Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1213

(09/2017)

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

Sécurité du cyberespace – Cybersécurité

Capacités requises en matière de sécurité pour lutter contre les réseaux zombies (ou botnets) ciblant des smartphones

Recommandation UIT-T X.1213

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 (1)	
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 (1)	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 spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1360–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1429
Protocoles de sécurité (2)	X.1450–X.1459
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.1213

Capacités requises en matière de sécurité pour lutter contre les réseaux zombies (ou botnets) ciblant des smartphones

Résumé

La Recommandation UIT-T X.1213 analyse le contexte des réseaux zombies (ou botnets) ciblant des smartphones et les risques potentiels qu'ils représentent pour la sécurité et décrit les capacités requises en matière de sécurité.

Dans le contexte du développement rapide des dispositifs mobiles utilisant l'Internet et de la généralisation de l'utilisation des smartphones, des études menées par des organisations du monde entier montrent que les réseaux zombies (ou botnets), qui prenaient auparavant pour cible principalement les réseaux d'ordinateurs personnels (PC), sont en train de se développer à un rythme très rapide en ciblant les smartphones. A l'heure actuelle, des pays et des régions présentant des conditions et des écosystèmes différents n'imposent pas tous les mêmes niveaux de contraintes pour faire face à la multiplication des réseaux zombies visant les smartphones. Des rapports analytiques établis par diverses entreprises de sécurité et divers organismes d'enquête présentent des données statistiques très différentes en ce qui concerne la gravité de la multiplication des botnets ciblant des smartphones. La menace potentielle que représentent les réseaux zombies ciblant des smartphones prend rapidement de l'ampleur dans certaines régions et pourrait même s'étendre au monde entier, faisant de ce problème régional un enjeu de première importance à l'échelle mondiale.

Les smartphones ont une puissance de traitement plus faible, un espace de stockage plus réduit et des batteries à durée de vie plus courte que les PC et les serveurs. Cependant, les effets négatifs des botnets ciblant des smartphones pourraient être encore plus dommageables pour les utilisateurs, et ce pour les raisons suivantes: 1) les smartphones contiennent souvent des informations d'identification personnelle (PII) très importantes et 2) en cas d'attaque visant des smartphones ou les infrastructures d'un opérateur, la qualité de l'expérience utilisateur risque de se dégrader de manière significative en raison de l'omniprésence des smartphones et du fait que les utilisateurs en sont de plus en plus dépendants.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1213	06-09-2017	17	11.1002/1000/13261

Mots clés

Botnet, commande et contrôle (C&C), logiciel malveillant, informations d'identification personnelle (PII), smartphone.

* 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

		Page
1	Domaine d'application	1
2	Références	1
3	Définitions	1
3.1	Termes définis ailleurs	1
3.2	Termes définis dans la présente Recommandation	1
4	Abréviations et acronymes	1
5	Conventions	2
6	Rappel	2
6.1	Aperçu des considérations touchant à la sécurité	3
6.2	Evolution de menaces que font peser les botnets sur les smartphones	3
6.3	Protection des smartphones	4
7	Caractéristiques des botnets ciblant des smartphones	4
7.1	Informations d'identification personnelle sur les bots	4
7.2	Diversité des moyens de propagation	5
7.3	Ouverture	5
7.4	Infection ciblée	5
7.5	Dissimulation	5
7.6	Intérêts commerciaux	6
7.7	Evolution constante des connexions au réseau	6
8	Menaces sur la cybersécurité	6
8.1	Divulgation d'informations d'identification personnelle	6
8.2	Prélèvements frauduleux	7
8.3	Comportements peu scrupuleux	7
8.4	Détérioration de la qualité de fonctionnement	8
8.5	Transmission malveillante	8
8.6	Perte de crédibilité	8
9	Capacités requises en matière de sécurité	9
9.1	Capacités requises en matière de sécurité du réseau	9
9.2	Capacités requises en matière de sécurité des smartphones	11
Appendice I – Connexion de logiciels malveillants aux botnets		13
I.1	Avant-propos	13
I.2	Considérations générales	13
I.3	Environnement macroscopique en Chine	14
I.4	Problèmes liés aux iPhones	14
I.5	Exemples de nouveaux logiciels malveillants et évolution	15
I.6	Conclusion	17
Bibliographie		18

Recommandation UIT-T X.1213

Capacités requises en matière de sécurité pour lutter contre les réseaux zombies (ou botnets) ciblant des smartphones

1 Domaine d'application

La présente Recommandation vise à définir les capacités requises en matière de sécurité pour lutter contre les réseaux zombies (ou botnets) ciblant des smartphones. L'objet de cette Recommandation est d'étudier les problèmes que posent les réseaux zombies (ou botnets) ciblant des smartphones, ainsi que les menaces particulières qu'ils font peser sur les réseaux des opérateurs et sur les smartphones eux-mêmes et les exigences associées. La présente Recommandation est axée sur l'analyse des menaces et l'énumération des conditions requises. L'objectif est de préserver les infrastructures des opérateurs et les smartphones, de garantir la qualité des services offerts par les opérateurs ainsi que la qualité des services et d'améliorer l'expérience utilisateur. Les solutions techniques détaillées et les autres terminaux intelligents tels que les tablettes n'entrent pas dans le cadre de la présente Recommandation.

2 Références

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation emploie les termes suivants définis ailleurs:

3.1.1 bot [b-UIT-T X-Sup.8]: programme logiciel automatique utilisé pour effectuer des tâches particulières conçues à des fins malveillantes. Les termes "bot" et "robot" peuvent être utilisés indifféremment.

3.1.2 botmaster [b-UIT-T X-Sup.8]: personne responsable du contrôle et de la gestion d'un botnet.

3.1.3 botnet [b-UIT-T X-Sup.8]: robots logiciels malveillants (bots) commandés à distance, qui sont exécutés de manière autonome ou automatique sur des ordinateurs contaminés, en association avec un serveur de commande et de contrôle appartenant à des botmasters.

3.1.4 information d'identification personnelle (PII, *personally identifiable information*) [b-UIT-T X.1252]: toute information: a) identifiant ou permettant d'identifier, de contacter ou de localiser la personne à laquelle cette information se rapporte; b) permettant d'obtenir les informations d'identification ou les coordonnées d'une personne; ou c) étant ou pouvant être directement ou indirectement liée à une personne physique.

3.2 Termes définis dans la présente Recommandation

Néant.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

2FA authentification à deux facteurs (*two factor authentication*)

2G télécommunications mobiles de deuxième génération (*second generation of mobile telecommunication*)

3G télécommunications mobiles de troisième génération (*third generation of mobile telecommunication*)

4G télécommunications mobiles de quatrième génération (*fourth generation of mobile telecommunication*)

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

C&C commande et contrôle

CPU unité centrale de traitement (*central processing unit*)

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

DNS système de noms de domaine (*domain name system*)

GPS système mondial de localisation (*global positioning system*)

HTTP protocole de transfert hypertexte (*hyper text transfer protocol*)

IDS système de détection des intrusions (*intrusion detection system*)

IoT Internet des objets (*Internet of things*)

IP protocole Internet (*Internet protocol*)

IPS système de prévention des intrusions (*intrusion prevention system*)

MITM "homme du milieu", intercepteur (*man-in-the-middle*)

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

NFC communication en champ proche (*near-field communication*)

OTP code secret à usage unique (*one-time passcode*)

P2P d'homologue à homologue (*peer-to-peer*)

PC ordinateur personnel (*personal computer*)

PII information d'identification personnelle (*personally identifiable information*)

PNG graphique de réseau portable (*portable network graphics*)

QoS qualité de service (*quality of service*)

QRcode code de réponse rapide (*quick response code*)

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

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

USB bus série universel (*universal serial bus*)

WiFi fidélité sans fil (*wireless-fidelity*)

5 Conventions

Aucune.

