Capítulo 8:

Android y malware para Android

Android es un sistema operativo para dispositivos móviles. Se trata de uno de los dos principales sistemas operativos, siendo iOS de Apple el otro y su principal competidor[1]. Si quiere saber más sobre Android y su relación con el proyecto Android Open Source, el artículo de Wikipedia le resultará útil.

Como nota, los ejercicios de este capítulo requieren que tenga acceso a un teléfono Android. Cualquier teléfono servirá, incluido su propio dispositivo personal. No tendrá que realizar ninguna modificación en el teléfono. Si no tiene acceso a un teléfono de este tipo y aún así quiere hacer los ejercicios, es posible instalar una versión de máquina virtual de Android en VirtualBox, aunque puede resultar un poco engorroso.

Versiones de Android y una nota sobre Google

En el momento de redactar este artículo, este contenido estaba actualizado. Sin embargo, Google, que desarrolla Android, actualiza constantemente el sistema operativo. En general, ¡pero no siempre!, estas actualizaciones mejoran la privacidad y la seguridad, así como su capacidad para controlar los ajustes de seguridad y privacidad. Tenga esto en cuenta al leer este texto, especialmente si lo lee bastante tiempo después de su última actualización. Para conocer las últimas actualizaciones, consulte la página oficial de Android y su guía para desarrolladores.

Además, tenga en cuenta que el aspecto externo de Android varía mucho de un teléfono a otro, incluso cuando los teléfonos utilizan la misma versión de Android. A veces, la forma en que las cosas funcionan "internamente" también varía. Puede que las cosas que se comentan en este capítulo sean ligeramente diferentes en el teléfono que esté utilizando, aunque se han probado en varios teléfonos.

Además, hay que tener en cuenta que este capítulo se centra en las aplicaciones maliciosas y se ha escrito partiendo del supuesto de que el propio Google no está en el modelo de amenazas del usuario. Si no realiza copias de seguridad de los datos en la nube de Google sin cifrar, Google no podrá leer los mensajes de Signal o WhatsApp. Sin embargo, Google puede ver qué aplicaciones hay instaladas en su teléfono y podría verse obligado a entregar estos datos a las autoridades.

¿Qué probabilidad hay de que exista malware para Android?

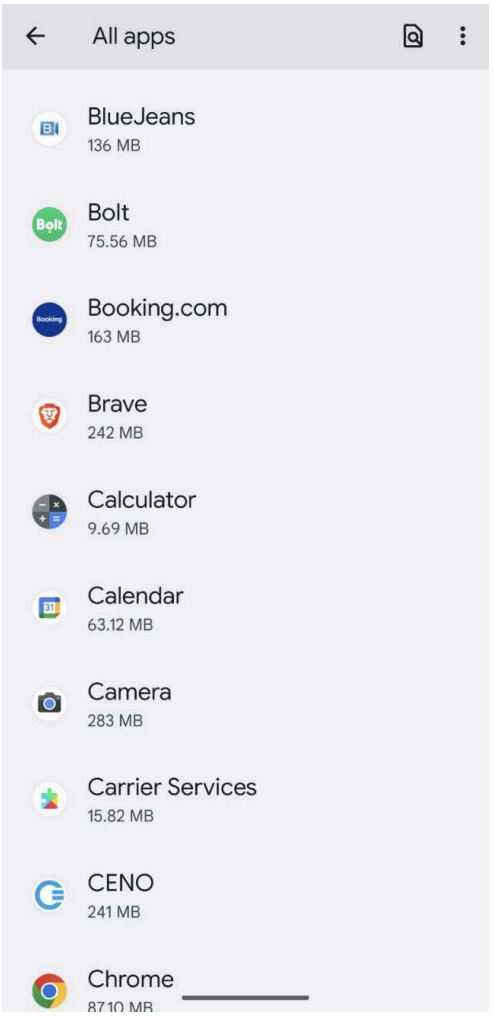
El malware para Android es real, y sin duda es algo que cualquier organización de la sociedad civil debería incluir en su modelo de amenazas. El presente capítulo le ayudará a analizar los dispositivos Android en busca de aplicaciones potencialmente maliciosas.

Sin embargo, antes de comenzar, puede que sea una buena idea considerar hasta qué

[1] Aunque no funcionan en los mismos dispositivos: un iPhone no puede ejecutar Android y un teléfono fabricado para Android no puede ejecutar iOS.

punto es probable el malware para Android. El malware para Android, aunque más común que el malware para iOS, es relativamente poco frecuente. El malware para Android más común realiza fraudes publicitarios y tiene un impacto bastante reducido en el dispositivo[2].

