Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1126

(03/2017)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Applications et services sécurisés – Sécurité des télécommunications mobiles

Lignes directrices relatives à l'atténuation des effets négatifs des terminaux infectés dans les réseaux mobiles

Recommandation UIT-T X.1126

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	**X.1120–X.1139**
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
Recommandations relatives aux infrastructures de clé publique	X.1340–X.1349
Sécurité de l'Internet des objets	X.1360–X.1369
Sécurité des systèmes de transport intelligent	X.1370–X.1379
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1126

Lignes directrices relatives à l'atténuation des effets négatifs des terminaux infectés dans les réseaux mobiles

Résumé

La Recommandation UIT-T X.1126 fournit aux opérateurs mobiles des lignes directrices visant à restreindre le nombre de terminaux infectés en utilisant, dans le réseau mobile, des technologies destinées à protéger à la fois les abonnés et les opérateurs mobiles. La présente Recommandation décrit les caractéristiques et les effets des logiciels malveillants dont l'existence est rendue possible par des écosystèmes malsains dans l'environnement mobile. Fondée sur des technologies côté réseau, la présente Recommandation traite essentiellement de l'atténuation des effets pervers causés par les terminaux infectés. Elle définit et organise les mesures d'atténuation ainsi que les techniques correspondantes.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1126	30-03-2017	17	11.1002/1000/13194

Mots clés

Infection, logiciel malveillant, réseau mobile, terminal.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Introduction

L'expansion et le développement rapides des systèmes d'exploitation des dispositifs mobiles ont conduit à la naissance d'un vaste marché très dynamique pour le secteur des communications mobiles. De nombreux écosystèmes se sont développés autour de ce marché lucratif afin de tirer parti de ses avantages. Toutefois, les puissantes fonctionnalités des dispositifs mobiles actuels pourraient aussi être utilisées de manière abusive par des logiciels malveillants, qui exploiteraient les failles des terminaux, des réseaux et des services, ce qui provoquerait des dégâts importants.

Il est à noter qu'un écosystème sain doit être préféré à un "jardin clos" dans le cas des systèmes mobiles d'ancienne génération, afin de sécuriser le marché mobile et de protéger les intérêts de toutes les parties prenantes concernées. Des écosystèmes sains ont été mis en place avec succès dans certains pays.

Il est aussi à noter que, dans certains pays, les écosystèmes du marché mobile sont très variés et que certains d'entre eux sont "irresponsables", malsains, voire dangereux. Outre les logiciels malveillants, les effets négatifs d'écosystèmes "irresponsables" pourraient causer des torts considérables aux abonnés mobiles et endommager gravement les réseaux mobiles. Dans certains cas, même des abonnés et des réseaux mobiles évoluant dans un écosystème sain peuvent être victimes eux aussi de terminaux infectés, étant donné qu'à l'heure actuelle, la plupart des services Internet mobiles sont assurés à l'échelle mondiale.

Les risques éventuels liés à la propagation de logiciels malveillants, principalement dans les écosystèmes "irresponsables", sont les suivants:

Pour les abonnés:

- vol d'informations liées à la vie privée, par exemple, écoutes illicites ou traçage de la localisation;
- dégâts matériels, par exemple, dysfonctionnement du système ou destruction de données;
- transaction et consommation malveillantes, par exemple, envoi de messages coûteux ou appels vers des centres d'appel internationaux;
- propagation du logiciel malveillant en vue d'attaquer d'autres terminaux;
- envoi de spams pour importuner d'autres abonnés;
- fraude et chantage.

Pour les opérateurs, les attaques touchant les entités de réseau, les services mobiles et d'autres terminaux comportent les risques suivants:

- exploitation massive des ressources des réseaux ou des services mobiles, entraînant leur dysfonctionnement et des réclamations de la part des abonnés concernant la qualité de service;
- piratage de serveurs de services et même d'entités du réseau.

