الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1213

(2017/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – الأمن السيبراني

متطلبات القدرات الأمنية لمكافحة البرمجيات الروبوتية القائمة على استعمال الهواتف الذكية

التوصية ITU-T X.1213

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المنزلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	**X.1229–X.1200**
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة	
الاتصالات في حالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1319–X.1310
أمن شبكة الكهرباء الذكية	X.1339–X.1330
البريد المعتمد	X.1349–X.1340
أمن إنترنت الأشياء (IoT)	X.1369–X.1360
أمن أنظمة النقل الذكية (ITS)	X.1389–X.1370
أمن تكنولوجيا سجل الحسابات الموزع	X.1429–X.1400
بروتوكولات الأمن	X.1459–X.1450
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أشكال أخرى لأمن الحوسبة السحابية	X.1699–X.1680

لمزيد من التفاصيل، يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1213

متطلبات القدرات الأمنية لمكافحة البرمجيات الروبوتية القائمة على استعمال الهواتف الذكية

ملخص

تحلل التوصية ITU-T X.1213 المعلومات الأساسية والتهديدات الأمنية المحتملة للبرمجيات الروبوتية القائمة على استعمال الهواتف الذكية وتقدم متطلبات القدرات الأمنية.

مع التطور السريع لأجهزة الإنترنت المتنقلة والاستعمال الواسع للهواتف الذكية، تبين الدراسات الاستقصائية التي أجرتها منظمات في جميع أنحاء العالم أن البرمجيات الروبوتية التي كانت تستهدف سابقاً الشبكات القائمة على الحواسيب الشخصية (PC) أساساً، يجري تكرارها الآن بشكل سريع على الهواتف الذكية. وفي الوقت الحالي، فإن البلدان والمناطق ذات الظروف والأنظمة الإيكولوجية المختلفة لديها مستويات متفاوتة من القيود المفروضة على انتشار البرمجيات الروبوتية القائمة على استعمال الهواتف الذكية. وتُظهر التقارير التحليلية التي أعدتها مختلف الشركات الأمنية والمنظمات الاستقصائية بيانات إحصائية مختلفة بصورة ملحوظة بشأن خطورة انتشار البرمجيات الروبوتية على الهواتف الذكية. ويزداد التهديد المحتمل للبرمجيات الروبوتية على الهواتف الذكية بسرعة كبيرة في بعض المناطق وربما ينتشر في جميع أنحاء العالم ويتحول من قضية إقليمية إلى قضية عالمية خطيرة.

للهواتف الذكية قدر أقل من حيث قدرة المعالجة ومساحة التخزين وعمر البطارية بالمقارنة مع الحواسيب الشخصية والمخدمات. ومع ذلك، يمكن للتأثير العدواني للبرمجيات الروبوتية القائمة على استعمال الهواتف الذكية أن يكون له انعكاسات أكبر على المستعملين للأسباب التالية: 1) غالباً ما تخزن الهواتف الذكية معلومات محددة لهوية الشخص (PII) بالغة الأهمية و2) في حال وقوع هجمات على الهواتف الذكية أو على البنية التحتية للمشغل، قد تتدهور تجربة المستعمل بدرجة كبيرة بسبب انتشار الهواتف الذكية واعتماد المستعمل عليها.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1213	2017-09-06	17	11.1002/1000/13261

مصطلحات أساسية

برمجيات روبوتية، تحكم ومراقبة (C&C)، برمجيات ضارة، معلومات محددة لهوية الشخص (PII)، هواتف ذكية.

* للنفاذ إلى توصية، يرجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

التوصية ITU-T X.1213

متطلبات القدرات الأمنية لمكافحة البرمجيات الروبوتية القائمة على استعمال الهواتف الذكية

1 مجال التطبيق

ترمي هذه التوصية إلى تقديم متطلبات القدرات الأمنية لمكافحة البرمجيات الروبوتية القائمة على استعمال الهواتف الذكية. والغرض من هذه التوصية دراسة التحديات التي تشكلها هذه الشبكات وما تطرحه من تهديدات محددة لشبكات المشغل والمتطلبات المتعلقة بهذه الشبكات والهواتف الذكية نفسها. وتركز هذه التوصية على تحليل التهديدات وتعداد المتطلبات. والهدف المنشود هو الحفاظ على البنية التحتية للمشغل والهواتف الذكية وضمان توفير خدمات المشغل وجودتها وتعزيز تجربة المستعمل. ويخرج عن نطاق هذه التوصية الحلول التقنية المفصلة والمطاريف الذكية الأخرى كالحواسيب اللوحية.

2 المراجع

لا توجد

3 التعاريف

1.3 مصطلحات معرَّفة في وثائق أخرى

تَستعمل هذه التوصية المصطلحات التالية المعرّفة في وثائق أخرى:

1.1.3 برمجية روبوتية (bot) [b-ITU-T X-Sup.8]: برنامج حاسوبي مؤتمت يُستخدم لتنفيذ مهام محددة مصممة لأغراض ضارة. وهذا المصطلح مرادف لمصطلح روبوت.

2.1.3 خبير برمجية روبوتية (botmaster) [b-ITU-T X-Sup.8]: شخص مسؤول عن مراقبة برمجية روبوتية وصيانتها.

3.1.3 شبكة برمجيات روبوتية (botnet) [b-ITU-T X-Sup.8]: روبوتات برمجية خبيثة (برمجيات روبوتية) يتم التحكم فيها عن بُعد وتشغيلها بشكل مستقل أو أوتوماتي على حواسيب ملوثة جنباً إلى جنب مع مخدم التحكم والمراقبة الذي يملكه خبير البرمجية الروبوتية.

4.1.3 المعلومات المحددة لهوية الشخص (PII) [b-ITU-T X.1252]: أيّ معلومات أ) تحدد أو يمكن استعمالها لتحديد هوية الشخص الذي تتعلق به هذه المعلومات أو للاتصال به أو لتحديد مكانه؛ ب) يمكن أن يُستمد منها تعرّف هوية الشخص أو معلومات الاتصال الخاصة به؛ أو ج) ترتبط أو يمكن أن ترتبط بشخص طبيعي بشكل مباشر أو غير مباشر.

2.3 مصطلحات معرّفة في هذه التوصية

لا توجد.

4 الاختصارات والأسماء المختصرة

تَستعمل هذه التوصية المختصرات التالية:

2G الاتصالات المتنقلة من الجيل الثاني *(Second Generation of mobile telecommunication)*

2FA استيقان بعاملين *(Two Factor Authentication)*

3G الاتصالات المتنقلة من الجيل الثالث *(Third Generation of mobile telecommunication)*

4G الاتصالات المتنقلة من الجيل الرابع *(Fourth Generation of mobile telecommunication)*

API السطح البيني لبرمجة التطبيقات *(Application Programming Interface)*

C&C التحكم والمراقبة *(Command and Control)*

CPU وحدة المعالجة المركزية *(Central Processing Unit)*

DDoS رفض الخدمة الموزع *(Distributed Denial of Service)*

DNS نظام أسماء الميادين *(Domain Name System)*

GPS النظام العالمي لتحديد المواقع *(Global Positioning System)*

HTTP بروتوكول نقل النصوص الإلكترونية *(Hyper Text Transfer Protocol)*

IDS نظام كشف الاقتحام *(Intrusion Detection System)*

IoT إنترنت الأشياء *(Internet of Things)*

IP بروتوكول الإنترنت *(Internet Protocol)*

IPS نظام منع الاقتحام *(Intrusion Prevention System)*

MITM اعتراض وسيط *(Man-in-the-Middle)*

MMS خدمة الرسائل متعددة الوسائط *(Multimedia Messaging Service)*

NFC اتصالات المجال القريب *(Near Field Communication)*

OTP شفرة مرور لمرة واحدة *(One-Time Passcode)*

P2P من الند إلى الند *(Peer-to-Peer)*

PC حاسوب شخصي *(Personal Computer)*

PII معلومات محددة لهوية الشخص *(Personally Identifiable Information)*

PNG الرسوم البيانية المحمولة للشبكة *(Portable Network Graphic)*

QoS جودة الخدمة *(Quality of Service)*

QRcode شفرة الاستجابة السريعة *(Quick Response code)*

SIM وحدة تعرّف هوية المشترك *(Subscriber Identity Module)*

SMS خدمة الرسائل القصيرة *(Short Message Service)*

USB الناقل التسلسلي العالمي *(Universal Serial Bus)*

WiFi شبكة لاسلكية عالية الدقة *(Wireless Fidelity)*

5 اصطلاحات

لا توجد.

