الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1126

(2017/03)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تطبيقات وخدمات آمنة – أمن الخدمات المتنقلة

مبادئ توجيهية للتخفيف من الآثار السلبية للمطاريف المتضررة في الشبكات المتنقلة

التوصية ITU-T X.1126

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 المحلية	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	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
التوصيات ذات الصلة بالبنية التحتية للمفاتيح العمومية	X.1340-X.1349
أمن إنترنت الأشياء	X.1369-X.1360
أمن أنظمة النقل الذكية	X.1379-X.1370
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
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680

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

التوصية ITU-T X.1126

مبادئ توجيهية للتخفيف من الآثار السلبية للمطاريف المتضررة في الشبكات المتنقلة

ملخص

توفر التوصية ITU-T X.1126 مبادئ توجيهية لمشغلي الاتصالات المتنقلة من أجل كبح المطاريف المتضررة باستخدام تكنولوجيات في شبكة الاتصالات المتنقلة لحماية المشتركين ومشغلي الاتصالات المتنقلة على حد سواء. وتصف هذه التوصية خصائص وآثار البرمجيات الضارة الناجمة عن الأنظمة الإيكولوجية غير الصحية في بيئة الاتصالات المتنقلة. واستناداً إلى تكنولوجيات الجانب الشبكي، فإن هذه التوصية تركز على التخفيف من الآثار المؤذية الناجمة عن المطاريف المتضررة. وتحدد التوصية وتنظم تدابير التخفيف والتكنولوجيات المناظرة.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1126	2017-03-30	17	11.1002/1000/13194

مصطلحات أساسية

تضرر، برمجية ضارة، شبكة اتصالات متنقلة، مطراف.

* للنفاذ إلى توصية، ترجى 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 مجال 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

1 مجال التطبيق 1
2 المراجع 1
3 التعاريف 1
1.3 المصطلحات المعرَّفة في وثائق أخرى 1
2.3 المصطلحات المعرّفة في هذه التوصية 1
4 المختصرات والأسماء المختصرة 2
5 الاصطلاحات 2
6 الإطار والعمليات 2
7 الاكتشاف 3
1.7 جمع التطبيقات وتقارير الهجمات 4
2.7 تحليل المطاريف المتضررة والبرمجيات الضارة المعروفة 4
3.7 تحليل البرمجيات الضارة الجديدة 4
8 التحكم 6
1.8 تدابير التحكم 7
2.8 الوقاية 7
3.8 التقييد 8
9 تبادل المعلومات 8
بيبليوغرافيا 9

مقدمة

أدى التوسع والتطور السريعان في أنظمة تشغيل الأجهزة المتنقلة إلى نشوء سوق واسعة ومفعمة بالحيوية لصناعة الاتصالات المتنقلة. وحول هذه السوق القيِّمة، نمت العديد من الأنظمة الإيكولوجية بغية الاستفادة من فوائدها. على أن القدرات القوية للهواتف المتنقلة الحالية يمكن أيضاً أن تستغل من جانب البرمجيات الضارة للسطو على نقاط ضعف المطاريف والشبكات والخدمات، مما يتسبب في ضرر بالغ.

ويشار إلى أنه ينبغي ترويج نظام إيكولوجي صحي في إطار "حديقة مغلقة" في الأنظمة المتنقلة التقليدية لضمان سوق الاتصالات المتنقلة وحماية الفوائد لكل الشركاء المعنيين. وقد حققت بعض الأنظمة الإيكولوجية الصحية النجاح في عدد من البلدان.

ويشار أيضاً إلى أن الأنظمة الإيكولوجية لسوق الاتصالات المتنقلة بالغة التنوع في بعض البلدان، وأن منها ما هو غير مسؤول، وغير صحي، بل وخطر. ويمكن للتأثيرات السلبية للأنظمة الإيكولوجية غير المسؤولة أن تسبب ضرراً كبيراً لمشتركي الاتصالات المتنقلة وشبكات هذه الاتصالات، إضافةً إلى البرمجيات الضارة. وفي بعض الأحيان فإن المطاريف المصابة قد تلحق الضرر حتى بمشتركي الاتصالات والشبكات المتنقلة في نظام إيكولوجي صحي، حيث إن معظم خدمات الإنترنت المتنقلة هي ذات طابع عالمي في الوقت الراهن.

