الفصل 8:
نظام أندرويد والبرمجيات الضارة على أجهزة أندرويد

أندرويد (Android) هو نظام تشغيل للأجهزة المحمولة وأحد نظامَي التشغيل الرئيسيين، ليقابله نظام آي أو إس (iOS) الخاص بأجهزة آبل (Apple) وهو منافسه الرئيسي[25]. وفي حال كنت ترغب في معرفة المزيد عن أندرويد وعن علاقته بمشروع أندرويد أوبن سورس (Android Open Source)، فيمكنك الاستفادة من المقالة على موقع ويكيبيديا.

تجدر الإشارة إلى أنك تحتاج إلى استخدام هاتف يعمل بنظام أندرويد لإنجاز التمارين الواردة في هذا الفصل، وأي هاتف سيفي بالغرض بما في ذلك جهازك الشخصي إذ لن يُطلب منك إجراء أي تعديلات عليه. وإذا كنت غير قادر على استخدام مثل هذا الهاتف ولا تزال ترغب في القيام بالتمارين، فمن الممكن تثبيت إصدار جهاز افتراضي من أندرويد في فيرتشول بوكس (VirtualBox) إلا أن الأمر قد يتسم بشيء من التعقيد.

إصدارات أندرويد وملاحظة حول غوغل (Google)

كان هذا المحتوى محدثًا في وقت كتابته، مع العلم أن غوغل وهي الشركة القائمة على تطوير نظام أندرويد تقوم بتحديث نظام التشغيل باستمرار. وتجدر الإشارة إلى أن هذه التحديثات تعمل بشكل عام، ولكن ليس على الدوام، على تحسين ميزتَي الخصوصية والأمان وكذلك قدرتك على التحكم في إعدادات الأمان والخصوصية. ضع ذلك في الاعتبار عند قراءة هذا النص وبالأخص إذا قرأته بعد فترة طويلة من آخر تحديث له. للتعرف على آخر التحديثات، يمكنك الرجوع إلى موقع أندرويد الرسمي ودليل مطور برامجه.

ضع أيضًا في الاعتبار أن الجزء الأكبر من الشكل الخارجي لأندرويد يختلف كثيرًا من هاتف لآخر، حتى وإن كانت الهواتف تستخدم إصدار أندرويد ذاته. وقد تختلف أيضًا طريقة عمل الأشياء «تحت الغطاء» في بعض الأحيان. ومن الممكن أن تجد بعض الاختلاف بين الأمور التي يتناولها هذا الفصل والهاتف الذي تستخدمه إلا أنه تم اختبارها على هواتف مختلفة.

ومن الأمور الأخرى التي عليك أن تضعها في اعتبارك هو أن هذا الفصل يركز على التطبيقات الضارة وتمت كتابته بافتراض أن غوغل ليست في نموذج تهديد المستخدم. إذا كنت لا تنسخ البيانات احتياطيًا إلى سحابة غوغل غير المشفرة فلن تتمكن غوغل من قراءة رسائل سيغنال (Signal) أو واتسآب (WhatsApp)، لكن بإمكان غوغل رصد التطبيقات التي قمت بتثبيتها على هاتفك ويمكن إرغامها على تسليم هذه البيانات إلى السلطات.

ما مدى احتمالية وجود برمجيات ضارة على أجهزة أندرويد؟

لا لبس في أن البرمجيات الضارة على أجهزة أندرويد أمر واقع، ويتحتم على أي منظمة مجتمع مدني إدراج ذلك في نموذج التهديد الخاص بها. من شأن هذا الفصل أن يساعدك على تحليل أجهزة أندرويد بحثًا عن تطبيقات قد تكون ضارة.