Les logiciels malveillants provoquent davantage de dégâts sur l'Internet mobile que sur l'Internet filaire traditionnel pour les raisons suivantes:

- L'Internet mobile est un marché émergent et l'élaboration des mécanismes de sécurité associés est relativement lente.
- Des transactions commerciales privées et confidentielles passent souvent par des terminaux mobiles qui constituent des cibles très attrayantes pour les pirates.
- Les réseaux mobiles disposent de moins de ressources et les attaques par inondation mobilisent ces ressources plus facilement et en plus grande quantité.

- Beaucoup de terminaux mobiles sont très étroitement liés aux réseaux auxquels ils sont rattachés. Les services malveillants et les vols d'informations liées à la vie privée pourraient entrainer un manque à gagner pour les opérateurs, des réclamations de la part des abonnés et des problèmes juridiques.
- Les systèmes d'exploitation mobiles libres ou piratés fournissent des terrains propices aux logiciels malveillants, échappant au contrôle de l'opérateur.
- Les terminaux mobiles sont souvent équipés de nombreuses interfaces d'échange de données, telles que les bus série universels (USB), les lecteurs de carte numérique sécurisée (SD) et le Bluetooth, dont beaucoup ne peuvent pas être sécurisées par les opérateurs.

Afin d'atténuer les dégâts causés par les logiciels malveillants et de remonter jusqu'aux sources des menaces, il est essentiel de prendre en charge, côté réseau, les terminaux infectés, une responsabilité et une obligation qui reviennent aux opérateurs mobiles.

Recommandation UIT-T X.1126

Lignes directrices relatives à l'atténuation des effets négatifs des terminaux infectés dans les réseaux mobiles

1 Domaine d'application

La présente Recommandation fournit des lignes directrices relatives à l'atténuation, côté réseau, des effets négatifs des terminaux infectés dans les réseaux mobiles. Elle décrit un cadre dans lequel ces lignes directrices sont structurées en fonction des procédures. On y trouvera en outre un examen des principes, des politiques et des techniques liés à ces procédures.

La conformité à la présente Recommandation ne doit pas être considérée comme une preuve permettant de déclarer la conformité à une législation, une réglementation ou une politique, nationale ou régionale. Les moyens techniques et ceux relatifs à l'organisation et aux procédures décrits dans la présente Recommandation ne garantissent en aucune façon de parvenir à un niveau de sécurité susceptible d'être imposé pour certaines correspondances par une législation, une réglementation ou une politique nationale ou régionale spécifique.

2 Références

Néant.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 liste noire [b-UIT-T X.1245]: liste de personnes ou de sources utilisant des services de communication auxquelles l'accès à certaines ressources de communication est refusé.

3.1.2 logiciel malveillant [b-UIT-T X.1211]: logiciel conçu expressément pour endommager ou perturber un système, et nuire à la confidentialité, à l'intégrité et/ou à la disponibilité.

NOTE – A titre d'exemple, on peut citer les virus, les logiciels de demande de rançon, les logiciels espions, les logiciels publicitaires et les faux logiciels antivirus.

3.1.3 réseau mobile [b-UIT-T X.1121]: réseau fournissant des points d'accès hertzien à des terminaux mobiles.

3.1.4 terminal mobile [b-UIT-T X.1121]: entité dotée d'une fonction d'accès hertzien et qui peut être connectée à un réseau mobile pour des communications de données avec des serveurs d'application ou d'autres terminaux mobiles.

3.1.5 envoi de spams [b-UIT-T X.1244]: chaîne d'activités réalisées par des spammeurs pour envoyer des spams (établissement de listes de cibles, création de spams, distribution de spams, etc.).

