OPÉRATION « SAFETY-NET » (FILET DE SÉCURITÉ)

MEILLEURES PRATIQUES FACE AUX MENACES EN LIGNE, MOBILES ET DE TÉLÉPHONIE

Preparé par le groupe
Malware and Mobile
Anti-Abuse Working Group (M^3AAWG)
et
LONDON ACTION PLAN (LAP)

Le 1ier juin, 2015
(in French)

PRÉAMBULE

En octobre 2011, les membres du Plan d'action de Londres (LAP) et du Groupe de travail anti-abus pour la messagerie, les programmes malveillants et les mobiles (M^{3}AAWG) ont présenté un exposé au Comité de la politique à l'égard des consommateurs (CCP) de l'OCDE concernant les perspectives qui se dessinent actuellement dans les recommandations antispam de l'OCDE face aux menaces futures en ligne.

Lors de la réunion, un délégué canadien du LAP a noté que bien que l'ensemble actuel de recommandations antispam de l'OCDE ait donné d'excellents résultats en mobilisant l'industrie et les gouvernements pour intervenir et lutter contre le courrier indésirable (spam), il serait bénéfique de s'employer à mieux comprendre la prochaine génération de menaces en ligne, plus sophistiquée. S'appuyant sur un suivi initial avec le délégué canadien du CCP et le président du CCP, l'organisme de coordination national contre le spam d'Industrie Canada a préparé le plan général d'un rapport qui sera élaboré par des membres bénévoles du M^{3}AAWG et du LAP. Ce plan a été partagé avec les membres du M^{3}AAWG et du LAP qui l'ont approuvé, et puis examiné par le Secrétariat du CCP.

Le 6 juin 2012, les membres du LAP et du M^{3}AAWG se sont réunis à Berlin pour entamer le processus d'élaboration du rapport qu'ils ont publié en octobre de la même année. Trois ans plus tard, ce rapport a été mis à jour pour le garder fidèle au contexte en évolution et refléter les nouvelles méthodes que pratiquent les cybercriminels pour éviter la détection.

Le rapport original est divisé en quatre sections principales, à savoir :

i) les programmes malveillants et les réseaux zombies,
ii) les FSI et le DNS,
iii) l'hameçonnage et l'ingénierie sociale, et
iv) les menaces mobiles.

Cette deuxième version du rapport comprend une mise à jour des quatre sections originales, et couvre de nouveaux domaines, dont la fraude liée au protocole voix sur IP (VoIP) et à la téléphonie vocale, la mystification de l'identité de l'appelant, les problèmes d'abus d'hébergement et de services en nuage, ainsi que le harcèlement en ligne.

Le processus de mise à jour de ce rapport des meilleures pratiques impliquait l'invitation des dirigeants du M^{3}AAWG et du LAP pour solliciter leur contribution au présent rapport. Les experts de l'industrie choisis comme chefs de section se sont également employés à obtenir des commentaires et des contributions d'experts en dehors des membres du M^{3}AAWG et du LAP. Une liste des collaborateurs se trouve à la fin du rapport.

Le M^{3}AAWG, le LAP et la CAUCE (la Coalition contre le courrier commercial indésirable) ont officiellement approuvé ce rapport. En outre, les contributeurs sauraient gré au Comité de la politique à l'égard des consommateurs (CCP) de l'OCDE, son Groupe de travail sur la sécurité de l'information et la vie privée (GTSIVP) et le Comité de l'information, des communications et de la politique informatique (ICCP) de leur fournir des commentaires sur ce rapport. Le cas échéant, les contributeurs se féliciteraient d'une collaboration supplémentaire concernant cette initiative dans d'autres instances.

TABLE DES MATIÈRES

RÉSUMÉ ANALYTIQUE

Le lecteur trouvera dans ce rapport un exposé en langage clair des menaces qui pèsent sur les entreprises, les fournisseurs de réseaux et les consommateurs dans le contexte des menaces en ligne et mobiles. Comme bon nombre d'entre nous le savent, les technologies mobiles et de l'Internet ont été des moteurs clés de l'économie mondiale au cours des vingt dernières années. Ces technologies touchent presque tous les aspects de notre vie quotidienne et sont incorporées dans presque tous les modèles commerciaux et toutes les chaines logistiques. Nos ordinateurs portables, smartphones et tablettes se sont vus intégrés dans nos vies personnelles et professionnelles quotidiennes, si bien que notre dépendance vis-à-vis de ces dispositifs a augmenté. Nous utilisons ces appareils pour nous connecter à la famille et les amis, des magasins et des banques en ligne, pour interagir avec des organismes civiques et des élus, des partenaires et des collègues, pour rationaliser les chaines logistiques et livrer des produits en temps voulu des usines aux points de vente.

La croissance de la dépendance du consommateur et des entreprises et la migration rapide des transactions commerciales à des plateformes en ligne et mobiles s'accompagnent des menaces de cybercriminels. Les cybercriminels profitent de l'envoi de courrier indésirable, de l'hameçonnage, de l'injection de programmes malveillants sur les sites Web, de la diffusion de réseau zombie, de la redirection du trafic Internet vers des sites malveillants, du piratage de nuage et services d'hébergement et de l'insertion d'espiogiciels sur les ordinateurs et les appareils mobiles.

L'impact économique de ces attaques incessantes n'est pas facilement mesurable, que ce soit par pays ou à l'échelle mondiale, car les pertes dues à la cybercriminalité souvent ne sont pas signalées ou passées sous silence par les victimes, par les institutions financières qui couvrent les frais de la perte, ou par les entreprises qui supportent le cout de la protection et de l'élimination ou subissent les interruptions de service en raison des attaques.

Ce rapport cherche non seulement à examiner les menaces à l'environnement en ligne et VoIP auxquelles sont confrontés les consommateurs, les entreprises et les gouvernements tous les jours, mais surtout à proposer de meilleures pratiques à l'industrie et aux gouvernements afin qu'ils puissent mieux contrer ces menaces. Le rapport est axé sur cinq domaines principaux :

PROGRAMMES MALVEILLANTS ET RÉSEAUX ZOMBIES

Les programmes malveillants et les réseaux zombies comptent parmi les plus graves menaces à l'économie numérique. Les criminels créent ou utilisent des programmes malveillants, dits également « malware », pour perturber les opérations informatiques, pour recueillir des renseignements de nature délicate, ou pour accéder à des systèmes informatiques privés. Les réseaux zombies sont des groupes d'ordinateurs infectés par des programmes malveillants qui communiquent (souvent par le biais d'un réseau complexe d'ordinateurs infectés) afin de coordonner leurs activités et de collecter les informations recueillies par les différentes infections dues aux programmes malveillants. Un réseau zombie exploite la puissance informatique et les capacités de bande passante impressionnantes associées au contrôle de plus d'un million d'ordinateurs.

Les criminels modifient ou transforment en permanence leurs programmes malveillants pour éviter leur détection et leur élimination. Il s'ensuit que la plupart des logiciels antivirus ont du mal à identifier les menaces émergentes et relativement récentes. De plus en plus de programmes

malveillants peuvent détecter qu'ils sont « surveillés », peut-être par un chercheur de virus, alors qu'ils s'exécutent et modifieront leurs caractéristiques pour se rendre impossibles à détecter par les experts de programmes malveillants ou rendre leurs fonctions impossibles à analyser. Certains programmes malveillants réagiront aux tentatives de surveillance et d'analyse par une contrattaque au moyen d'un déni de Service distribué (DDOS).

De fait, il devient de plus en plus difficile pour la communauté en ligne de suivre le rythme de l'environnement des menaces de logiciels malveillants.

HAMEÇONNAGE ET INGÉNIERIE SOCIALE

L'hameçonnage désigne les techniques utilisées par des acteurs malveillants pour inciter une victime à révéler des données personnelles, commerciales ou financières de nature délicate.

La fréquence, la sophistication et les dégâts de l'hameçonnage n'ont cessé d'augmenter depuis que celui-ci a émergé au nombre des menaces vers le milieu des années '90, et se poursuivent au même rythme. En réalité, l'hameçonnage ne fait que grimper depuis 2011 : presque le quart des destinataires ouvrent les courriers hameçons et plus de 10 % cliquent sur des pièces jointes malveillantes. Le type des données recherchées par l'hameçonnage est devenu de plus en plus utile, évoluant d'un simple accès au courriel et aux comptes bancaires du consommateur qui subirait des pertes estimées à des milliers de dollars pour viser des cibles de grande valeur actuellement.

Ces cibles-là, à savoir les comptes de sociétés qui contiennent des secrets industriels ou ceux qui accordent des privilèges spéciaux relatifs à des comptes bancaires ou financiers, ont été souvent exploitées, de manière persistante. Conséquence : des pertes financières qui s'élèvent à des centaines de millions de dollars, des cas catastrophiques d'atteinte à la propriété intellectuelle, et un nombre incalculable de ces évènements qui surviennent chaque année.

L'hameçonnage n'est pas nouveau, mais sa recrudescence, le choix des cibles et la sophistication des méthodes utilisées pour les attaques ces dernières années représentent une menace croissante aux entreprises, aux gouvernements et aux consommateurs et mine la confiance en l'économie numérique. Les moyens de défense doivent être coordonnés pour tirer parti de solutions ouvertes, transparentes et multipartites, en maximiser l'efficacité, en réduire les couts et renforcer la confiance publique.

CODES MALVEILLANTS QUI EXPLOITENT LES FAILLES DES PROTOCOLES INTERNET ET DU SYSTÈME DE NOM DE DOMAINE

De multiples activités illégales exploitent les vulnérabilités du système de nom de domaine (DNS) et des adresses du protocole Internet (IP). Les codes malveillants les plus graves de ceux qui exploitent les vulnérabilités du DNS sont les exploitations de résolveur ou la pollution de cache DNS, par le biais desquels des acteurs malveillants introduisent des données falsifiées pour rediriger le trafic Internet vers des versions falsifiées de sites Web populaires.

Chaque ordinateur connecté à l'Internet possède une adresse IP qui permet de l'identifier de la même manière que les téléphones sont identifiés par leur numéro de téléphone. Les adresses IP traditionnelles, dites des adresses IPv4 (Protocole Internet version 4), sont constituées de nombres binaires codés sur 32 bits, exprimés par quatre nombres décimaux de la manière suivante 64.57.183.103. La première partie de l'adresse, dans ce cas précis 64.57.183, indique souvent le réseau, et le reste de l'adresse, en l'occurrence 103, identifie un ordinateur particulier (« hôte ») sur

le réseau. La division entre le réseau et l'hôte varie en fonction de la taille du réseau, donc l'exemple ci-dessus n'est que typique. Étant donné qu'il peut être difficile aux personnes de se souvenir des adresses IP et que celles-ci sont liées à des réseaux physiques, le DNS est une base de données distribuée contenant des noms et permettant à une personne d'utiliser un nom comme www.google.com à la place de l'adresse IP correspondante 173.194.73.105.

Malgré sa taille énorme, le DNS offre une excellente performance grâce à des caches et des délégations. Autrement dit, différentes organisations sont responsables chacune pour sa part du système des noms de domaine, et des sites finaux me souviennent de résultats récents qu'ils ont reçus du DNS. Parce qu'il serait impossible de stocker tous les noms en une seule base de données au sein du DNS, il est divisé en zones stockées sur des serveurs différents, mais reliées logiquement dans une immense base de données distribuée interopérable.

Les codes malveillants qui exploitent les failles du DNS et des adresses IP présentent des risques élevés, car, dans bien des cas, les consommateurs ignorent totalement qu'ils sont redirigés vers un faux site au lieu du site qu'ils souhaitent visiter.

MENACES MOBILES, DE TÉLÉPHONIE ET DE VOIP

L'environnement du commerce électronique s'est développé avec l'apparition du smartphone et des marchés d'application pour Android, Apple, Windows et BlackBerry, pour inclure les appareils mobiles. Il va sans dire que les consommateurs ayant migré leurs activités de commerce électronique vers les plateformes mobiles, les acteurs malveillants dans leur chasse effrénée de profit et de fraude se sont empressés de faire de même. En outre, l'environnement mobile crée des opportunités uniques donnant lieu à de nouveaux types d'attaques et de menaces ciblant les consommateurs et les entreprises.

Les appareils mobiles offrent aux consommateurs des fonctionnalités accrues et une facilité d'utilisation. Ils sont souvent portés par des utilisateurs individuels, typiquement gardés à l'état actif, dotés du GPS et conscients de leur emplacement. C'est pour cela que les attaques malveillantes trouvent immanquablement plus attrayants les appareils mobiles.