وتتمثل المخاطر المحتملة للبرمجيات الضارة المنتشرة أساساً في الأنظمة الإيكولوجية غير المسؤولة بما يلي:

بالنسبة إلى المشتركين:

- سرقة الخصوصية، مثل التنصت، وتتبع الموقع؛
- فقدان الأصول، مثل تعطل الأنظمة، وتدمير البيانات؛
- التعامل والاستهلاك الضاران، مثل إرسال رسائل باهظة التكاليف، والاتصال بمراكز النداء الدولية؛
- انتشار البرمجيات الضارة لمهاجمة المطاريف الأخرى؛
- إرسال رسائل اقتحامية لإزعاج المشتركين الآخرين؛
- التدليس والابتزاز.

وبالنسبة إلى المشغلين فإن الهجمات على الكيانات الشبكية، والخدمات المتنقلة، والمطاريف الأخرى، تتضمن ما يلي:

- احتلال موارد ضخمة من الشبكات أو الخدمات المتنقلة، مما يؤدي إلى الإخلال بها وشكاوى المشتركين بشأن جودة الخدمة؛
- اختطاف مضيفي الخدمات بل وحتى الكيانات الشبكية.

وتُلحق البرمجيات الضارة آثاراً مؤذية أكثر بالإنترنت المتنقلة أكثر مما تلحقه بالإنترنت السلكية التقليدية وذلك للأسباب التالية:

- أن الإنترنت المتنقلة هي سوق ناشئة مصحوبة بتطوير بطيء نسبياً للآليات الأمنية المناظرة.
- غالباً ما تكون المطاريف المتنقلة حاملة للصفقات التجارية الخاصة والسرية، وهو ما يمثل أهدافاً جذابة جداً للقراصنة.
- للشبكات المتنقلة موارد أقل، كما أن الهجمات ذات الطابع الفيضي تستهلكها بصور أيسر وأشد.
- يقترن العديد من المطاريف المتنقلة بشدة بشبكاتها. ويمكن أن تؤدي الخدمة الضارة وسرقة الخصوصية إلى فقدان المشغل للإيرادات، وإلى شكاوى المشتركين ومسائل قانونية.
- وتوفر أنظمة التشغيل المتنقلة المفتوحة أو المتصدعة أرضاً خصبة للبرمجيات الضارة خارج سيطرة المشغل.
- أن للمطاريف المتنقلة في الغالب العديد من السطوح البينية لتبادل البيانات، مثل الناقل التسلسلي العام (USB)، وشق بطاقة الذاكرة الرقمية الآمنة، والبلوتوث، التي يعجز المشغل عن ضمان أمن العديد منها.

وبغية التخفيف من أضرار البرمجيات الضارة وتعقب مصادر التهديدات فإن من الحيوي إدارة المطاريف المتضررة من الجانب الشبكي، أي أنها مسؤولية والتزام على كاهل مشغلي الاتصالات المتنقلة.

مبادئ توجيهية للتخفيف من الآثار السلبية للمطاريف المتضررة في الشبكات المتنقلة

1 مجال التطبيق

توفر هذه التوصية مبادئ توجيهية للتخفيف من الآثار السلبية للمطاريف المتضررة على الجانب الشبكي في الشبكات المتنقلة. وتطرح هذه التوصية إطاراً ينظم المبادئ التوجيهية طبقاً للعمليات. وفضلاً عن ذلك، تناقش هذه التوصية المبادئ، والسياسات، والتكنولوجيات في تلك العمليات.

ولا يجوز اعتبار الامتثال لهذه التوصية دليلاً يتيح الادعاء بالامتثال لأي قانون، أو لائحة، أو سياسة على المستوى الوطني أو الإقليمي. ولا تكفل الوسائل التقنية، والتنظيمية، والإجرائية الموصوفة في هذه التوصية بأي حال من الأحوال تشكيل أي مستوى من الأمن الذي يمكن أن يُرسى على أساس التوافق مع أي قوانين، أو لوائح، أو سياسات وطنية أو إقليمية.

2 المراجع

لا يوجد.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 القائمة السوداء (blacklist) [b-ITU-T X.1245]: قائمة تحدد أشخاصاً أو مصادر تستعمل خدمات الاتصالات يُرفض نفاذ هؤلاء الأشخاص أو تلك المصادر إلى بعض موارد الاتصالات فيها.

2.1.3 البرمجيات الضارة (malware) [b-ITU-T X.1211]: برمجيات خبيثة مصممة خصيصاً لإلحاق الضرر بنظام أو تعطيله، مهاجمةً السرية و/أو السلامة و/أو التيسر.

ملاحظة – تشمل الأمثلة: الفيروسات، وبرمجيات طلب الفدية، والتجسس، والإعلان، والتفزيع.

3.1.3 شبكة متنقلة (mobile network) [b-ITU-T X.1121]: شبكة توفر نقاط نفاذ الشبكة اللاسلكية إلى المطاريف المتنقلة.