6 معلومات أساسية

مع التطور السريع لأجهزة الإنترنت المتنقلة، أصبحت المطاريف المتنقلة أكثر ذكاءً مع قدرات أداء أعلى. وفي هذه التوصية، يشير مصطلح الهاتف الذكي إلى نوع الهاتف المحمول ذي الخصائص التالية:

– نظام تشغيل مستقل؛

- القدرة على توسيع وظائف وقدرات الهاتف بصورة مستمرة عن طريق تثبيت تطبيقات الطرف الثالث؛
- القدرة على النفاذ إلى الشبكة اللاسلكية بما في ذلك القدرة على النفاذ إلى شبكة الإنترنت المتنقلة من خلال شبكة الاتصالات لمشغل الخدمة المتنقلة.

في السنوات الأخيرة، استمر عدد السكان الذين يستخدمون الهواتف الذكية في النمو بسرعة. وعلى الرغم من أن الهواتف الذكية تسمح بتوفير الراحة للناس، تزداد أيضاً التهديدات الأمنية التي تتعرض لها.

1.6 نظرة عامة عن الاعتبارات الأمنية

نظراً إلى النمو السريع لعدد السكان الذين يستخدمون الهواتف الذكية، يجب منع البرمجيات الروبوتية القائمة على استعمال الهواتف الذكية والتحكم فيها بفعالية لمنعها من أن تصبح عاملاً هاماً يؤثر على الاستقرار الاجتماعي ويهدد الأمن العام.

بالنسبة إلى مشغلي الاتصالات المتنقلة، يمكن للبرمجيات الروبوتية واسعة النطاق أن تعيق بشدة الاستخدام الفعّال لشبكة المشغل وتؤدي إلى انخفاض جودة الخدمة (QoS) المقدمة إلى المستعملين، مما يؤدي إلى عدم رضا المستعمل وفقدان المشتركين. وبالنسبة إلى المستعملين الذين تعرضت هواتفهم الذكية إلى القرصنة والتحكم عبر برمجيات روبوتية، يمكن أن تكون الخسارة المحتمل تكبدها كبيرة، علماً أن معلوماتهم المحددة (PII) لهوية الشخص الأكثر أهمية، كقوائم جهات الاتصال ومعلومات الدفع الإلكتروني غالباً ما تكون مخزنة في هواتفهم المحمولة.

ولذلك، فإن العمل المتعلق بمكافحة البرمجيات الروبوتية القائمة على استعمال الهواتف الذكية تطلعي وعملي على السواء. وينبغي أن يعزز المشغلون وعيهم الأمني في هذا المجال من أجل منع النمو السريع للبرمجيات الروبوتية وتقليل الخسائر التي يتكبدها المشتركون والحد من شكاوى المستعملين وما إلى ذلك.

2.6 تطور التهديدات الروبوتية على الهواتف الذكية

يمكن أن يرجع ظهور فيروسات الهواتف الذكية إلى 2004 عند اكتشاف *Cabir*، أول دودة قائمة على الهاتف الذكي. وفي 2009، بدأت البرمجية الخبيثة *iKee.B* تكتسب خصائص البرمجيات الروبوتية وتمكنت من التحكم في هواتف الآيفون المصابة وإرسال المعلومات المحددة لهوية المستعمل إلى خبير البرمجية الروبوتية. وفي 2011، تم العثور على برمجية روبوتية متنقلة تمثيلية، *Android.Geinimi*. وتمكنت هذه البرمجية الروبوتية من إخفاء أساليب الاتصال وكان لديها وحدات هجوم وفيرة واعتُبرت ضارة للغاية.

واقترن الاستعمال واسع الانتشار للهواتف الذكية بنمو استثنائي في البرمجيات الضارة القائمة على الهواتف الذكية، التي تستخدم في الغالب وظائف معيّنة لهذه الهواتف كوسيلة للانتشار. وبعد تنزيل وتثبيت البرمجية الضارة في الهاتف الذكي تقوم، بشكل متكرر وسري، بعرض إعلانات وحفز حركة إضافية على الهاتف الذكي وخصم رسوم وغير ذلك؛ مما يتسبب في خسائر لمستعملي الهاتف الذكي. وعلاوةً على ذلك، قد يواجه مستعملو الهواتف الذكية أيضاً قضايا من قبيل: توجيههم إلى مواقع إلكترونية احتيالية، وإصابة هواتفهم الذكية بفيروسات أو بفيروسات متخفية (أحصنة طروادة) وكشف قوائم جهات الاتصال و/أو دفاتر العناوين لديهم أو سرقتها أو سرقة حساباتهم وكلمات السر الخاصة بهم. ويعتبر الكشف عن المعلومات الشخصية والحسابات الشخصية وكلمات السر من بين الجرائم التي تطرأ في معظم الأحيان.

وفي السنوات الأخيرة، ازدادت البرمجيات الضارة في الهواتف الذكية زيادة هائلة. والبرمجيات الضارة هي السبب الرئيسي في انتشار فيروس الشبكة الروبوتية نظراً إلى أن نسبة متزايدة من البرمجيات الضارة تستخدم أساليب أو وظائف التحكم المستتر عن بُعد وهي سمة مميزة للبرمجيات الروبوتية القائمة على استعمال الهواتف الذكية. ويتمثل الغرض الرئيسي لخبير البرمجية الروبوتية في جني أرباح من سرقة المعلومات المحددة لهوية الشخص (PII) وخصم الرسوم بطريقة خبيثة. وتشمل البرمجيات الضارة الأكثر شيوعاً في الوقت الحالي: سرقة المعلومات PII وخصم الرسوم بطريقة خبيثة والسلوك الاحتيالي وتدهور الأداء وانتشار البرمجيات الخبيثة.

3.6 حماية الهواتف الذكية

تمثل المكالمات المزعجة وخدمة الرسائل القصيرة (SMS) والبريد الاقتحامي وغيرها من الأحداث الأمنية الأخرى الناتجة عن تصفح الإنترنت وتنزيل الملفات والدفع بالوسائل المتنقلة وغيرها، القضايا الأمنية الرئيسية التي يواجهها مستعملو الهواتف الذكية. وتخفف برمجيات الأمن المثبتة في الهواتف الذكية من وطأة هذه التهديدات بشكل رئيسي.

والوظيفتان الرئيسيتان لبرمجيات أمن الهواتف الذكية هي إدارة الهاتف والحماية الأمنية. وتشمل وظيفة إدارة الهاتف ترتيب الذاكرة وتمديد الوقت الاحتياطي وإدارة برنامج التشغيل الأوتوماتي وإدارة خدمة الرسائل القصيرة وإدارة رقم الهاتف وما إلى ذلك. والغرض من وظيفة إدارة الهاتف جعل الهاتف الذكي يعمل بشكل سلس وتحسين كفاءة استخدام الجهاز. وتشمل وظيفة الحماية الأمنية أساساً مراقبة حركة البيانات ومنع المكالمات المزعجة والمسح المنتظم وإزالة الفيروسات بانتظام، وغير ذلك. والغرض من وظيفة الحماية الأمنية حماية الهواتف الذكية من التهديدات الأمنية.

ويمكن أن يساعد تثبيت برمجية الأمن في حماية الهواتف الذكية من بعض البرمجيات الروبوتية والضارة على مستوى المحطة الطرفية للمستعمل، ولكن نظراً إلى تحسن مهارات مهاجمي الهواتف الذكية وتنوع نُهج الهجوم التي يتبعونها، ستستمر الهواتف الذكية في مواجهة التهديدات الأمنية المتزايدة. وإلى جانب تعزيز الحماية الأمنية على مستوى المحطة الطرفية، يتعين على المشغلين أيضاً توفير مزيد من الحماية الأمنية في جانب الشبكة. وسيعزز التنسيق والتعاون بين كلا الطرفين إلى حد كبير قدرة الهواتف الذكية على الصمود في وجه الهجمات التي تشنها البرمجيات الروبوتية.

7 خصائص البرمجيات الروبوتية القائمة على استعمال الهواتف الذكية

تستغل البرمجيات الروبوتية القائمة على استعمال الهواتف الذكية خصائص الهواتف الذكية والشبكات المتنقلة وتستخدم الإنترنت لنشر البرمجيات الضارة على نطاق واسع. ومن خلال تحليل خصائص الهواتف الذكية والشبكات المتنقلة وغرض الهجوم الذي يشنه خبير البرمجية الروبوتية، يمكن تلخيص خصائص البرمجيات الروبوتية القائمة على استعمال الهواتف الذكية ويمكن إدراك التهديدات الأمنية المحتملة.

1.7 المعلومات المحددة لهوية الأشخاص على البرمجيات الروبوتية

تتكون البرمجيات الروبوتية القائمة على استعمال الهواتف الذكية من عدد كبير من البرمجيات الروبوتية القائمة على الهواتف الذكية. وعلى عكس الحواسيب الشخصية (PC) التقليدية، تُخزّن كثير من المعلومات PII والمعلومات الشخصية مركزياً في الهواتف الذكية مما يجعل البرمجيات الروبوتية القائمة على استعمال الهواتف الذكية تشكل تهديداً أكبر بالنسبة إلى مستعملي الهواتف الذكية الذين يمكن أن يعانون من خسارة قدر كبير من البيانات.