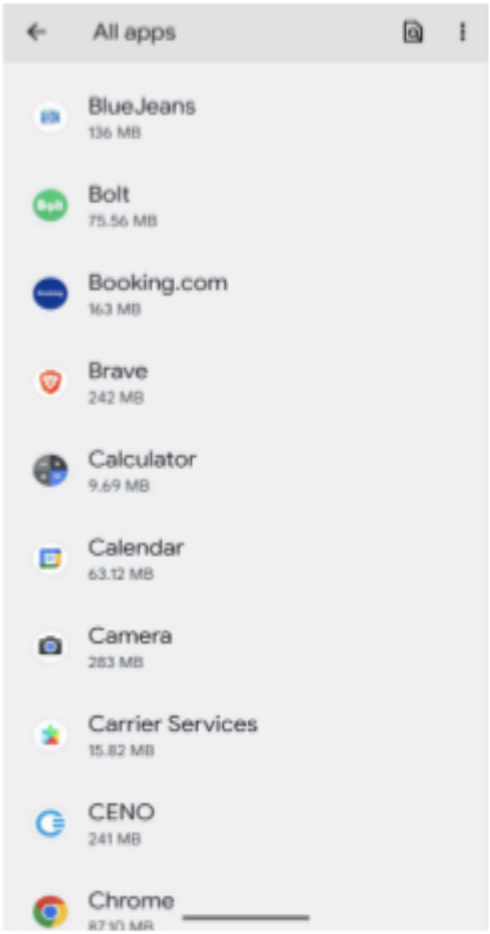
ولكن قبل أن تبدأ، لعله من المستحسن التفكير في مدى احتمالية وجود برمجيات ضارة على جهاز أندرويد. بالرغم من أن البرمجيات الضارة على أجهزة أندرويد نادرة نسبيًا، إلا أنها أكثر شيوعًا من البرمجيات الضارة التي تستهدف أجهزة آي أو إس (iOS). تُشارك البرمجيات الضارة على أجهزة أندرويد الأكثر شيوعًا في الاحتيال الإعلاني وتترك تأثيرًا ضئيلًا نسبيًا على الجهاز.[26]

يعود ذلك إلى كيفية عمل تطبيقات أندرويد. ليس من السهل دفع مستخدم لتثبيت تطبيق ضار، لا سيما عندما يريد المهاجم أن يقوم فرد معين بتثبيته. وإذا كان المهاجم لا يستغل الثغرات في نظام تشغيل أندرويد (وهو أمر نادر وقد يتطلب الكثير من التطور التقني)، سيقتصر عمل التطبيقات المثبتة على ما يمكنها فعله. لذلك وقبل البت بوجود برمجيات ضارة على جهاز أندرويد، يجب النظر في المسائل التالية:

[25] أنها لا تعمل على الأجهزة ذاتها، فلا يمكن لجهاز آيفون تشغيل نظام أندرويد ولا يمكن لهاتف مصنوع لنظام أندرويد تشغيل نظام آي أو إس (iOS)
[26] النقر على الإعلانات في الخلفية أو عرض عدد كبير من الإعلانات على المستخدم

خيارات أخرى (على سبيل المثال، اختراق حساب من خلال كلمة مرور مسروقة)، تحديدًا إذا كان العمل الذي ارتكبته الجهة الفاعلة المشتبه فيها لا يبدو متطورًا بما يكفي لتشكيل حملة ضارة.

السؤال 8.1. تتلقى صحفية رسالة بريد إلكتروني مجهولة المصدر تفيد بأن المرسل يعرف أنها كانت في حانة معينة في الليلة الفائتة. وكانت هناك في الواقع وتجد بطبيعة الحال البريد الإلكتروني مقلقًا جدًا. باستخدام هذه المعلومات فحسب، ما مدى احتمالية وجود برمجية ضارة على هاتفها كانت قد قامت بمشاركة موقعها؟ (انظر



تطبيقات وأذونات أندرويد

عادة ما يشار إلى البرامج على أندرويد باسم «التطبيقات». وبصفتك مستخدمًا لنظام آندرويد، ستعرف بشأن تطبيقات نتيجة استخدامك الدائم لها وهي تحظى برموز على شاشتك الرئيسية، ولكن تتوفر أيضًا تطبيقات لست ملمًا بها بما يكفي، مثل التطبيقات التي تم تثبيتها بواسطة الشركة المصنعة للهاتف (سامسونغ (Samsung) وإتش تي سي (HTC) وهواوي (Huawei) وما إلى ذلك) أو تطبيقات الأنظمة التي توفر وظائف معينة ولكنها مخفية عن المستخدم.