Esto se debe al funcionamiento de las aplicaciones Android. Lograr que un usuario instale una aplicación maliciosa no es fácil, especialmente cuando el atacante quiere que la instale una persona en particular. Si el atacante no está explotando vulnerabilidades en el sistema operativo Android (lo que no es frecuente y puede requerir mucha sofisticación técnica), las aplicaciones instaladas tienen restringido lo que pueden hacer. Así que antes de llegar a la conclusión de que debe haber malware en un dispositivo Android, vale la pena considerar otras opciones (por ejemplo, una cuenta comprometida a través de una contraseña robada), en particular, si la acción cometida por el actor sospechoso no parece lo suficientemente sofisticada como para ser una campaña de malware.



Pregunta 8.1 Una periodista recibió un correo electrónico anónimo en el que se le informaba de que el remitente sabía que ella había estado anoche en un bar determinado. Efectivamente, así fue, y ella encuentra el correo electrónico, comprensiblemente, muy perturbador. Con sólo esta información, ¿qué probabilidad usted estima que se trataba de un malware en su teléfono que compartía su ubicación? (Ver la respuesta en el apéndice).

Aplicaciones y permisos de Android

Los programas en Android suelen denominarse "aplicaciones". Como usuario de Android, conocerá algunas aplicaciones porque las utiliza con regularidad y tienen iconos en su pantalla de inicio, pero también hay aplicaciones con las que está menos familiarizado, como las instaladas por el fabricante del teléfono (Samsung, HTC, Huawei, etc.) o las aplicaciones del sistema que brindan cierta funcionalidad pero que, por lo demás, están ocultas para el usuario.

Por motivos de privacidad y seguridad, el sistema operativo Android utiliza permisos para limitar el acceso de las aplicaciones a los recursos. Por ejemplo, una aplicación no puede acceder a los contactos almacenados en el teléfono a no ser que se le haya concedido permiso para ello.

Salvo en el caso de algunos programas maliciosos muy avanzados (de los que hablaremos en un capítulo posterior), lo mismo ocurre con las aplicaciones maliciosas, tanto si se instalan desde Google Play como si se **"transfieren localmente"** al teléfono[3].

[2] Hacer clic en anuncios en segundo plano o mostrar un gran número de anuncios al usuario.
[3] La transferencia local es el acto de instalar aplicaciones fuera de la tienda oficial de aplicaciones, en

Puede ver los permisos concedidos a una aplicación accediendo a los ajustes y buscando la aplicación en cuestión en la lista de aplicaciones. Esto puede ayudarle a determinar si una aplicación, por ejemplo, está rastreando su ubicación o escuchando sus conversaciones: necesitará su permiso para hacerlo.

Así pues, una forma natural de buscar aplicaciones maliciosas en un teléfono Android sería examinar todas las aplicaciones instaladas – la configuración del teléfono le permite hacerlo – y luego ver si alguna de ellas tiene permisos inusuales. Hay algunos inconvenientes en este enfoque:

- Un teléfono puede tener fácilmente más de 100 aplicaciones instaladas. Lleva mucho tiempo revisarlas todas.
- Las aplicaciones maliciosas a menudo se hacen pasar por algo totalmente inocente (como una aplicación de calculadora), y podría pasarlas por alto al revisar las aplicaciones.
- Hay muchas aplicaciones instaladas en un teléfono Android de las que el propietario nunca ha oído hablar, normalmente porque vienen con el sistema operativo. A veces, la gente se pone nerviosa al ver estas aplicaciones ("Mi teléfono tiene una aplicación para el carro. ¡Yo ni siquiera tengo carro! Debe de ser un programa espía").

  Una forma muy distinta de enfocar esto es conectar el teléfono a una computadora y escanear el teléfono con un software especial diseñado para detectar malware. Esto puede ser útil en algunos casos, pero también tiene inconvenientes:

- Exige que el analista tenga acceso físico al teléfono, cuando la ayuda en la mayoría de los casos es a distancia.
- Establece un nivel bastante alto para el análisis en términos de herramientas, conocimientos y experiencia. Si bien la mayoría de los problemas pueden ser detectados incluso por el propio usuario del teléfono si se le guía en el proceso, estas herramientas avanzadas son menos accesibles para los usuarios comunes.
- No todo el mundo, y ciertamente no todas las personas de alto riesgo, confiarán en que otra persona conecte su teléfono a la computadora de otra persona.