6 Rappel

Parallèlement au développement rapide des dispositifs mobiles utilisant l'Internet, les terminaux mobiles sont dotés de fonctionnalités de plus en plus performantes en matière d'intelligence et de qualité de fonctionnement. Dans la présente Recommandation, le terme "smartphone" désigne un téléphone mobile présentant les caractéristiques suivantes:

– système d'exploitation indépendant;

– l'installation d'applications tierces;
– capacité d'accéder au réseau sans fil, et notamment capacité d'accéder à l'Internet mobile via le réseau de communication d'un opérateur mobile.

Ces dernières années, le nombre d'utilisateurs de smartphones a continué d'augmenter à un rythme rapide. Bien qu'ils soient pratiques dans la vie quotidienne des utilisateurs, les smartphones présentent des risques de plus en plus importants pour la sécurité.

6.1 Aperçu des considérations touchant à la sécurité

Etant donné que le nombre d'utilisateurs de smartphones progresse rapidement, les réseaux zombies (ou botnets) ciblant des smartphones doivent être supprimés et contrôlés de façon à éviter qu'ils ne jouent un rôle toujours plus important susceptible d'influer sur la stabilité de la société et de menacer la sécurité publique.

Pour les opérateurs mobiles, le développement à grande échelle des botnets pourrait gravement compromettre l'efficacité d'utilisation du réseau des opérateurs et nuire à la qualité de service (QoS) offerte aux utilisateurs, entraînant ainsi un mécontentement des usagers et une perte d'abonnés. Pour les utilisateurs dont les smartphones sont piratés et contrôlés via des botnets, le préjudice potentiel peut-être important, en ce sens que bon nombre de leurs informations d'identification personnelle (PII) les plus importantes, par exemple les listes de contacts et les informations concernant les paiements en ligne, sont souvent mémorisées sur leurs smartphones.

En conséquence, les mesures destinées à lutter contre les réseaux zombies (ou botnets) ciblant des smartphones sont à la fois tournées vers l'avenir et d'ordre pratique. Les opérateurs devraient sensibiliser davantage les intéressés à la sécurité dans ce domaine, afin de freiner l'essor rapide des botnets, de limiter la perte d'abonnés et de réduire le nombre de réclamations des utilisateurs, etc.

6.2 Evolution de menaces que font peser les botnets sur les smartphones

L'apparition des premiers virus visant des smartphones remonte à 2004, lorsque *Cabir*, le premier vers informatique ciblant des smartphones, a été découvert. En 2009, le logiciel malveillant *iKee.B* a commencé à présenter des caractéristiques de botnet et pouvait prendre le contrôle d'iPhones infectés, puis renvoyer au botmaster les informations PII d'un utilisateur. En 2011, un botnet mobile représentatif, baptisé *Android.Geinimi*, a été détecté. Il pouvait dissimuler des méthodes de communication, disposait de nombreux module d'attaque et était considéré comme très préjudiciable.

La généralisation de l'utilisation des smartphones est allée de pair avec un développement spectaculaire des logiciels malveillants ciblant des smartphones, logiciels qui utilisent essentiellement certaines fonctions des smartphones comme support de propagation. Une fois téléchargé et installé sur un smartphone, le logiciel malveillant affichera fréquemment et secrètement des messages publicitaires, engendrera un trafic supplémentaire sur le smartphone, prélèvera des frais, etc., ce qui entraînera un préjudice pour les utilisateurs de smartphones. De plus, les utilisateurs de smartphones seront peut-être confrontés à des problèmes très divers: ainsi, ils seront redirigés vers des sites web de hameçonnage, leur smartphone sera infecté par des virus ou des chevaux de Troie, leurs listes de contacts ou leurs répertoires d'adresses seront divulgués ou dérobés, ou leurs comptes et leurs mots de passe seront subtilisés. Les délits de ce type les plus répandus sont la divulgation d'informations PII, de comptes personnels et de mots de passe.

Ces dernières années, les logiciels malveillants ciblant les smartphones se sont développés de manière exponentielle. Ces logiciels malveillants constituent la principale cause de la prolifération des virus par botnet, étant donné que de plus en plus de logiciels malveillants utilisent des moyens ou des fonctions détournés commandés à distance, qui constituent une particularité des bots ciblant les smartphones. Le principal objectif des botmasters est de tirer parti du vol d'informations PII et de percevoir des frais de manière malveillante. Actuellement, les logiciels malveillants les plus répandus

sont les suivants: vol d'informations PII, prélèvement malveillant de frais, comportement malhonnête, dégradation de la qualité de fonctionnement et propagation malveillante.

6.3 Protection des smartphones

Les appels de harcèlement, les spams acheminés par le service de messages courts (SMS) et d'autres incidents de sécurité résultant de la navigation sur le web, du téléchargement de fichiers, de paiements sur mobile, etc., constituent les principaux problèmes de sécurité auxquels sont confrontés les utilisateurs de smartphones. Ces menaces sont pour l'essentiel atténuées par les logiciels installés sur les smartphones.

Les deux principales fonctions des logiciels de sécurité des smartphones sont la gestion du téléphone et la protection de la sécurité. La fonction de gestion du téléphone comprend le nettoyage de la mémoire, l'extension du temps de veille, la gestion du programme de démarrage automatique, la gestion des SMS, la gestion des numéros de téléphone, etc. Elle a pour but d'améliorer le fonctionnement du smartphone ainsi que l'efficacité d'utilisation du dispositif. La fonction de protection de la sécurité comprend essentiellement la surveillance du trafic de données, le blocage des appels de harcèlement, l'analyse régulière, la suppression régulière des virus, etc. Elle a pour but de protéger les smartphones contre les menaces de sécurité.

L'installation de logiciels de sécurité pourrait contribuer à la protection des smartphones contre certains botnets et logiciels malveillants au niveau du terminal de l'utilisateur, mais étant donné que les pirates qui ciblent des smartphones sont de plus en plus ingénieux et que leurs méthodes d'attaque sont de plus en plus diversifiées, les smartphones continueront d'être exposés à des menaces de sécurité croissantes. Les opérateurs doivent non seulement renforcer la protection de la sécurité au niveau du terminal, mais aussi assurer une plus grande protection de la sécurité au niveau du réseau. La coordination et la coopération des deux parties permettra d'améliorer considérablement la capacité de résistance des smartphones aux attaques par botnets.