4.1.3 مطراف متنقل (mobile terminal) [b-ITU-T X.1121]: كيان يقوم بوظيفة النفاذ إلى شبكة لاسلكية ويوصل شبكة متنقلة لإرسال البيانات بمخدمات التطبيق أو مطاريف متنقلة أخرى.

5.1.3 الاقتحام (spamming) [b-ITU-T X1244]: سلسلةُ الأنشطة التي يقوم بها المقتحِمون من أجل إرسال رسائل اقتحامية، مثل تجميع قائمة المستهدفين، واستحداث الرسائل الاقتحامية وتسليمها، وما إلى ذلك.

2.3 المصطلحات المعرّفة في هذه التوصية

تعرّف هذه التوصية المصطلح التالي:

1.2.3 شبكة روبوتية (botnet): مجموعة من الأنظمة الحاسوبية المخترقة المتضررة من برمجية ضارة والموصولة في أسلوب منسق لأغراض مؤذية دون معرفة المالك، مثل بث البرمجيات الضارة أو الرسائل الاقتحامية، أو شن الهجمات.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

App تطبيق عامل في المطاريف المتنقلة *(Application running in mobile terminals)*

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

C&C القيادة والتحكم *(Command and Control)*

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

GGSN عقدة دعم بوابة الخدمة الراديوية الرزمية العامة *(Gateway General Packet Radio Service Support Node)*

IP بروتوكول الإنترنت *(Internet Protocol)*

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

MMSC مركز خدمة الرسائل متعددة الوسائط *(Multimedia Messaging Service Centre)*

SD بطاقة ذاكرة رقمية آمنة *(Secure Digital)*

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

SMS خدمة الرسائل القصيرة *(Short Message Service)*

SMSC مركز خدمة الرسائل القصيرة *(Short Message Service Centre)*

URL محدد الموارد الموحد *(Uniform Resource Locator)*

USB الناقل التسلسلي العام *(Universal Serial Bus)*

VAS خدمة القيمة المضافة *(Value-Added Service)*

WAP بروتوكول التطبيقات اللاسلكية *(Wireless Application Protocol)*

5 الاصطلاحات

لا توجد.