في ما يتعلق بالخصوصية والأمان، يستخدم نظام التشغيل أندرويد الأذونات للحد من الموارد التي يمكن للتطبيقات استخدامها، فعلى سبيل المثال لا يمكن لتطبيق الوصول إلى جهات الاتصال المخزنة على الهاتف ما لم يتم منحه الإذن للقيام بذلك.

ربما باستثناء بعض البرمجيات الضارة المتقدمة جدًا (سنتحدث أكثر عنها في فصل لاحق)، ينطبق هذا أيضًا على التطبيقات الضارة سواء كانت مثبتة من غوغل بلاي (Google Play) أو «**محملة جانبيًا**» على الهاتف.[27]

يمكن إيجاد الأذونات الممنوحة لتطبيق عن طريق مراجعة الإعدادات والبحث عن التطبيق الفردي في قائمة التطبيقات. يمكن أن يساعدك هذا في تحديد ما إذا كان يمكن لتطبيق القيام على سبيل المثال بتتبع موقعك أو الاستماع إلى محادثاتك، وهذا سيتطلب أن تمنحه الإذن للقيام بذلك.

وبالتالي تكمن أفضل طريقة للبحث عن التطبيقات الضارة على هاتف آندرويد في معاينة جميع التطبيقات المثبتة، وذلك من خلال الإعدادات على الهاتف، لتعرف ما إذا كان أي منها يعمل بأذونات غير عادية، إلا أن هذه الطريقة لا تخلو من بعض السلبيات:

- يحتوي الهاتف بسهولة على أكثر من 100 تطبيق مثبت، وبذلك سيستغرق الأمر وقتًا طويلًا جدًا لمعاينة التطبيقات كلها.
- غالبًا ما تتنكر التطبيقات الضارة بصورة شيء بريء تمامًا (مثل تطبيق آلة حاسبة) وقد تفوتك أثناء التحقق من التطبيقات.
- يتوفر على هاتف أندرويد الكثير من التطبيقات المثبتة التي لم يسمع بها صاحب الهاتف من قبل وذلك لأنها عادةً ما تأتي مع نظام التشغيل، وبالتالي يشعر الناس أحيانًا بالتوتر عند رؤية هذه التطبيقات (« يحتوي هاتفي على تطبيق للسيارات، ولكنني لا أملك سيارة حتى! لا بد من أنه برنامج تجسس»).

[27] التحميل الجانبي هو فعل تثبيت التطبيقات من خارج متجر التطبيقات الرسمي، مثل غوغل بلاي (Google Play) في هذه الحالة، ويمكن حدوث ذلك على جهاز أندرويد ولكنه يتطلب من المستخدم النقر على بعض التحذيرات للوصول إليه. وبالتالي يتطلب الأمر شيئًا من الهندسة الاجتماعية أو أن يتمكن المتطفل من الوصول لبعض الوقت إلى الجهاز غير المقفل.

يمكن القيام بذلك بطريقة مختلفة جدًا وذلك من خلال توصيل الهاتف بجهاز كمبيوتر ومسح الهاتف باستخدام برمجية خاصة مصممة للكشف عن البرمجيات الضارة، وهذه طريقة مفيدة في بعض الحالات ولكن لها سلبياتها أيضًا:

- تتطلب من المحلل الوصول الفعلي إلى الهاتف في حين أن معظم الدعم يتم عن بُعد.
- ترفع سقف التحليل عاليًا إلى حدّ ما لناحية الأدوات والمعرفة والخبرة. ففي حين أنه يمكن حتى لمستخدم الهاتف الكشف عن معظم المشكلات إن تم إرشاده خلال العملية، يصعب على المستخدم العادي الوصول إلى هذه الأدوات المتقدمة.
- لن يثق الجميع ولا كل شخص معرض لمخاطر عالية بأن يقوم شخص آخر بوصل هاتفهم بجهاز كمبيوتر شخص آخر.