وتشمل الوظائف المدمجة في الهواتف الذكية ما يلي: إدارة المعلومات الشخصية والجدول الزمني وجدول الأعمال واليوميات وترتيبات المهام وتطبيقات الوسائط المتعددة وتصفح صفحات الويب وغيرها. ووفرة المعلومات الشخصية المخزنة في تطبيقات الهاتف الذكي تجعل الهواتف الذكية أحد الأهداف الرئيسية للمهاجمين. وعلاوةً على ذلك، يمكّن النظام العالمي لتحديد المواقع (GPS) الخاص بالهاتف الذكي من الحصول على معلومات عن موقع المستعمل وهو نوع آخر من المعلومات المحددة لهوية الأشخاص (PII). وعندما يحصل المهاجمون على هذه المعلومات، من الممكن الكشف عن المعلومات PII الخاصة بالمستعمل.

2.7 وسائل الانتشار المختلفة

أولاً، يمكن للبرمجيات الروبوتية القائمة على استعمال الهواتف الذكية أن تنتشر بشكل خبيث من خلال تطبيقات ضارة يجدها وينزلها المستعمل عادة من مستودعات التطبيقات أو منتديات الهاتف المحمول التي لا تتطلب أي استيقان آمن.

وثانياً، يمكن للبرمجيات الروبوتية القائمة على استعمال الهواتف الذكية أن تنتشر من خلال البلوتوث والواي فاي (WiFi) والناقل التسلسلي العالمي (USB) والسطوح البينية الطرفية الأخرى للهواتف الذكية.

وثالثاً، يمكن للبرمجيات الروبوتية القائمة على استعمال الهواتف الذكية أن تنتشر من خلال بروتوكول نقل النصوص الفائقة (HTTP) وخدمة الرسائل القصيرة (SMS)، وخدمة الرسائل متعددة الوسائط (MMS) وشفرة الاستجابة السريعة (QRcode) وما إلى ذلك.

تجعل وسائط الانتشار المختلفة البرمجيات الروبوتية القائمة على استعمال الهواتف الذكية سهلة الانتشار نسبياً مما يفرض متطلبات أعلى على الحماية الأمنية تبعاً لذلك.

3.7 الانفتاح

تزود أنظمة التشغيل المتنقلة الهواتف الذكية بعدد كبير من الخيارات المتعلقة ببرامج التطبيق، ولكن في الوقت نفسه، تعرّض هذه البرامج الهواتف الذكية لزيادة احتمال التهديدات والقراصنة. ويسمح الانفتاح للقراصنة بتضمين الفيروسات أو الفيروسات المتخفية (أحصنة طروادة) في تطبيقات موسعة مما يسهّل انتشار البرمجيات الروبوتية القائمة على استعمال الهواتف الذكية.

للهواتف الذكية أنواع متعددة من السطوح البينية الطرفية منها: البلوتوث واتصالات المجال القريب (NFC) والناقل العالمي التسلسلي (USB). ويمكن للمهاجمين استعمال أي توصيل من توصيلات السطوح البينية الطرفية هذه. وعلاوةً على ذلك، تدعم الهواتف الذكية عموماً النفاذ إلى الشبكات المتنقلة من الجيل الثاني والثالث والرابع (2G أو 3G أو 4G) فضلاً عن النفاذ بتقنية واي فاي التي يمكن للمستعملين النفاذ إلى الإنترنت من خلالها. وتتمتع هذه الوظائف بقيمة تطبيقية وتجارية فريدة ولكنها تزود المهاجمين بعدة قنوات هجومية أيضاً.

4.7 إصابة مستهدفة

تستهدف البرمجيات الروبوتية القائمة على استعمال الهواتف الذكية عادة أنواعاً معيّنة من الأهداف من خلال إصابتها عن طريق النسخ المباشر أو خداع المستعمل بحمله على تنزيل برمجيات ضارة أو برمجيات متخفية (أحصنة طروادة). ويمكن أن يستهدف المهاجمون أيضاً الهواتف الذكية التي تشغل نفس نظام التشغيل من أجل إصابته. وهذا الأسلوب يزيد إلى حد كبير من كفاءة الهجوم ويخفض تكلفته في الوقت نفسه.

5.7 التستر

أصبحت البرمجيات الروبوتية القائمة على استعمال الهواتف الذكية أكثر تعقيداً. وبعض هذه البرمجيات قادرة على إخفاء سلوكياتها الهجومية بإزالة جميع آثار التثبيت بعد إلحاق الضرر بنجاح بهاتف ذكي. ويمكن لبعض البرمجيات الروبوتية القائمة على استعمال الهواتف الذكية أن تمسح توصيل الشبكة وآثار صندوق البريد لديها بعد أن ترسل المعلومات PII الخاصة بالمستعمل عن طريق النفاذ إلى الإنترنت. ويمكن لبرمجيات روبوتية أخرى أن تطلب خدمات مصممة حسب الطلب من جهة معينة من جهات تقديم الخدمات وأن تعترض أوتوماتياً رسائل التحقق الموجهة من مشغلي الخدمة المتنقلة.

وبعض الفيروسات المتخفية (أحصنة طروادة) والبرمجيات الضارة التي تسرق المعلومات PII أو تتسبب في خصم رسوم بطريقة خبيثة لا تشن هجماتها بعد تثبيتها بنجاح مباشرة. وبدلاً من ذلك تقوم بإطلاق هجماتها وفقاً لفترات زمنية تحددها البرمجية الضارة أو بالاستفادة من وقت توقف تشغيل الهواتف الذكية المصابة.

واليوم، تتمتع نسبة كبيرة من البرمجيات الضارة بأبواب خلفية ذات تحكم عن بُعد باعتبارها وظيفة أساسية وتشكل واحدة من السمات المميزة للبرمجيات الروبوتية على الهواتف الذكية.

وتنتشر العديد من البرمجيات الروبوتية من خلال برامج خبيثة مدمجة في تطبيقات متنقلة شائعة. وعند قيام المستعمل بتنزيل وتثبيت تطبيقات من مستودعات التطبيقات أو منتديات الهاتف المحمول بدون آليات استيقان آمنة، تُشغل البرامج الضارة المخبأة في التطبيقات.

6.7 المصالح التجارية

وعلى عكس البرامج الضارة الأكثر تقليدية التي تهدف إلى التخريب، فإن غرض البرمجيات الروبوتية القائمة على الهواتف الذكية غالباً ما يحركه الربح. فعلى سبيل المثال، تستفيد البرمجيات الروبوتية القائمة على الهواتف الذكية من سرقة المعلومات PII الخاصة

بالمستعمل أو من بدء خصم الرسوم بطريقة خبيثة مشكّلةً بذلك صناعة غامضة قائمة على الاحتيال عبر الإنترنت. وتحفز الأرباح التجارية المهاجمين على استثمار مزيد من الموارد في تطوير البرمجيات الروبوتية القائمة على الهواتف الذكية وتعزيز تنمية صناعة الاحتيال عبر الإنترنت. وهذا يعني أن هذه البرمجيات ستؤدي إلى زيادة التهديدات الأمنية التي يتعرض لها المستعملون وسيكون من الصعب على نحو متزايد تأمين الحماية ضد هذه التهديدات.

7.7 توصيلات الشبكة المتغيرة باستمرار

تؤدي خصائص التنقلية العالية للهواتف الذكية إلى توصيلات الشبكة المتغيرة التي ينتج عنها زيادة تنوع البرمجيات الروبوتية القائمة على الهواتف الذكية. وتستطيع الهواتف الذكية التجوال ليس فقط بين الشبكات التي تستعمل تكنولوجيات التوصيل الشبكي ذاتها، وإنما أيضاً بين الشبكات التي تستعمل مختلف تكنولوجيات التوصيل الشبكي، مثلاً من شبكة 3G إلى نقطة ساخنة WiFi. وبالتالي، ربما تحتاج البرمجيات الروبوتية في الهواتف الذكية الملوثة لأن تغير قنوات الاتصال الخاصة بها ومخدم القيادة والتحكم (C&C) بشكل أكثر تواتراً بالمقارنة مع البرمجيات الروبوتية القائمة على الحواسيب. وهذا يؤدي إلى تعقيد إضافي في كشف البرمجيات الروبوتية القائمة على الهواتف الذكية من خلال تحديد قنوات الاتصال الخاصة بها.

8 التهديدات الأمنية

1.8 الإفصاح عن المعلومات المحددة لهوية الشخص

- بطاقة وحدة تعرّف هوية المشترك (SIM):

حالما يتعرض هاتف ذكي للإصابة ببرمجية روبوتية، يمكن لخبير البرمجيات الروبوتية أن يقوم بسرقة معلومات البطاقة الهاتفية للمستعمل بما في ذلك معلومات تسجيل الهاتف ومعلمات تشكيل الجهاز وغيرها. ويستطيع خبراء البرمجية الروبوتية توليد مكاسب مالية كبيرة من بيع المعلومات PII أو الإفصاح عنها. ومما يثير المزيد من القلق هو إمكانية شن خبراء البرمجيات الروبوتية لهجمات أكثر خطورة على الهواتف الذكية ذات التشكيلات نفسها من خلال تحليل مواطن الضعف في هذه الهواتف.