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit le terme suivant:

3.2.1 réseau zombi: groupe d'ordinateurs infectés par un logiciel malveillant et connectés de façon coordonnée à des fins malveillantes à l'insu de leur propriétaire, par exemple dans le but de transmettre un logiciel malveillant, d'envoyer des spams ou de lancer des attaques.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

API interface de programmation d'applications *(application programming interface)*

App application exécutée sur des terminaux mobiles

C&C commande et contrôle

DDoS déni de service réparti *(distributed denial of service)*

GGSN noeud passerelle de prise en charge du service général de radiocommunication en mode paquet (*gateway general packet radio service support node)*

IP protocole Internet *(Internet protocol)*

MMS service de messagerie multimédia *(multimedia messaging service)*

MMSC centre du service de messagerie multimédia *(multimedia messaging service centre)*

SD numérique sécurisé (*secure digital*)

SIM module d'identification de l'abonné *(subscriber identity module)*

SMS service de messages courts *(short message service)*

SMSC centre du service de messages courts *(short message service centre)*

URL localisateur uniforme de ressources *(uniform resource locator)*

USB bus série universel *(universal serial bus)*

VAS service à valeur ajoutée *(value-added service)*

WAP protocole d'application sans fil *(wireless application protocol)*

5 Conventions

Néant.

6 Cadre et procédures

Dans la plupart des cas, après avoir été infectés par un logiciel malveillant, les terminaux mobiles peuvent toujours accéder au réseau, utiliser, comme à l'ordinaire, tous les types de services, mais aussi commencer à provoquer des effets négatifs sur les réseaux et les services, sans que les abonnés n'en soient nécessairement conscients. L'opérateur mobile doit prendre conscience de l'infection et imposer des restrictions appropriées au terminal infecté afin de maintenir la stabilité des fonctionnalités de son réseau et de son service et conserver sa crédibilité en protégeant les intérêts des abonnés. La Figure 1 décrit un cadre pour l'atténuation des effets négatifs des terminaux infectés qui définit trois rôles: celui des opérateurs, celui des abonnés et celui des autres organismes. Les opérateurs jouent le rôle principal et leurs tâches s'articulent autour de trois procédures: la détection, le contrôle et l'échange d'informations. Le cadre prévoit, à l'appui de ces trois procédures, une base de données sur les sources et les logiciels malveillants. Les opérateurs suivent les procédures définies dans ce cadre en tenant compte des obligations légales et réglementaires nationales auxquelles ils sont soumis au sein des différents Etats Membres dont ils relèvent.

Les trois rôles dont il est question interagissent: les opérateurs détectent et contrôlent, côté réseau, les anomalies présentées par les terminaux des abonnés et informent ensuite ces derniers des menaces qu'elles constituent. Les opérateurs peuvent en outre échanger des informations concernant les logiciels malveillants avec d'autres opérateurs et organismes associés.

Au cours de la procédure de détection, des exemples d'applications exécutées sur des terminaux mobiles ainsi que des rapports relatifs aux attaques peuvent être recueillis et analysés en vue de détecter des anomalies dans le réseau mobile. Ces anomalies et les terminaux affectés sont signalés au cours de la procédure de contrôle. Pendant cette étape, les anomalies sont confirmées et des mesures appropriées sont prises afin d'atténuer les effets négatifs pour les abonnés et les opérateurs. Afin de pouvoir fournir des informations en temps utile permettant de neutraliser les logiciels mobiles malveillants ou de leur faire face, il est recommandé de mettre en place une procédure d'échange d'informations dans le cadre de laquelle les informations concernant les logiciels malveillants seront échangées avec les opérateurs et les organismes qui travaillent en collaboration en vue d'améliorer la sécurité de l'ensemble de secteur.

Base de données sur les sources et les logiciels malveillants: tout au long des trois procédures, une base de données sur les sources et les logiciels malveillants répertorie le code utilisé et fournit des informations à ce sujet, notamment en ce qui concerne des schémas de comportement ou des sources. Ces renseignements sont mis à profit au cours des trois procédures pour la détection des anomalies, le contrôle des terminaux infectés et la publication d'informations sur les logiciels malveillants. En outre, si de nouvelles informations sur les logiciels malveillants sont recueillies pendant les procédures de détection et d'échange d'informations, il est possible de les télécharger dans la base de données afin que la protection assurée soit constamment actualisée.