L'environnement mobile a connu ces dernières années un développement accru des programmes malveillants, le premier réseau zombie mobile, des arnaques par message SMS facturés au prix fort, et des codes malveillants exploitant des failles du système associés au débridage (déverrouillage d'un appareil pour éliminer les restrictions imposées par une source officielle sure pour le téléchargement des applications) d'appareils mobiles.

Avec la croissance des abonnements à haut débit mobile, les menaces relatives au protocole voix sur IP (VoIP) et à la téléphonie sont à la hausse. La fréquence et la gravité des arnaques par automate d'appel sont de plus en plus marquées ; la nouvelle technologie permettant aux acteurs malveillants de cacher ou de modifier leur numéro de téléphone sortant pour tromper les cibles non averties rend ces fraudes d'autant plus efficaces. À mesure que les services téléphoniques se tournent vers l'Internet, le nombre des attaques de refus de service téléphonique augmente et elles deviennent de plus en plus fréquentes. Ces types d'attaques peuvent être dévastateurs lorsque des services essentiels sont ciblés afin que les systèmes téléphoniques soient submergés et des appels placés par des personnes légitimes essayant d'atteindre les pompiers ou une ambulance par exemple ne puissent être effectués.

Les cybercriminels marquent une nette préférence pour les environnements transnationaux, ce qui complique davantage les efforts d'application. À titre d'exemple, un vendeur illégal de pilules en ligne résidant aux États-Unis pourrait envoyer des courriels publicitaires non sollicités à partir d'un ordinateur infecté au Brésil, redirigeant les acheteurs potentiels vers un site Web dont le nom de domaine est russe, tout en hébergeant physiquement ce site en France. Le paiement des commandes par carte de crédit peut être traité par une banque en Azerbaïdjan, les commandes expédiées directement de l'Inde, et les bénéfices canalisés vers une banque à Chypre. Ce faisant, les criminels savent qu'un certain nombre de facteurs compliqueraient toute enquête officielle concernant leurs crimes en ligne, réduisant le risque de se faire prendre. Ces facteurs comprennent notamment le manque de coopération, les différences entre les juridictions, ainsi que le cout des enquêtes internationales.

HÉBERGEMENT ET NUAGE

L'hébergement désigne les prestataires de services permettant aux entreprises d'accéder à des sites Web, des fichiers et des réseaux intranet, et fournissant un accès Internet via des serveurs connectés multiples et non pas par le biais d'un serveur unique ou d'un serveur virtuel. Les hôtes sont des sociétés fournissant un espace sur un serveur qui leur appartient ou qu'ils louent et qu'ils mettent à la disposition des clients ; il se peut qu'ils fournissent également un centre de données et une connectivité Internet. Les services d'hébergement les plus ordinaires sont ceux qui hébergent un petit nombre de fichiers ou encore de sites Web. De nombreux fournisseurs de services Internet (FSI) assurent gratuitement ces services à leurs abonnés. Ces hôtes contrôlent les détails d'ordre pratique faisant fonctionner l'Internet et leur taille est variable : ils peuvent être des entreprises individuelles comme ils peuvent être des sociétés Internet multinationales.
L'informatique en nuage désigne le stockage de données et de programmes sur une infrastructure Internet ou l'accès à ces données et programmes plutôt que l'utilisation du disque dur de votre propre ordinateur pour le faire. Le nuage est une métaphore de l'Internet. Elle remonte au temps des organigrammes et des présentations qui représentaient la gigantesque ferme de serveurs qu'était l'infrastructure de l'Internet comme un nuage blanc moutonné.

Les menaces en ligne et mobiles exploitant des sources d'hébergement et de nuages se multiplient. Elles comprennent le courrier indésirable, le courriel publicitaire indésirable, l'hameçonnage, les sites piratés, les DDOS (attaques par déni de service distribué), analyse des ports à la recherche de vulnérabilités exploitables, les sites Web modifiés, les atteintes aux marques ou aux droits d'auteur et les programmes malveillants. Le présent document classe les types d'hébergement et définit les domaines particulièrement préoccupants. Il dresse le portrait des menaces actuelles à l'environnement en ligne, hébergé ou en nuage, et donne un aperçu des méthodes d'élimination employées dans le traitement de ces questions critiques.

CONCLUSION

Afin de protéger l'Internet et d'assurer son engagement envers les citoyens du monde, il est essentiel d'identifier des réponses efficaces et rationnelles à ces nombreuses menaces. Le présent rapport, soumis par un groupe international d'experts de l'industrie et des gouvernements, résume les meilleures pratiques recommandées pour aller au-devant des menaces en ligne, mobile ou téléphoniques émergentes et plus sophistiquées. Nous espérons que le présent rapport facilitera une collaboration permanente et utile entre ce groupe et la communauté internationale visant à éliminer ces menaces.

INTRODUCTION : ÉVOLUTION DES MENACES EN LIGNE

Depuis 2006, l'Internet mondial et l'économie mobile ont vu les menaces en ligne se développer et de nouvelles attaques se manifester. Les outils utilisés pour frauder et voler des informations dans l'environnement en ligne et mobile sont aujourd'hui de plus en plus sophistiqués, fournissant aux acteurs malveillants et aux fraudeurs une panoplie d'outils plus élargie.

Dans ce contexte, comme vous le trompétaient probablement souvent vos parents, mieux vaut prévenir que guérir. Le présent rapport non seulement décrit l'environnement des menaces en ligne, mobiles, ou de la téléphonie de manière qui puisse être aisément comprise, mais il fournit une liste d'outils que les gouvernements et l'industrie pourraient adopter à titre de meilleures pratiques pour empêcher que ces types de menaces se transforment en cyberattaques réussies.

Une grande partie de cette activité illicite en ligne est neutralisée avant d'atteindre des utilisateurs finaux ordinaires par les techniques de filtrage et de blocage modernes, mais le courrier indésirable demeure un véhicule important, transmettant souvent des charges malveillantes aussi bien que des messages non sollicités et dans la généralité des cas malveillants. Le spam n'est pas seulement un phénomène de courriel. Il continue à se développer dans diverses sortes de nouveaux médias. Le spam de la messagerie mobile et du protocole voix sur IP (VOIP) est désormais courant, tout comme les commentaires indésirables sur les réseaux sociaux, les blogues et les sites Web et les résultats non sollicités qui polluent et dégradent la qualité des résultats de recherche des moteurs de recherche.

Le secteur du domaine (composé principalement de la Société pour l'attribution des noms de domaine et des numéros sur Internet [ICANN], des bureaux d'enregistrement et des opérateurs de registre) peut jouer un rôle crucial dans l'espace anti abus, étant donné les nouveaux protocoles Internet (IPv6 par exemple) de plus en plus répandus et l'introduction d'un nombre considérable de nouveaux domaines de premier niveau (TLD). Auparavant, il y avait quelque 24 TLD tels que le .com, le .org, le .net, le .gov, en plus des codes de pays à deux lettres, tels que le .ca pour le Canada ou le .jp pour le Japon. L'ICANN a récemment introduit de nouveaux TLD génériques, dont le .bike, le .city, et le .clothing, des centaines étant encore dans la phase de traitement de la demande.

Nous proposons aux participants à l'OCDE et à d'autres organisations internationales de renforcer leur participation au sein de l'entité de coordination principale de l'espace du domaine, le Comité consultatif gouvernemental de l'ICANN, qui s'emploie à encourager l'ICANN pour que celle-ci redouble ses efforts et ses activités dans la conformité contractuelle et la supervision des bureaux d'enregistrement et des opérateurs de registre.

De considérables efforts ont été consacrés à l'abolition des cloisons et la facilitation des initiatives de coopération entre les entités commerciales, les gouvernements, les régulateurs et les organismes chargés d'appliquer la loi. L'OCDE, le LAP, le M^{3}AAWG et d'autres organisations internationales ont été efficaces dans le développement de la coordination public-privé existante et la collaboration interorganisationnelle. Par exemple, le Groupe de travail sur le virus DNS Changer (DNS Changer Working Group)[1] et le Groupe de travail sur le virus Conficker (Conficker Working Group)[2] sont des amalgames d'experts techniques, d'agents d'application de la loi, et de représentants de l'industrie, qui ont obtenu de très bons résultats en appliquant un modèle de confiance mutuelle et en mettant de côté leurs préoccupations au regard de la concurrence. Le succès de cette collaboration s'est trouvé confirmé ; elle demeure de la plus haute importance dans la lutte contre les abus.

Cependant, une législation antispam et anti abus, plus complète, plus rigoureuse et technologiquement neutre ainsi que des régimes de règlementation facilitant la coopération transfrontalière demeurent nécessaires. Une partie de la solution réside peut-être dans la sphère diplomatique, en particulier lorsqu'il s'agit de favoriser des activités d'application de la loi plus performantes au niveau transfrontalier. Une sensibilisation et une information mieux conçues de l'utilisateur final sont des aspects qui comptent pour la mise en œuvre de mesures anti abus performantes.

PROGRAMMES MALVEILLANTS ET RÉSEAUX ZOMBIES

Les programmes malveillants, dits également « malware », sont créés ou utilisés par les criminels pour perturber les opérations informatiques, pour recueillir des renseignements de nature délicate, ou pour accéder à des systèmes informatiques privés. Ils peuvent prendre des formes diverses allant des programmes compilés jusqu'aux scripts, en passant par les bits de code insérés dans des logiciels par ailleurs légitimes. L'expression « Programme malveillant » désigne de manière générale plusieurs formes de logiciel hostile, importun ou agaçant. Les programmes malveillants comprennent généralement les virus, les vers, les chevaux de Troie, les injecteurs, les espiogiciels, les logiciels de publicité, les rootkits, les programmes produisant du spam, ainsi que d'autres programmes malveillants. Un programme malveillant est conçu pour remplir une ou plusieurs fonctions, allant de la facilitation de l'introduction d'autres programmes malveillants (injecteurs/téléchargeurs) à la collecte d'informations (espiogiciels). D'autres programmes malveillants peuvent se spécialiser dans la perturbation de réseaux, d'utilisateurs et d'ordinateurs.

Les réseaux zombies sont des groupes d'ordinateurs infectés par des programmes malveillants similaires qui communiquent (souvent par le biais d'un réseau complexe de taille moyenne d'ordinateurs infectés) afin de coordonner leurs activités et de collecter les informations recueillies par les différentes infections dues aux programmes malveillants. Les réseaux zombies portent le plus souvent le nom du programme malveillant spécifique qui applique et coordonne cette communication, par exemple, Zeus et SpyEye. Toutefois, chaque machine dans un réseau zombie peut contenir une variété de composants malveillants. Un nœud d'un réseau zombie Zeus pourrait contenir le programme malveillant Zeus (pour coordonner la communication du réseau, le vol de données et le téléchargement de programmes malveillants supplémentaires), ainsi que d'autres menaces telles que des programmes produisant du spam (tels que Cutwail) ou des éléments « attaque » (tels que Pushdo et des programmes malveillants DDOS).

Un réseau zombie peut être assez large. Certains composés de plus d'un million de machines ont été observés, contrôlés par un seul botmaster. Il n'est toutefois pas nécessaire qu'un réseau zombie soit aussi large pour être extrêmement préjudiciable. Même un réseau zombie composé de 1000 ou 2000 nœuds (ordinateurs) peut causer des ravages massifs.

À leurs débuts, les programmes malveillants étaient le plus souvent mis au point par des amateurs, des personnes ayant des compétences en informatique et qui souhaitaient se distraire ou cherchaient de nouveaux défis. Depuis, les criminels, et de plus en plus le crime organisé, ont réalisé que le domaine des programmes malveillants peut générer des bénéfices financiers de taille. Le cas du WinFixer illustre cela parfaitement : les criminels ont essayé d'amener les victimes, en leur faisant peur, à payer les frais d'enregistrement de logiciels[3]. Dans l'état actuel des choses, tous les logiciels malveillants sont pratiquement créés et utilisés à des fins criminelles. Dans une moindre mesure, les programmes malveillants pourraient également être commandités par des États et utilisés par des agences de renseignements pour mener des actions secrètes contre les systèmes informatiques d'autres États ou espionner des militants, des journalistes et des dissidents ou utilisés par des hacktivistes et des extrémistes à des fins idéologiques, politiques ou sociales.