7 Caractéristiques des botnets ciblant des smartphones

Les botnets ciblant des smartphones qui utilisent l'Internet pour propager à grande échelle des logiciels malveillants exploitent les caractéristiques des smartphones et des réseaux mobiles. En analysant les caractéristiques des smartphones et des réseaux mobiles, ainsi que l'objectif des attaques du botmaster, il sera possible de récapituler les caractéristiques des botnets ciblant des smartphones et de reconnaître des menaces potentielles contre la sécurité.

7.1 Informations d'identification personnelle sur les bots

Les botnets ciblant des smartphones comprennent un grand nombre de bots ciblant des smartphones. A la différence des ordinateurs personnels (PC) classiques, une grande partie des informations PII et des informations confidentielles sont centralisées dans les smartphones, de sorte que les botnets ciblant des smartphones constituent une menace bien plus grave pour les utilisateurs de smartphones, qui risquent de perdre une grande quantité de données.

Les fonctions intégrées dans les smartphones sont les suivantes: gestion des informations personnelles, calendrier et agenda, journal, organisation des tâches, applications multimédias, navigation sur les pages web, etc. L'abondance d'informations personnelles mémorisées dans les applications des smartphones font de ces derniers une cible privilégiée des auteurs d'attaques. De plus, le système mondial de localisation (GPS) d'un smartphone permet l'acquisition d'informations sur l'emplacement de l'utilisateur, qui constituent un autre type d'information PII. Une fois que les auteurs d'attaques obtiennent ces informations, les informations PII d'un utilisateur pourront être révélées.

7.2 Diversité des moyens de propagation

En premier lieu, les botnets ciblant des smartphones pourront se répandre de façon malveillante via des applications affectées que les utilisateurs trouvent et téléchargent généralement dans les magasins App (App stores) ou sur les forums de discussion des téléphones mobiles, qui ne nécessitent pas d'authentification sécurisée.

En deuxième lieu, les botnets ciblant des smartphones pourront se propager par l'intermédiaire de Bluetooth, du WiFi, d'un bus série universel (USB) et d'autres interfaces périphériques des smartphones.

En troisième lieu, les botnets ciblant des smartphones pourront se propager par le biais du protocole de transfert hypertexte (HTTP), de SMS, du service de messagerie multimédia (MMS), du code à réponse rapide (QRcode), etc.

Ces différents modes de propagation font que les botnets ciblant des smartphones se propagent relativement facilement, imposant ainsi de plus grandes exigences pour assurer la protection et la sécurité requises.

7.3 Ouverture

Les systèmes d'exploitation sur mobile ouverts permettent aux smartphones d'offrir un plus grand choix de programmes d'applications, mais parallèlement, ces programmes exposent les smartphones à des menaces potentielles et à des attaques accrues. L'ouverture permet aux pirates d'insérer des virus ou des chevaux de Troie dans des applications étendues, ce qui facilite la propagation des botnets ciblant des smartphones.

Les smartphones sont dotés de nombreux types d'interfaces périphériques, à savoir: Bluetooth, communication en champ proche (NFC) et USB. Les auteurs d'attaques peuvent utiliser les connexions à toutes ces interfaces périphériques. De plus, les smartphones prennent généralement en charge l'accès au réseau mobile de deuxième, troisième ou quatrième génération (2G, 3G ou 4G) ainsi que l'accès WiFi, par l'intermédiaire duquel les utilisateurs peuvent accéder à l'Internet. Ces fonctions sont d'une valeur inestimable, tant sur le plan des applications que sur le plan commercial, mais offrent aussi de nombreux angles d'attaque aux auteurs d'attaques.

7.4 Infection ciblée

Les botnets ciblant des smartphones visent certains types de cibles et les infectent pas copie directe, ou en amenant par ruse les utilisateurs à télécharger des logiciels malveillants ou des chevaux de Troie. Les auteurs d'attaques peuvent également cibler les smartphones qui utilisent les mêmes systèmes d'exploitation en vue de les infecter. Cette méthode rend l'attaque encore plus efficace, et en réduit en même temps le coût.

7.5 Dissimulation

Les botnets ciblant des smartphones sont de plus en plus complexes. Certains sont capables de dissimuler leurs attaques en supprimant toute trace d'installation après avoir contaminé avec succès un smartphone. D'autres peuvent effacer leur connexion au réseau et toute trace dans la boîte d'envoi, après avoir envoyé les informations PII de l'utilisateur via l'accès à l'Internet. D'autres peuvent même commander des services personnalisés auprès de certains fournisseurs de services et bloquer automatiquement les messages de vérification émanant des opérateurs mobiles.

Certains chevaux de Troie et logiciels malveillants sur des smartphones, qui dérobent des informations ou provoquent le prélèvement frauduleux de frais, ne lancent pas leurs attaques immédiatement après avoir été installés avec succès. En revanche, ils lanceront leurs attaques dans les délais prévus par le logiciel malveillant ou en utilisant la période d'inactivité du smartphone infecté.

Actuellement, de plus en plus de logiciels malveillants comportent des portes dérobées commandées à distance en tant que fonction de base, ce qui constitue l'une des spécificités des bots ciblant des smartphones.

Un grand nombre de botnets se propagent par le biais de programmes malveillants intégrés dans des applications mobiles très répandues. Lorsqu'un utilisateur télécharge et installe des applications depuis des App stores ou des forums de téléphone mobile dépourvus de mécanismes d'authentification sécurisée, les programmes malveillants dissimulés dans les applications seront activés.

7.6 Intérêts commerciaux

A la différence de la plupart des logiciels malveillants classiques, dont la finalité est le sabotage, les botnets ciblant des smartphones sont souvent animés par l'appât du gain. Ils forment ainsi un "secteur gris" de la fraude sur Internet, en tirant profit du vol des informations PII d'un utilisateur ou en procédant au prélèvement frauduleux de frais. L'appât du gain incite les auteurs d'attaques à investir davantage de ressources dans la conception de botnets ciblant des smartphones et encourage le développement d'une industrie de la fraude sur l'Internet. Autrement dit, les botnets ciblant des smartphones imposeront toujours plus de menaces de sécurité aux utilisateurs, menaces contre lesquelles il deviendra de plus en plus difficile de se prémunir.

7.7 Evolution constante des connexions au réseau

La très grande mobilité qui caractérise les smartphones fait que les connexions au réseau évoluent en permanence, ce qui entraîne une diversité accrue des botnets ciblant des smartphones. Les smartphones peuvent se déplacer non seulement entre des réseaux utilisant les mêmes techniques de réseau, mais aussi entre des réseaux utilisant des techniques de réseau différentes, par exemple d'un réseau 3G à un point d'accès WiFi. En conséquence, les bots de smartphones infectés devront peut-être remplacer leur canal de communication par le serveur de commande et de contrôle (C&C) plus fréquemment que les bots sur PC, ce qui compliquera encore la détection des botnets ciblant des smartphones au moyen de l'identification de leurs canaux de communication.

8 Menaces sur la cybersécurité

8.1 Divulgation d'informations d'identification personnelle

– Informations figurant sur la carte SIM (module d'identité de l'abonné mobile):

  Une fois qu'un smartphone est infecté par un bot, les botmasters pourront dérober les informations figurant sur la carte téléphonique de l'utilisateur, notamment les informations relatives à l'enregistrement du téléphone, les paramètres de configuration matérielle, etc. Les botmasters pourront retirer encore plus de gains financiers en revendant ou en divulguant ces informations PII et, ce qui est encore plus préoccupant, pourront lancer des attaques plus dangereuses sur les smartphones présentant les mêmes configurations, en analysant les vulnérabilités de ces téléphones.