Un mejor enfoque: examinar los permisos de las aplicaciones

Sin embargo, hay un enfoque mejor, que es usar el Administrador de permisos en la configuración de un teléfono Android. Esta función muestra la mayoría[4] de los permisos que las aplicaciones pueden solicitar y, para cada permiso, qué aplicaciones han recibido dichos permisos. En algunos casos, también muestra un nivel de detalle para el permiso.

Por ejemplo, si está preocupado por la posibilidad de que una aplicación maliciosa del teléfono tenga acceso al micrófono, puede ver a qué aplicaciones se les ha concedido este permiso y comprobar si son aplicaciones legítimas. Tenga en cuenta que, lamentablemente, incluso las aplicaciones legítimas a veces solicitan demasiados permisos. El hecho de que

---

este caso Google Play. En Android es posible, pero requiere que el usuario haga clic en algunas advertencias. Por tanto, requiere cierta ingeniería social, o que un adversario tenga acceso por poco tiempo al dispositivo desbloqueado.

[4] Algunos permisos son muy poco claros y no son del todo relevantes en este contexto. Otros dos se analizan más adelante en el capítulo.

una aplicación de linterna solicite su ubicación no significa automáticamente que se trate de malware, aunque probablemente usted no quiera que tenga este permiso.

La forma de hacerlo es buscar el Administrador de permisos en la configuración y después comprobar los permisos individuales.

Para saber si la solicitud de permiso de una aplicación es preocupante, tenga en cuenta la forma en que suele utilizar la aplicación. Si utiliza Ubicación, Micrófono, SMS, Contactos y Archivos con esa aplicación, es posible que los permisos sean razonables. Si no utiliza esos permisos con una aplicación, el uso de esas partes de su dispositivo puede ser una señal de que algo va mal, así que busque solicitudes de permiso inesperadas.

El objetivo aquí no es entender completamente lo que las aplicaciones están haciendo, sino limitar su investigación a un pequeño número (¡a veces cero!) de aplicaciones desconocidas que pueda querer investigar más a fondo. Como ventaja adicional, también podrá descubrir qué aplicaciones legítimas requieren permisos con los que usted o la persona cuyo teléfono está investigando se siente incómodo; es posible que pueda desactivar estos permisos.

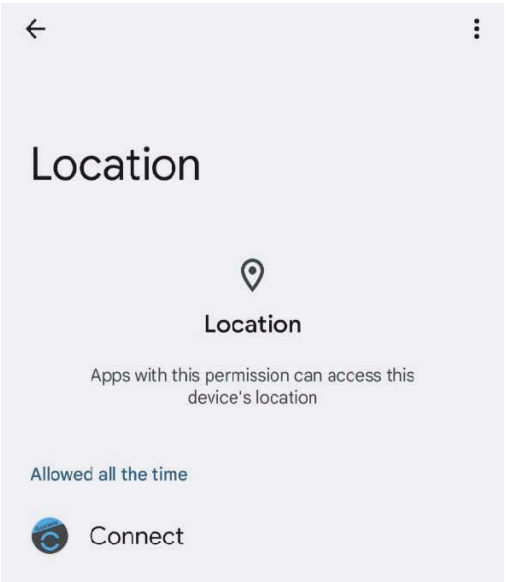
En ocasiones, no es posible cambiar los permisos de una aplicación preinstalada (la página web oficial de Android tiene información[wayback machine] al respecto. Puesto que muchas personas están menos familiarizadas con estas aplicaciones preinstaladas, pueden sospechar que una aplicación de este tipo está haciendo algo malicioso. Si es un teléfono con el que no está familiarizado, puede que tenga que investigar un poco sobre estas aplicaciones para entender lo que hacen y tranquilizar al usuario (y quizá también a usted mismo).

Ubicación

Las aplicaciones a las que se ha concedido este permiso pueden acceder a la ubicación GPS del teléfono. Entre los ejemplos más obvios se encuentran las aplicaciones de mapas y las de taxi: necesitan la ubicación para funcionar bien.

A una aplicación se le puede conceder acceso a la ubicación todo el tiempo o sólo cuando se esté utilizando la aplicación. También puede tener que preguntar cada vez que requiera la ubicación. Lo más probable es que las aplicaciones que hacen cosas en secreto, como los programas espía, necesiten permiso todo el tiempo. Desconfíe especialmente de las aplicaciones a las que se hayan concedido este tipo de permisos.

Este capítulo no trata de si puede y debe confiar sus datos a las empresas que están detrás de estas aplicaciones. Sin embargo, independientemente de si confía en las empresas, hay varias formas en las que un adversario puede obtener acceso a los datos de localización obtenidos mediante las aplicaciones.