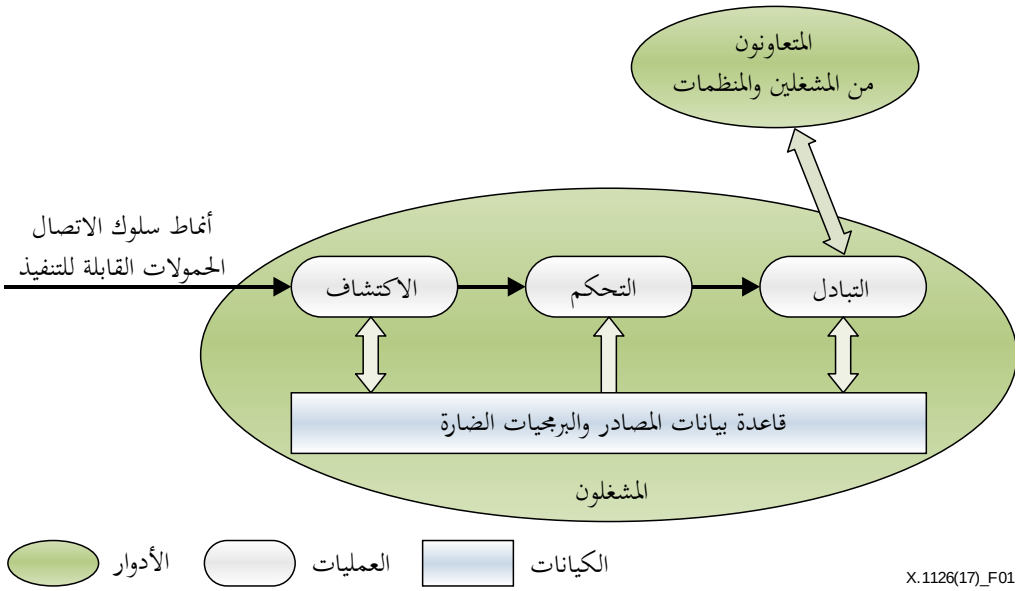
6 الإطار والعمليات

تظل معظم المطاريف بعد التضرر من برمجية ضارة قادرة في أغلب الحالات على النفاذ إلى الشبكة وعلى الاستخدام المعتاد لكل الخدمات والبدء بإطلاق آثار سلبية على الشبكات والخدمات، والتي قد لا يكون المشتركون على علم بها. ومن واجب مشغل الخدمات المتنقلة أن يكون على علم بالعدوى وأن يكبح المطراف المتضرر على النحو المناسب للحفاظ على شبكته وقدراته الخدمية في حالة مستقرة وصون مصداقيته عبر حماية فوائد المشتركين. ويعرض الشكل 1 إطاراً لتخفيف الآثار السلبية للمطاريف المتضررة يتضمن ثلاثة أنواع من الأدوار: للمشغلين، والمشتركين، والمنظمات الأخرى. ويضطلع المشغلون بالدور الأساسي في الإطار ويمكن تقسيم عملهم إلى ثلاث عمليات هي: الاكتشاف، والتحكم، وتبادل المعلومات. وبغية مساندة كل العمليات الثلاث فقد تم إدراج البرمجيات الضارة وبيانات المصادر ضمن الإطار. ويتولى المشغلون العمليات في هذا الإطار على أن تُراعى الالتزامات القانونية والتنظيمية الوطنية في الدول الأعضاء المنفردة التي يعملون فيها.

وثمة علاقات بين الأدوار الثلاثة: فالمشغلون يكتشفون ويتحكمون بالحالات الشاذة لمطاريف المشتركين من الجانب الشبكي، ثم يقومون بإعلام المشتركين بالتهديدات التي تطرحها هذه الحالات الشاذة. وفضلاً عن ذلك، فإن المشغلين قد يتبادلون المعلومات المتعلقة بالبرمجيات الضارة مع المتعاونين من المشغلين والمنظمات.

وفي عملية الاكتشاف قد يتم جمع عينات من التطبيقات العاملة في المطاريف المتنقلة ويمكن جمع تقارير الهجمات وتحليلها لاكتشاف الحالات الشاذة في الشبكة المتنقلة. ويتم الإبلاغ عن الحالات الشاذة والمطاريف المتضررة أثناء عملية التحكم. وخلال عملية التحكم يتم التحقق من الحالات الشاذة، واتخاذ تدابير معينة للتخفيف من الآثار السلبية على المشتركين والمشغلين. وبغية توفير المعلومات في الوقت المناسب لمجابهة أو مناولة البرمجيات المتنقلة الضارة فإنه ينبغي إرساء عملية تبادل المعلومات. وفي عملية تبادل المعلومات يتم تبادل المعلومات المتعلقة بالبرمجية الضارة مع المتعاونين من المشغلين والمنظمات، لتعزيز أمن الصناعة ككل.

قاعدة بيانات المصادر والبرمجيات الضارة: على امتداد هذه العمليات هناك قاعدة بيانات للمصادر والبرمجيات الضارة تعمل على تخزين وتوفير المعلومات عن هذه الشفرة بما في ذلك أنماط سلوكها ومصادرها. وتدعم هذه المعرفة تحديد الحالات الشاذة، والتحكم بالمطاريف المتضررة، ونشر معلومات البرمجيات الضارة في العمليات الثلاث. وفضلاً عن ذلك، فإن بالمستطاع تحميل المعارف الجديدة المتعلقة بالبرمجيات الضارة الواردة من عمليتي الاكتشاف وتبادل المعلومات في قاعدة البيانات لتوفير حماية "محدَّثة على الدوام".