– Mémoire du téléphone:

  Les botmasters des botnets ciblant des smartphones peuvent utiliser le nuage pour commander à distance tous leurs bots. Ils peuvent ainsi dérober depuis le bot: les informations PII d'un utilisateur, notamment leur numéro de téléphone, leur liste de contacts, leurs journaux d'appel, leurs messages électroniques, leurs informations de localisation, leurs photos et leurs vidéos, etc. Les botmasters peuvent charger les bots de transférer ces informations vers des serveurs distants.

– Comptes bancaires et mots de passe:

Lorsqu'un utilisateur effectue un paiement via un smartphone, les auteurs d'attaques sont capables de prendre le contrôle total du smartphone de l'utilisateur en exploitant ses failles, ce qui leur permet de dérober les numéros de compte bancaire et les mots de passe de ce dernier. De plus, les auteurs d'attaques peuvent intercepter le code de vérification par SMS et procéder à des transferts d'argent malveillants, et effacer parallèlement toute trace de l'attaque, ce qui leur permet de dérober aisément de l'argent sans que l'utilisateur du smartphone s'en aperçoive.

– Comptes et mots de passe des applications:

En ayant recours aux mêmes moyens, les auteurs d'attaques peuvent dérober les comptes et les mots de passe utilisés par un utilisateur pour des applications. Ils pourront ensuite utiliser ces informations pour commettre de nouveaux actes de fraude et en retirer un profit en conséquence.

8.2 Prélèvements frauduleux

– Téléchargement automatique ou suppression de logiciels:

Une fois qu'un smartphone est contrôlé par un bot, il recevra des instructions émanant d'un serveur C&C et le botmaster pourra demander au téléphone de faire pratiquement n'importe quoi. Suivant les instructions données par le botmaster, le smartphone pourra télécharger automatiquement des applications inutiles, ou désinstaller certaines applications. Ces comportements sont susceptibles d'entraîner un accroissement des frais liés à la consommation de trafic de données et, partant, occasionner des pertes financières pour l'utilisateur.

– Spam par SMS:

Certains logiciels malveillants peuvent demander à des smartphones d'envoyer un spam par SMS au moyen de la liste des contacts du smartphone. Dans un premier temps, l'auteur d'une attaque incite l'utilisateur à télécharger et à installer un logiciel malveillant, après quoi le smartphone, une fois contaminé, contactera automatiquement les serveurs C&C pour obtenir des instructions. Après avoir reçu les instructions du spam par SMS, le smartphone enverra des messages spam par SMS conformément à la liste de contacts du téléphone, ce qui aura pour conséquence une baisse de la qualité de fonctionnement et la perception de prélèvements frauduleux pour l'accès à l'Internet et la messagerie SMS. Des spams par SMS fréquents risquent d'encombrer les canaux mobiles, entraînant ainsi une détérioration de la qualité de fonctionnement et l'indisponibilité du smartphone. De plus, un smartphone contaminé appartient à une entreprise ou à un établissement public, l'image de l'entreprise risque d'en pâtir, étant donné que la liste des contacts mémorisés dans le smartphone peut contenir les contacts de partenaires commerciaux ou de services gouvernementaux importants. Lorsque des spams par SMS sont reçus fréquemment en provenance du smartphone infecté, le numéro du smartphone pourra être ajouté sur les listes noires des destinataires, ce qui engendrera des pertes financières imprévisibles et portera préjudice à la coopération avec l'entreprise.

8.3 Comportements peu scrupuleux

– Attaques par déni de service réparti (DDoS):

Parallèlement à la généralisation de l'utilisation des smartphones et à l'essor rapide des applications Internet sur mobile, les botmasters peuvent lancer des attaques DDoS si le nombre de bots contrôlés est très élevé. Les botmasters peuvent contrôler un grand nombre de smartphones infectés et lancer des attaques simultanées sur un site web donné, ce qui engendre des défaillances des serveurs web. En particulier, si le smartphone contaminé appartient à une entreprise ou à un établissement public donné, l'image de cette entreprise ou

de cet établissement risque d'en pâtir considérablement, étant donné que les listes de contacts mémorisées dans ces smartphones contiennent probablement les contacts de partenaires commerciaux ou de services gouvernementaux importants. Dès qu'elle détecte une attaque DDoS, la cible répondra en bloquant les numéros de téléphone des auteurs de l'attaque, ce qui risque également d'engendrer des pertes financières imprévisibles et de porter préjudice aux relations commerciales.

– Tromperie par annonces publicitaires malveillantes:

  Un smartphone infecté peut devenir un récepteur de messages publicitaires par spam. Les utilisateurs pourront recevoir divers messages publicitaires et chaque clic générera des recettes pour le botnet. De cette façon, les botmasters tireront des profits considérables de frais de publicité frauduleux. Toutefois, ce n'est pas l'utilisateur du smartphone qui clique en fait sur la publicité, mais plutôt le bot malveillant installé sur le smartphone.

– Accès non autorisé au réseau de l'entreprise:

  Les botnets ciblant des smartphones peuvent autoriser les auteurs d'attaques à avoir accès aux réseaux sécurisés de l'entreprise via des dispositifs réseaux infectés. Un dispositif infecté peut analyser la vulnérabilité des serveurs du réseau de l'entreprise et en informer le botmaster. Les auteurs d'attaques peuvent encore tirer parti de cette faille en attaquant les serveurs du réseau de l'entreprise et en dérobant des informations confidentielles.

8.4 Détérioration de la qualité de fonctionnement

Les botmasters peuvent compromettre la qualité de fonctionnement de smartphones, en ayant recours aux méthodes suivantes:

– Des éléments de virus peuvent prendre l'apparence d'images graphiques de réseaux portables (PNG), alors qu'en réalité, il s'agit de scripts automatisés. Après l'infection, le virus sera chargé automatiquement lors du démarrage du smartphone et sera exécuté en permanence en arrière-plan, ce qui entraînera une grave détérioration de la qualité de fonctionnement du système d'exploitation.
– Le fait de se connecter fréquemment à des serveurs chevaux de Troie pour obtenir des instructions endommagera de manière prolongée le smartphone.
– Le téléchargement automatique d'application contenant des spams en arrière-plan consommera d'énergie de la batterie et entraînera en peu de temps une forte diminution de la qualité de fonctionnement.
– L'envoi répété de spams par SMS aux smartphones infectés par les botmasters aura pour conséquence que le smartphone ne fonctionnera plus et que la batterie sera complètement épuisée.

8.5 Transmission malveillante

Certains logiciels malveillants peuvent télécharger des applications dans un smartphone infecté, en arrière-plan, sans l'autorisation de l'utilisateur, puis afficher des messages frauduleux qui apparaissent en incrustation sur l'écran, amenant ainsi l'utilisateur à toucher l'écran, ce qui provoque l'installation du logiciel malveillant. Une fois l'application installée, elle aura accès à un site web donné en arrière-plan, afin d'être mieux placée pour le téléchargement, ce qui induira en erreur un plus grand nombre d'utilisateurs en les incitants à télécharger les applications malveillantes. De cette façon, le champ d'action du botnet sera plus large et les auteurs d'attaques en retireront des profits accrus.