الطريقة الأفضل: الاطلاع على أذونات التطبيق

ولكن تتوفر طريقة أفضل تتمثل باستخدام مدير الأذونات في إعدادات هاتف أندرويد، إذ تعرض هذه الخاصية معظم[28] الأذونات التي يمكن للتطبيقات طلبها وكذلك، بموجب الإذن، التطبيقات التي تم منحها هذه الأذونات، كما تُظهر في بعض الحالات بضعة تفاصيل في ما يتعلق بالإذن.

على سبيل المثال، إذا كنت قلقًا بشأن احتمال وجود تطبيق ضار على الهاتف يتنصت على الميكروفون، فيمكنك معرفة التطبيقات التي تم منحها هذا الإذن والتحقق مما إذا كانت تطبيقات مشروعة، علمًا أن حتى بعض التطبيقات المشروعة تتطلب لسوء الحظ الكثير من الأذونات في بعض الأحيان. إن طلب تطبيق المصباح موقعك لا يعني ذلك حكمًا أنه برمجية ضارة، ولو أنك كنت لا ترغب ربما في حصوله على هذا الإذن.

ما يجب فعله في هذه الحالة هو البحث عن مدير الأذونات في الإعدادات ثم التحقق من الأذونات الفردية.

ولمعرفة ما إذا كان طلب التطبيق للحصول على إذن يشكل مصدر قلق، فكر في الطريقة التي تستخدم بها التطبيق عادةً، فإذا كنت تستخدم الموقع والميكروفون والرسائل النصية القصيرة وجهات الاتصال والملفات مع هذا التطبيق، فقد تكون الأذونات معقولة. ولكن عندما لا تستخدم هذه الأذونات مع أحد التطبيقات، فيمكن أن يشير استخدام تلك الأجزاء من جهازك إلى حدوث خطب ما، وبالتالي توقع طلبات أذونات غير متوقعة.

ليس الهدف هنا أن تفهم تمامًا ما تقوم به التطبيقات ولكن أن تحصر بحثك بعدد صغير (أحيانًا صفر**!**) من التطبيقات غير المعروفة التي قد ترغب في التحقيق فيها بشكل أعمق. وعلاوةً على ذلك، ستكتشف أيضًا التطبيقات المشروعة التي تتطلب أذونات تقلقك أنت أو الشخص الذي تحقق في هاتفه وقد تتمكن من إيقاف تشغيل هذه الأذونات.

من غير الممكن في بعض الأحيان تغيير أذونات تطبيق مثبت مسبقًا (يحتوي موقع أندرويد الرسمي على بعض المعلومات واي باك ماشين حول ذلك الأمر. ونظرًا لأن الكثير من الأشخاص غير ملمين بما يكفي بمثل هذه التطبيقات المثبتة مسبقًا فقد يظنون أن تطبيقًا كهذا يفعل شيئًا ضارًا. وفي حال كنت تستخدم هاتفًا لست معتادًا عليه، فقد يتعين عليك إجراء بعض الأبحاث في هذه التطبيقات لفهم ما تفعله وطمأنة المستخدم (وربما نفسك أيضًا).

الموقع

يمكن للتطبيقات التي تم منحها هذا الإذن الوصول إلى موقع نظام تحديد المواقع العالمي (GPS) للهاتف، ومن الأمثلة الواضحة على ذلك تطبيقات الخرائط وتطبيقات طلب سيارات الأجرة التي تحتاج إلى الموقع لتؤدي وظيفتها جيدًا.