Las más obvias son tener acceso al teléfono y, por lo tanto, a la aplicación en sí, o a una cuenta en línea correspondiente, y tener la capacidad de ver el historial de ubicaciones. Por ejemplo, Google proporciona esto para Google Maps. Un adversario también podrá solicitar legalmente estos datos mediante una citación judicial.

Por lo tanto, si desea evaluar si los datos de ubicación de alguien están seguros, debe fijarse en lo fácil que le resulta (y, por lo tanto, a cualquier persona que consiga hacerse pasar por ella) acceder al historial de ubicaciones y en cómo responde la empresa a las solicitudes de datos; muchas grandes empresas publican informes de transparencia.

Independientemente de eso, para la mayoría de estas aplicaciones, no debería haber ningún problema en configurar el permiso para que sólo se utilice cuando la aplicación esté en uso o para que pida permiso cada vez. Esto significa que la aplicación no tiene acceso a los datos de ubicación todo el tiempo.

Finalmente, tenga en cuenta que el GPS es muy preciso. Puede indicar una ubicación con una precisión de 30 cm. En algunos casos puede ocurrir que a alguien le preocupe que se filtre su ubicación aproximada, por ejemplo, en qué ciudad o país se encuentra. Esta información puede filtrarse de muchas formas explícitas (por ejemplo, a través de la dirección IP) y a veces también de forma implícita (a través de información compartida públicamente). Este capítulo no trata sobre mostrar cómo se puede evitar esto, ¡pero es muy desafiante!

Micrófono

Las aplicaciones a las que se les haya concedido este permiso pueden acceder a su micrófono y por tanto grabar cualquier cosa que diga, así como los sonidos ambientales.

Existen muchas razones legítimas para que las aplicaciones utilicen este permiso, por ejemplo, las aplicaciones que le permiten enviar mensajes de voz, las que graban vídeos o aquellas a las que se puede acceder por medio de comandos de voz.

Del mismo modo que con el permiso de ubicación, el acceso al micrófono se puede conceder todo el tiempo, sólo cuando la aplicación se esté ejecutando o haciendo que la aplicación pregunte cada vez. Hay muy pocas buenas razones para que una aplicación tenga este permiso todo el tiempo. Por lo tanto, una aplicación a la que se le haya concedido este permiso es una gran señal de alarma.

SMS

Una aplicación a la que se le haya concedido permiso para leer mensajes SMS puede espiarlos. Dependiendo de si el usuario utiliza activamente los SMS para comunicarse, esto puede suponer un motivo de preocupación en lo que respecta al programa espía.

Ahora bien, los SMS también se utilizan para la autenticación multifactor, por lo que una app con acceso a los SMS puede tranquilamente leer los códigos enviados por esta vía[5]. En este sentido, algunas aplicaciones utilizan los SMS como forma de confirmar el número de teléfono del dispositivo y solicitan este permiso para evitar que el usuario tenga que ingresar un código manualmente. Así pues, este permiso puede ser utilizado de forma maliciosa por una aplicación que quiera hacerse pasar por el usuario.

La aplicación de SMS predeterminada del teléfono dispone automáticamente de este

[5] Esta es una de las diversas razones por las que utilizar SMS para la autenticación multifactor es menos seguro que otras opciones, como una app autenticadora o un token de hardware.

permiso, al igual que otras aplicaciones que pueden utilizarse para gestionar SMS, como Signal.

Dado que los SMS llegan en segundo plano, las aplicaciones con acceso a SMS necesitarán esto todo el tiempo. No existe ninguna opción para conceder este permiso únicamente mientras la aplicación está en ejecución o para solicitarlo cada vez.

Contactos

Las aplicaciones que tienen este permiso pueden acceder a los contactos de un teléfono. También lo utiliza la propia aplicación del teléfono; por ejemplo, las aplicaciones de mensajería como Signal y WhatsApp que identifican a los usuarios basándose en sus números de teléfono. Los contactos generalmente incluyen números de teléfono, pero dependiendo de cómo se esté utilizando el teléfono, también puede incluir contactos de correo electrónico. Para muchos usuarios de alto riesgo, su lista de contactos es información muy delicada.

Al igual que con los SMS, este permiso se permite de forma permanente o se deniega.

Archivos

Este permiso autoriza a las aplicaciones a acceder a los archivos del dispositivo. Un administrador de archivos o un producto de seguridad son ejemplos de aplicaciones legítimas que requieren este permiso. El permiso Archivos ha cambiado mucho en las últimas versiones de Android y se ha vuelto más detallado. Si desea buscar una aplicación maliciosa, al menos al principio, lo mejor es asumir que si la aplicación tiene permiso para acceder a los archivos, puede acceder a cualquier archivo que esté almacenado allí.