8.6 Perte de crédibilité

Les smartphones infectés par des botnets pourront servir à envoyer des spams dans des messages électroniques ou à participer à des attaques DDoS; ces comportements auront non seulement pour conséquence une augmentation des coûts du réseau et de la consommation de la batterie, mais se

traduiront également par une perte de crédibilité de l'utilisateur. Ainsi, lorsqu'un smartphone infecté par un botnet envoie en masse des spams dans des messages ou des courriers électroniques aux contacts mémorisés dans le smartphone, l'expéditeur (propriétaire du smartphone) perdra de sa crédibilité. En particulier, si le smartphone infecté appartient à une entreprise ou à un établissement public donné, la perte sera encore plus grande, dans la mesure où les contacts mémorisés dans ces smartphones contiennent probablement les noms de partenaires commerciaux ou gouvernementaux importants.

9 Capacités requises en matière de sécurité

9.1 Capacités requises en matière de sécurité du réseau

9.1.1 Surveillance du trafic du réseau

Les opérateurs devraient offrir la possibilité de surveiller le trafic Internet sur un smartphone. Ils pourront créer un mécanisme de surveillance du trafic ou un tableau contenant tous les utilisateurs, et analyser de manière intelligente le trafic Internet sur un smartphone. En cas de détection de trafic anormal, les opérateurs pourront immédiatement envoyer une alarme ou des informations pertinentes à un utilisateur et, en cas de besoin, intercepter le trafic suspect.

9.1.2 Détection de code malveillant sur mobile

Les dispositifs de protection de la sécurité du réseau d'un opérateur devraient déceler et analyser tout code malveillant dans leurs applications. En cas de détection d'un code malveillant dans une application, l'opérateur pourra envoyer dans les meilleurs délais une alarme ou des informations pertinentes aux utilisateurs, qui téléchargent ou utilisent l'application.

9.1.3 Transmission chiffrée d'informations à caractère sensible

Le réseau d'un opérateur devrait prendre en charge la transmission chiffrée des informations envoyées par des smartphones. Une fois que les utilisateurs de smartphones activent cette fonction, les dispositifs du réseau de l'opérateur devraient garantir l'intégrité et la confidentialité des informations transmises, notamment les listes de contacts, les emplacements, les comptes et les mots de passe, etc.

9.1.4 Utilisation d'un réseau "honeypot" ("pot de miel")

Le réseau d'un opérateur devrait mettre en place un système informatique "honeypot" destiné à servir de leurre pour les réseaux botnets et les programmes malveillants qui tentent d'accéder au smartphone. Après avoir détecté les réseaux botnets et rassemblé leurs informations de commande, les opérateurs pourront procéder aux observations et au suivi nécessaires, pour déterminer comment assurer une meilleure protection des smartphones.

9.1.5 Protection contre les attaques par déni de service réparti (DDoS)

– Les dispositifs de protection de la sécurité et les serveurs du système des noms de domaine (DNS) du réseau d'un opérateur devraient être à même de configurer leur politique en matière de sécurité, de façon à empêcher les serveurs de botnets de se connecter à leurs contrôleurs.

– Les pare-feu, les systèmes de détection des intrusions (IDS), les systèmes de prévention des intrusions (IPS) et les autres dispositifs de protection de la sécurité du réseau d'un opérateur devraient être en mesure de configurer leur politique en matière de sécurité de manière à bloquer les attaques contre le trafic.

– Les dispositifs de protection du réseau et de la sécurité du réseau d'un opérateur devraient pouvoir configurer leur politique de blocage du trafic DDoS de manière à bloquer le trafic DDoS du serveur cible dans d'autres domaines.

9.1.6 Détection des botnets

Les dispositifs de protection de la sécurité du réseau d'un opérateur devraient être en mesure de détecter la mutation des botnets et rassembler et partager l'ensemble d'adresses du protocole Internet (IP) disponibles à l'échelle mondiale, de façon à pouvoir établir une base de données des ensembles d'adresses IP des contrôleurs et des serveurs de botnets pour procéder à un filtrage du trafic malveillant et à une analyse de l'action des bots, et de recourir à des mécanismes relatifs à l'ensemble d'adresses IP et à d'autres méthodes de protection.

9.1.7 Détection et suppression des spams par SMS

Le réseau d'un opérateur devrait disposer de mécanismes permettant de détecter et de supprimer des spams par SMS. Lorsqu'on constate qu'un terminal mobile reçoit une grande quantité de messages spam, il convient de bloquer dans les meilleurs délais le spam de façon à éviter tout effondrement dû à la réception de messages spam diffusés en masse. Lors de la détection, les opérateurs devraient être en mesure d'informer les utilisateurs, de façon à pouvoir appliquer les mesures correspondantes pour faire face à cette situation.

9.1.8 Mécanisme fondé sur une liste noire/liste blanche

Les dispositifs de protection de la sécurité du réseau d'un opérateur devraient pouvoir inscrire des logiciels malveillants, des codes malveillants et des sites web malveillants sur leurs listes noires. Si les contrôleurs de botnets demandent à leurs serveurs contrôlés de se connecter à un site web malveillant ou de télécharger un logiciel malveillant qui fait partie d'une liste noire, les dispositifs de protection de la sécurité devraient pouvoir bloquer rapidement ces connexions.

En conséquence, les dispositifs de protection de la sécurité du réseau d'un opérateur devraient également offrir un mécanisme fondé sur une liste blanche. Dans certaines conditions particulières, les utilisateurs sont autorisés à se connecter à des sites web de confiance et à télécharger des applications de confiance faisant partie d'une liste blanche.

9.1.9 Capacité de coopération

Afin d'améliorer l'intégrité et la crédibilité des logiciels de sécurité, les opérateurs devraient être à même de coopérer avec les fournisseurs de produits de sécurité pour smartphones. Grâce à ce mécanisme de coopération, la protection de la sécurité contre les botnets pourra être assurée aussi bien côté réseau que côté terminal mobile.

En outre, les opérateurs devraient également coopérer avec les services gouvernementaux et administratifs. Si un smartphone devient un bot, les opérateurs devraient informer le propriétaire du smartphone par l'intermédiaire des services administratifs concernés. En outre, pour contrer les botnets ciblant des smartphones et mettre fin à leurs comportements malveillants, les opérateurs devraient coopérer avec les services gouvernementaux et administratifs en vue de prendre des mesures et d'adopter une législation appropriée.

9.1.10 Garantie d'identité

Si le smartphone d'un utilisateur (en particulier d'un groupe d'utilisateurs) est contaminé et commence à envoyer des messages spam groupés, etc., l'utilisateur risque de perdre la confiance des destinataires de spams. Si les smartphones contaminés appartiennent à certaines sociétés ou à certains établissements publics, la perte sera d'autant plus importante que leurs listes de contacts contiennent probablement les noms de partenaires commerciaux ou d'organismes gouvernementaux importants.