---

[28] تتسم بعض الأذونات بغموض كبير وهي ليست ذات صلة تمامًا في هذا السياق وسيرد إذنان آخران لاحقًا في الفصل.

يمكن السماح لتطبيق بالوصول إلى الموقع طوال الوقت أو فقط عند استخدام التطبيق. وقد يتعين عليه أيضًا طلب الإذن في كل مرة يحتاج فيها إلى الموقع. وعلى الأرجح ستحتاج التطبيقات التي تفعل الأشياء خفيةً إلى إذن طوال الوقت، مثل برامج التجسس. ويجب الحذر تحديدًا من التطبيقات التي تم منحها هذه الأنواع من الأذونات!

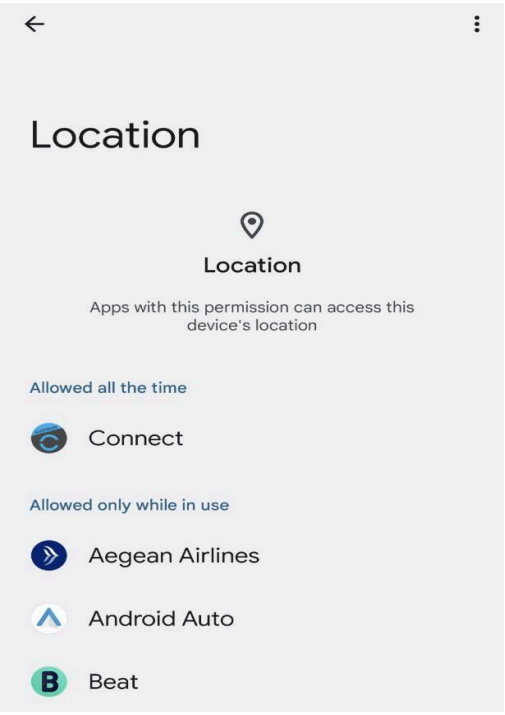
لا يتناول هذا الفصل مسألة ما إذا كان من الممكن الوثوق بهذه التطبيقات أو من الضروري ائتمانها على بياناتك. ولكن سواء كنت تثق بالشركات أم لا تثق بها، تتوفر طرق كثيرة يمكن للخصم من خلالها الوصول إلى بيانات الموقع التي حصلت عليها التطبيقات.

من أبرز هذه الطرق إمكانية الوصول إلى الهاتف وبالتالي التطبيق المستهدف أو إلى حساب مطابق عبر الإنترنت، والقدرة على عرض سجل المواقع، ومثال على ذلك غوغل التي توفر ذلك لخرائط غوغل (Google Maps). يمكن للخصم أيضًا تقديم طلبات قانونية للحصول على هذه البيانات من خلال أمر استدعاء.

وبالتالي إذا كنت ترغب في تقييم ما إذا كانت بيانات موقع شخص ما آمنة، فيجب عليك النظر في مدى سهولة وصوله (وبالتالي سهولة وصول أي شخص ينجح بانتحال شخصيته) إلى سجل المواقع وكيفية استجابة الشركة لطلبات البيانات، علمًا أن الكثير من الشركات الكبرى تنشر تقارير شفافية.

وبغض النظر عن ذلك، لا بأس في ما يتعلق بمعظم التطبيقات إن تم ضبط الإذن حتى لا يُستخدم إلا عندما يكون التطبيق قيد الاستخدام أو طلب الإذن في كل مرة، وهذا يعني أن التطبيق لا يمكنه الوصول إلى بيانات الموقع طوال الوقت.

وأخيرًا تجدر الإشارة إلى أن استخدام نظام تحديد المواقع العالمي يستهلك الكثير من البطارية، فالشخص الذي يتم تتبع موقعه طوال الوقت من خلال نظام تحديد المواقع العالمي سيلاحظ ذلك حتمًا لأن بطاريته تنفد بسرعة. ولكن يمكن أن تنفد البطارية بسرعة لأسباب عديدة ولذلك لا يشكل ذلك دليلًا قاطعًا على وجود برمجيات ضارة على الجهاز.