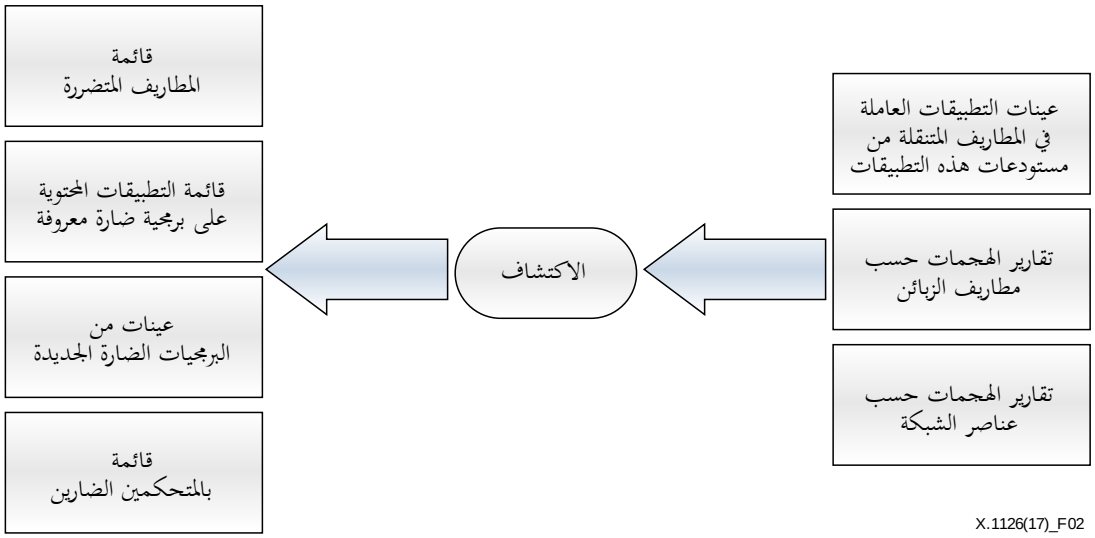


الشكل 1 – إطار التخفيف من الآثار السلبية للمطاريف المتضررة

7 الاكتشاف

يتم في عملية الاكتشاف جمع عينات من التطبيقات الموجودة في مستودعات التطبيقات وكذلك تقارير الهجمات من كل من المطاريف وعناصر الشبكات، على السواء، وذلك لتحليل الحالات الشاذة في الشبكة المتنقلة التي قد تشكل مؤشرات أو علامات على المطاريف المتضررة والمصادر الضارة. ويعرض الشكل 2 مسار العمل في عملية الاكتشاف.

ويمكن جمع كل البيانات المستخدمة في هذا البند والبيانات التالية من عينات التطبيقات الموجودة في مستودعات التطبيقات وتقارير الهجمات من مطاريف المشتركين أو عناصر الشبكة. وقد يتعلق أي استخدام للبيانات بخصوصية المشترك في عملية الاكتشاف وقد يحتاج إلى موافقة أو ترخيص من جانب المشترك وفقاً للتشريعات المحلية. وينبغي اقتصار استخدام البيانات حصراً على مسألة تحليل البرمجية الضارة وأنشطتها ذات الصلة ولا شيء غير ذلك.



الشكل 2 – العلاقات التفاعلية لعملية الاكتشاف

1.7 جمع التطبيقات وتقارير الهجمات

يمكن خلال عملية الاكتشاف جمع نوعين من البيانات لتحديد خصائص الحالات الشاذة الشبكية:

- تقارير الهجمات من مطاريف المشتركين وعناصر الشبكة؛
- عينات من التطبيقات من مستودعات/أسواق التطبيقات.

2.7 تحليل المطاريف المتضررة والبرمجيات الضارة المعروفة

قد يكون بالمستطاع تحديد بعض المطاريف المتضررة من تقارير الهجمات. ويمكن للتدابير الإضافية لمطابقة التوقيعات أن تساعد في العثور على بعض التطبيقات الجديدة المحتوية على برمجيات ضارة معروفة.

ويهدف تحليل المطاريف المتضررة والبرمجيات الضارة إلى تحديد مواقع المتحكمين الضارين المختبئين في الشبكة.

ويجب تحليل عناوين بروتوكول الإنترنت في رزم التحكم في المطاريف المتضررة لتحديد مصادر بروتوكول الإنترنت التي تتحكم بالمطاريف المتضررة أو لجمع المعلومات عن حالة المطاريف المتضررة.

وسيُعتمد التحليل الدينامي للبرمجيات الضارة المعروفة التي يتم العثور عليها في التطبيقات للتحقق عما إذا كان هناك أي تحديث للمتحكمين الضارين.

3.7 تحليل البرمجيات الضارة الجديدة

استناداً إلى التطبيقات المستخلصة من مستودعات التطبيقات فإنه يمكن اكتشاف برمجية ضارة جديدة من خلال تحليل السلوك، والتحليل السكوني، والتحليل الدينامي.

1.3.7 الشفرات الخبيثة وتحليل التطبيقات القابلة للتنفيذ

التحليل السكوني: يُستخدم هذا النهج لفهم البرمجية الضارة المشتبه بها عند المستوى السكوني. وعلى سبيل المثال، يمكن تفكيك تطبيق متنقل عبر تقنيات الهندسة العكسية لاستخلاص ملف بيان موجوداته (المحتوي على معلومات عن التصاريح التي ينفذ إليها التطبيق) وشفرات المصادر. وبفحص ملف بيان الموجودات ومسح السطح البيني لبرمجة التطبيقات لطلب إعمال الخصائص فإن بالمستطاع التعرف على عدد من المحاولات الضارة من زاوية بعض سياسات الكشف التقليدية:

- إذا ما كان هناك سماح بأي امتيازات نفاذ غير ضرورية وحساسة؛
- إذا ما تم طلب إعمال السطح البيني لبرمجة التطبيقات للنفاذ إلى مصادر الإنترنت الضارة؛

- إذا ما تم طلب إعمال السطح البيني لبرمجة التطبيقات الخاص بالعملية لإنهاء تطبيق ما؛
- إذا ما تم طلب إعمال السطح البيني لبرمجة التطبيقات الخاص بالعملية لتصدير معلومات الاتصال إلى موقع معين؛
- إذا ما كان سلوك بطاقة الذاكرة الرقمية الآمنة أو بطاقة وحدة تعرّف هوية المشترك غير طبيعي؛
- إذا ما كان هناك تبادل للمعطيات مع محدد موارد موحد ضار معروف؛
- إذا ما كان هناك اشتراك خدمة في خدمة الرسائل القصيرة دون طلب من المشترك؛
- إذا ما كانت هناك تعليمات للتحكم عن بُعد بالمطراف المتنقل.