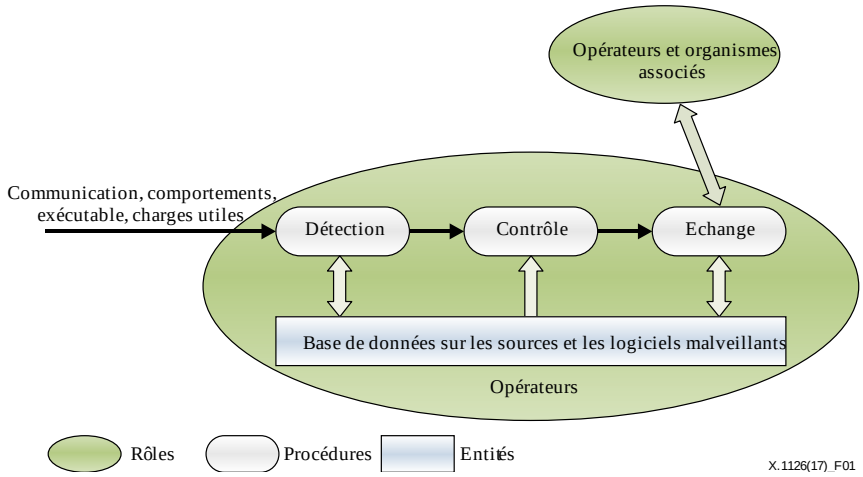

Figure 1 – Cadre pour l'atténuation des effets négatifs des terminaux infectés

7 Détection

Lors de la procédure de détection, des exemples d'applications provenant de boutiques d'applications ainsi que des rapports d'attaque provenant de terminaux et d'éléments de réseau sont recueillis en vue d'analyser les anomalies dans le réseau mobile, ce qui peut permettre d'identifier ou de repérer des terminaux infectés et des sources malveillantes. La Figure 2 décrit le déroulement de la procédure de détection.

L'ensemble des données dont il est question dans ce paragraphe et dans les suivants peuvent être obtenues à partir d'exemples d'applications provenant de boutiques d'applications et de rapports d'attaque provenant de terminaux d'abonné ou d'éléments de réseau. Toute utilisation de données peut relever du respect de la vie privée des abonnés lors de la procédure de détection et nécessiter l'accord ou l'autorisation desdits abonnés, conformément à la législation locale. L'utilisation des données devrait être strictement limitée à l'analyse des logiciels malveillants et de leurs activités.