Les programmes malveillants représentent l'une des principales menaces à l'économie numérique et sont utilisés pour mener les activités suivantes :

- capturer des données personnelles ou commerciales en :
    - enregistrer les frappes
    - collecter des identifiants et des mots de passe
    - copier des carnets d'adresses
    - voler des renseignements confidentiels d'entreprise, des documents, ou des secrets industriels et même capturer des informations gouvernementales ou militaires de nature délicate
    - collecter des renseignements bancaires et transactionnels
- faciliter des attaques DDoS catastrophiques visant, entre autres, des nations, ou dans le cadre d'un activisme politique, ou comme prélude à l'extorsion de fonds
- Envoyer du courrier indésirable par courriel, par SMS ou par d

Les criminels modifient en permanence leurs programmes malveillants pour éviter leur détection et leur élimination. La plupart des antivirus (A/V) ont un bilan lamentable quand il s'agit d'identifier les menaces actuelles et récentes. De plus en plus de programmes malveillants peuvent détecter qu'ils sont « observés » (peut-être par un chercheur de virus) et modifieront leurs comportements pour rendre impossible aux chercheurs et analystes d'analyser leur fonctionnement. Certains programmes malveillants tenteront même de décourager leur surveillance en contrattaquant par un DDOS les chercheurs et les analystes. De fait, il devient de plus en plus difficile pour la communauté en ligne de suivre le rythme auquel évoluent les menaces des programmes malveillants.

PAYSAGE ACTUEL DES MENACES LIÉES AUX PROGRAMMES MALVEILLANTS ET AUX RÉSEAUX ZOMBIES

Le paysage n'a pas changé et il est improbable qu'il le fasse. La réticence générale des gouvernements, des banques et des sociétés à partager des données privées ou confidentielles, entravées par des obstacles juridiques et règlementaires réels ou perçus ou par la crainte d'une responsabilité, signifie que les producteurs de programmes malveillants continuent à avoir le dessus et livrer avec précision leurs produits. Il est impossible de mesurer rigoureusement l'ampleur du problème, car il n'existe pas d'indicateurs universellement reconnus pour la détection des infections par programmes malveillants, des bots ou des réseaux zombies.

Dans les programmes malveillants transmis par courriel, les textes mal orthographiés et invraisemblables ont été remplacés par de nouvelles techniques d'hameçonnage dont il sera question plus loin dans le présent rapport. Bien que le volume mondial du spam ait baissé ces dernières années, les techniques de « clickjacking » ou de « likejacking » sont de plus en plus courants sur les réseaux sociaux ; un utilisateur clique sur le lien d'un site Web pour visionner une vidéo qui le tente et l'attaquant utilise ce clic pour envoyer des commentaires à tous les amis de l'utilisateur sur Facebook et les inciter à cliquer ce même lien malveillant. Facebook a, dans une large mesure, remédié à cette attaque en demandant à l'utilisateur de confirmer un « aimer » avant sa publication lorsque le domaine « aimé » n'est pas fiable.

En ce qui concerne les programmes malveillants transmis sur le Web, Symantec[4] a conclu que les attaques basées sur le Web ont augmenté de 23 % en 2013 et que sur 8 sites Web, un site présentait de graves vulnérabilités. Cela signifie que les attaquants s'efforcent de contourner les contremesures de sécurité en transmettant les programmes malveillants à l'aide du Web plutôt que de les attacher à un courriel.

Les menaces contre les systèmes d'exploitation OSX et iOS de Apple, bien que relativement peu nombreuses, illustrent bien la propagation des programmes malveillants vers des plateformes qui étaient jusqu'à présent plus ou moins exemptes de programmes malveillants. Les méthodes que les attaques utilisent sont similaires à celles qui sont observées sur les plateformes Windows et Android. Le fait que de nombreux outils d'attaque sont devenus multiplateformes, utilisant des vulnérabilités Java, par exemple, constitue en lui-même une nouvelle méthode de propager les programmes malveillants.

PAYSAGE FUTUR DES MENACES LIÉES AUX PROGRAMMES MALVEILLANTS ET AUX RÉSEAUX ZOMBIES

D'après le rapport de prédiction des menaces préparé par McAfee[5], les programmes malveillants pour appareils mobiles seront en 2015 des agents de croissance, tant pour leur innovation technique que pour le volume des attaques sur le « marché » des programmes malveillants. Les attaques malveillantes de type rançongiciel se multiplient de plus en plus, stimulées par la croissance de la devise virtuelle. Le déploiement d'un nombre grandissant d'applications d'entreprise reposant sur l'informatique en nuage devrait également engendrer de nouvelles surfaces d'attaque qui les cybercriminels pourraient exploiter.

Enfin, on voit mal dans les prochaines années des menaces qui seraient plus considérables que celles posées par l'Internet des objets. Au fur et à mesure que des milliards d'appareils se connectent à l'Internet, la menace à l'infrastructure fondamentale augmente, étant donné les périphériques non patchés ou par définition vulnérables. Il est probable que de nombreux appareils connectés ne recevront pas régulièrement de correctifs ; certains fournisseurs ne considèrent pas que la sécurité fait partie de leur responsabilité et accordent la priorité à la prochaine version de leur produit ou se concentrent davantage sur les aspects esthétiques ou pratiques.

Les consommateurs ne feraient peut-être pas pression sur les fournisseurs de matériel en ce qui a trait aux correctifs. Si, par exemple, un appareil fonctionne de façon satisfaisante, que ce soit entre autres un réfrigérateur, une ampoule ou un thermostat, mais que sa cyberfonctionnalité l'expose à des problèmes de sécurité, les consommateurs peuvent ne pas être motivés à le remplacer pour cette seule raison. La longue queue des appareils vulnérables continuera donc à s'alourdir.

MEILLEURES PRATIQUES POUR COMBATTRE LES PROGRAMMES MALVEILLANTS

Bien que la majeure partie du contenu de cette section met l'accent sur la sensibilisation des particuliers et des FSI, il faut reconnaitre que la lutte contre les programmes malveillants est problématique à l'échelle de l'écosystème et nécessitera une approche et des mesures à volets multiples de la part de différentes parties, et ne se limite pas aux FSI ou à la sensibilisation de l'utilisateur final.

Pour les gouvernements et les éducateurs, la présente section porte sur la prévention, la détection et l'élimination des programmes malveillants. Pour les FSI, cette section vise à fournir des conseils sur ce qu'un FSI peut faire pour aider les particuliers à détecter un programme malveillant. La section se termine par une discussion des aspects juridiques et règlementaires concernant les programmes malveillants, qui intéresseraient les gouvernements, ainsi que les meilleures pratiques de l'industrie.

MEILLEURES PRATIQUES POUR LES ÉDUCATEURS ET LES UTILISATEURS

A) Meilleures pratiques : Prévention

Ces recommandations sont axées sur la manière dont un particulier peut éviter d'être infecté par des programmes malveillants.

1. **Choisir un système d'exploitation sécurisé et actuel :** Lorsque vous choisissez un système d'exploitation (OS), cherchez celui qui propose des capacités éprouvées pour réduire votre exposition aux programmes malveillants. Quel que soit le système d'exploitation choisi, assurez-vous d'exécuter sa version la plus récente. Les systèmes d'exploitation modernes ont des mesures d'atténuation prédéfinies qui aident à protéger contre les attaques des programmes malveillants visant à compromettre un système.
2. **Exécutez les correctifs de sécurité et les mises à jour :** Assurez-vous que les systèmes d'exploitation et toutes les applications, y compris les applications auxiliaires (telles qu'Acrobat Reader, Flash Player, Java, et QuickTime) sont entièrement patchées (c.-à-d. que toutes les mises à jour ont été téléchargées au fur et à mesure qu'elles sont devenues disponibles) et actualisés. La plupart des failles exploitées par les programmes malveillants ont des correctifs disponibles depuis plus d'un an. Microsoft recommande de nombreux téléchargements pour les systèmes fonctionnant sous Microsoft Windows.[6] Secunia PSI[7] est également un outil populaire qui permet de garder à jour les applications tiers.
3. **N'utilisez que ce dont vous avez besoin** : En général, il est conseillé de ne télécharger ou utiliser que les logiciels qui vous sont nécessaires. Évitez de télécharger des logiciels ou des fichiers qui n'ajoutent pas de fonctionnalités utiles ou nécessaires, fonctionnalité et supprimez les logiciels non utilisés.
4. **Consultez un expert** : Demandez aux experts quel choix répond le mieux à vos besoins. (Les « experts » pourraient vous fournir des réponses différentes, mais si vous dépendez de leur soutien, suivre leurs conseils vous sera toujours plus utile.)
5. **Ayez recours à un antivirus** : Bien que les produits antivirus ne sont pas toujours parfaits, ils peuvent aider, donc choisissez-en un et utilisez-le, gardez-le à jour en téléchargeant les mises à jour dont vous serez notifié. Prévoyez une analyse complète de votre système au moins une fois par semaine. Veillez à choisir un véritable antivirus, et évitez d'être trompé en installant un faux antivirus qui serait lui-même un programme malveillant. (Si votre antivirus ne vous protège pas également contre les espiogiciels, installez également un logiciel anti espion.)
6. **Utilisez un pare-feu** : Bien que les pare-feux ne soient pas infaillibles, qu'ils soient à base de matériel ou de logiciel, ils permettent d'ajouter, du moins potentiellement, une protection supplémentaire.
7. **Utilisez des mots de passe forts** : Les mots de passe devraient être suffisamment complexes pour résister aux renifleurs et au craquage. Certaines personnes choisissent des mots de passe d'au moins huit caractères, comprenant un mélange de majuscules, de minuscules, de chiffres et de symboles spéciaux. D'autres préfèrent un ensemble de trois à

cinq mots indépendants, plus faciles à retenir et plus difficiles à renifler. Quoi qu'il en soit, n'utilisez pas le même mot de passe sur plusieurs sites. Certaines applications pour les mots de passe facilitent ce processus.[8]

8. **Effectuez régulièrement des sauvegardes** : Si votre système est infecté, une sauvegarde non infectée peut s'avérer extrêmement utile pour nettoyer votre système et le remettre en ligne.
9. **Nettoyez les fichiers temporaires dont vous n'avez plus besoin** : Certains programmes malveillants peuvent cacher des copies parmi vos fichiers temporaires, mais même s'il n'y a aucun fichier temporaire infecté, le simple fait de les nettoyer vous permettra d'accélérer les analyses du système et de réduire la taille de vos sauvegardes. CCleaner est un outil largement utilisé pour nettoyer les fichiers sous Windows.
10. **N'exécutez pas régulièrement en tant qu'administrateur** : Les comptes « administrateur » ou « racine » disposent de privilèges qui ne devraient être utilisés que lorsque vous faites quelque chose qui requiert les privilèges associés à ces comptes à haute performance (l'installation volontaire de nouveaux logiciels, par exemple). Pour les tâches normales, utilisez un compte normal.
11. **Désactivez JavaScript (ou utilisez NoScript**) : JavaScript (un langage de script qui, nonobstant son nom, n'est pas apparenté à Java) permet de nombreuses applications interactives passionnantes ; toutefois, il est également largement exploité et il est utilisé pour injecter des programmes malveillants dans les systèmes vulnérables. Si vous n'avez pas besoin de JavaScript, ne l'activez pas dans votre navigateur.
12. **Bloquez les noms de domaine malveillants du DNS** : Certains programmes malveillants font appel à leur capacité de convertir les noms de domaines symboliques en chiffres. Si vous bloquez la conversion de ces noms via votre serveur de nom de domaine, le programme malveillant en question ne pourra s'exécuter. La société OpenDNS propose, par exemple, un tel DNS pouvant ainsi filtrer les programmes malveillants.
13. **Filtrez/éliminez le courriel potentiellement dangereux** : Votre administrateur de courriel devrait analyser les courriels qui vous sont envoyés à la recherche de pièces jointes, liens, ou contenu potentiellement dangereux. MIMEDefang est un logiciel qui pourrait, par exemple, aider à le faire.
14. **Les fichiers téléchargés via les applications P2P sont souvent infectés** : Sachez qu'un grand nombre de fichiers partagés via des services de pair à pair (P2P) sont intentionnellement ou accidentellement infectés de programmes malveillants.
15. Supposez que chaque clé USB a été « piégée » : Si quelqu'un vous donne une clé USB ou si vous en trouvez une, ne la connectez **jamais** à votre ordinateur. Il se peut qu'elle soit intentionnellement infectée de programmes malveillants et puis abandonnée où vous pourriez la trouver dans le but de placer des programmes malveillants sur votre système.
16. **Évitez d'utiliser les points d'accès Wifi inconnus** : Certains points d'accès Wifi ouverts peuvent intercepter tout le trafic non chiffré, portant potentiellement atteinte à votre vie privée. L'utilisation d'un réseau privé virtuel (VPN) pourrait vous aider à vous protéger. Veillez à ce que les points d'accès Wifi dont vous êtes responsables soient sécurisés par WPA2 (un protocole de sécurité et un programme de certificat de sécurité élaboré par l'Alliance Wifi pour sécuriser les réseaux d'ordinateurs sans fil) pour limiter l'accès.