التحليل الدينامي: يُطبق النهج ويرصد البرمجيات الضارة المتنقلة في بيئة محكومة (بل وحتى افتراضية) (مثل الصناديق الرملية). وفيما يلي بعض سياسات الكشف التقليدية:

أ) اتصالات الشبكة الروبوتية:

'1' الوصف: على الروبوت أن يقوم بإبلاغ مخدِّم للقيادة والتحكم عن وجوده كي ينضم للشبكة الروبوتية، ويتولى هذا المخدم إعطاء التعليمات للشبكة المذكورة لممارسة الأنشطة الضارة. ويمكن أن يكون المخدم مخدماً للويب أو مطرافاً في شبكة متنقلة، وبالمستطاع إصدار التعليمات عبر خدمات الإنترنت، والرسائل القصيرة، والرسائل متعددة الوسائط (MMS).

'2' سياسات الكشف:

1) عدد كبير من المطاريف يرتبط بمضيف ضار معروف.
2) مطراف يرتبط بمضيف ضار معروف بانتظام لفترة طويلة.
3) مطراف يُرسل رسائل قصيرة اثنينية إلى عدد كبير من المطاريف.

ب) الانتشار والاقتحام:

'1' الوصف: تنشر البرمجية الضارة نفسها أو ترسل رسالة اقتحامية إلى المشتركين الآخرين عبر مختلف الخدمات (الإنترنت، الرسائل متعددة الوسائط، الرسائل القصيرة، وما إلى ذلك) على أوسع نطاق ممكن.

'2' سياسات الكشف:

1) عدد كبير من المطاريف يُرسل رسائل متعددة الوسائط أو رسائل قصيرة (تُقارن الرسائل بفرم وحيد الاتجاه)، ويكون توزيعها الجغرافي عشوائياً.
2) ارتفاع حجم الخدمة بشكل دراماتيكي خلال زمن الراحة.
3) إجراء نداءات ثلاثية.
4) إرسال رسائل قصيرة.
5) إرسال رسائل متعددة الوسائط.
6) في حال قيام برمجية بطلب إعمال نداء منتَحل الهوية.
7) في حال قيام برمجية بتصدير معلومات بطاقة وحدة تعرّف هوية المشترك إلى مخدِّم.
8) في حال قيام برمجية بطلب إعمال نداء ضار بعد فترة قصيرة.
9) في حال استحثاث تحميل إضافي بصورة لا داعي لها.
10) النفاذ إلى متحكمين ضارين معروفين.

ج) الاشتراك والاستهلاك الضاران:

'1' الوصف: ستشترك المطاريف المتضررة بخدمات القيمة المضافة، وبخدمات النداءات الثلاثية، لإجراء مكالمات ذات تعريفات أولية أو مكالمات دولية، وإرسال أعداد كبيرة من الرسائل. ولن يكون المشترك على علم بهذه الرسوم.

'2' سياسات الكشف:

1) قيمة فاتورة المشترك ترتفع بشكل غير مبرر.

2) كثيراً ما يجري المطراف المتضرر مكالمات التعريفة الأولية أو المكالمات الدولية في فترات معينة.

3) قيام الكثير من المطاريف باستمرار بإرسال الرسالة ذاتها لمرات عديدة في فترات معينة.

4) يشترك المطراف بخدمات النداءات الثلاثية ويستخدمها بصورة متكررة بل وحتى طيلة الوقت.

د) هجوم رفض الخدمة الموزّع:

'1' الوصف: حشد من المطاريف يغرق الموارد الراديوية والموارد الأخرى في الشبكة المتنقلة للإخلال بجودة الخدمة.

'2' سياسات الكشف:

1) ارتفاع الحركة بصورة دراماتيكية في عقدة دعم بوابة الخدمة الراديوية الرزمية العامة أو الكيانات الشبكية الأخرى، ومعظم الحركة يتخذ الوجهة ذاتها.

والتحليل السكوني غير مناسب للبرمجيات الضارة المشتبه بها المخفية أو المموهة بينما يعجز التحليل الدينامي عن تغطية شفرة البرنامج الكاملة. ولذلك ينبغي إجراء التحليل السكوني والتحليل الدينامي على حد سواء لاستخلاص فهم كامل حول طريقة عمل برمجية ضارة معينة.

