correos electrónicos, además de capturar la actividad del teclado (keylogging) y la información en pantalla (screen scraping). También pueden activar el micrófono para escuchar conversaciones y reuniones, o actuar como un botnet para robar contactos o mensajes de texto (mensajes SMS).	**DETECTAR**: Se necesita realizar evaluaciones de riesgo del dispositivo para detectar esos dispositivos con jailbreak e investigar el comportamiento real de las comunicaciones en el dispositivo. **PREVENIR**: Para bloquear el tráfico y contener las infecciones mRAT (mobile Remote Access Trojan), se necesitan remediaciones en el dispositivo y mitigaciones basadas en red.

MAN-IN-THE-MIDDLE (MITM)

QUÉ HACEN Y CÓMO FUNCIONAN	VECTORES DE INFECCIÓN – CÓMO ENTRAN	DAÑO QUE PUEDEN CAUSAR	CÓMO DETECTARLOS Y EVITARLOS
Los ataques MitM pueden espiar y escuchar, así como interceptar y modificar el tráfico entre dos dispositivos informáticos. El usuario cree que está interactuando con una entidad conocida de confianza (normalmente un sitio Web). Los signos de alerta y advertencia en los PCs y portátiles son mucho más sutiles en los dispositivos móviles. El tamaño limitado de sus pantallas oculta las URLs al usuario, haciendo complicado la validación de la URL a la que está apuntando en realidad el navegador en cuestión.	Los ataques Wi-Fi MitM suceden cuando un dispositivo móvil se conecta a un hotspot Wi-Fi. El atacante puede crear una red Wi-Fi falsa (por ejemplo 'Free-Starbucks') o simplemente conectarse a las misma red Wi-Fi legítima que está usando la víctima. Finalmente todas las comunicaciones terminan pasando a través del dispositivo de red controlado por el atacante.	Los ataques MitM pueden usarse para espiar y escuchar e incluso alterar las comunicaciones cifradas (SSL) de la red usando certificados fraudulentos o rebajando el enlace de comunicación, con el objetivo de desencriptar y abrirlo al atacante.	**DETECTAR**: Se necesita un análisis de comportamiento de aplicaciones que pueda detectar hotspots Wi-Fi señuelos y otros factores de riesgo. **PREVENIR**: Se necesita una remediación en el dispositivo que pueda, de forma dinámica, lanzar una VPN para aislar la comunicación del usuario de la red comprometida y una mitigación basada en red que bloquee el tráfico desde el hotspot señuelo.



Check Point®
SOFTWARE TECHNOLOGIES LTD.

CONTACTE CON CHECK POINT

Oficinas centrales
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
Oficinas centrales en EE.UU.
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com
Oficinas centrales en España
C/ Vía de las Dos Castillas, 33. Edificio Ática 6, Pta. 3ª. Oficina D-1 | 28224 Pozuelo de Alarcón | Tel: +34 917992714