- تخزين الهاتف:

بإمكان خبراء البرمجيات الروبوتية للبرمجيات الروبوتية القائمة على الهواتف المحمولة استعمال الحوسبة السحابية لتنفيذ التحكم عن بُعد فيما يتعلق بجميع البرمجيات الروبوتية. وبهذه الطريقة، يمكن لهؤلاء الخبراء أن يسرقوا من البرمجية الروبوتية: المعلومات PII الخاصة بالمستعمل، بما في ذلك رقم هاتفه وقائمة جهات الاتصال ومدونات النداء ورسائل البريد الإلكتروني ومعلومات الموقع والصور والتسجيلات الفيديوية وغير ذلك. ويمكن أن يأمر هؤلاء الخبراء البرمجية الروبوتية بتحميل هذه المعلومات إلى مخدمات بعيدة.

- الحسابات المصرفية وكلمات السر:

عندما يقوم المستعمل بالدفع عبر هاتف ذكي، ربما يكون المهاجم قادراً على اكتساب التحكم الكامل في الهاتف الذكي للمستعمل من خلال الاستفادة من مواطن ضعفه، وعندئذ، يستطيع أن يسرق الحسابات المصرفية وكلمات السر الخاصة به. وعلاوةً على ذلك، يمكن للمهاجم اعتراض رمز التحقق لخدمة الرسائل القصيرة والشروع في تحويل المال بطريقة ماكرة، وإزالة أي أثر للهجوم في آن واحد. وبهذه الطريقة يستطيع المهاجم سرقة المال بسهولة وبدون إدراك مستعمل الهاتف الذكي.

- حسابات التطبيقات وكلمات السر:

وبنفس الطريقة، يستطيع المهاجمون سرقة حسابات المستعمل وكلمات السر الخاصة به اللازمة للتطبيقات. ويمكن أن يستفيدوا من هذه المعلومات لمواصلة الاحتيال وتوليد الأرباح وفقاً لذلك.

2.8 خصم الرسوم بطريقة خبيثة

- تحميل تلقائي أو حذف البرمجيات:

بمجرد أن تتحكم برمجية روبوتية في هاتف ذكي، يتلقى تعليمات صادرة من مخدم القيادة والتحكم ويكون بمقدور خبير البرمجية الروبوتية أن يأمر الهاتف بالقيام بأي شيء إلى حد ما. ووفقاً لتعليمات الخبير، يمكن للهاتف الذكي أن يقوم تلقائياً بتنزيل تطبيقات لا ضرورة لها أو أن يلغي تطبيقات محددة. وقد تؤدي هذه التصرفات إلى زيادة تكاليف استهلاك حركة البيانات والتسبب في خسارة مالية للمستعمل.

- الرسائل الاقتحامية في خدمة الرسائل القصيرة:

يمكن لبعض البرمجيات الروبوتية أن تأمر الهواتف الذكية بإرسال رسائل اقتحامية في خدمة الرسائل القصيرة باستعمال قائمة جهات الاتصال المتاحة في الهاتف الذكي. ويخدع المهاجم المستعمل أولاً بدفعه إلى تحميل برمجية ضارة وتثبيتها، وبمجرد إصابة الهاتف الذكي يقوم بالاتصال تلقائياً بمخدمات القيادة والتحكم للحصول على التعليمات. وبعد تلقي تعليمات الرسائل الاقتحامية في خدمة الرسائل القصيرة، يرسل الهاتف الذكي رسائل اقتحامية في خدمة الرسائل القصيرة وفقاً لقائمة جهات الاتصال المتاحة في الهاتف، مما يؤدي إلى تدهور الأداء وخصم رسوم بطريقة خبيثة مقابل النفاذ إلى الإنترنت وإرسال رسائل في خدمة الرسائل القصيرة. وقد تؤدي الرسائل الاقتحامية المتكررة في خدمة الرسائل القصيرة إلى تداخل القنوات المتنقلة مما يؤدي إلى تدهور الأداء وعدم تيسر الهاتف الذكي. وعلاوةً على ذلك، إذا كان الهاتف الذكي الملوث ينتمي إلى شركة معينة أو مؤسسة عامة، قد تقوض سمعة الشركة علماً أن قائمة جهات الاتصال المخزنة في الهاتف الذكي قد تحتوي على أرقام مهمة لشركاء من دوائر الأعمال أو دوائر حكومية. وعند استقبال رسائل اقتحامية متكررة في خدمة الرسائل القصيرة موجهة من هاتف ذكي مصاب، قد يُضاف رقم الهاتف الذكي إلى القوائم السوداء للمستقبلين مما يؤدي إلى خسارة مالية لا يمكن التنبؤ بها وعرقلة التعاون التجاري.

3.8 السلوك الاحتيالي

- هجمات رفض الخدمة الموزع (DDoS):

مع انتشار استخدام الهواتف الذكية والنمو السريع لتطبيقات الإنترنت المتنقلة، يمكن لخبراء البرمجيات الروبوتية أن يشنوا هجمات رفض الخدمة الموزع إذا كان عدد البرمجيات الروبوتية المتحكم فيها كبيراً للغاية. وقد يتحكم هؤلاء الخبراء في عدد كبير من الهواتف الذكية المصابة ويمكنهم شن هجمات متزامنة في موقع ويب محدد مما يؤدي إلى فشل مخدمات الويب. وعلى وجه التحديد، إذا كانت الهواتف الذكية الملوثة تنتمي إلى شركة معينة أو مؤسسة عامة، قد تقوض سمعة الشركة إلى حد كبير علماً أن قائمة جهات الاتصال المخزنة في الهاتف الذكي ربما تحتوي على أرقام مهمة لشركاء من دوائر الأعمال أو دوائر حكومية. وعند كشف هجوم DDoS، يستجيب المستهدف بمنع أرقام هاتف المهاجم مما قد يؤدي إلى خسارة مالية لا يمكن التنبؤ بها وعرقلة التعاون التجاري.

- خداع الدعاية الخبيثة:

يُمكن أن يُحوّل هاتف ذكي مصاب إلى مستقبِل إعلاني اقتحامي. وقد يتلقى المستعملون إعلانات مختلفة بحيث أن كل نقرة من شأنها أن تولد الدخل للبرمجية الروبوتية. وبهذه الطريقة، يجمّع خبراء البرمجيات الخبيثة أرباحاً ضخمة من رسوم الإعلانات الاحتيالية. ومع ذلك، لا يتم في الواقع النقر على الإعلان من جانب مستعمل الهاتف الذكي وإنما بواسطة البرمجية الروبوتية الخبيثة المثبتة في الهاتف الذكي.

- النفاذ غير المرخص به إلى شبكة المؤسسة:

يمكن للبرمجيات الروبوتية القائمة على الهواتف الذكية أن تسمح للمهاجمين بالنفاذ إلى شبكات المؤسسة الآمنة عبر أجهزة الشبكة المصابة. ويمكن لجهاز مصاب أن يقوم بتحليل ضعف الجهات المضيفة في شبكة المؤسسة وإبلاغ خبير البرمجية الروبوتية بها. وقد يواصل المهاجمون استغلال هذا الضعف لشن هجوم على الجهات المضيفة في شبكة المؤسسة وسرقة المعلومات السرية.

4.8 تدهور الأداء

يمكن أن يتسبب خبراء البرمجيات الروبوتية في تدهور أداء الهواتف الذكية عبر الطرق التالية:

- يمكن أن تتنكر مكونات الفيروسات في شكل رسوم بيانية للشبكات المحمولة (PNG)، في حين أنها في الواقع نصوص تلقائية. وبعد الإصابة، سيجري تحميل الفيروس تلقائياً عند بدء تشغيل الهاتف الذكي وسيستمر تشغيله في الشبكة الخلفية مما يؤدي إلى تدهور شديد في أداء نظام التشغيل؛
- التوصيل بشكل متكرر بمخدمات طروادة للحصول على تعليمات، من شأنه إلحاق ضرر متواصل بالهاتف الذكي؛
- تنزيل تطبيقات اقتحامية بشكل تلقائي في الشبكة الخلفية، من شأنه أن يؤدي إلى استهلاك البطارية وتدهور شديد في فترة زمنية قصيرة؛
- إرسال خبراء البرمجيات الخبيثة لرسائل اقتحامية مستمرة في خدمة الرسائل القصيرة إلى هواتف ذكية مصابة يتسبب في توقف تشغيل الهاتف الذكي ونضوب البطارية بشكل تام.