وتُعتبر المحاولات أو أنماط السلوك غير الطبيعية التي يكتشفها ويتعرف عليها التحليلان السكوني والدينامي مفيدة في تحديث السياسات عند تحليل السلوك فيما يتعلق بأحدث سيناريوهات الحالات الشاذة. وفضلاً عن ذلك فإن هذه الخصائص المكتشفة يمكن أن تساعد أيضاً المشغل على اكتشاف محددات الموارد الموحدة أو عناوين بروتوكول الإنترنت الضارة غير المعروفة.

2.3.7 النهج الموحد

لهذا فإن من المقترح عمل توليفة من النهجين التحليليين الاثنين لتحسين الأداء والحد من الإيجابيات الخاطئة في عملية الاكتشاف.

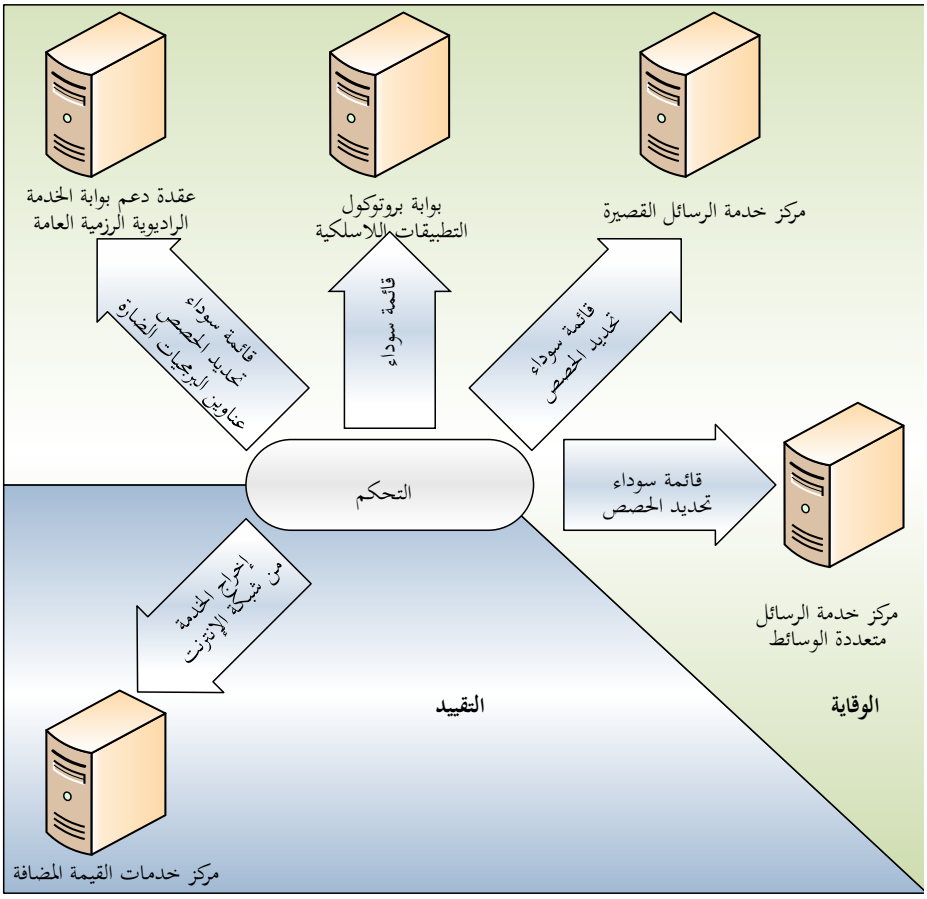
ويمكن توليد نواتج مختلفة في عملية الاكتشاف لمساندة عملية التحكم التالية. وينبغي أن تتضمن نواتج عملية الاكتشاف على سبيل المثال لا الحصر ما يلي:

- قائمة بالمطاريف المتضررة.
- عينات من التطبيقات المحتوية على برمجيات ضارة معروفة.
- عينات من البرمجيات الضارة الجديدة.
- قائمة بالمتحكمين الضارين.

وتعتبر المعلومات الواردة أعلاه حيوية للمشغلين لاتخاذ التدابير المناسبة في العمليات الموضحة في الفقرتين 8 و9.

8 التحكم

يتم في عملية التحكم تحليل نواتج عملية الاكتشاف والتحقق منها بصورة أوتوماتيكية أو شبه أوتوماتيكية. وتطبق تدابير التحكم بعد ذلك وفقاً لمدى شدة الحالات الشاذة. ويعرض الشكل 3 العلاقات التفاعلية بين عملية التحكم والكيانات الشبكية والخدمية الأخرى.