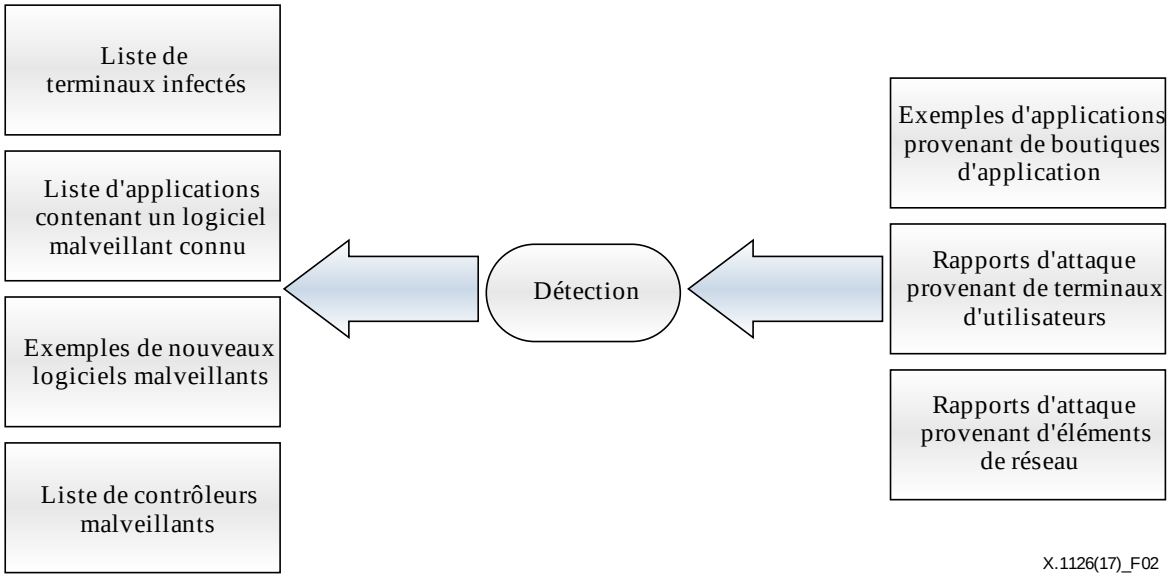

Figure 2 – Déroulement de la procédure de détection

7.1 Recueil d'applications et de rapports d'attaque

Lors de la procédure de détection, il est possible de recueillir deux types de données pour déceler les anomalies du réseau:

- des rapports d'attaque provenant de terminaux d'abonné et d'éléments de réseau;
- des exemples d'applications provenant de boutiques/marchés d'applications.

7.2 Analyse des terminaux infectés et des logiciels malveillants connus

Les rapports d'attaque peuvent permettre d'identifier certains terminaux infectés. En outre, une analyse de concordance de signature peut faciliter la détection de nouvelles applications contenant un logiciel malveillant connu.

L'analyse des terminaux infectés et des logiciels malveillants connus est utilisée pour localiser les contrôleurs malveillants dissimulés au sein du réseau.

Les adresses utilisant le protocole Internet (IP) figurant dans les paquets de commande des terminaux infectés doivent faire l'objet d'une analyse en vue de repérer celles qui correspondent aux sources qui pilotent les terminaux infectés ou qui recueillent des informations les concernant.

Les logiciels malveillants connus détectés dans des applications doivent faire l'objet d'une analyse dynamique afin que soient constatés les éventuels changements effectués par des contrôleurs malveillants.

7.3 Analyse de nouveaux logiciels malveillants

De nouveaux logiciels malveillants peuvent être découverts sur la base des applications prélevées dans les boutiques d'applications, grâce à des analyses de comportement, des analyses statiques ainsi que des analyses dynamiques.

7.3.1 Analyse de codes et d'exécutables malveillants

Analyse statique: Cette méthode est utilisée afin de comprendre le fonctionnement d'un logiciel malveillant présumé au niveau syntaxique. Par exemple, des techniques de retro-ingénierie peuvent être utilisées pour désassembler une application mobile et ainsi obtenir son fichier "manifeste" (contenant des informations concernant les autorisations sollicitées par l'application) et son code source. L'examen du fichier "manifeste" ainsi que des invocations pouvant être effectuées par l'interface de programmation d'application (API) permet de repérer un certain nombre de tentatives malveillantes en s'appuyant sur plusieurs principes de détection:

- si un privilège d'accès sensible et injustifié est accordé;
- si l'interface API de réseau est invoquée pour accéder à des sources Internet malveillantes;
- si l'interface API de processus est invoquée pour arrêter une application;
- si l'interface API de processus est invoquée pour exporter des coordonnées vers une destination particulière;
- si le comportement du lecteur de carte (mémoire) numérique sécurisée (SD) ou du module d'identification de l'abonné (SIM) est anormal;
- si des données sont échangées avec des localisateurs uniformes de ressources (URL) malveillants connus;
- si un abonnement à un service de messages courts (SMS) est souscrit sans que l'abonné ne l'ait demandé;
- si des instructions visant à contrôler le terminal mobile à distance sont présentes.