5.8 الإرسال الخبيث

يمكن لبعض البرمجيات الضارة أن تقوم بتنزيل تطبيقات إلى هاتف ذكي مصاب، في الشبكة الخلفية، بدون إذن من المستعمل ويمكنها أن تقوم فيما بعد بإرسال رسائل احتيالية فجائية وخداع المستعمل بحمله على لمس الشاشة وبالتالي التسبب في تثبيت البرمجية الضارة. وعند تثبيت التطبيق، تقوم بالنفاذ إلى موقع إلكتروني محدد في الشبكة الخلفية لرفع مرتبتها ضمن البرامج المنزّلة ومن ثم خداع المزيد من المستعملين لتنزيل التطبيقات الخبيثة. وبهذه الطريقة، يتم توسيع نطاق البرمجية الروبوتية ويحقق المهاجمون المزيد من الأرباح.

6.8 فقدان المصداقية

يمكن استعمال الهواتف الذكية المصابة القائمة على البرمجيات الروبوتية لإرسال رسائل اقتحامية بالبريد الإلكتروني أو المشاركة في هجمات رفض الخدمة الموزع؛ ولا تؤدي هذه السلوك إلى زيادة تكاليف الشبكة واستهلاك البطارية فحسب بل وتؤدي أيضاً إلى فقدان مصداقية المستعمل. فعلى سبيل المثال، عندما يقوم هاتف ذكي مصاب قائم على برمجية روبوتية بإرسال رسائل اقتحامية أو بريد إلكتروني اقتحامي بالجملة إلى جهات اتصال مخزنة في الهاتف الذكي، سيفقد المرسِل (صاحب الهاتف الذكي) المصداقية. وعلى وجه التحديد، إذا كان الهاتف الذكي الملوث ينتمي إلى شركة معينة أو مؤسسة عامة، قد تكون الخسارة أكبر بكثير علماً أن قائمة جهات الاتصال المخزنة في هذه الهواتف الذكية ربما تحتوي على أرقام مهمة لشركاء من دوائر الأعمال أو دوائر حكومية.

9 متطلبات القدرات الأمنية

1.9 متطلبات القدرات الأمنية للشبكة

1.1.9 مراقبة حركة الشبكة

ينبغي أن يوفر المشغلون القدرة على مراقبة حركة الإنترنت في الهاتف الذكي. وبإمكانهم وضع آلية لمراقبة الحركة أو جدول يحتوي على جميع المستعملين، وتحليل حركة الإنترنت في الهاتف الذكي بطريقة ذكية. وعند كشف حركة شاذة، يمكن للمشغلين أن يقوموا على الفور بتوجيه إنذار أو معلومات ذات صلة إلى المستعمل واعتراض الحركة المشبوهة عند اللزوم.

2.1.9 كشف الشفرة الخبيثة المتنقلة

ينبغي أن تقوم أجهزة الحماية الأمنية في شبكة المشغل بكشف الشفرة الخبيثة وتحليلها في تطبيقاتها. وإذا تم كشف شفرة خبيثة في تطبيق ما، ينبغي أن يوجه المشغل إنذاراً أو معلومات ذات صلة في الوقت المناسب إلى المستعملين الذين يقومون بتنزيل التطبيق أو استعماله.

3.1.9 إرسال مجفر للمعلومات الحساسة

ينبغي أن تدعم شبكة المشغل الإرسال المجفر للمعلومات المرسلة عن طريق الهواتف الذكية. وبعد تشغيل مستعمل الهاتف الذكي لهذه الوظيفة، ينبغي أن تضمن أجهزة شبكة المشغل سلامة المعلومات المرسلة وسريتها، بما في ذلك قوائم جهات الاتصال والمواقع والحسابات وكلمات السر وغيرها.

4.1.9 استعمال شبكة مزودة بمصيدة

ينبغي أن تنشئ شبكة المشغل نظام حاسوب مزوداً بمصيدة ليكون بمثابة شرك يغري البرمجيات الروبوتية والبرامج الخبيثة للنفاذ إلى الهاتف الذكي. وبعد كشف البرمجيات الروبوتية وجمع معلومات التحكم الخاصة بها، يمكن أن يطبق المشغلون المراقبة والتتبع لمعرفة كيفية توفير حماية أفضل للهواتف الذكية.

5.1.9 الحماية من هجوم رفض الخدمة الموزع

- ينبغي أن تكون أجهزة الحماية الأمنية ومخدمات نظام أسماء الميادين (DNS) في شبكة المشغل قادرة على توفير تشكيلة السياسة الأمنية التي تمنع الجهات المضيفة للبرمجيات الروبوتية من أن تُوصل بمراقبيها.
- ينبغي أن تكون جدران الحماية وأنظمة كشف التسلل (IDS) وأنظمة منع التسلل (IPS) وغيرها من أجهزة الحماية الأمنية في شبكة المشغل قادرة على توفير تشكيلات السياسة الأمنية التي تمنع الهجوم على الحركة.
- ينبغي أن تكون الشبكة وأجهزة الحماية الأمنية في شبكة المشغل قادرة على توفير تشكيلات سياسة منع حركة رفض الخدمة الموزع (DDoS) التي ينبغي أن تمنع الحركة DDoS للمخدم المستهدف في ميادين أخرى.

6.1.9 كشف البرمجيات الروبوتية

ينبغي أن تكون أجهزة الحماية الأمنية في شبكة المشغل قادرة على كشف تغيّر البرمجيات الروبوتية وجمع الائتمان الإجمالي لعناوين بروتوكول إنترنت (IP) وتقاسمه وهكذا يمكن إنشاء قاعدة بيانات ائتمان عناوين بروتوكول الإنترنت لمراقبي البرمجية الروبوتية والجهات المضيفة لتوفير ترشيح الحركة الخبيثة وتحليل أعمال البرمجية الروبوتية وآليات الائتمان لعناوين بروتوكول الإنترنت وغيرها من وسائل الحماية.

7.1.9 كشف الرسائل الاقتحامية في خدمة الرسائل القصيرة والتخلص منها

ينبغي أن تكون شبكة المشغل مجهزة بالآليات اللازمة لكشف الرسائل الاقتحامية في خدمة الرسائل القصيرة والتخلص منها. وعند ملاحظة أن مطرافاً متنقلاً يتلقى كمية كبيرة من الرسائل الاقتحامية، ينبغي منع هذه الرسائل في الوقت المناسب لتفادي وقوع انهيار ناجم عن استقبال رسائل اقتحامية جماعية. وينبغي أن يكون المشغل أثناء عملية الكشف قادراً على إبلاغ المستعملين بحيث يتسنى لهم تطبيق التدابير ذات الصلة للتعامل مع هذه الظروف.

8.1.9 آلية القائمة السوداء والقائمة البيضاء

ينبغي أن تكون أجهزة الحماية الأمنية في شبكة المشغل قادرة على أن تضيف إلى قوائمها السوداء البرمجيات الضارة والشفرات الخبيثة والمواقع الإلكترونية الخبيثة. وإذا طلب مراقبو البرمجية الروبوتية من الجهات المضيفة المتحكم فيها الخاصة بهم التوصيل بموقع إلكتروني خبيث أو تنزيل برمجية ضارة، تشكل جزءاً من قائمة سوداء، ينبغي أن تكون أجهزة الحماية الأمنية قادرة على منع هذه التوصيلات في الوقت المناسب.

وتبعاً لذلك، ينبغي أن تقدم أجهزة الحماية الأمنية في شبكة المشغل أيضاً آلية قائمة بيضاء. وفي بعض الظروف الخاصة، يُسمح للمستعملين بالتوصيل بمواقع إلكترونية موثوقة وتنزيل تطبيقات تشكل جزءاً من قائمة بيضاء.

9.1.9 القدرة على التعاون

بغية تحسين سلامة البرمجيات الأمنية ومصداقيتها، ينبغي أن تكون جهات التشغيل قادرة على التعاون مع مقدمي المنتجات الأمنية الخاصة بالهواتف الذكية. ومن خلال آلية التعاون هذه، يمكن تأمين الحماية الأمنية ضد البرمجيات الروبوتية على جانبي الشبكة والمطراف المتنقل.

وعلاوةً على ذلك، ينبغي أن تتعاون جهات التشغيل مع الإدارات الحكومية والإدارية. فإذا أصبح الهاتف الذكي برمجية روبوتية، ينبغي أن تبلّغ جهات التشغيل صاحب الهاتف الذكي بذلك من خلال الدوائر الإدارية. وعلاوةً على ذلك، بغية وقف البرمجيات الروبوتية القائمة على الهواتف الذكية وسلوكياتها الضارة، ينبغي أن تتعاون جهات التشغيل مع الإدارات الحكومية والإدارية لتحديد مسارات مناسبة للعمل والتشريع.

10.1.9 ضمان الهوية

في حال تَلوّثَ الهاتف الذكي للمستعمل (لا سيما مجموعة مستعملين) وبدأ بإرسال رسائل اقتحامية جماعية وغيرها، يمكن أن يتسبب ذلك في خسارة المستعمل لثقة مستقبلي الرسائل الاقتحامية. وإذا كانت الهواتف الذكية تنتمي إلى شركات معيّنة أو مؤسسات عمومية، يمكن أن تكون الخسارة أكبر بكثير علماً أن قوائم الاتصال الخاصة بها ربما تحتوي على جهات اتصال مهمة لشركاء من دوائر الأعمال ودوائر حكومية.