الشكل 3 – العلاقات التفاعلية لعملية التحكم

1.8 تدابير التحكم

هناك نوعان من التدابير المرتبطة بالشدة المختلفة للحالات الشاذة وهما: الوقاية والتقييد. ويستخدم كلاهما قدرات الكيانات الشبكية ومنصات دعم الخدمات فحسب.

- الوقاية: إذا ما كانت الحالة الشاذة معتدلة ويمكن التحكم بها دون قطع الخدمات المقدمة إلى المشتركين فإن بالمستطاع اعتماد طريقة الوقاية لمناولة المشكلة.
- التقييد: إذا ما فشل نهج الوقاية وعانى المشترك بالفعل من خسارة مالية كبيرة فإن التقييد يُستخدم لتعليق الخدمة المتضررة بطريقة انتقائية أو بشكل كامل.

2.8 الوقاية

1.2.8 القائمة السوداء

عند إطلاق الحالة الشاذة من جانب متحكم ضار فإنه يمكن إضافة هذا المتحكم إلى القائمة السوداء. ويتم بعد ذلك اعتراض أي طلبات لاحقة من هذا المتحكم وإليه. وهناك العديد من الكيانات الشبكية مثل عقدة دعم بوابة الخدمة الراديوية الرزمية العامة، وبوابة بروتوكول التطبيقات اللاسلكية، ومركز خدمة الرسائل متعددة الوسائط، التي تدعم وظيفة القوائم السوداء. وبالإمكان الاحتفاظ بقوائم سوداء متعددة لاعتراض مختلف أنواع المتحكمين الضارين مثل أسماء نطاقات المواقع الإلكترونية، وعناوين بروتوكول الإنترنت، ومخدمات القيادة والتحكم. وتجدر الإشارة إلى أن المصادر في القائمة السوداء سيتم تأكيدها وتحديثها بانتظام بغية تفادي اعتراض المصادر المشروعة.

ويمكن اعتراض أي عناوين مرتبطة بتحميل أي تطبيق يحتوي على برمجية ضارة باستخدام عقدة دعم بوابة الخدمة الراديوية الرزمية العامة.

2.2.8 تحديد الحصص

حينما يكون النشاط الاقتحامي هو السبب الرئيسي في الحالات الشاذة في الشبكة، مثل إحدى هجمات رفض الخدمة الموزَّع، فإن بالمستطاع استخدام نهج تحديد الحصص للحد من سرعة الانتشار. ويعيِّن هذا النهج عتبة للعدد الأقصى من الرسائل التي يمكن إرسالها خلال فترة محددة (شهر مثلاً) مع ضمانة كاملة لقدرة الاتصالات الأساسية أو الطارئة لأي مطراف. وحينما يتجاوز عدد الرسائل العتبة فإنه لا يُسمح بإرسال أي رسالة أخرى.

3.8 التقييد

1.3.8 إخراج خدمة المشغل من شبكة الإنترنت

إذا ما كان متحكم ضار يكمن ضمن خدمة المشغل، وهو ما قد يكون ناجماً عن القرصنة، فإن بمقدور المشغل ممارسة الحق والالتزام بإخراج خدمته من شبكة الإنترنت مؤقتاً واستخدام الخدمة الاحتياطية إذا ما كان ذلك ضرورياً بفعل الالتزام بتوفير اتصالات الطوارئ.

9 تبادل المعلومات

لا يمكن أن يكون التحكم هو الهدف النهائي حيث إنه يحاول التقليل فحسب من الأثر السلبي على المشتركين والشبكات. ويتمثل الهدف النهائي في إعادة الأمور إلى وضعها الطبيعي والسعي إلى منع عدوى أوسع. ولذلك فإن عملية تبادل المعلومات تتسم بالأهمية لكمال الإطار كله.

وتعزيزاً لمصلحة الصناعة، يتم تبادل عينات البرمجيات الضارة فقط بين المشغلين.

ويُشار إلى أن عملية تبادل المعلومات ينبغي أن تتمثل للتشريعات المحلية ولعقود الاشتراك.

بيبليوغرافيا

[b-ITU-T X.1121] Recommendation ITU-T X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.

[b-ITU-T X.1211] Recommendation ITU-T X.1211 (2014), *Techniques for preventing web-based attacks*.

[b-ITU-T X.1244] Recommendation ITU-T X.1244 (2008), *Overall aspects of countering spam in IP-based multimedia applications.*

[b-ITU-T X.1245] Recommendation ITU-T X.1245 (2010), *Framework for countering spam in IP-based multimedia applications*.

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، 2018