وأخيرًا، تجدر الملاحظة أن نظام تحديد المواقع العالمي دقيق جدًا ويمكن أن يُظهر الموقع بدقة ضمن مسافة 30 سم (حوالي 1 قدم). وفي بعض الحالات، يتخوف أحدهم من تسرب موقعه التقريبي مثل المدينة أو البلد الذي يتواجد فيه، مع العلم أن هذه المعلومات يمكن أن تتسرب بعدة طرق صريحة (على سبيل المثال، من خلال عنوان بروتوكول إنترنت) وأحيانًا أيضًا بطرق ضمنية (من خلال معلومات تتم مشاركتها علنًا). يقع خارج نطاق هذا الفصل كيفية الوقاية من ذلك، ولكنه أمر صعب جدًا!

الميكروفون

يمكن للتطبيقات التي تم منحها هذا الإذن الوصول إلى الميكروفون وبالتالي تسجيل أي شيء تقوله بالإضافة إلى الأصوات المحيطة.

يتوفر الكثير من الأسباب المشروعة التي تبرر استخدام التطبيقات لذلك، على سبيل المثال التطبيقات التي تسمح لك بإرسال رسائل صوتية أو التطبيقات التي تسجل مقاطع الفيديو أو تلك التي يمكن الوصول إليها من خلال الأوامر الصوتية.

تمامًا كما هو الحال مع إذن الوصول إلى الموقع، يمكن منح الوصول إلى الميكروفون طوال الوقت أو فقط عندما يكون التطبيق قيد الاستخدام، أو عن طريق جعل التطبيق يطلبه في كل مرة. لا تتوفر أسباب وجيهة كثيرة ليحظى تطبيق بهذا الإذن طوال الوقت، وبالتالي يعدّ التطبيق الذي تم منحه هذا الإذن باعث قلق كبيرًا.

الرسائل النصية القصيرة

بإمكان تطبيق حائز على الإذن لقراءة الرسائل النصية القصيرة أن يتجسس على تلك الرسائل، وقد يشكل ذلك مصدر قلق عندما يتعلق الأمر ببرامج التجسس إذا كان المستخدم يستخدم الرسائل النصية القصيرة بنشاط للتواصل.

ولكن تُستخدم الرسائل النصية القصيرة أيضًا للمصادقة متعددة العوامل وبذلك يستطيع تطبيق قادر على الوصول إلى الرسائل النصية القصيرة قراءة الرموز المرسلة بهذه الطريقة بهدوء[29]. وفي هذا الصدد تستخدم بعض التطبيقات الرسائل النصية القصيرة كطريقة لتأكيد رقم هاتف الجهاز وتطلب هذا الإذن لتجنب المستخدم من أن يضطر إلى إدخال رمز يدويًا، وبالتالي يمكن استخدام هذا الإذن بشكل ضار من قبل تطبيق يريد انتحال شخصية المستخدم.

يحظى تطبيق الرسائل النصية القصيرة التلقائي في الهاتف بهذا الإذن تلقائيًا وكذلك بعض التطبيقات الأخرى التي يمكن استخدامها للتعامل مع الرسائل النصية القصيرة مثل سيغنال.

ونظرًا لأن الرسائل النصية القصيرة تصل إلى الخلفية فستحتاج التطبيقات التي يمكنها الوصول إلى الرسائل النصية القصيرة إلى ذلك طوال الوقت، ولا يتوفر خيار لمنح هذا الإذن في وقت تشغيل التطبيق فحسب أو لطلب هذا الإذن في كل مرة.