وبغية تجنب فقدان هذه الثقة، ينبغي أن تكون جهات التشغيل قادرة على ضمان هوية مستعمل الهاتف الذكي (خاصة بالنسبة إلى مجموعة مستعملين) عند الكشف عن عمليات تشغيل غير عادية، مثل مراسلة المجموعات. فعلى سبيل المثال، ينبغي أن يكون المشغل قادراً على أن يكشف عمليات مراسلة المجموعات للمستعمل، وأن يختار، استناداً إلى سياسات محددة مسبقاً، تبليغه عن طريق المراسلة، أو تعليق تشغيل مراسلة المجموعات مؤقتاً وأن يطلب تأكيد المستعمل قبل أن يواصل المستعمل التشغيل.

2.9 متطلبات القدرات الأمنية للهواتف الذكية

1.2.9 التخزين المجفر للمعلومات المحددة لهوية الشخص

ينبغي أن تدعم الهواتف الذكية التخزين المجفر لقوائم جهات الاتصال وخدمة الرسائل القصيرة والصور وسجلات النداء وغيرها من المعلومات المحددة لهوية الشخص. وينبغي تخزين المعلومات PII في الهواتف الذكية باستعمال أساليب التجفير.

2.2.9 النفاذ المجفر للمعلومات المحددة لهوية الشخص

ينبغي أن توفر الهواتف الذكية آلية النفاذ المجفر لقوائم جهات الاتصال وخدمة الرسائل القصيرة والصور وسجلات النداء وغيرها من المعلومات المحددة لهوية الشخص. وينبغي أن تكون الهواتف الذكية قادرة على إنشاء كلمات السر وبصمات الأصابع أو غيرها من النماذج للنفاذ إلى أنواع معينة من المعلومات الشخصية (كبعض الصور أو خدمة الرسال القصيرة المحددة).

3.2.9 استعمال برمجية الأمن

ينبغي لمستعملي الهواتف الذكية أن يبادروا إلى تثبيت برمجية الحماية الأمنية في هواتفهم الذكية. وهذا يمكن أن يساعد المستعملين على كشف التهديدات أو نقاط الضعف المحتملة والتخلص منها، وتوفير تدابير الحماية اللازمة في إطار الهجوم. وإذا لم يكن الهاتف الذكي مجهزاً ببرمجية حماية، ينبغي أن يكون قادراً على حث المستعمل على تثبيتها. وإذا تم تثبيت البرمجية، ينبغي أن يكون الهاتف الذكي قادراً على تذكير المستعمل بفحص النظام بصورة منتظمة وتحديث برمجية الأمن بأحدث إصدار.

4.2.9 تحذير ملزم للحسابات المصرفية

إذا اختار المستعمل حفظ أرقام الحسابات أو كلمات السر أثناء استخدام وظائف الدفع المتنقل، ينبغي أن يكون الهاتف الذكي قادراً على تحذير المستخدم بأنه لا يُنصح بحفظ كلمات السر أو أرقام الحساب في الهاتف الذكي.

5.2.9 مراقبة حركة الإنترنت على الهواتف الذكية

ينبغي أن تكون برمجية الحماية الأمنية على الهواتف الذكية قادرة على أن تحلل بذكاء استخدام المستعمل لحركة الإنترنت. وعندما تكشف هذه البرمجية حركة غير طبيعية خلال فترة قصيرة من الزمن، ينبغي أن يكون قادرة على عرقلة الحركة المشبوهة، بأسرع ما يمكن، وأن تطالب المستعمل بإيقاف تشغيل توصيلات الشبكة أو وقف تصفح أي مواقع إلكترونية مشبوهة.

6.2.9 التخلص من الشفرة الخبيثة المتنقلة

بعد كشف شفرة خبيثة في التطبيقات أو برمجية ضارة، ينبغي أن يكون الهاتف الذكي قادراً على إبلاغ المستعمل بذلك. وينبغي أن يقرر المستعمل ما إذا كانت هناك حاجة إلى حذف البرمجية والإبلاغ عن المعلومات إلى السلطات المختصة.

7.2.9 الاستعمال الآمن لتقنية واي فاي

بغية حماية المعلومات المحددة لهوية المستعمل كأرقام الحسابات وكلمات السر ومنع هجمات الاعتراض الوسيط (MITM) عند استخدام تقنية واي فاي، ينبغي أن توفر الهواتف الذكية التدابير اللازمة لضمان الاستخدام الآمن لتقنية واي فاي. فعلى سبيل المثال، عندما يقوم المستعمل بتشغيل التوصيل واي فاي، ينبغي أن يكون الهاتف الذكي قادراً على تشغيل وظيفة الإرسال المجفر تلقائياً ووقف تشغيله تلقائياً عند إيقاف تشغيل الواي فاي.

8.2.9 آليات التحقق من الطرف الثالث

عندما يقوم مستعمل الهاتف الذكي باستخدام الدفع المتنقل أو أي تطبيق آخر يتطلب تسجيل الدخول إلى الحساب، يجب أن يدعم الهاتف الذكي التحقق من الطرف الثالث لإجراء الدفع كالتعرف على الصوت أو استخدام شفرة التحقق من الصورة.

9.2.9 مراقبة الأداء واستهلاك الطاقة

ينبغي أن يكون الهاتف الذكي قادراً على مراقبة أداء وحدة المعالجة المركزية (CPU) واستهلاكها للطاقة. وعندما يكون أداء وحدة المعالجة المركزية أو استهلاك طاقة البطارية غير عادي، يجب أن يوجه الهاتف الذكي إخطاراً للمستعمل لتنبيهه.

التذييل I

توصيل البرمجية الضارة بالبرمجية الروبوتية

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

1.I تمهيد

يستند هذا التذييل إلى البحوث المكتبية التي تستخدم البحوث القائمة بدلاً من البحث الأساسي. وتم جمع البيانات والتقارير التحليلية من منظمات صينية ومنظمات تشاورية في العالم، فضلاً عن شركات برامج مكافحة الفيروسات. ويُعتقد أن استنتاجات هذه الشركات والمنظمات تستند إلى كمية هائلة من البيانات المجمعة وتحليل البيانات الضخمة.

تتسم البلدان بتنوع الثقافات والعادات الثقافية والقوانين والقواعد التنظيمية وقوانين إنفاذ القوانين التنظيمية، مما يفضي إلى نظم إيكولوجية وبيئات إيكولوجية مختلفة لنشر فيروسات الهاتف الذكي والبرمجيات الضارة. وقد تميل شركات برامج مكافحة الفيروسات، لأسباب خاصة بها، إلى المبالغة في تقدير عدد الهجمات التي تم الكشف عنها على أساس تعاريف فضفاضة ومنظورات تحليلية مؤاتية. ومن ثم، قد تبين التقارير الواردة من مختلف الشركات والمنظمات أرقاماً إحصائية مختلفة. ومع ذلك، تبقى الاستنتاجات والاتجاهات الأساسية هي نفسها بصورة عامة.

وبالإضافة إلى ذلك: 1) الكثير من البرمجيات الضارة التي تم الكشف عنها، إن لم نقل معظمها، تنطوي على ميزات وقدرات يمكن للبرمجيات الروبوتية أن تستخدمها بسهولة؛ و2) تشير الدراسات الاستقصائية المتعلقة باتجاهات البرمجيات الضارة والتجارب بشأن الهواتف الذكية إلى التهديد الذي تشكله البرمجيات الروبوتية القائمة على الهواتف الذكية في المستقبل القريب؛ و3) نظراً إلى العولمة اليوم، يمكن أن تنتقل بعض القضايا الإقليمية المتعلقة بالبرمجيات الضارة المتنقلة والبرمجيات الروبوتية إلى مناطق أخرى وتصبح قضايا أكبر في المستقبل ما يجعل من الضروري التأهب لها.

2.I معلومات أساسية

النمو السريع للهواتف الذكية، هو ربما، أحد أعظم النجاحات في عصرنا. ففي الصين، على سبيل المثال، بلغ العدد الإجمالي لمستخدمي الهواتف المتنقلة ما يزيد على 1,3 مليار، من بينهم أكثر من 0,68 مليار من مستخدمي الهواتف الذكية ومستخدمي الإنترنت.

وتُصمم الهواتف الذكية اليوم مع أقل قدر ممكن من العيوب مما يؤدي إلى إصابات أقل بالفيروسات. وفي الواقع، أفضى تصميم الهواتف الذكية إلى منتجات هاتفية ذكية لا تتأثر إلا في جزء صغير منها. ومع ذلك، على الرغم من ضآلة احتمال الإصابة، قد يتسبب هاتف مصاب في خسائر لا تطاق ولا رجعة فيها بالنسبة إلى المستعمل الذي ربما تكون أهم المعلومات PII الخاصة به، مثل أرقام الحسابات المصرفية، وكلمات السر، وعنوان المنزل والصور العائلية الحميمة، مخزنة في هاتفه الذكي.