Afin d'éviter cette perte de confiance, les opérateurs devraient être en mesure de garantir l'identité de l'utilisateur d'un smartphone (en particulier de groupes d'utilisateurs) lorsqu'un fonctionnement anormal, par exemple la messagerie de groupe, est détecté. Par exemple, un opérateur devrait pouvoir détecter les opérations de messagerie de groupe d'un utilisateur et, sur la base de politiques définies au préalable, choisir de les informer par messagerie, ou suspendre temporairement l'opération de

messagerie groupée et demander la confirmation de l'utilisateur avant que celui-ci ne procède à l'opération.

9.2 Capacités requises en matière de sécurité des smartphones

9.2.1 Stockage chiffré des informations d'identification personnelle

Les smartphones devraient prendre en charge le stockage chiffré des listes de contacts, des messages SMS, des photos, des relevés d'appel et d'autres informations PII. Les informations PII devraient être stockées dans les smartphones au moyen de méthodes de chiffrement.

9.2.2 Accès chiffré aux informations d'identification personnelle

Les smartphones devraient comporter un mécanisme d'accès chiffré pour les listes de contacts, les messages SMS, les photos, les relevés d'appel et d'autres informations PII. Les utilisateurs de smartphones devraient pouvoir créer des mots de passe, des empreintes ou d'autres mécanismes pour accéder à certains types d'informations personnelles (par exemple certaines photos ou certains SMS).

9.2.3 Utilisation de logiciels de sécurité

Les utilisateurs de smartphones devraient installer des logiciels de protection de la sécurité sur leur smartphone, afin de pouvoir mieux détecter et supprimer les menaces ou failles potentielles et de prendre les mesures de protection nécessaires en cas d'attaque. Si le smartphone n'est pas doté de logiciel de protection, il devrait être en mesure d'inviter l'utilisateur à installer un tel logiciel. Si le logiciel a été installé, le smartphone devrait pouvoir rappeler à l'utilisateur qu'il doit inspecter le système à intervalles réguliers et actualiser le logiciel de sécurité, de façon à utiliser la version la plus récente.

9.2.4 Message d'avertissement concernant le compte bancaire

Si un utilisateur choisit de sauvegarder des numéros de compte ou des mots de passe lorsqu'il utilise des fonctions de paiement sur mobile, le smartphone devrait pouvoir le prévenir qu'il n'est pas recommandé de sauvegarder des numéros de compte ou des mots de passe dans le smartphone.

9.2.5 Surveillance du trafic Internet sur les smartphones

Le logiciel de protection de la sécurité installé sur un smartphone devrait pouvoir analyser de manière intelligente l'utilisation du trafic Internet par un utilisateur. Lorsqu'il détecte un trafic anormal sur une courte période, il devrait être à même de bloquer dès que possible le trafic suspect et inciter utilisateur à désactiver les connexions au réseau ou à cesser de naviguer sur des sites web suspects.

9.2.6 Suppression de code malveillant sur mobile

Après avoir détecté un code malveillant dans des applications ou des logiciels malveillants, le smartphone devrait être à même d'en informer l'utilisateur. Celui-ci devrait déterminer s'il y a lieu de supprimer le logiciel et signaler l'information aux autorités compétentes.

9.2.7 Utilisation sécurisée du WiFi

Pour protéger les informations PII d'un utilisateur, par exemple les numéros de compte et les mots de passe, et empêcher les attaques par intercepteur (MITM) lors de l'utilisation du WiFi, les smartphones devraient prendre des mesures visant à garantir l'utilisation sécurisée du WiFi. Ainsi, lorsqu'un utilisateur active une connexion WiFi, le smartphone devrait être en mesure d'activer automatiquement la fonction de transmission chiffrée et de la désactiver automatiquement lorsque la connexion WiFi est désactivée.

9.2.8 Mécanismes de vérification par des parties tierces

Lorsque l'utilisateur d'un smartphone utilise un paiement sur mobile ou une autre application nécessitant la connexion à un compte, le smartphone devrait prendre en charge la vérification par des

parties tierces pour l'opération de paiement, par exemple la reconnaissance vocale ou l'utilisation d'un code-image de vérification.

9.2.9 Suivi de la qualité de fonctionnement et de la consommation d'énergie

Un smartphone devrait être capable de contrôler le suivi de la qualité de fonctionnement de son unité centrale de traitement (CPU) et sa consommation d'énergie. Lorsque la qualité de fonctionnement ou la consommation d'énergie des batteries de l'unité CPU est anormale, il devrait créer une notification d'avertissement pour informer l'utilisateur.

Appendice I

Connexion de logiciels malveillants aux botnets

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

I.1 Avant-propos

Le présent Appendice a été élaboré sur la base de recherches informatiques fondées sur des travaux de recherche actuels, et non pas sur des travaux de recherche préliminaire. Des données et des rapports analytiques ont été obtenus auprès d'organismes de consultation chinois et internationaux ainsi que de sociétés de production de logiciels antivirus. Les conclusions de ces entreprises et organisations sont fondées sur des volumes considérables de données et sur une analyse de mégadonnées.

Du fait de la diversité des cultures, des habitudes culturelles, des législations, des réglementations, et des textes d'application des réglementations, les virus et les logiciels malveillants qui affectent les smartphones se propagent dans des écosystèmes et des environnements écologiques eux-mêmes différents. Pour des raisons qui leur appartiennent, les sociétés de production de logiciels antivirus auront parfois tendance à surestimer le nombre d'attaques détectées, en s'appuyant sur des définitions vagues et des perspectives d'analyse favorables. En conséquence, il se peut que les rapports établis par des sociétés et des organisations différentes contiennent des données statistiques différentes. Cependant, les principales conclusions et tendances qui se dégagent restent généralement les mêmes.

De plus: 1) un grand nombre de logiciels malveillants détectés, pour ne pas dire la totalité, présentent des caractéristiques et des fonctionnalités que les réseaux botnets pourront facilement utiliser; 2) des études relatives à l'évolution des logiciels malveillants et à l'expérience acquise concernant les smartphones donnent à penser que les botnets ciblant des smartphones constituent une menace à brève échéance; 3) à l'heure actuelle, en raison de la mondialisation, certains problèmes régionaux liés aux logiciels malveillants et aux botnets sur mobile risquent de s'étendre à d'autres régions et de s'aggraver à terme, d'où la nécessité de s'y préparer.

I.2 Considérations générales

L'essor rapide des smartphones constitue peut-être l'un des plus éclatants succès de notre époque. En Chine, par exemple, on dénombre aujourd'hui plus de 1,3 milliard d'utilisateurs de téléphones mobiles, dont plus de 0,68 milliard sont à la fois des utilisateurs de smartphones et des internautes.

Aujourd'hui, les smartphones sont conçus de manière à présenter le moins d'anomalies possibles, si bien que les infections par des virus ont diminué. De fait, les smartphones sont conçus de telle sorte que parmi les produits qui les composent, seule une infime partie sera compromise. Cela étant, même si le risque d'infection est faible, un téléphone infecté risque d'entraîner des pertes intolérables et irréversibles pour un utilisateur, en ce sens que les informations PII les plus importantes, telles que les numéros de compte bancaire, les mots de passe, l'adresse du domicile et des photos de famille seront peut-être stockées sur son smartphone.