جهات الاتصال

يمكن للتطبيقات التي تحظى بهذا الإذن الوصول إلى جهات الاتصال الموجودة على الهاتف إذ يستخدمه تطبيق الهاتف أيضًا، على سبيل المثال من خلال تطبيقات المراسلة مثل سيغنال وواتسآب التي تعرّف عن المستخدمين بناءً على أرقام هواتفهم. تتضمن جهات الاتصال عادةً أرقام الهواتف ولكن يمكن أن تتضمن أيضًا جهات اتصال البريد الإلكتروني، حسب كيفية استخدام الهاتف. وبالنسبة إلى الكثير من المستخدمين المعرضين لمخاطر عالية تعدّ قائمة جهات الاتصال لديهم معلومات حساسة جدًا.

وكما هو الحال مع الرسائل النصية القصيرة، إما يُسمح بهذا الإذن بشكل دائم أو يتم رفضه.

الملفات

يمنح هذا الإذن التطبيقات إمكانية الوصول إلى الملفات الموجودة على الجهاز، ومن الأمثلة على التطبيقات المشروعة التي تتطلب هذا الإذن مدير الملفات أو منتجات الأمان. لقد شهد إذن الملفات تغييرات كثيرة في إصدارات أندرويد الحديثة وأصبح أكثر دقة. وإذا كنت ترغب في البحث عن تطبيق ضار، أقلّه في البداية، من الأفضل افتراض أنه إذا كان التطبيق يحظى بالإذن للوصول إلى الملفات فهو قادر على الوصول إلى أي ملف مخزن هناك.

تجدر الملاحظة أن هذا الأمر لا يمنح التطبيقات إمكانية الوصول إلى الدردشات من سيغنال وواتسآب وما إلى

ذلك. كما أن هذا الإذن إما يُمنح بشكل دائم أو يُرفض.

التمرين 8.2 لكل من الأذونات الخمسة المدرجة، تحقق على هاتف أندرويد من التطبيقات التي تم منحها هذا الإذن.

التمرين 8.3 يسرد مدير الأذونات على أندرويد أكثر من هذه الأذونات الخمسة. راجع الأذونات الأخرى وفكر في ما إذا كانت البرمجيات الضارة تستطيع استخدامها.

[29] هذا أحد الأسباب العديدة التي تجعل استخدام الرسائل النصية القصيرة للمصادقة متعددة العوامل أقل أمانًا من الخيارات الأخرى مثل تطبيق المصادقة أو رمز الجهاز المميز

يتوفر نوعان خاصان من الأذونات تم إدراجهما في بندين مستقلين وذلك لأنهما ليسا واردين في مدير الأذونات، وهما تسهيلات الاستخدام والإشعارات، غير أنهما مهمان جدًا إذ غالبًا ما تستخدمهما التطبيقات الضارة. تختلف طريقة الوصول إلى هذه الإعدادات بين الهواتف: إن لم تتمكن من إيجادها بسهولة في قائمة الخصوصية في الإعدادات، استخدم وظيفة البحث في الإعدادات.

تسهيلات الاستخدام

تسمح تسهيلات الاستخدام بجعل استخدام التطبيقات على الهاتف أكثر سهولة للأشخاص الذين يعانون من إعاقات معينة، على سبيل المثال من خلال مساعدتهم على التفاعل مع برامج قراءة الشاشة. يمكن لتطبيق مسجل على أنه خدمة تسهيل استخدام التحكم بالهاتف إلى حد معين، فيمكنه النقر على الأزرار أو التسجيل عند نقر زرّ أو ملء النماذج النصية أو تسجيل ما تم تعبئته في النماذج.

لا يزال الكثير من التطبيقات المشروعة التي لا تقدم خدمات للأشخاص ذوي الإعاقة تسجل على أنها خدمة تسهيل استخدام، ومن الأمثلة على ذلك تطبيقات إدارة كلمات المرور التي تلزم هذه الخاصية بملء كلمات المرور المخزنة في التطبيقات.

يمكنك العثور على التطبيقات المسجلة كخدمة لتسهيل الاستخدام من خلال البحث عن «تسهيلات الاستخدام» في إعدادات الهاتف ثم البحث عن الخدمات المثبتة.