وقد تسبب تزايد شعبية الهواتف الذكية في انتقال الفيروسات والبرمجيات الضارة المعدة بالتركيز على الحواسيب الشخصية إلى الهواتف الذكية – التي أصبحت الآن هدفاً رئيسياً للهجمات التي يشنها القراصنة. وبالإضافة إلى ذلك، فإن معظم الجرائم الإلكترونية التي تستهدف الهواتف الذكية ليست بدافع المصلحة الشخصية والفضول، وإنما بدافع تحقيق مكاسب مالية عن طريق الحصول على فدية والاحتيال المالي. ووراء أنشطة الجريمة السيبرانية، توجد صناعة غامضة قائمة على الاحتيال عبر الإنترنت مع احتمال ضئيل لكي تتغير في المستقبل القريب. وعلاوةً على ذلك، تتيح إنترنت الأشياء (IoT) توصيل المطاريف الصغيرة لأغراض كفاءة إرسال وتقاسم البيانات والمعلومات. وتتوقع بحوث غارتنر [b-Gartner] الأخيرة وجود أكثر من 4,9 مليار جهاز موصول بإنترنت الأشياء في بيئة المنازل الذكية للمستهلك في 2015 و25 مليار جهاز في 2020. ومع ذلك، سيشكل هذا الأمر تهديداً أكبر للمعلومات PII الخاصة بالمستعمل بوصفه عيباً أو ثغرة أو تسرباً في سلسلة تدفق البيانات وقد يؤدي تجزؤ جمع المعلومات من روابط إنترنت الأشياء إلى تسرب المعلومات PII الخاصة بالمستعمل وسيطرح تحديات جديدة لأمن الخدمات المتنقلة.

ومن ثم، يميل مستعملو الهواتف الذكية إلى إيلاء مزيد من الاهتمام إلى أمن الخدمات المتنقلة لا سيما عندما يتعلق الأمر بحماية المعلومات PII الخاصة بهم. وتفيد الشركة التحليلية العالمية *mSecurity* [b-mSecurity] إلى أن الاستثمارات في أمن الخدمات المتنقلة بلغت 11 مليار دولار أمريكي في 2014 وسوف تزيد بمعدل نمو مركب بنسبة 20% في السنوات الست المقبلة [b-GNSM].

3.I البيئة العيانية في الصين

هناك بيانات ملموسة تدعم الاتجاه المتزايد أسياً في البرمجيات الضارة المتنقلة.

في الصين، مثلاً، نمت شعبية الهواتف الذكية بسرعة في السنوات الأخيرة. واستناداً إلى الدراسات الاستقصائية التي أجرتها شركة *Qihoo 360*، واحدة من أكبر شركات برمجيات أمن الشبكات والمعلومات في الصين، فإن عدد مستخدمي الهواتف المحمولة ارتفع من مليار في 2012 إلى 1,3 مليار في 2015، وخلال نفس الفترة الزمنية زاد عدد مستخدمي الهواتف الذكية (مستعملو الإنترنت) من 270 مليون مستعمل في 2012 إلى 680 مليون في 2015.

ونشأت مشاكل أمنية عديدة خلال هذه الفترة من الزمن. وفي 2012، تم العثور على 000 175 عينة جديدة من عينات البرمجيات الضارة المتنقلة، وتعرضت الهواتف الذكية للإصابة 71 مليون مرة. وفي 2015، تم العثور على 18,7 مليون عينة جديدة من عينات البرمجيات الضارة المتنقلة، وتعرضت الهواتف الذكية للإصابة 370 مليون مرة. ومع تسرب المعلومات PII في إطار تقنية واي فاي المجانية وتوليد حركة زائدة بواسطة نصوص البرمجيات الضارة، اضطر المستعملون إلى اقتناء خدمة التأمين عن خسارة الدفع المتنقل غير المتوقعة، والمكالمات الهاتفية المزعجة، وتسرب المعلومات PII من الهواتف الذكية المستعملة وتسرب المعلومات PII بسبب برمجيات التواصل الاجتماعي وجميع أنواع الرسائل الاقتحامية. ولكي يعمل هاتف ذكي في بيئة سليمة وآمنة، من الضروري توفر الحماية من الفيروسات والبرمجيات الضارة، ومراقبة الحركة وحماية المعلومات PII ورصدها ورصد سرعة الشبكة وأمن الواي فاي. ويتمثل الاتجاه السائد في ضرورة التعاون الوثيق بين شركات البرمجيات الأمنية المتنقلة وجهات تصنيع الهواتف الذكية من أجل تحسين حماية الهواتف الذكية وأمنها.

4.I المشاكل المتصلة بهاتف آيفون

يحتفظ نظام "Apple iPhone" بمستوى أعلى من التحكم في البرمجيات التي يمكن للمستعملين تثبيتها بالمقارنة مع منصات أخرى مثل نظام Android. وتدّعي شركة أبل أنها توفر أمناً أفضل [b-AppleSecurity] إذ لديها ما يحفزها على ذلك وتتخذ الإجراءات اللازمة لتصميم مثل هذا النظام الإيكولوجي للبرمجيات. وانتقلت شركة أبل تدريجياً نحو نموذج تتكامل فيه المعدات وأنظمة التشغيل بشكل وثيق، ويحصل المستعملون على البرمجيات من مستودع التطبيقات الرسمي عموماً.

ومع ذلك، أفيد بأنه يجري تصميم عدد متزايد من البرمجيات الخبيثة لإصابة الأجهزة التي تستعمل النظام iOS [b-AppleThreat]. وتبين التحقيقات الجديدة أن التصور العام لأمن الآيفون يُقوض مع النمو السريع لمستعملي هواتف الآيفون وتطبيقاتها.

برمجية XcodeGhost (تم الكشف عنها عن طريق Symantec كبرمجية OSX.Codgost على حواسيب Mac OS X وكبرمجية IOS.Codgost على أجهزة iOS) هي نسخة معدلة من بيئة التطوير Xcode وتعتبر برمجية ضارة. وتقوم هذه البرمجية بتشكيل تطبيقات لجمع المعلومات المتعلقة بالأجهزة وتحميل المعلومات إلى مخدمات الاستيقان والقيادة. وبالإضافة إلى ذلك، تتمتع تطبيقات طروادة بالقدرة على تلقي الأوامر من مخدمات الاستيقان والقيادة لشن هجمات التصيد الاحتيالي. وقد تمكن عدد كبير من التطبيقات التي أُنشئت باستعمال برمجية XcodeGhost من تجاوز التدقيق الأمني لشركة أبل، وتم استضافتها في مستودع التطبيقات الرسمي، مما يدل على أن عملية الفحص لم تضمن خلو مستودع التطبيقات الرسمي من البرمجيات الضارة. وفي نوفمبر 2015، اكتُشف شكل جديد من برمجية XcodeGhost في نسخ غير رسمية للشفرة Xcode 7 مكّن مطوري البرامج من إنشاء تطبيقات للنظام iOS 9.

وتبين الدراسات الاستقصائية أن ما يقرب من نصف مستخدمي الآيفون لم يعودوا يعتقدون بأن هواتف الآيفون لديهم آمنة تماماً. وتبين التحقيقات أن حوالي 33% من الهواتف الذكية قد تم اختراقها، بينما تبلغ هذه النسبة 23,9% فيما يخص هواتف الآيفون.

وحالياً، تتمتع هواتف الآيفون على خلاف الهواتف العاملة بنظام أندرويد، بتحكم أفضل على تنفيذ التطبيقات/الشفرات من خلال آلية مفتاح الإذن الخاص بالمطور. وبمجرد العثور على هذه التطبيقات/الشفرات الخبيثة في أجهزة أبل، يمكن لشركة أبل أن تمنعها من العمل في جميع أجهزتها من خلال رفض مفتاح التوقيع الخاص بالمطور لا غير.

وعلى الرغم من أن النظام iOS منصة برمجية غير مفتوحة المصدر، لا يزال ينطوي على نقاط صعوبة خاصة به، لا سيما المكالمات المزعجة والتصيد الاحتيالي. ولهذا السبب، كشفت شركة أبل علناً عن السطح البيني لبرمجة التطبيقات "Ident-A-Call" في المؤتمر العالمي لمطوري البرامج الذي نظمته في سان فرانسيسكو في يونيو 2016. وهذا سيحرر إلى حد كبير مستعملي الآيفون من تلقي المكالمات المزعجة والتصيد الاحتيالي، كما أنه يوضح أن أمن الخدمات المتنقلة أصبح قضية خطيرة جداً ولم يعد مسألة تقنية محضة بل قضية اجتماعية.