En raison du succès grandissant des smartphones, les virus et les logiciels malveillants, qui affectaient auparavant essentiellement les ordinateurs personnels, visent à présent les smartphones, devenant ainsi la cible principale des attaques des pirates informatiques. De surcroît, la plupart des cyberdélits dont sont victimes les smartphones n'ont pas pour motivation l'intérêt personnel et la curiosité, mais plutôt l'appât du gain (rançons et fraude financière). Les activités cybercriminelles ont pour toile de fond un "secteur gris" de la fraude sur Internet qui n'est guère susceptible d'évoluer à brève échéance. De plus, l'Internet des objets (IoT) permet de connecter des terminaux intelligents pour assurer la transmission et le partage efficaces de données et d'informations. D'après des travaux de recherche menés récemment par Gartner [b-Gartner], on dénombrera plus de 4,9 milliards de dispositifs connectés via l'IoT en 2015 et 25 milliards en 2020, ce qui fera peser encore plus de menaces sur les

informations PII des utilisateurs, en ce sens qu'une seule faille/brèche/fuite dans la chaîne des flux de données, ou la collecte d'informations de fragmentation des liens de l'IoT, risque d'entraîner la divulgation des informations PII des utilisateurs et de poser de nouveaux problèmes pour la sécurité des télécommunications mobiles.

C'est pourquoi les utilisateurs de smartphones accordent désormais une attention accrue à la sécurité des télécommunications mobiles, en particulier lorsqu'ils protègent leurs informations PII. D'après la société d'analyse internationale *mSecurity* [b-mSecurity], les investissements dans la sécurité des télécommunications mobiles ont atteint 11 milliards USD en 2014 et augmenteront à un taux, de croissance composé de 20% au cours des six prochaines années [b-GNSM].

I.3 Environnement macroscopique en Chine

Des données concrètes viennent étayer la tendance à la hausse exponentielle des logiciels malveillants affectant les dispositifs mobiles.

Ainsi, en Chine, les smartphones suscitent un engouement accru depuis quelques années. D'après les études de *Qihoo 360*, l'une des principales sociétés spécialisées dans la conception de logiciels de sécurité des réseaux et de l'information en Chine, le nombre d'utilisateurs de téléphones mobiles est passé de 1 milliard en 2012 à 1,3 milliard en 2015, tandis que pendant la même période, le nombre d'utilisateurs de smartphones (cybercitoyens) est passé de 270 millions en 2012 à 680 millions en 2015.

De nombreux problèmes de sécurité se sont posés pendant cette période. En 2012, 175 000 nouveaux échantillons de logiciels malveillants sur mobile ont été détectés et des smartphones ont été infectés 71 millions de fois. En 2015, 18,7 millions de nouveaux échantillons de logiciels malveillants sur mobile ont été détectés et des smartphones ont été infectés 370 millions de fois. En raison de la fuite d'informations PII par accès WiFi gratuit, et du trafic supplémentaire généré par des scripts de logiciels malveillants, les utilisateurs se sont vus dans l'obligation de contracter une assurance pour couvrir les pertes imprévues de paiements sur mobile et faire face aux appels téléphoniques de harcèlement, à la fuite d'informations PII provenant de smartphones d'occasion, à la fuite d'informations PII due à des logiciels de réseaux sociaux et à divers messages spam. Pour qu'un smartphone fonctionne dans un environnement sain et sécurisé, il est indispensable de disposer d'une protection contre les virus et les logiciels malveillants, de contrôler le trafic, de protéger les informations PII, de surveiller le débit du réseau et de contrôler la sécurité du système WiFi. En règle générale, les sociétés spécialisées dans les logiciels de sécurité mobiles doivent coopérer étroitement avec les fabricants de smartphones, afin d'améliorer la protection et la sécurité de ces derniers.

I.4 Problèmes liés aux iPhones

Comparé à d'autres plates-formes comme Android, Apple assure pour les iPhones une meilleure maîtrise des logiciels pouvant être installés par les utilisateurs. La société Apple revendique une sécurité accrue [b-AppleSecurity], affirme qu'elle est déterminée à concevoir un écosystème de logiciels et prend des mesures dans ce sens. Apple s'est progressivement tourné vers un modèle dans lequel le matériel et les systèmes d'exploitation sont étroitement intégrés et dans lequel les utilisateurs acquièrent généralement des logiciels auprès de l'App Store officiel.

Cependant, selon certaines sources, de plus en plus de logiciels malveillants sont conçus de manière à infecter des dispositifs exploitants iOS [b-AppleThreat]. Il ressort de nouvelles études que l'augmentation rapide du nombre d'utilisateurs d'iPhones et l'essor des applications de l'iPhone vont de pair avec une confiance moindre dans la sécurité des iPhones.

XcodeGhost (détecté par Symantec sous le nom de OSX.Codgost sur les ordinateurs Mac OS X. et de IOS.Codgost sur les dispositifs exploitant le système iOS), constitue une version modifiée de l'environnement de développement Xcode et est considéré comme un logiciel malveillant. Il configure des applications afin de recueillir des informations sur les dispositifs, puis transfère les

informations sur des serveurs de commande et de contrôle (C&C). En outre, les applications contenant des chevaux de Troie sont capables de recevoir des commandes en provenance de serveurs C&C pour mener des attaques par hameçonnage (phishing). Un grand nombre d'applications créées au moyen d'XcodeGhost sont parvenues à contourner les contrôles de sécurité d'Apple et ont été hébergées sur le répertoire d'applications officiel d'Apple (App store), ce qui démontre que le processus de filtrage ne garantit pas que l'App store est exempt de logiciels malveillants. En novembre 2015, une nouvelle variante d'XcodeGhost a été repérée dans des versions non officielles d'Xcode 7, ce qui a permis aux concepteurs de créer des applications pour iOS 9.

Des études montrent que près de la moitié des utilisateurs d'iPhone ne considèrent plus que leur iPhone est d'une sécurité absolue. Il ressort d'études que près de 33% des smartphones ont été infectés, contre 23,9% pour les iPhones.

A l'heure actuelle, à la différence des téléphones Android, les téléphones Apple maîtrisent mieux l'exécution des applications /codes grâce à un mécanisme de clé d'autorisation du développeur. Une fois que ces applications/codes malveillants sont repérés sur des dispositifs Apple, Apple peut interrompre leur fonctionnement sur tous ses dispositifs en se contentant de rejeter la clé de signature du développeur.

Même si iOS constitue une plate-forme logicielle non libre, il présente des points faibles qui lui sont propres, à savoir les appels de harcèlement et le hameçonnage (phishing). C'est pourquoi en juin 2016, lors de la Conférence internationale des développeurs d'Apple (WWDC) qui s'est tenue à San Francisco, Apple a dévoilé son interface de programmation d'application (API) Ident-A-Call. Grâce à cette interface, qui montre combien la sécurité mobile est une question cruciale, les utilisateurs d'iPhone recevront moins d'appels téléphoniques de harcèlement et seront moins exposés au hameçonnage (phishing).