Analyse dynamique: Cette méthode exécute et surveille les logiciels mobiles suspectés d'être malveillants au sein d'un environnement contrôlé (voire virtualisé), par exemple un "bac à sable" (*sandbox*). Les principes de détection sont notamment les suivants:

a) Communications relatives aux réseaux zombis:

   i) Description: Afin de rejoindre le réseau zombi, une machine doit signaler son existence à un serveur de commande et de contrôle (C&C) et ce dernier transmet à la machine infectée des instructions pour qu'elle entreprenne des activités malveillantes. Le serveur C&C peut être un serveur web ou un terminal du réseau mobile et les instructions peuvent être transmises par le biais de l'Internet ou de services SMS ou MMS.

   ii) Principes de détection:

      1) Un nombre important de terminaux se connectent à un serveur malveillant connu.

      2) Un terminal se connecte à un serveur malveillant connu de manière régulière et prolongée.

      3) Un terminal envoie des messages SMS binaires à un grand nombre de terminaux.

b) Propagation et envoi de spams:

   i) Description: Le logiciel malveillant se propage ou envoie des spams à d'autres abonnés par le biais de divers services (Internet, MMS, SMS, etc.) en couvrant un rayon aussi large que possible.

   ii) Principes de détection:

      1) Un grand nombre de terminaux envoient les mêmes messages MMS ou SMS (comparés avec un hachage unidirectionnel) et présentent une répartition géographique arbitraire.

      2) Le volume d'un service augmente brusquement pendant une période d'inactivité.

      3) Des triples appels sont émis.

      4) Des messages SMS sont envoyés.

5) Des messages MMS sont envoyés.

6) Si un appel utilisant un numéro usurpé est émis sous l'action d'un logiciel.

7) Si les informations contenues dans la carte SIM sont exportées vers un serveur par un logiciel.

8) Si un appel malveillant est émis sous l'action d'un logiciel après un court laps de temps.

9) Si un téléchargement supplémentaire injustifié est effectué.

10) Si un accès avec un contrôleur malveillant connu est établi.

c) Souscription et consommation malveillantes:

i) Description: Les terminaux infectés souscriront à des services à valeur ajoutée (VAS) ainsi qu'à des services de triple appel, afin d'émettre des appels kiosque ou des appels internationaux et d'envoyer un grand nombre de messages. L'abonné n'aura pas connaissance de ces dépenses.

ii) Principes de détection:

1) Augmentation inexpliquée de la facture de l'abonné.

2) Le terminal infecté effectue des appels kiosque ou des appels internationaux fréquents, séparés par des intervalles de temps réguliers.

3) De nombreux terminaux envoient sans cesse les mêmes messages, un grand nombre de fois et avec des intervalles de temps réguliers.

4) Le terminal souscrit aux services de triple appel et les utilise fréquemment, voire en permanence.

d) Attaque par déni de service réparti (DDoS):

i) Description: Une multitude de terminaux inondent les ressources radioélectriques ainsi que d'autres ressources du réseau mobile en vue de réduire la qualité de service.

ii) Principes de détection:

1) Le trafic au niveau du noeud passerelle de prise en charge du service général de radiocommunication en mode paquet (GGSN) ou d'autres entités de réseau augmente drastiquement et une très grande partie de ce trafic est dirigée vers la même destination.

L'analyse statique ne permet pas d'identifier les logiciels malveillants présumés lorsqu'ils sont dissimulés ou offusqués et l'analyse dynamique ne permet pas de vérifier la totalité du code du programme. Ainsi, pour comprendre le fonctionnement d'un logiciel malveillant donné dans son intégralité, les deux types d'analyse doivent être réalisés.

Les tentatives ou comportements anormaux repérés et reconnus grâce aux analyses statiques et dynamiques permettent de mettre à jour les principes sur lesquels est fondée l'analyse de comportement par rapport aux scénarios correspondant aux anomalies les plus récentes. De plus, les caractéristiques ainsi identifiées peuvent aider les opérateurs à découvrir des adresses URL ou IP malveillantes encore inconnues jusqu'alors.