B) MEILLEURES PRATIQUES : DÉTECTION

Ces recommandations se concentrent sur la manière de détecter les programmes malveillants si les efforts de prévention ont échoué.

1. Ne laissez pas une détection par une analyse locale vous échapper : Les analyses par antivirus demeurent l'une des méthodes de détection de programmes malveillants les plus courantes. Une option similaire consisterait à exécuter une analyse unique en utilisant un outil conçu sur mesure pour détecter et éliminer les programmes malveillants, tel que l'outil « cleanup only »[9].
2. **Si votre système commence à se comporter bizarrement, relevez-le :** Un autre indicateur important que quelque chose ne va pas est lorsque le système commence à se comporter de manière « bizarre ». Les comportements bizarres peuvent comprendre un fonctionnement lent, un blocage, l'affichage de fenêtres indésirables (p. ex., de fausses notifications d'antivirus), la demande d'une page Web qui vous emmène sur une autre, l'impossibilité d'accéder à certains sites (en particulier si ces sites sont des sites de mise à jour ou liés à la sécurité), etc.
3. **Prenez des mesures si votre FSI vous indique que votre système fait de « mauvaises » choses** : Par exemple, votre FSI peut vous avertir que votre système a été observé en train d'envoyer du spam ou d'attaquer un autre système sur Internet.

C) MEILLEURES PRATIQUES : ÉLIMINATION

Ces recommandations se concentrent sur la manière de traiter les systèmes infectés.

1. **Nettoyage en place** : Cette approche implique que l'utilisateur (ou une personne agissant à sa place) analyse avec un ou plusieurs produits antivirus le système infecté dans le but de la nettoyer (les experts peuvent supprimer certains fichiers infectés dans certains cas). Ce processus peut être laborieux et risque de ne pas fonctionner. Même après avoir consacré des efforts substantiels au nettoyage d'un système infecté, l'infection peut subsister, ou le système peut être instable ou inutilisable.
2. **Restauration** : Si l'utilisateur a une sauvegarde non infectée, une autre option consiste à restaurer cette sauvegarde non infectée. Cette option peut entrainer la perte du travail effectué depuis la dernière sauvegarde non infectée, à moins que ces fichiers soient conservés séparément et peuvent être restaurés (notez que cela, le cas échéant, doit être fait très soigneusement pour faire en sorte que la restauration de ces fichiers n'entraine pas une réinfection). De manière générale, une stratégie de restauration fonctionne mieux lorsque les sauvegardes sont fréquentes et que plusieurs générations de sauvegardes restent disponibles pour une sélection potentielle.
3. **Réinstallation complète** : Cette option implique un reformatage du système ; le système d'exploitation et les applications sont remis en place à partir de zéro. Ce processus peut être laborieux et souvent frustrant en raison du manque de support d'origine (de nombreux fournisseurs n'expédient plus une copie du système d'exploitation sur un support physique lorsqu'ils vendent du matériel informatique).
4. **Remplacer le système** : Enfin, au moins une fraction des utilisateurs peut décider tout simplement de remplacer le système infecté plutôt que d'essayer de le nettoyer. Il se peut que ce soit la seule façon de désinfecter en toute sécurité une machine. Cette option semble plus acceptable lorsque le système infecté est ancien ou n'est pas très puissant en premier

lieu, ou si l'utilisateur souhaite modifier son système d'exploitation ou passer d'un ordinateur de bureau à un ordinateur portable, par exemple. Le jargon de l'industrie pour ce type d'action est « nuke & pave ».

MEILLEURES PRATIQUES POUR L'INDUSTRIE ET LE GOUVERNEMENT

A) Meilleures pratiques de détection et de notification (FSI-utilisateur)

De nombreux FSI informent les clients s'ils sont infectés par des programmes malveillants. Les FSI peuvent utiliser différentes techniques pour aviser les particuliers d'une infection. Cette section fournit une liste de mesures que les FSI devraient prendre pour notifier les utilisateurs finaux, mais cela ne revient pas à dire que l'une de ces techniques a été identifiée comme une meilleure pratique. Chaque forme de notification comporte des avantages et des inconvénients. En voici quelques exemples :

1. **Courriel** : Quand l'infection d'un système est observée, le FSI peut notifier l'utilisateur par courrier électronique. Malheureusement, les utilisateurs souvent ne vérifient pas le courrier électronique que le FSI met à leur disposition, et l'utilisateur peut ne jamais avoir fourni au FSI l'adresse électronique qu'il utilise régulièrement. Les utilisateurs peuvent aussi devenir méfiants des notifications par courriel en raison des attaques fréquentes par hameçonnage et des arnaques de soutien Tech qui induit en erreur les consommateurs sur la présence de programmes malveillants sur leurs ordinateurs.
2. **Téléphone** : Le FSI peut notifier l'utilisateur par téléphone. En contactant le client, il est important de considérer que bien que les appels automatisés peuvent être efficaces, les utilisateurs peuvent se méfier des notifications par téléphone en raison des attaques d'hameçonnage basées sur les voix. D'autre part, l'utilisation d'un personnel pour notifier les utilisateurs est une tâche fastidieuse et laborieuse, surtout s'il faut notifier un grand nombre d'utilisateurs.
3. **Message texte** : Au cas où le FSI connait le numéro de téléphone du client, une autre option serait d'envoyer une notification par message texte aux utilisateurs.
4. **Par la poste régulière (papier)** : Un FSI peut envisager une notification de l'utilisateur par courrier postal traditionnel, peut-être via un ajout à la facture mensuelle. Toutefois, si le FSI n'envoie pas déjà de courrier postal au client, une notification ad hoc par la poste pourrait être couteuse et d'une efficacité limitée, en particulier si l'utilisateur est prédisposé à se débarrasser du courrier postal sans le consulter parce qu'il croit que ce courrier ne serait probablement que publicitaire.
5. **Tournées en camion** : Si l'utilisateur a payé pour un contrat de soutien sur place, une autre approche de la notification consisterait à lui rendre visite, en personne, sur place. Il est évident que le technicien du FSI devra être en mesure de satisfaire le client quant à ses informations d'identification, et il convient de noter que cette option peut être très couteuse.
6. **Notification en bande (Web)** : Cette démarche invite un FSI à notifier l'utilisateur en interposant un message interstitiel lorsque l'utilisateur essaie de visiter un site Web normal. Cette façon d'aborder l'utilisateur pourrait dans une certaine mesure le déconcerter, mais elle demeure moins perturbatrice que les autres approches, telles que l'approche imposant un domaine privé « walled-garden » (voir ci-dessous).
7. **Domaine privé** : Si un FSI a besoin de limiter immédiatement les dégâts qu'un utilisateur infecté peut causer, une option serait de la placer dans un soi-disant « domaine privé »

(walled-garden). Lorsque cela est fait, l'utilisateur est autorisé à accéder à des sites sélectionnés à des fins d'élimination et de sécurisation renforcée, et peut être autorisé à avoir accès au VoIP pour des choses comme les services d'urgence. De manière générale, il ne pourra cependant accéder à la plupart des autres ressources sur Internet. Il convient de souligner que cette stratégie n'est pas censée être punitive. Les domaines privés se sont révélés extrêmement efficaces pour diminuer le nombre des infections au niveau du FSI du consommateur, et semblent avoir précipité en fait le déplacement des programmes malveillants et des réseaux zombies vers les services d'hébergement.

Pour de plus amples renseignements, veuillez consulter le RFC6561 du Groupe de travail de génie Internet « Recommendations for the Remediation of Bots in ISP Networks ».[10]

La notification de l'utilisateur final ne se limite pas aux FSI. D'autres parties de l'écosystème de l'Internet en rapport avec l'utilisateur final peuvent envoyer des notifications et l'ont déjà fait dans le passé. Il a été largement diffusé que Google et Facebook ont tous les deux tenté de notifier leurs utilisateurs finaux quant à des infections potentielles associées au programme malveillant DNS Changer.

B) Meilleures pratiques pour la sensibilisation

1. **Moments « enseignables » individualisés** : si par malheur le système d'un client est infecté, ce moment serait parfaitement « enseignable », car certaines techniques pour prévenir la réinfection peuvent alors s'avérer particulièrement marquantes.
2. **Site Web sur la sécurité du client** : l'exemple le plus fondamental de l'information et de la sensibilisation des clients est probablement celui de la création d'un site Web sur la sécurité du client, qui offre des conseils et un accès à des outils.
3. **Note insérée avec la facture** : si le FSI envoie régulièrement des informations aux clients par la poste, il pourra également profiter de cette occasion pour partager les recommandations concernant la sécurisation du système du client ; il pourra distribuer ces recommandations à tous ses clients, y compris ceux dont les systèmes n'ont jamais présenté de signes d'infection.
4. **Messages d'intérêt public (PSA) :** une autre occasion d'informer les utilisateurs finaux sur les programmes malveillants serait par des messages d'intérêt public diffusés à travers la radio ou la télévision. À titre d'exemple, la campagne nationale de sensibilisation à la cybersécurité aux États-Unis, *STOP THINK CONNECT*, a élaboré et mis en circulation plusieurs PSA chaque année depuis 2010.
5. **Matériel promotionnel** : il existe également différents matériels promotionnels tels que des tapis de souris, des tasses, des t-shirts, des ouvre-bouteilles, des stylos ou des crayons personnalisés, ainsi que d'autres cadeaux promotionnels qui peuvent aider à mieux faire connaitre les menaces des programmes malveillants et des réseaux zombies.
6. **Concours** : le message au sujet de la cybersécurité peut être également partagé en l'associant à des concours, en particulier des concours de rédaction visant des utilisateurs l'âge scolaire.
7. **Enseignement formel :** un autre élément essentiel de l'information et de la sensibilisation est l'intégration d'un programme d'étude sur la cybersécurité ou sur la citoyenneté numérique dans les écoles. Se pencher sur la cybersécurité en général et en particulier sur

les programmes malveillants et réseaux zombies est une question de sécurité publique à long terme, et comme toute autre question de ce domaine, elle est abordée de préférence en établissant des normes sociétales qui, dans bien des cas, sont mieux transmises aux individus dans le cadre d'un enseignement formel.

En raison de l'évolution rapide des menaces et de sa complexité en ce qui a trait aux programmes malveillants et aux réseaux zombies, l'information et la sensibilisation ne peuvent être que partiellement efficaces à protéger les utilisateurs finaux. Des efforts juridiques, règlementaires et techniques, ainsi que des initiatives de l'industrie, resteront à l'avant-garde de la lutte contre les programmes malveillants et les réseaux zombies. Il n'empêche que l'éducation de base et la sensibilisation sur les menaces en ligne restent des éléments nécessaires à la protection des utilisateurs finaux.

L'industrie, les associations et les gouvernements devraient élaborer et promouvoir des programmes de communication qui offrent aux utilisateurs finaux une notion de base des menaces ainsi que des techniques simples à comprendre sur les moyens de se protéger.

Un grand nombre de ces initiatives existent déjà et peuvent servir de modèle ou simplement de source pour le matériel d'enseignement (voir ci-dessous). Plusieurs de ces ressources portent sur la thématique générale au lieu d'être strictement axées sur les questions pertinentes aux programmes malveillants et aux réseaux zombies. Il est toutefois préférable de fournir aux utilisateurs finaux le plus souvent un message combiné concernant la sécurité sur Internet plutôt que de nombreuses suggestions non coordonnées. En d'autres termes, à chaque fois que cela est possible, l'information doit être concise et cohérente.