Recuerde que esto no permite a las aplicaciones acceder a los chats de Signal, WhatsApp, etc.

Este permiso también se autoriza permanentemente o se deniega

Ejercicio 8.2. Para cada uno de los cinco permisos mencionados, verifique en un teléfono Android a qué aplicaciones se les ha concedido este permiso.

Ejercicio 8.3. El Administrador de permisos en Android muestra una lista con más de estos cinco permisos. Revise los demás y piense si podrían ser utilizados por malware.

Hay dos tipos de permisos especiales que se indican por separado, ya que no se encuentran en el Administrador de permisos: la accesibilidad y las notificaciones. Sin embargo, son muy relevantes porque las aplicaciones maliciosas suelen abusar de ellos. La forma en que puede accederse a este ajuste varía de un teléfono a otro: si no la encuentra fácilmente en el menú Privacidad en los Ajustes, utilice la función de búsqueda en los Ajustes.

Accesibilidad

La accesibilidad hace que las aplicaciones de un teléfono sean más accesibles para las personas con ciertas discapacidades, por ejemplo, ayudándolas a integrarse con los lectores

de pantalla. Una aplicación registrada como servicio de accesibilidad puede controlar el teléfono hasta un cierto punto: puede hacer clic en botones, registrar cuándo se hace clic en un botón, llenar formularios de texto o registrar lo que se ha llenado en los formularios.

Algunas aplicaciones legítimas que no ofrecen servicios para personas con discapacidad siguen registrándose como servicio de accesibilidad. Un ejemplo son los gestores de contraseñas, que requieren esta función para poder completar las contraseñas almacenadas en las aplicaciones.

Puede encontrar qué aplicaciones están registradas como servicio de accesibilidad buscando "Accesibilidad" en los ajustes del teléfono y buscando después los servicios instalados.

Hay que señalar que a partir de Android 13, lanzado en agosto de 2023, sólo las aplicaciones instaladas a través de Google Play podrán solicitar permisos de accesibilidad.

Notificaciones

Las notificaciones son las ventanas emergentes que se muestran en el teléfono cuando se recibe un nuevo mensaje o cuando hay algún otro tipo de alerta. Las notificaciones que reciba dependerán de la configuración de cada aplicación.

Las aplicaciones pueden solicitar acceso a las notificaciones, lo que significa que pueden ver todas las notificaciones y la aplicación que las envió. Una aplicación que sincroniza un teléfono con un reloj inteligente y muestra notificaciones es un ejemplo de aplicación legítima que requiere acceso a las notificaciones.

El software malicioso puede utilizar esto, y a veces lo hace, para espiar las actividades del usuario, aunque las notificaciones sólo muestren los mensajes entrantes, no los salientes.

Ejercicio 8.4. Al igual que antes, verifique en un teléfono Android a qué aplicaciones se les han concedido permisos de notificación y accesibilidad.

Analizar el malware para Android y el malware avanzado para Android

En el capítulo anterior, usted aprendió cómo VirusTotal puede enseñarle bastante sobre el malware haciendo pivoting. Por ejemplo, puede encontrar que un malware para Android se conecta a un determinado dominio, al que también se conecta otro malware, y este malware ha sido analizado. Eso sugiere que el archivo que usted está analizando podría ser una versión diferente de ese malware, aunque, como siempre, hay muchas advertencias.

También existe apklab, un servicio de la empresa de seguridad Avast. Es como VirusTotal pero más adaptado a Android y puede ser de gran utilidad a la hora de analizar malware para Android. El sitio requiere una cuenta, que es gratuita pero debe ser aprobada por sus administradores. Le recomendamos solicitar una cuenta.

También puede ejecutar el archivo en un sandbox (más sobre esto en el capítulo 10). Esto suele ser suficiente para comprender lo que hace un archivo en particular.

Para conocer a fondo el análisis del malware para Android, existe un curso excelente de la investigadora de Google Maddie Stone.

También es importante señalar que hay algunos programas espía avanzados que se ocultan tan profundamente en los teléfonos que no se ejecutan como una aplicación. Realizar análisis forenses en teléfonos en busca de ese tipo de programas espía es realmente complicado, especialmente en el caso de los teléfonos Android. Es probable que tenga que trabajar con expertos, como los de Citizen Lab o Amnesty Tech, hasta que desarrolle sus propias habilidades.

Esperamos profundizar en el análisis de malware para Android en próximas adiciones a esta guía.