7.3.2 Approche combinée

Du fait des considérations précédentes, il est conseillé de faire appel aux deux méthodes analytiques afin de réduire le nombre de faux positifs au cours de la procédure de détection et d'améliorer son efficacité.

Lors de cette procédure, divers résultats peuvent être produits en vue de faciliter la procédure de contrôle ultérieure. Les résultats de la procédure de détection devraient, au minimum, contenir les éléments suivants:

- une liste de terminaux infectés;
- des exemples d'applications contenant un logiciel malveillant connu;
- des exemples de nouveaux logiciels malveillants;
- une liste de contrôleurs malveillants.

Les informations ci-dessus sont primordiales pour que les opérateurs puissent prendre les mesures appropriées au cours des procédures décrites dans les § 8 et 9.

8 Contrôle

Lors de la procédure de contrôle, les résultats de la procédure de détection sont analysés et validés de façon automatique ou semi-automatique. Des mesures de contrôle sont ensuite mises en oeuvre en fonction de la gravité des anomalies. La Figure 3 décrit les interactions entre la procédure de contrôle et les autres entités de réseau et de service.

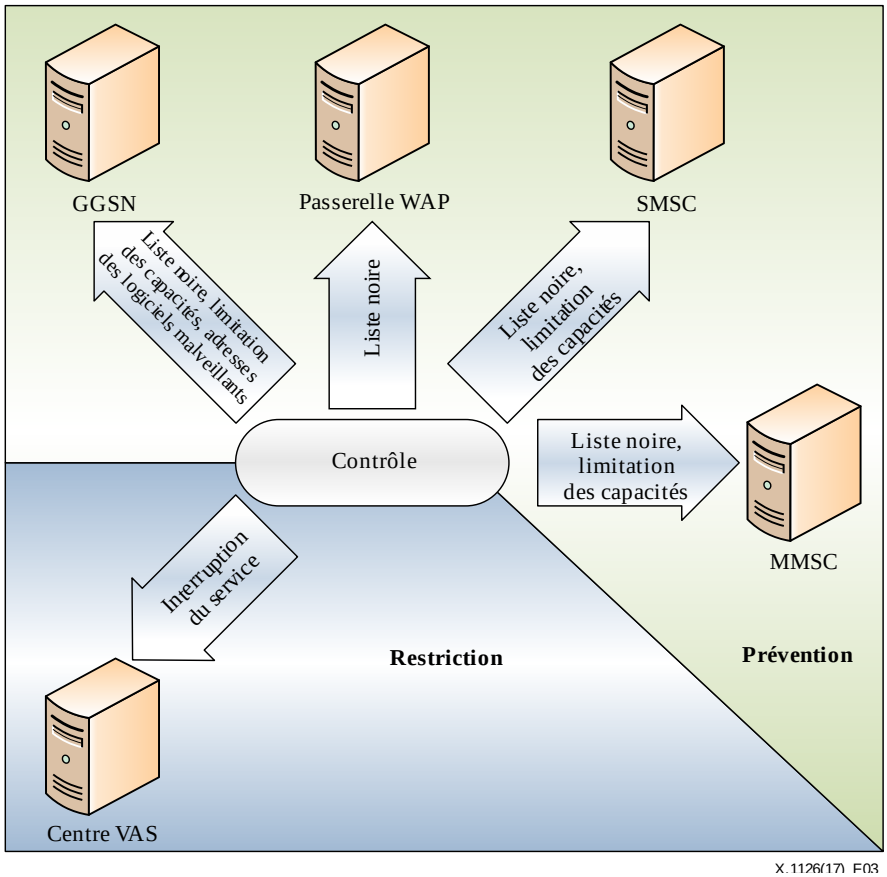

Figure 3 – Interactions relatives à la procédure de contrôle

8.1 Mesures de contrôles

Deux types de mesures sont envisageables, en fonction de la gravité des anomalies: les mesures de prévention et les mesures de restriction. Dans les deux cas, il est seulement fait appel aux fonctionnalités des entités de réseau et des plates-formes de support de service.