- National Cybersecurity Alliance — Keep a Clean Machine — http://www.stopthinkconnect.org/campaigns/keep-a-clean-machine (dans le cadre de la campagne nationale de sensibilisation à la cybersécurité « STOP THINK CONNECT » qui se focalise sur les programmes malveillants et les réseaux zombies)
- Bureau fédéral d'enquêtes (FBI) : http://www.fbi.gov/scams-safetyhttp://www.fraud.org/tips/internet/general.htm
- Gendarmerie royale du Canada (GRC) : http://www.rcmp-grc.gc.ca/is-si/index-eng.htmhttp://www.rcmp-grc.gc.ca/is-si/index-eng.htm
- Initiative américaine nationale pour la sensibilisation à la cybersécurité (US National Initiative for Cybersecurity Education) : http://csrc.nist.gov/nice/
- Commission fédérale américaine du commerce (U.S. Federal Trade Commission - FTC) : https://www.onguardonline.gov
  et http://www.consumer.ftc.gov/media/video-0103-hijacked-computer-what-do
  http://csrc.nist.gov/nice/

C) Meilleures pratiques juridiques et règlementaires

En ce qui concerne l'aspect judiciaire des programmes malveillants, *Malware Forensics: Investigating and Analyzing Malicious Code*[11] propose certaines meilleures pratiques pour enquêter sur ces programmes, notamment :

- Cadrez et recadrez tôt les objectifs et finalités de l'investigation et faites-le souvent.
- Dès le début, comprenez qu'il est essentiel d'identifier les preuves inculpatoires, disculpatoires et manquantes.

- Concevez une méthodologie garantissant que les mesures d'enquête ne modifieront, ne supprimeront, ni ne créeront des éléments de preuve, et qu'elles n'alerteront pas un suspect ni ne compromettront l'enquête.
- Créez et maintenez une documentation analytique et de la chaine de conservation, qui soit minutieuse et graduelle.
- Ne jamais perdre le contrôle des éléments de preuve
- Définir, redéfinir et adapter ces principes directeurs tout au long de l'enquête afin d'aider à clarifier les objectifs et finalités de l'enquête et les rendre plus réalisables.
- Réfléchissez dès le début aux questions importantes suivantes :
    - La juridiction compétente pour mener l'enquête a-t-elle besoin d'un certificat ou d'une licence spéciale pour mener une investigation numérique ?
    - Quelle autorité est habilitée à mener l'enquête, et quelles sont les limites à ses compétences ?
    - Quelle est la portée de l'enquête autorisée ?
    - Comment éviter d'atteindre à la vie privée des dépositaires de données pertinents ?

D) Meilleures pratiques pour une collaboration de l'industrie et du gouvernement, menée par celui-ci

Des pratiques sures dans le développement logiciel sont une des meilleures pratiques visant à limiter la propagation de programmes malveillants. Le Software Assurance Forum for Excellence in Code[12] (SAFECode) est une initiative mondiale pilotée par l'industrie pour identifier et promouvoir les meilleures pratiques de développement et de livraison de logiciels, de matériels et de services plus surs et fiables dans ce domaine.

Le Groupe de travail #7 du Conseil de la Commission fédérale américaine des communications (FCC) sur la sécurité, la fiabilité et l'interopérabilité (CSRIC) a publié le 22 mars 2012 un Code de conduite antibot pour les FSI et les opérateurs de réseaux, dans le cadre d'une collaboration industrie-gouvernement[13]. Le Code se concentre sur les utilisateurs résidentiels de l'Internet et comprend cinq domaines d'intérêt pour les FSI : l'information, la détection, la notification, l'élimination et la collaboration. Pour participer à ce Code, un FSI est tenu de participer au moins à une activité (c'est à dire, prendre des mesures significatives) dans chacun des domaines généraux suivants :

- Sensibilisation – aider à informer et sensibiliser davantage l'utilisateur final aux questions relatives aux réseaux zombies et à la manière de prévenir les infections par bot ;
- Détection – identifier l'activité d'un réseau zombie dans le réseau du FSI, obtenir des informations sur l'activité du réseau zombie dans le réseau du FSI, ou permettre aux utilisateurs finaux d'autodéterminer les infections par bot potentielles sur leurs appareils finaux ;
- Notification – informer les clients des infections par bot soupçonnées ou permettre aux clients de déterminer s'ils sont infectés par un bot ;
- Élimination – fournir des informations aux utilisateurs finaux sur la façon dont ils peuvent éliminer les infections par bot ou les aider à éliminer ces infections ;
- Collaboration — partager avec d'autres FSI une rétroaction et l'expérience acquise à travers la participation du FSI aux activités de SAFECode.

Les systèmes d'exploitation et les applications correctement configurés (à sécurité renforcée) peuvent également contribuer à réduire le taux d'infection due aux programmes malveillants. L'Agence de sécurité nationale américaine (NSA) fournit des orientations sur la « sécurisation renforcée » d'un ordinateur contre toutes les menaces, y compris les programmes malveillants[14]. Des informations supplémentaires sont disponibles au même endroit concernant les routeurs, les sans-fils, les commutateurs, le VoIP, les serveurs de bases de données et les applications. En outre, des ressources concernant la « sécurisation renforcée » des systèmes d'exploitation et des applications pour lutter contre les programmes malveillants sont disponibles dans les liste de contrôle du National Institute of Standards and Technology (NIST)[15] (y compris pour les appareils Android).

L'Agence coréenne chargée de la sécurité et de l'Internet (KISA) fournit gratuitement un service qui protège des attaques DDOS aux petites entreprises ne disposant pas des outils appropriés pour se protéger contre une de ces attaques. Ce service filtre le trafic malveillant de l'attaque DDoS et ne laisse passer que le trafic normal. En outre, la KISA détecte les IP des zombies présumés dans un piège à spam et laisse les FSI nationaux prendre des mesures appropriées contre ces IP sur leurs réseaux.

D'autres initiatives spécifiques à certains pays sont disponibles sur les liens ci-dessous :

- International : https://code.google.com/p/evidenceontology
- Botfrei : https://www.botfrei.de/
- Melani - Suisse : http://www.melani.admin.ch
- Ficora - Finlande : http://www.ficora.fi/en
- Projet AC/DC de l'UE : http://www.acdc-project.eu/
- Canada http://fightspam.gc.ca
- Australie : http://www.acma.gov.au/Citizen/Stay-protected/My-mobile-world/Dealing-with-mobile-spam/dealing-with-spam-i-acma

E) Meilleures pratiques pour les FSI

La menace que posent les programmes malveillants peut être minimisée en réduisant ou en éliminant les vecteurs d'infection. Le courriel demeure l'une des méthodes de propagation les plus frappantes. Pour mitiger ce vecteur, la plupart des FSI, des hôtels et des points d'accès gratuits suivent les meilleures pratiques qui consistent à bloquer le courrier sortant (port 25) à partir d'un ordinateur de leur réseau autre que leurs propres serveurs de courriel. Ceci empêche les ordinateurs infectés de propager le programme malveillant via courriel direct.

En Europe, certains FSI ont pris des dispositions supplémentaires. Les utilisateurs de ces réseaux par défaut n'ont accès qu'au Web. Le trafic provenant d'autres ports est refusé. Pour permettre aux utilisateurs sophistiqués plus de flexibilité, ces FSI fournissent des outils permettant à certains utilisateurs spécifiques autorisés d'accéder à d'autres ports/protocoles et services.

Dans les deux cas, le suivi des tentatives de trafic bloquées peut être utilisé comme indicateurs d'alerte précoce aux machines infectées par des programmes malveillants ainsi que pour faire obstacle à la propagation de ces programmes et aux communications de contrôle et de commande.

F) Meilleures pratiques pour les serveurs et les fournisseurs d'hébergement

Les serveurs Web compromis sont l'un des réservoirs principaux de programmes malveillants à l'heure actuelle. Ces serveurs sont compromis soit lorsque les correctifs de sécurité les plus récents

ne sont pas appliqués pour l'OS, les applications de soutien, ainsi que les cadres Web, soit en raison d'un choix de mot de passe faible par l'utilisateur. Ces vulnérabilités sont accentuées dans les petites et moyennes entreprises et chez de nombreux fournisseurs d'hébergement en raison de petits abus commis par le personnel ou les équipes. Certains ont recours à l'automatisation pour améliorer ces questions et ceci devrait être considéré comme l'une des meilleures pratiques mondiales.

1. **Conditions générales d'utilisation des clients concernant une mise à jour de sécurité diligente** : tous les clients doivent accepter d'appliquer avec diligence les correctifs de sécurité actuels ou permettre au fournisseur d'hébergement de mettre à jour les cadres qui existent dans leurs répertoires.
2. **Maintenir des correctifs de sécurité actuels :** les correctifs de sécurité doivent être à jour. Ce processus peut être effectué manuellement pour les très petits systèmes ou par script pour les fournisseurs d'hébergement plus importants.
3. **Utiliser des outils de vérification pour identifier les hôtes :** des outils permettant de vérifier l'ensemble du serveur pour des versions de logiciels non sécurisées doivent être exécutés au moins à la quinzaine et les logiciels identifiés doivent être patchés.
4. **Utiliser des logiciels de sécurité informatique :** des outils (tels que Tripwire) doivent être utilisés pour contrôler l'intégrité de chaque serveur.
5. **Exécuter un antivirus** : exécutez un logiciel antivirus fréquemment (si possible deux programmes différents) pour surveiller la contagion de fichiers hôtes variables.
6. **Pensez à utiliser des serveurs en nuage :** comme les serveurs cloud, ou en nuage, sont professionnellement entretenus et utilisés par de nombreux clients ; ils ont tendance à être mieux sécurisés. Ils peuvent toutefois représenter des cibles plus attrayantes pour les attaques DDoS. Toujours est-il que les serveurs en nuage devraient être envisagés comme une solution permettant une sécurité accrue, tout en ne perdant pas de vue la réputation du fournisseur de services en nuage, les mesures de sécurité mises en place, et si les serveurs ont déjà été attaqués ou non. De plus amples renseignements sur les menaces à l'hébergement et au nuage ainsi que les meilleures pratiques y afférentes sont disponibles plus loin dans le présent rapport.

HAMEÇONNAGE ET INGÉNIERIE SOCIALE

L'hameçonnage désigne les techniques utilisées par des acteurs malveillants afin de tromper une victime et l'amener à faire une chose qu'autrement elle n'aurait pas faite en ligne, révélant souvent des informations confidentielles telles que des données personnelles ou financières. Les fraudeurs se font passer pour des entités connues (amis ou entreprises), tirant parti de relations de confiance existantes pour compromettre leurs victimes.

La fréquence, la sophistication et les dégâts de l'hameçonnage n'ont cessé d'augmenter depuis que celui-ci a émergé au nombre des graves menaces vers le milieu des années '90, et se poursuivent au même rythme. Le type des données recherchées par l'hameçonnage est devenu de plus en plus utile, évoluant d'un simple accès au courriel et aux comptes bancaires du consommateur qui subirait des pertes estimées à des milliers de dollars pour viser des cibles de grande valeur

actuellement telles que les comptes de grandes sociétés associés à des privilèges spéciaux (« superutilisateur ») et les renseignements bancaires des entreprises.

Ces attaques peuvent entrainer un piratage informatique monstrueux où les informations personnelles des clients sont volées « en masse », la propriété intellectuelle d'une entreprise est exfiltrée, ou des données et même des systèmes physiques sont détruits. Un nombre incalculable de ces évènements se produit chaque année ; chacun d'entre eux peut occasionner une atteinte à la propriété intellectuelle d'une entreprise et imposer des pertes financières s'élevant à des dizaines, voire des centaines de millions de dollars, et

Les hameçonneurs falsifient des messages et des pages Web impossibles à distinguer des originaux, en utilisant une légion de machines compromises légitimes (réseaux zombies) et des programmes malveillants infectieux pour obtenir le même résultat qui nécessitait auparavant l'interaction plus manifeste de l'utilisateur final. Les hameçonneurs ont également développé des programmes malveillants mobiles pouvant rendre certaines mesures de protection inefficaces.