I.5 Exemples de nouveaux logiciels malveillants et évolution

I.5.1 Exemple 1

Si les logiciels utilisés dans les réseaux sociaux et les logiciels destinés aux paiements sur mobile deviennent de nouvelles cibles pour les virus et les logiciels malveillants, c'est principalement parce qu'ils sont étroitement liés et qu'ils prennent de plus en plus d'importance dans la vie quotidienne de tout un chacun.

Un logiciel malveillant connu sous le nom de "*a.privacy.BankSteal.a*" se fait passer pour une application logicielle pour réseaux sociaux portant le même logo connu, d'où la difficulté pour les utilisateurs de différencier le logiciel malveillant du logiciel légitime. Après qu'un smartphone a été infecté, le logiciel malveillant induit en erreur l'utilisateur en introduisant des informations PII – numéros de carte bancaire, mots de passe, noms d'utilisateur, numéros de carte d'identité et numéros de téléphone par exemple –, puis commence à fonctionner en arrière-plan; il intercepte ainsi les messages SMS de l'utilisateur. Le logiciel malveillant envoie ensuite ces informations aux pirates par courrier électronique. Ce logiciel malveillant compromet gravement les informations PII d'un utilisateur ainsi que la sécurité de ce qui lui appartient.

I.5.2 Exemple 2

En 2015, on a constaté dans toutes les régions une utilisation croissante des smartphones pour les services bancaires en ligne. Un grand nombre d'organismes proposent à présent une application Android qui utilise une authentification à deux facteurs (2FA), ce qui a encore accéléré la propagation des logiciels malveillants sur mobile [b-FinancialThreat].

La méthode d'attaque la plus répandue consiste à intercepter des messages textuels faisant partie du processus 2FA, puis à les retransmettre au serveur C&C du logiciel malveillant qui sera utilisé par l'auteur de l'attaque. Comme cela est généralement le cas des logiciels malveillants sur Android, l'application demande l'autorisation de recevoir, d'écrire et d'envoyer des messages textuels, ainsi que plusieurs autres autorisations pendant la phase de son installation.

Dans un système 2FA type, le deuxième facteur, qui est généralement un code secret créé pour un usage unique (OTP), est envoyé par SMS au numéro de mobile enregistré d'un utilisateur. Pour améliorer la sécurité de la fourniture du code OTP, certaines organisations financières ont commencé à fournir des codes OTP par appel vocal, et non plus par SMS. Au dernier trimestre de 2015, une nouvelle variante d'*Android.Bankosy* est apparue. Il s'agit d'une menace sur Android qui dérobe des informations et qui est capable de tromper les systèmes 2FA utilisant des appels vocaux. Le serveur C&C de la menace peut charger le smartphone affecté de retransmettre tous les appels en utilisant un code de service spécial.

L'utilisation de fausses applications bancaires autonomes constitue un autre type d'attaque de plus en plus répandu. Ces applications peuvent paraître tout à fait crédibles pour les utilisateurs, par exemple lorsqu'un logiciel malveillant sur mobile se fait passer pour un jeton 2FA légitime. L'aspect le plus inquiétant de ce type d'application malveillante est qu'elle demande à l'utilisateur le nom de son compte et son mot de passe pendant la phase d'installation, obtenant ainsi toutes les informations nécessaires pour escroquer l'utilisateur, ce qui peut conduire à des fraudes sur les comptes bancaires, sans qu'un ordinateur portable infecté ait été utilisé. Dans d'autres cas, les auteurs d'attaques remplacent des logiciels bancaires sur mobile légitimes et déjà installés par leur propre logiciel malveillant. Une autre menace sur Android, appelée *Android.Fakelogin,* s'appuie sur des techniques souples d'ingénierie sociale pour dérober des données d'identification bancaire à un grand nombre d'utilisateurs. Au lieu de se faire passer pour une application spécifique, *Android.Fakelogin* identifie l'application bancaire qui fonctionne sur le dispositif de l'utilisateur et superpose une page de connexion frauduleuse personnalisée sur l'interface de l'utilisateur. Pour ce faire, elle a accès à un programme de logique basé sur le nuage qui est hébergé sur un serveur C&C distant, afin de déterminer la page de hameçonnage (phishing) exacte à afficher. Si l'utilisateur essaie de se connecter par l'intermédiaire de la page frauduleuse, ses justificatifs d'identité pour la connexion seront directement envoyés au serveur C&C de l'auteur de l'attaque. Même si le logiciel malveillant cible des applications légitimes disponibles sur Google Play, les applications qui téléchargent *Fakelogin* ne sont pas disponibles sur Google Play.

I.5.3 Exemple 3

L'une des nombreuses tendances nouvelles qui se dégagent est que les nouveaux logiciels malveillants sont de plus en plus trompeurs et complexes lorsqu'il s'agit d'exercer un chantage sur les utilisateurs de smartphones. Ainsi, depuis 2014, des logiciels malveillants de plus en plus nombreux ciblent des utilisateurs actuels par le biais d'attaques d'homologue à homologue (P2P).

Un logiciel malveillant appelé "*a.rogue.SimpleLocker.a*" oblige l'utilisateur d'un smartphone à exécuter le logiciel malveillant en tant que priorité absolue puis verrouille fréquemment l'écran du smartphone. L'utilisateur du smartphone est tenu de payer pour le déverrouillage de l'écran, faute de quoi aucune autre application ne pourra être exécutée sur le smartphone. En arrière-plan, le logiciel malveillant est connecté via l'Internet et pourra déverrouiller à distance l'écran une fois le paiement effectué. Le logiciel malveillant ne se dissimule plus, devient sans scrupule et a l'audace de faire chanter les utilisateurs pour obtenir une rançon. Plus le nombre de smartphones infectés sera important, plus les gains seront élevés pour les auteurs d'attaques.

I.6 Conclusion

Parallèlement au développement rapide de l'Internet sur mobile, les smartphones sont dotés de fonctionnalités de plus en plus performantes en matière d'intelligence et de qualité de fonctionnement. L'essor rapide de l'utilisation des smartphones constitue peut-être l'un des succès les plus éclatants de notre époque et il ressort d'études que les botnets prenant pour cible des ordinateurs personnels (PC) sont en train de se développer très rapidement en ciblant les smartphones. La vitesse à laquelle se propagent les virus et les logiciels malveillants est aussi spectaculaire que ne l'est l'utilisation croissante des smartphones. En conséquence, les mesures destinées à lutter contre les botnets ciblant des smartphones seront à la fois d'ordre pratique et tournées vers l'avenir.

Bibliographie

[b-UIT-T X.1205] Recommandation UIT-T X.1205 (2008), *Aperçu général de la cybersécurité*.

[b-UIT-T X.1252] Recommandation UIT-T X.1252 (2010), *Termes et définitions de base relatifs à la gestion d'identité*.

[b-UIT-T X.1546] Recommandation UIT-T X.1546 (2014), *Enumération et caractérisation des attributs de logiciels malveillants*.

[b-UIT-T X-Sup.8] Recommandations UIT-T de la série X − Supplément 8 (2010), UIT-T X.1205 − *Supplément sur les bonnes pratiques de lutte contre les menaces liées aux botnets*.

[b-AppleSecurity] Page web: *Apple Claims Better Security with iOS 9, Gets Hacked before Its Release*, 13 septembre 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, 11 février 2016.

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

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

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

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

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, 2018