تجدر الملاحظة أنه منذ إصدار أندرويد 13 في أغسطس 2023 لم يعد يُسمح إلا للتطبيقات المثبتة من خلال غوغل بلاي (Google Play) بطلب أذونات تسهيل الاستخدام.

الإشعارات

الإشعارات هي النوافذ المنبثقة التي تتلقاها على الهاتف عندما تصلك رسالة جديدة أو في حال وصول تنبيه من نوع آخر. تعتمد الإشعارات التي تتلقاها على إعدادات التطبيق الفردي.

يمكن للتطبيقات طلب الوصول إلى الإشعارات، ما يعني أن بإمكانها رؤية جميع الإشعارات والتطبيق الذي أرسلها، ومن الأمثلة على التطبيقات المشروعة التي تتطلب الوصول إلى الإشعارات هي التطبيقات التي تقوم بمزامنة الهاتف مع ساعة ذكية تعرض الإشعارات.

يمكن لا وبل تستخدم البرامج الضارة ذلك أحيانًا للتجسس على أنشطة المستخدم، حتى وإن كانت الإشعارات لا تعرض سوى الرسائل الواردة دونًا عن الصادرة.

التمرين 8.4 كما سبق، تحقق من هاتف أندرويد لمعرفة التطبيقات التي تم منحها أذونات الإشعارات وتسهيلات الاستخدام.

تحليل البرمجيات الضارةعلى جهاز أندرويد والبرمجيات الضارة المتقدمة على جهاز أندرويد

تعلمت في الفصل السابق كيف يمكن لتطبيق فايروس توتال (VirusTotal) أن يخبرك الكثير عن البرمجيات الضارة من خلال تتبع المحور. وعلى سبيل المثال، قد ترى أن برمجية ضارة على جهاز أندرويد تتصل بنطاق معين، وتتصل بها برمجية ضارة أخرى، وقد تم تحليل تلك البرمجية الضارة. يُشير ذلك إلى أن الملف الذي تقوم بتحليله قد يكون إصدارًا مختلفًا من هذه البرمجية الضارة، علمًا أن هناك تحذيرات كثيرة كالعادة.

تتوفر أيضًا خدمة apklab التي تقدمها شركة أفاست (Avast) الأمنية وهي تشبه فايروس توتال (VirusTotal) ولكنها أكثر ملاءمة لنظام أندرويد ويمكن أن تساعد جدًا في تحليل البرمجيات الضارة لنظام أندرويد. يتطلب الموقع حسابًا مجانيًا ولكن يحتاج إلى موافقة المشرفين عليه، ونوصي بطلب حساب.

يمكنك أيضًا تشغيل الملف في بيئة اختبار معزولة (سنتحدث عنها بتفصيل أكبر في الفصل 10). غالبًا ما يكون هذا كافيًا لفهم ما يفعله ملف معين.

لإحاطة كاملة بتحليل البرمجيات الضارة التي تستهدف أجهزة أندرويد، تتوفر دورة رائعة تقدمها باحثة غوغل مادي ستون (Maddie Stone).

من المهم أيضًا ملاحظة أن ثمة برامج تجسس متقدمة متخفية عميقًا في الهواتف ولا تعمل بشكل تطبيق. ويُعدّ إجراء تحقيقات جنائية على الهواتف للبحث عن هذا النوع من برامج التجسس أمرًا معقدًا جدًا، لا سيما في ما يتعلق بهواتف أندرويد، وستحتاج على الأرجح إلى العمل مع خبراء مثل سيتزن لاب (Citizen Lab) أو آمنستي تك (Amnesty Tech) كي تتمكن من تحسين مهاراتك.

نأمل في التوسع أكثر في تحليل البرمجيات الضارة على أجهزة أندرويد في الصفحات التي سنضيفها مستقبلًا إلى هذا الدليل.