> ***Pourquoi le « ph » ?***
>
> ***Le terme anglais désignant l'hameçonnage, « phishing » est dérivé de « fishing », pêche, car les escrocs d'Internet se servent d'appât pour capturer les données financières et les mots de passe des utilisateurs. Les pirates informatiques (hackeurs) aiment bien à remplacer la lettre « F » par un « PH », et le mot « phishing » en est un bon exemple. La transformation du F-ph n'est pas une tendance nouvelle parmi les pirates informatiques ; ce phénomène est apparu à la fin des années 60 parmi les pirates du système téléphonique qui s'appelaient eux-mêmes « phone phreaks » (en français « les mordus du téléphone »).***

DOMMAGES POUR LE CONSOMMATEUR ET L'INDUSTRIE

Mesurer l'impact de l'hameçonnage pour les consommateurs et l'économie est une tâche difficile dont les résultats sont largement variables. L'avis général est que les attaques par hameçonnage sont à la hausse. Le rapport annuel sur la violation des données (Data Breach Investigation Report) de l'opérateur américain Verizon a révélé qu'après un bref plongeon en 2010, l'hameçonnage est à la hausse depuis plusieurs années. En 2014, l'hameçonnage était reconnu comme étant la cause #3 de la violation de données[16] ayant augmenté de 23% en 2013, soit de 253 à 312. En 2014 également, les attaquants ont continué à violer des réseaux avec des attaques d'hameçonnage hautement ciblé, ce qui s'est élevé à 8% de l'ensemble des attaques. Ces attaques étaient plus sophistiquées et plus ciblées, avec 14 % moins de courriels envoyés vers 20% moins de cibles.[17]

Le groupe de travail antihameçonnage (APWG) réalise des rapports trimestriels sur les tendances de l'hameçonnage ; leur rapport de 2014 a signalé le plus grand nombre d'attaques par hameçonnage qui ait été observé depuis 2009. Ce même rapport a recensé un ciblage de marques plus fort que jamais, avec 756 institutions ciblées au cours de la première moitié de 2014.[18,19] le rapport mensuel du RSA sur la fraude pour décembre 2014 estime que les pertes dues à l'hameçonnage, pour ce mois, s'élèvent mondialement à près de 453 millions USD et les pertes annuelles à quelque 5 milliards USD, avec 75 % des attaques survenant aux États-Unis et au Canada[20]. Bien que l'hameçonnage n'est qu'une petite part des pertes estimées dues à la cybercriminalité à l'échelle mondiale qui s'élèvent à 445 milliards USD[21], il en reste que 5 milliards USD représentent des pertes considérables et évitables.

La prévention est devenue une tâche considérable, avec le temps médian pour cliquer (time-to-click) observé à une minute et vingt-deux secondes et les données du APWG suggérant que l'infrastructure servant à ces campagnes est assez vaste avec plus de 9000 domaines et près de 50 000 URL d'hameçonnage suivies chaque mois par les membres du Groupe.

PANORAMA DE L'HAMEÇONNAGE

On distingue l'hameçonnage par le type d'information recherchée, les types de cibles attaquées et les canaux par lesquels les attaques sont menées. Il est identifié par un courriel, un SMS, ou d'autres messages contenant un lien qui redirige le destinataire à une fausse page Web lui demandant ses informations de compte comme son nom d'utilisateur et son mot de passe, le numéro de sa carte de crédit ou d'autres informations personnelles.

OBJECTIFS DE L'HAMEÇONNAGE — CE QU'ILS RECHERCHENT

Les informations obtenues par hameçonnage sont généralement utilisées pour un certain type de vol financier, soit directement contre la victime, ou sur une autre cible, comme l'employeur de la victime. La monétisation des renseignements relatifs aux cartes de crédit et des numéros de Sécurité sociale étant devenue d'une difficulté croissante, « les pirates informatiques attaqueront les personnes ayant des informations de soins de santé » dit John Pescatore, directeur des tendances émergentes en matière de sécurité du SANS Institute, ajoutant que, ces dernières années, les pirates informatiques ont de plus en plus visé les dossiers informatisés de santé (EHR) qu'ils peuvent facilement monétiser.[22] En outre, l'hameçonnage a été utilisé comme une première étape dans la violation des réseaux d'entreprise et de gouvernement, permettant d'obtenir des informations d'identification pour accéder aux systèmes.

L'hameçonnage en lui-même n'est généralement qu'une première étape et ne crée pas nécessairement des vols financiers directs dans l'immédiat. La tendance à la hausse qui consiste à voler des dossiers de santé est entamée normalement par un hameçonnage visant l'accès au système. Une fois l'accès obtenu, les voleurs utilisent d'autres outils, tels que les programmes malveillants et les espiogiciels, pour voler les informations sensibles — au cours du premier trimestre de l'année 2015, plus de 120 millions de patients aux États-Unis ont connu un vol de leurs dossiers.[23] En outre, l'hameçonnage ciblé visant des employés d'entreprises est souvent l'un des premiers pas d'une violation de données à grande échelle, et constitue donc l'étape première d'une portion considérable des pertes énormes attribuée aux violations de données.

Fraude 419 — Premières formes d'hameçonnage, elles n'étaient pas sophistiquées et ont porté ce nom en référence au chapitre 38, section 419 du Code pénal du gouvernement nigérian qui criminalise ce type d'arnaque. ***« Quiconque aura, par des moyens frauduleux et dans l'intention de frauder, obtenu d'une autre personne toute chose susceptible d'être volée, ou incité une personne à livrer à quiconque une chose susceptible d'être volée est coupable d'une infraction grave et passible d'une peine d'emprisonnement de trois ans ».*** **Il s'agit des courriels nigérians notoires venant de princes ou d'autres escroqueries par avance de frais qui amènent la victime à dépenser de l'argent en échange de richesses incommensurables à la fin de la procédure.**

- Les techniques en ligne et hors ligne dupant des personnes pour les amener à divulguer des informations sont souvent appelées « piratage psychologique » et datent d'avant l'Internet. Au premier temps de l'hameçonnage par courriel, les attaquants n'étaient pas très exigeants. Ils envoyaient, pour l'essentiel, des courriels à des fins générales à autant de personnes que possible en espérant qu'un certain nombre d'entre elles serait dupé. Au fur et à mesure que les défenses se renforçaient contre ces attaques, les attaquants ont affiné leurs stratégies. Il existe quatre formes d'hameçonnage communément reconnues :

  i) la redirection via un lien contenu dans un message vers un endroit sur Internet qui peut contenir un faux site bancaire, commercial ou de courriel ;

  *II) les courriels assortis d'**une pièce jointe HTML** contenant une forme d'hameçonnage ;*

  III) un lien/listing d'un numéro de téléphone que la victime devrait cliquer ou appeler, ou

  IV) un hameçon simple de type « Répondre », dont le message contient une demande pour des informations d'identification et qui invite l'utilisateur à répondre avec les informations requises.

Dans les deux premières formes, le destinataire fournit des renseignements personnels le plus souvent en envoyant au criminel un courriel contenant les informations d'identification volées. L'hameçonnage basé sur le numéro de téléphone implique soit un répondeur téléphonique automatisé incitant la victime à fournir ses informations d'identification soit une personne en direct qui tente par le piratage psychologique d'extorquer ces informations. La Fraude 419 qui promettait des richesses incommensurables et diverses fraudes au paiement à l'avance étaient les toutes premières formes de piratage psychologique via courriel. Malgré les progrès dans la lutte contre l'hameçonnage, ces arnaques persistent.

- « **Spear Phishing » ou hameçonnage ciblé** — alors que les tentatives d'hameçonnage traditionnelles sont souvent envoyées sans discernement à presque tout le monde, les attaques par hameçonnage ciblé sont menées contre des individus ou des organisations spécifiques. Ce type d'hameçonnage exige en général des recherches approfondies de la part des fraudeurs, telles que la découverte des loisirs, des organismes de bienfaisance, des employeurs passés et des réseaux sociaux, pour rendre leur attaque beaucoup plus plausible et crédible. Il peut être personnalisé de manière à duper les victimes qui sont traditionnellement plus précieuses (et méfiantes) que les utilisateurs normaux. Elles peuvent être employées par une entreprise ciblée qu'un attaquant cherche à pénétrer. Une variante assez efficace de l'hameçonnage ciblé consiste à envoyer un faux message qui semble provenir d'un fournisseur, d'un créancier ou d'une organisation que la victime connait, contenant des instructions de paiement frauduleuses pour des transactions prévues ou normales.
- **VoIP / hameçonnage vocal** — au fur et à mesure que la téléphonie et d'autres activités vocales migrent vers des mécanismes basés sur l'Internet, collectivement connus comme « Voix sur IP » ou VoIP, les fraudes en font de même. Cette intégration des systèmes de téléphone dans les ordinateurs permet d'amener des victimes à cliquer des liens frauduleux qui automatiquement appellent un numéro de téléphone au lieu de visiter un site Web. L'appel peut lui-même générer directement des revenus à l'attaquant, ou peut diriger la victime vers un piratage psychologique qui convaincra la victime de révéler des informations. Les smartphones aggravent la menace en simplifiant cette intégration téléphonie/Internet pour les utilisateurs. Pour plus de détails, veuillez consulter la section Mobile et voix du présent rapport.

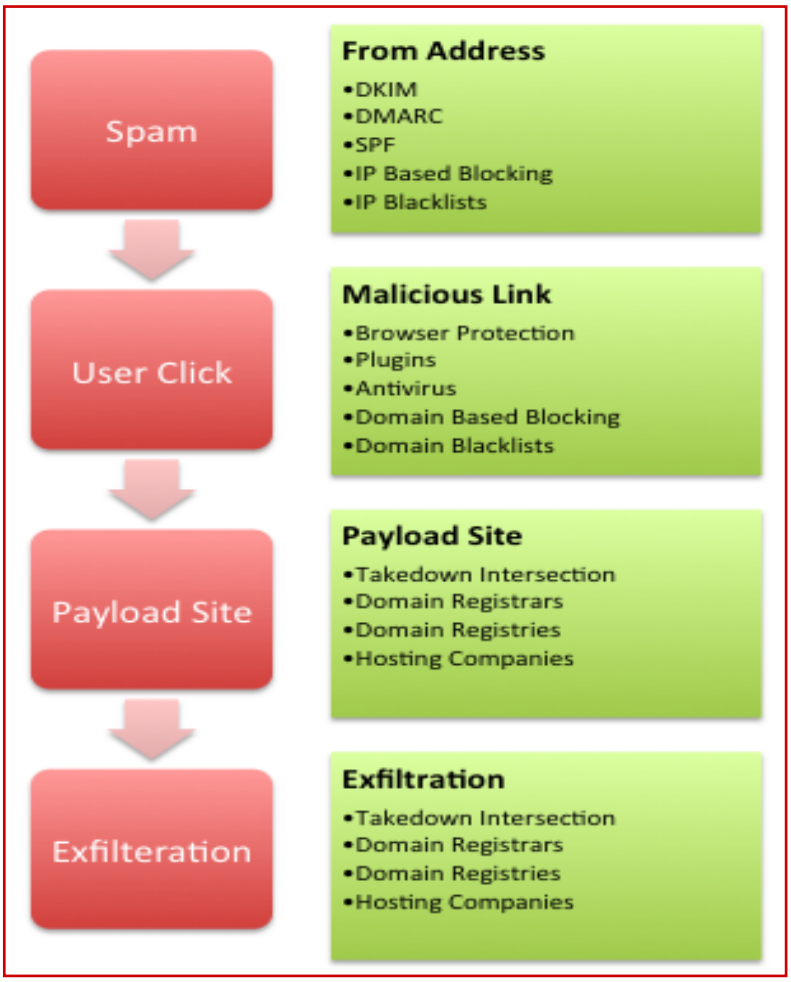
- **Télécopie** — la télécopie représente l'une de premières méthodes d'hameçonnage électronique et a été remplacée par les autres méthodes d'attaque décrites ici. Cependant, avec l'arrivée des télécopies sur Internet qui en a baissé le cout, cette méthode connait une résurgence. Étant donné qu'elle demeure rare, elle n'est pas toujours détectée.
- **Réseaux sociaux** — ceux-ci créent une expérience de groupe propice à un sentiment de confiance, qui à son tour est favorable au piratage psychologique qui exploite les relations en ligne de la victime. Cela fonctionne parfaitement quand l'attaquant imite un message d'un ami en ligne fiable ou a compromis le compte de l'ami.