5.I أمثلة واتجاهات جديدة للبرمجيات الضارة الجديدة

1.5.I المثال 1

أصبحت برمجية التواصل الاجتماعي وبرمجية الدفع المتنقل أهدافاً جديدة للفيروسات والبرمجيات الضارة؛ ويُعزى هذا أساساً إلى العلاقة الوثيقة بينهما وإلى تزايد أهمية هذه البرمجيات في حياة الناس.

وقد تنكرت برمجية "*a.privacy.BankSteal.a*" في شكل تطبيق برمجي معروف جيداً للتواصل الاجتماعي مع استعمال الشعار ذاته المعروف جيداً مما جعل من الصعب للمستعملين التمييز بين البرمجية الضارة والبرمجية الشرعية. وبعد اختراق الهاتف الذكي، تقوم البرمجية الضارة بخداع المستعمل بحمله على إدخال المعلومات PII كأرقام البطاقات المصرفية وكلمات السر وأسماء المستعمل وأرقام بطاقة الهوية وأرقام الهواتف، ثم تباشر التشغيل في الشبكة الخلفية؛ وتعترض الرسائل في خدمة الرسائل القصيرة للمستعمل. ثم ترسل البرمجية الضارة هذه المعلومات إلى القراصنة عن طريق البريد الإلكتروني. وتهدد هذه البرمجية الضارة إلى حد كبير المعلومات PII الخاصة بالمستعمل وسلامة ممتلكاته.

2.5.I المثال 2

لوحظت زيادة في استخدام الهواتف الذكية من أجل الخدمات المصرفية على الخط في جميع المناطق في 2015. وتقدم العديد من المؤسسات حالياً تطبيق أندرويد الذي يستخدم الاستيقان بعاملين (2FA). وهذا يزيد من التعجيل في اتجاه البرمجيات الضارة المتنقلة [b-FinancialThreat].

وأكثر أساليب الهجوم شيوعاً هو اعتراض الرسائل النصية التي تشكل جزءاً من عملية الاستيقان بعاملين (2FA) وتحويلها إلى مخدم القيادة والتحكم الخاص بالبرمجية الضارة لكي يستخدمها المهاجم. وكالمعتاد في البرمجية الضارة العاملة بنظام أندرويد، يطلب التطبيق الإذن لاستقبال الرسائل النصية وكتابتها وإرسالها فضلاً عن عدة أذونات أخرى أثناء مرحلة تثبيته.

وفي نظام 2FA نمطي، يُرسَل العامل الثاني، الذي يكون عادة في شكل شفرة مرور تُولد لمرة واحدة (OTP)، إلى رقم الهاتف المحمول المسجل لدى المستعمل من خلال خدمة الرسائل القصيرة. ولتحسين أمن تسليم شفرة المرور OTP، بدأت بعض المنظمات المالية بتسليم شفرات المرور OTP من خلال النداءات الصوتية بدلاً من خدمة الرسائل القصيرة. وفي الربع الأخير من 2015، تم العثور على شكل جديد للبرمجية الضارة *Android.Bankosy*. وهي عبار عن تهديد أندرويد لسرقة المعلومات قادر على خداع أنظمة الاستيقان بعاملين التي تستخدم النداءات الصوتية. ويمكن لمخدم القيادة والتحكم الخاص بالتهديد أن يأمر الهاتف الذكي المصاب بتحويل جميع النداءات باستخدام رمز خدمة خاصة.

وانتشرت فئة أخرى من الهجوم تتمثل في استخدام التطبيقات المصرفية المزيفة القائمة بذاتها. ويمكن أن تكون هذه التطبيقات مقنعة جداً بالنسبة إلى المستعملين عندما تتظاهر برمجية ضارة متنقلة مثلاً على أنها تطبيق تأشيرة مشروع قائم على استيقان بعاملين. وأخطر جانب لهذا النوع من التطبيقات الخبيثة هو أن هذه البرمجية الضارة تطلب من المستعمل اسم الحساب وكلمة السر لديه أثناء مرحلة التثبيت بحيث تحصل على جميع المعلومات اللازمة لنجاح عملية الاحتيال. ويمكن أن يؤدي ذلك إلى حسابات مصرفية احتيالية بدون استعمال حاسوب مكتبي مصاب. وفي حالات أخرى، يستعيض المهاجمون عن برمجية مصرفية متنقلة مشروعة مثبتة

بالفعل ببرمجية خبيثة خاصة بهم. ويستعمل تهديد أندرويد آخر يدعى *Android.Fakelogin*، تقنيات هندسية اجتماعية مرنة لسرقة إثباتات مصرفية من مجموعة واسعة من المستعملين. وبدلاً من التنكر في شكل تطبيق محدد، تحدد البرمجية الضارة *Android.Fakelogin* التطبيق المصرفي المشغل على جهاز المستعمل وتضع صفحة تسجيل مخصصة واحتيالية على السطح البيني للمستعمل. وتقوم بذلك من خلال النفاذ إلى نظام قائم على الحوسبة السحابية يستضيفه مخدم للقيادة والتحكم عن بُعد لتحديد صفحة التصيد الاحتيالي الواجب عرضها. وإذا حاول المستعمل تسجيل الدخول من خلال الصفحة التي تعرضت للاحتيال، تُرسل ثبوتياته لتسجيل الدخول إلى مخدم القيادة والتحكم الخاص بالمهاجم مباشرة. وعلى الرغم من أن البرمجية الضارة تستهدف تطبيقات مشروعة متاحة في "Google Play"، فإن التطبيقات التي تقوم بتحميل البرمجية *Fakelogin* لا تتاح في "Google Play".

3.5.I المثال 3

وأحد الاتجاهات الجديدة العديدة هو أن البرمجية الضارة الجديدة أصبحت احتيالية وجريئة على نحو متزايد في ابتزاز مستعملي الهواتف الذكية. فعلى سبيل المثال، منذ 2014 شرعت المزيد من البرمجيات الضارة في استهداف فرادى المستعملين عبر هجمات من ند إلى ند (P2P).

ترغم برمجية ضارة تدعى *"a.rogue.SimpleLocker.a"* الهاتف الذكي للمستعمل على تشغيل البرمجية الضارة كأولوية قصوى وتغلق شاشة الهاتف الذكي بصورة متكررة. ويُطلب من مستعمل الهاتف الذكي دفع رسم مقابل فتح الشاشة وإلا يتعذر عليه تشغيل أي تطبيقات أخرى على الهاتف الذكي. وفي الشبكة الخلفية، تُوصل البرمجية الضارة عبر شبكة الإنترنت ويكون بإمكانها فتح الشاشة بعد دفع الرسم. ولم تعد البرمجية الضارة تخفي نفسها، إذ تتحول إلى برمجية ضارة احتيالية وتقفز بجرأة إلى صدارة الأولويات لابتزاز المستعمل بهدف الحصول على فدية. وكلما كان عدد الهواتف الذكية الملوثة كبيراً، ازدادت الإيرادات التي يمكن أن يحققها القراصنة.

6.I خلاصة

مع التطور السريع للإنترنت المتنقلة، تزداد قدرات الهواتف الذكية من حيث الذكاء والأداء. وربما يكون النمو السريع في استعمال الهواتف الذكية أحد أعظم الإنجازات المحققة في عصرنا، وتبين الدراسات الاستقصائية أن البرمجيات الروبوتية القائمة على الحواسب الذكية يجري تكرارها على الهواتف الذكية بشكل سريع للغاية. وإن سرعة تكرار الفيروسات والبرمجيات الضارة مذهلة للغاية مثلما هو الحال بالنسبة إلى استخدام الهواتف الذكية. وبالتالي، تعد أعمال مكافحة البرمجيات الروبوتية القائمة على استعمال الهواتف الذكية عملية وتطلعية على السواء.

بيبليوغرافيا

[b-ITU-T X.1205] Recommendation ITU-T X.1205 (2008), *Overview of cybersecurity*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ITU-T X.1546] Recommendation ITU-T X.1546 (2014), *Malware attribute enumeration and characterization*.

[b-ITU-T X-Sup.8] ITU-T X-series Recommendations – Supplement 8 (2010), *ITU-T X.1205 – Supplement on best practices against botnet threats*.

[b-AppleSecurity] Webpage: Apple Claims Better Security with iOS 9, *Gets Hacked before Its Release*, September 13, 2015.
<https://lifars.com/2015/09/hacker-cracks-ios-9-with-a-jailbreak-before-its-public-release/>

[b-AppleThreat] O'Brien, Dick (2016), *The Apple threat landscape*, Symantec Security Response, Version 1.02, February 11, 2016.

[b-FinancialThreat] Candid, West (2015), *Financial* threats, Symantec Security Response Version 1.0, March 22, 2016.

[b-Gartner] Gartner Press Release, November 11.
<http://www.gartner.com/newsroom/id/2905717>

[b-GNSM] *Global Network Security Market 2015-019*.

[b-mSecurity] Mobile Security (mSecurity) Market Forecast 2014-2024.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2019