- Prévention: Si l'anomalie est de gravité modérée et si elle peut être contrôlée sans qu'il soit nécessaire d'interrompre la fourniture des services offerts aux abonnés, il est possible d'utiliser la méthode préventive pour traiter le problème.
- Restriction: Si l'approche préventive a échoué et si l'abonné accuse déjà une perte d'argent importante, des mesures restrictives sont mises en oeuvre afin d'interrompre le service touché, de façon sélective ou complète.

8.2 Prévention

8.2.1 Liste noire

Lorsqu'une anomalie est déclenchée par un contrôleur malveillant, ce dernier peut être ajouté à une liste noire. Toute demande ultérieure ayant ce contrôleur comme source ou comme destination est alors bloquée. De nombreuses entités de réseau, telles que les noeuds GGSN, les passerelles utilisant le protocole d'application sans fil (WAP) et les centres du service de messagerie multimédia (MMSC), prennent en charge les fonctions relatives aux listes noires. Plusieurs listes noires peuvent être utilisées afin de bloquer différents types de contrôleurs malveillants, tels que les noms de domaine de sites web malveillants ou encore les adresses IP de serveurs C&C. Il convient de noter que les sources figurant dans la liste noire devront faire l'objet d'une vérification et d'une mise à jour régulière, afin d'éviter que des sources légitimes ne soient bloquées.

Toute adresse dans laquelle figure un lien permettant de télécharger une application contenant un logiciel malveillant peut être bloquée par les noeuds GGSN.

8.2.2 Limitation des capacités

Lorsque la cause principale d'anomalie dans le réseau est l'envoi de spams, comme c'est notamment le cas lors d'une attaque DDoS, la technique de limitation des capacités peut être utilisée afin de réduire la vitesse de propagation du spam. Cette mesure consiste à fixer un nombre maximum de messages pouvant être envoyés en un intervalle de temps donné (par exemple, un mois), en garantissant pleinement les capacités de tous les terminaux en matière de communications essentielles ou d'urgence. Lorsque le nombre de messages envoyés dépasse le seuil fixé, il est alors impossible d'en envoyer d'autres.

8.3 Restriction

8.3.1 Interruption du service de l'opérateur

Si un contrôleur malveillant agit au sein du service d'un opérateur, par exemple suite à un piratage, l'opérateur peut faire valoir le droit ou l'obligation d'interrompre temporairement son propre service et, le cas échéant, utiliser le service de sauvegarde, tout en répondant à son obligation en matière de communications d'urgence.

9 Echange d'informations

Le contrôle ne peut pas être l'objectif final étant donné qu'il a uniquement pour but de réduire au minimum les effets négatifs sur les abonnés et les réseaux. L'objectif final est de revenir à une situation normale et de tenter d'empêcher l'infection de s'étendre davantage. Ainsi, la procédure d'échange d'informations est importante pour le parachèvement de l'ensemble du cadre.

En vue d'améliorer la santé du secteur, seuls les exemples de logiciels malveillants devraient être échangés entre les opérateurs.

Il est à noter que la procédure d'échange d'informations devrait être conforme à la législation locale et aux contrats d'abonnement.

Bibliographie

[b-UIT-T X.1121] Recommandation UIT-T X.1121 (2004), *Cadre général des technologies de la sécurité pour les communications mobiles de données de bout en bout.*

[b-UIT-T X.1211] Recommandation UIT-T X.1211 (2014), *Techniques pour prévenir les attaques sur le web.*

[b-UIT-T X.1244] Recommandation UIT-T X.1244 (2008), *Aspects généraux de la lutte contre le pollupostage dans les applications multimédias sur les réseaux IP.*

[b-UIT-T X.1245] Recommandation UIT-T X.1245 (2010), *Cadre de lutte contre le spam dans les applications multimédias IP.*

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2017