CHRONOLOGIE D'UNE CAMPAGNE D'HAMEÇONNAGE TYPIQUE

Une campagne d'hameçonnage normale visant des identifications de compte comporte quatre éléments :

1. **Message initial (Spam)** — un message est livré et vu par un utilisateur final. Ce message semble légitime, donc assez crédible, et contient généralement des éléments contrefaits d'un message légitime et ostensiblement émanant d'une source légitime telle que la banque de l'utilisateur.
2. **Incitation à l'action (Clic de l'utilisateur)** — la victime est invitée à cliquer sur un lien ou à répondre au message par des informations confidentielles. Les incitations à l'action les plus saisissantes exploitent la peur et la cupidité, que ce soit au niveau personnel ou sur le plan de l'organisation employant le destinataire. Un message visant à induire la peur pourrait indiquer que la victime a déjà été compromise ou peut perdre accès à une ressource si elle n'agit pas, ou même que son entreprise fait l'objet d'une action en justice ou d'une sanction pécuniaire. Un message fondé sur la cupidité pourrait promettre des rabais ou une récompense financière pour la réponse à un sondage ou la fourniture de renseignements.
3. **Charge utile** — ce contenu amène la victime à divulguer l'information ciblée. Il peut se trouver dans le message initial ou sur un site Web sur lequel la victime est dirigée, appelé une « page d'accueil ». Le site Web pourrait être compromis ou pourrait avoir un nom de domaine semblable afin de confondre l'utilisateur. La charge utile comporte généralement un formulaire que la victime devrait remplir avec des renseignements confidentiels. Certains sites contiennent également un mécanisme de téléchargement furtif (*drive-by download*) par lequel la visite du destinataire à la page Web démarre un processus automatisé d'inventaire du système ou d'exploitation qui installe de manière clandestine des programmes malveillants sur l'ordinateur de la victime, permettant aux criminels d'extraire des données confidentielles avant de rediriger la victime vers un site légitime.
4. **Exploitation/exfiltration/obtention d'information** — l'objectif ultime de toute campagne d'hameçonnage consiste à convertir les informations d'identification recueillies en valeur réelle au bénéfice des criminels. Un vaste éventail de mécanismes a été observé, le plus simple étant une connexion au compte pour transférer des fonds ou faire des achats. D'autres attaques bien plus sophistiquées commencent par un accès à un compte de courriel qu'elles utilisent ensuite comme base de piratage psychologique supplémentaire et/ou de distribution de programmes malveillants, avec la possibilité de s'infiltrer profondément dans l'organisation du destinataire. Des tentatives d'extorsion ont également été observées.

Le flux de travail d'une campagne d'hameçonnage peut être empêché ou perturbé à de nombreux stades, comme l'indique le graphique :



ÉVOLUTION DES MÉTHODES D'EXPLOITATION

Les formes d'hameçonnage originales les mieux connues faisaient connecter les criminels directement à un établissement financier et tenter de transférer des fonds du compte de la victime à un autre compte qu'ils contrôlent. Lorsque les établissements financiers ont commencé à détecter plus facilement et bloquer les transferts de fonds internationaux frauduleux, les criminels s'y sont adaptés. En en déplaçant les fonds vers un compte national ou au sein du même établissement, la fraude n'était souvent pas aussi facilement détectée. Ceci était accompli parfois par le paiement de factures en ligne ou de par simples transferts de compte à compte. Ces situations appelaient le criminel, se trouvant souvent à l'étranger, à acquérir les services de criminels nationaux qui faisaient office de mules pour faire passer les fonds.

Dans d'autres cas, l'incitation à l'action contenue dans le courriel d'hameçonnage était conçue de manière à inciter la divulgation des coordonnées d'une carte de crédit. Le numéro de la carte, sa date d'expiration et son code CVV obtenus, la carte pouvait soit être vendue sur le marché noir ou utilisée pour toutes sortes de fraudes en absence de carte. Le numéro de la carte de crédit, son

expiration et son code CVV permettent à l'hameçonneur de visiter presque n'importe quel détaillant en ligne et effectuer des achats. Pour échapper à la détection, des marchés criminels secondaires étaient utilisés pour la réexpédition, ainsi que des services de terminaux distants. Afin de vaincre les systèmes de détection de fraude dans le commerce de détail, les hameçonneurs achètent l'utilisation d'une adresse IP de services de terminaux distants dans une zone géographique correspondant à celle de la victime de la fraude par carte de crédit. De même, si des expéditions doivent être envoyées, un endroit pour recevoir les paquets correspondant à la zone géographique de la victime sera utilisé.

Les attaques par réutilisation de mot de passe sont encore une menace qui pèse sur le consommateur en ligne, résultant d'un hameçonnage. Étant donné que les gens utilisent souvent un même mot de passe pour plusieurs systèmes, les criminels peuvent utiliser ces mêmes noms d'utilisateur et mots de passe à plusieurs endroits, y compris des établissements financiers, des détaillants en ligne et même des systèmes VPN de société (voir la section sur les programmes malveillants et les réseaux zombies pour de plus amples informations concernant la création et la sauvegarde de mots de passe forts).

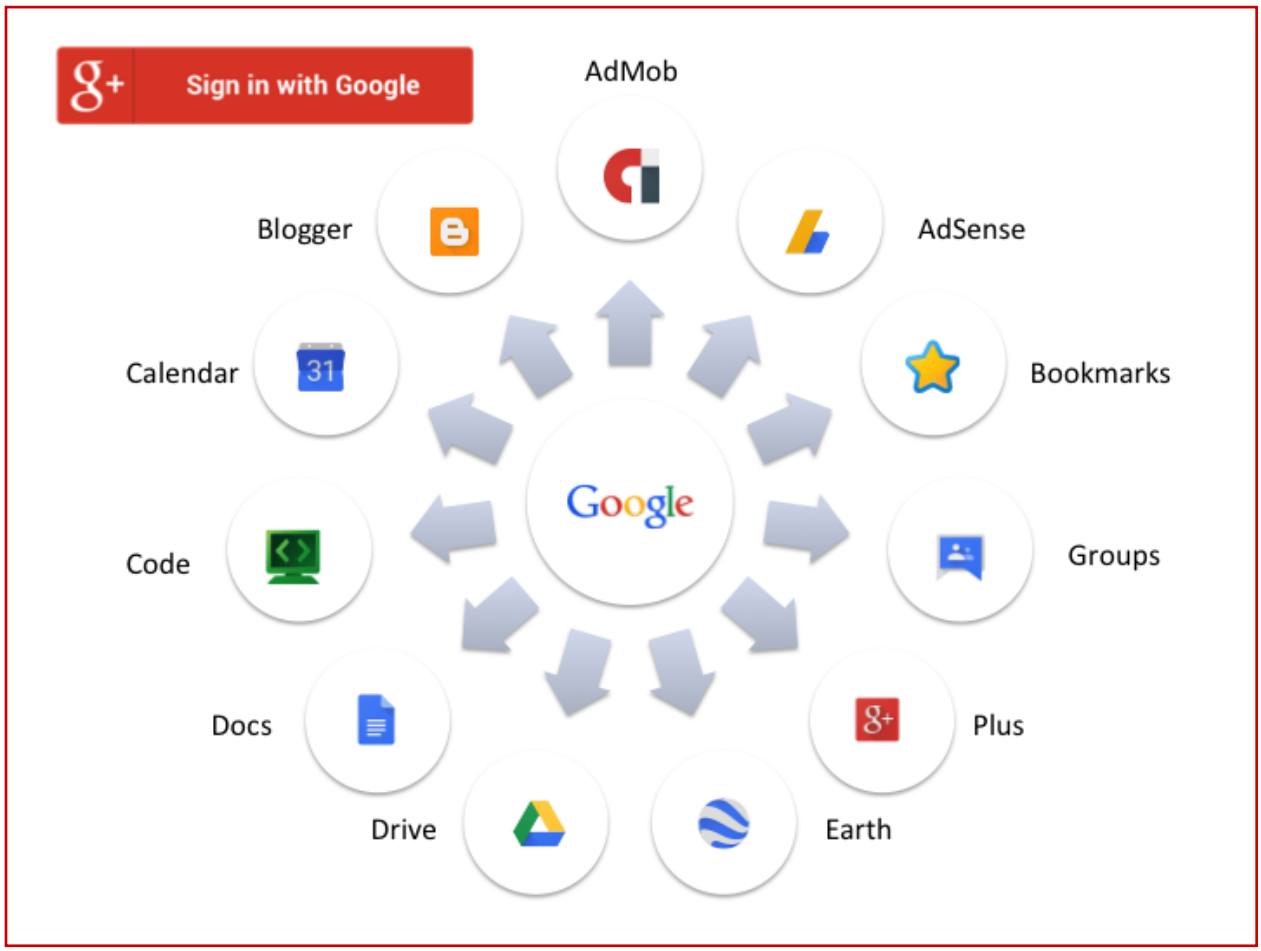
Les violations de données à large échelle qui ont fait les manchettes ces dernières années commencent souvent par une certaine forme d'hameçonnage ciblé de cadres exécutifs ou d'individus ayant accès aux commandes d'un réseau d'entreprise. De telles attaques ont donné lieu à des crimes financiers directs : le vol d'informations d'identification de l'utilisateur et de ses données personnelles peut avoir pour résultat la revente dans les réseaux criminels clandestins. Des campagnes d'hameçonnage ciblé de plus en plus vastes et nombreuses visent l'exécution d'espionnage industriel, de projets d'extorsion criminelle, d'infiltration par un État, ou d'autres crimes non financiers.

L'INFLUENCE CROISSANTE DES ATTAQUES D'HAMEÇONNAGE

Au fur et à mesure que le nombre d'organisations ayant migré vers les systèmes de messagerie basés sur le Web a augmenté, les attaques par hameçonnage sont devenues plus répandues, et cela pour deux raisons principales. Premièrement, et malheureusement, un grand nombre d'organisations utilisent des environnements appliquant une authentification unique, donc un même mot de passe pour les comptes de courriel et les tâches de ressources humaines telles que le compte bancaire où les fonds sont transférés le jour de paie. Deuxièmement, une fois qu'un criminel a pu accéder à un compte courriel d'entreprise, il dispose d'une plateforme à travers laquelle il peut analyser l'organisation, apprendre quelle personne a accès aux ressources numériques les plus précieuses de l'entreprise, y compris les comptes financiers et la propriété intellectuelle, et cibler ces employés-là. Ces attaques seront lancées depuis le compte de courriel d'un employé qu'ils connaissent et auquel ils font confiance, soit par piratage psychologique ou par envoi de programmes malveillants via pièces jointes à un courriel calqué sur des documents d'entreprise couramment trouvés dans le compte compromis.

Quant aux courriels individuels, les attaques par hameçonnage contre des fournisseurs de courriel comme Gmail, Yahoo, Outlook et AOL sont également de plus en plus courantes pour les mêmes raisons. Ces comptes peuvent sembler être des « cibles de faible valeur » et ne sont pas protégés aussi diligemment que d'autres, mais ils contrôlent la capacité d'effectuer des réinitialisations de mot de passe ou un accès direct à d'autres comptes pour un vaste d'éventail d'attaques. Ces comptes de courriel compromis se sont traduits par un volume considérable de crimes financiers (p. ex., piratage de comptes, virements bancaires frauduleux) bien documentés par les institutions financières.

D'autres services, tels que les réseaux sociaux, offrent une authentification unique pour une grande variété de services aux consommateurs. Ceci rend ces comptes de superbes cibles pour les fraudeurs, car ces derniers peuvent directement monétiser de tels services, rediriger les livraisons de produits ou généralement contrôler de nombreux aspects de l'identité en ligne d'une personne. Le graphique suivant indique que si un pirate informatique parvient à s'infiltrer dans un compte Google, il a souvent accès à une multitude d'autres informations. Il en va de même pour les comptes Apple et iTunes.



L'ingéniosité croissante des criminels les a amenés à viser des éléments d'une infrastructure qui leur fournissent encore plus de moyens potentiels. À titre d'exemple, les hameçonneurs accèdent maintenant aux fournisseurs tiers de services de courriels, qui envoient du courriel en nombre au nom des plus grandes marques du monde. Les criminels accèdent à l'infrastructure de ces fournisseurs via des comptes compromis, volent les listes de clients, puis envoient du spam à des fins d'hameçonnage ou des programmes malveillants à des destinataires qui deviennent involontairement victimes en croyant que le message provient de la liste de diffusion d'une compagnie légitime.

Une autre tendance à la hausse est le ciblage croissant d'éléments de l'infrastructure d'Internet tels que les comptes d'hébergement et les données d'enregistrement de domaines. Une fois que les hameçonneurs ont pu accéder aux contrôles fondamentaux de l'infrastructure, ils peuvent mettre en place des sites Web, lancer de nouvelles attaques et créer de nouveaux éléments d'infrastructure

comme les noms de domaine pour faire une rotation de leur mécanisme (voir la section Hébergement et services en nuage). Une tactique particulièrement nuisible consiste à ajouter des noms d'hôtes malveillants à un nom de domaine bien établi qui jouit d'une réputation solide, laissant le domaine original intact. Cette tactique permet aux criminels d'exploiter la bonne réputation d'un domaine dans leurs campagnes pour contourner les filtres et éviter d'être bloqués ou suspendus (voir la section Noms de domaine et adresses IP).

MEILLEURES PRATIQUES POUR LUTTER CONTRE L'HAMEÇONNAGE ET LE PIRATAGE PSYCHOLOGIQUE

Il existe toute une série de meilleures pratiques contre l'hameçonnage, qui sont disponibles aux organisations souhaitant protéger leur marque ainsi que leurs clients. Ceci dit, il n'existe pas de « remède miracle » aux dangers que pose l'hameçonnage, et ils doivent être abordés tout au long du cycle de vie complet du processus — toute étape contrecarrée à tout moment du processus permettra de protéger des dizaines de millions de victimes, en fonction de l'ampleur de l'attaque en question et de la portée des diverses solutions. Les entreprises devraient adopter à l'égard de ce problème une approche de « sécurité en profondeur », c'est-à-dire supposer que certaines mesures réussiraient à empêcher certains courriels initiaux d'arriver à destination, mais que d'autres pourraient aboutir et qu'il est nécessaire de mettre en place d'autres défenses. Cette section donnera un aperçu des techniques et meilleures pratiques principales, mais de plus amples détails ainsi que des conseils spécifiques peuvent être obtenus auprès de diverses organisations de l'industrie, dans les publications de gouvernements, et chez les fournisseurs de solutions antihameçonnages.

1. Empêcher la réussite des attaques par hameçonnage

Pour lutter contre les attaques par hameçonnage, il faut avant tout les empêcher d'atteindre les victimes ou empêcher les victimes de visiter les sites d'hameçonnage. Pour y parvenir, il faut s'intéresser à trois points sensibles : arrêter le flux des courriels-appâts, empêcher les appâts d'atteindre les utilisateurs, et bloquer l'accès aux sites Web d'hameçonnage et à d'autres éléments du processus.

a. Prévention de la livraison d'appâts sortants

Les mécanismes relativement récents d'authentification par courriel facilitent quelques protections facilement utilisées contre certaines formes d'hameçonnage et d'usurpation. Ces techniques reposent sur la création d'une infrastructure de courriel authentifié. Les mécanismes d'authentification de courriel les plus courants sont les SPF (Sender Policy Framework)[24] et le DKIM (DomainKeys Identified Mail)[25], qui emploient des noms de domaine[26] comme identifiants validés. Ceux-ci permettent à un propriétaire de nom de domaine de contrôler l'utilisation de ce domaine dans un message et de réduire les risques d'usurpation.

Pour résoudre avec succès les problèmes liés à l'hameçonnage et à l'usurpation de nom de domaine, les propriétaires de marques et les FSI devraient partager des informations sur leur activité de courrier, notamment les politiques d'authentification et les rapports concernant des problèmes. Ces arrangements étaient auparavant bilatéraux et privés, entre les propriétaires de marques et des FSI individuels. Toutefois, un consortium ad hoc de l'industrie a élaboré une spécification technique appelée DMARC (*Domain-based Message Authentication, Reporting & Conformance*)[27].

La DMARC, introduite au début de l'année 2012, tire profit à la fois du SPF et du DKIM pour fournir aux propriétaires de marque un moyen de communiquer facilement aux FSI leur préférence concernant le traitement des messages incorrectement authentifiés. La DMARC fournit également aux FSI et à d'autres destinataires de message un mécanisme permettant de distribuer en retour aux propriétaires de marques une rétroaction au sujet de la santé de l'authentification déployée pour leur courriel ainsi que des renseignements d'ordre judiciaire.

Pour les opérations d'envoi de courriel, l'approche recommandée est la suivante :

- *Vérifier* — en faisant un inventaire de toutes les machines et les systèmes qui envoient des courriels au nom de l'organisation, y compris les systèmes externes tels que les fournisseurs de services de courriel (ESP) et d'autres tiers autorisés
- *Publier* — les fichiers d'authentification et de politiques dans le DNS
- *Modifier* — le logiciel d'envoi de courriel afin qu'il utilise l'authentification et se conforme aux politiques
- *Établir* — des rapports afin de signaler toute activité qui utilise le nom de domaine
- *Surveiller* — tous les rapports disponibles à la recherche de structures nécessitant une attention
- *Maintenir* — des opérations pour une conformité continue

Pour les opérations de réception de courriel, le soutien à ces nouveaux mécanismes principalement implique l'ajout de certains modules aux systèmes de filtrage de courrier existants.

b. Filtrage du spam entrant

Une des plus importantes méthodes pour arrêter les méfaits d'une attaque par hameçonnage consiste à filtrer concrètement le courrier indésirable. L'activation d'un filtre antispam est importante, mais le filtrage concret nécessite plus que l'installation d'un produit commercial sur la passerelle de courriel. Les sociétés et les organismes publics devraient également améliorer leur filtre antispam en ajoutant les renseignements recueillis sur les menaces pour rendre le filtre antispam plus performant.

Cette information peut être puisée dans les listes noires que créent des organisations spécialisées telles que Spamhaus, SURBL et d'autres (voir les références à la fin de la présente section). Le filtrage du spam est étroitement lié à son signalement, car les courriels d'hameçonnage qui parviennent à pénétrer un filtre antispam sont les plus urgents à signaler. De nombreux services de courriel proposent un bouton « Signaler un spam » ou « Signaler un hameçon » que les utilisateurs devraient être encouragés à utiliser.

Les techniques permettant de filtrer le spam comprennent :

- *L'authentification* - les personnes envoyant du courriel peuvent tirer parti des méthodes d'authentification, dont le DomainKeys Identified E-mail (DKIM), le Sender Policy Framework (SPF), et le Domain-based Message Authentication, Reporting and Conformance (DMARC). À sa réception, un courriel est vérifié pour

s'assurer de la présence d'un jeton d'authentification. Pour le DMARC, le domaine d'envoi est vérifié pour voir s'il requiert une authentification. Si le jeton n'est pas valable ou s'il est manquant, le courriel pourrait être frauduleux.

- *La réputation des adresses IP* - l'adresse IP envoyant le courriel pourrait être déjà connue comme associée à un envoi de spam. En refusant de recevoir des courriels provenant d'adresse IP à mauvaise réputation, tant de spam peut être bloqué.
- *Le filtrage de contenu* - le filtrage à base de règles, la vérification du courriel pour la présence de mots ou phrases interdits, ou l'analyse statistique du courriel (filtre antispam Bayesian) peuvent déterminer quels courriels seraient probablement du spam. Alimenter les filtres de contenu les données des services de réputation pour les noms d'hôte ou les URL (par exemple, DNSBL comme Spamhaus/SURBL) améliore considérablement cette technique.
- *Les pièges à Spam* — en collectant les courriels envoyés aux adresses qui ne devraient recevoir aucun courriel (utilisateurs inexistants), un schéma peut être identifié et appliqué afin de bloquer les courriels envoyés à des adresses légitimes.

c. Blocage par navigateur ou autre

La protection contre les attaques par hameçonnage est intégrée dans de nombreux produits et services dont peuvent bénéficier les consommateurs, les entreprises et d'autres organisations. Les données issues des rapports massifs d'attaques par hameçonnage, provenant des marques et du public en général, sont introduites dans les produits exposés à de telles attaques comme les navigateurs, les serveurs et les clients de courriel, les dispositifs de sécurité (pare-feu, systèmes IDS/IPS, proxy Web, pare-feu du DNS), et les fournisseurs de services de courriel en ligne. Ces outils/appareils peuvent fournir une protection encore meilleure s'ils sont renforcés par des données les renseignant sur les menaces. En voici quelques exemples : les données sur la réputation des adresses IP, noms d'hôte et de domaines, URL, adresses électroniques et autres « indicateurs » de comportement douteux.

Ceux-ci peuvent être livrés sous des formes diverses, y compris les listes noires de DNS (DNSBL), listes noires de DNS en temps réel (RBL), les listes rouges d'URL, et une technologie relativement nouvelle appelée Zones de politiques de réponse du DNS (*Response Policy Zones* - RPZ). De telles technologies et données peuvent être appliquées pour suspendre toutes les communications vers les sites Internet bloqués. Les entreprises doivent élaborer des normes opérationnelles et des politiques pour veiller à mettre en œuvre ces services dans leurs environnements. Ceci est particulièrement important pour les produits passerelles de courriel et les outils de sécurisation de réseaux en général, afin de créer une défense multicouche. Ce maintien de la sécurité devrait être bien planifié et mis à jour régulièrement.

Les utilisateurs individuels peuvent aussi se protéger de nombreuses attaques simplement en activant ces services dans leur navigateur (par exemple, la navigation sécurisée de Google, le filtre antihameçonnage de Microsoft), en ajoutant une « barre d'outils » au navigateur, en activant les paramètres antihameçonnages ou antispam dans leur compte de courriel, et en activant les protections antihameçonnages de leur antivirus.

2. Détection

La détection des attaques par hameçonnage non seulement empêche l'attaque elle-même, mais également aide à détecter les attaques futures. En outre, sans détection, les sites ne peuvent pas être récupérés pour analyser les aspects criminalistiques, bloqués par les navigateurs et les filtres antispam, suspendus ou examinés. La détection peut prendre plusieurs formes qui varient en fonction de la position à partir de laquelle la détection a lieu. L'objectif ultime de la détection consiste à détecter les sites ou campagnes courriel d'hameçonnage les plus récents, mais souvent le moyen de le faire sera dans l'analyse du flux des messages entre les criminels et les victimes potentielles.

- Consommateur/employé : parce que les consommateurs sont les destinataires les plus susceptibles de recevoir le message, il est important que les marques potentiellement ciblées communiquent efficacement à leurs clients ce que ces derniers devraient faire au cas où ils reçoivent un courriel suspect. Les attaques d'hameçonnage ciblé visent les employés. La détection aura souvent sous la forme d'un courriel vu par un client ou un employé de la marque ciblée, donc les possibilités de signalement et la sensibilisation de l'utilisateur sont des étapes clés de la détection des attaques (voir ci-dessous).
- Courriel rejeté : depuis des années, l'une des méthodes les plus efficaces pour convaincre une victime potentielle qu'un message d'hameçonnage était légitime consistait à utiliser un domaine d'envoi de la marque imitée. Des courriels provenant de « @paypal.com » ou de « @bankofamerica.com » sont plus susceptibles d'être pris au sérieux par les victimes potentielles qui ignorent comme il est facile d'usurper l'adresse de l'expéditeur. Heureusement, lorsque de tels messages sont rejetés, souvent parce que le spammeur les a envoyés à un compte désactivé, fermé ou ne reçoit plus de messages, le serveur de courriel du destinataire renvoie ces messages à l'expéditeur. Comme décrit ci-dessus, dans le cas de l'authentification de courriel, DMARC fournit un protocole permettant de diriger où ces messages rejetés doivent être envoyés. L'analyse de ces messages rejetés peut souvent mener à la détection de nouvelles sources et sites d'hameçonnage.
- L'adresse URL de renvoi : lorsqu'un kit d'hameçonnage utilise un graphique, un fichier JavaScript, une feuille de style ou toute autre propriété de la marque imitée, le fichier journal de cette marque montrera que le fichier qui a été utilisé a reçu un renvoi d'un site Web tiers. Si « hackedsite.com/yourbank/verify.php » est une page d'hameçonnage et utilise un graphique de « yourbank.com/graphics/logo.gif », le fichier journal de celui-ci indiquera que « logo.gif » a reçu un renvoi de « hackedsite.com ». L'analyse de ces URL de renvoi est un excellent moyen de détecter les nouveaux sites Web d'hameçonnage. Ceci peut être accompli en interne par un personnel bien formé ou confié en externe à l'un de plusieurs fournisseurs.
- Spam sortant : du point de vue d'une entreprise, un fournisseur d'hébergement ou un FSI, il y a plusieurs façons de détecter les courriels d'hameçonnage générés par le réseau. Suivant les Conditions générales d'utilisation du service fourni, le réseau peut être en mesure de surveiller le courriel sortant pour la présence de caractéristiques suspectes, telles que la montée en flèche du volume, des domaines d'expéditeur en désaccord, des tentatives d'utilisation de port de courriel provenant d'un espace non autorisé du réseau, ou l'inclusion d'adresses IP appartenant au réseau sur diverses listes de réputation.

- Réutilisation des informations d'identification : une technique récente pour la détection des sites d'hameçonnage consiste à obliger les consommateurs d'utiliser une paire unique d'identifiant utilisateur et de mot de passe pour accéder à la marque de destination. Un plugiciel dans le navigateur du consommateur détecte toute tentative d'utilisation de la paire identifiant/mot de passe sur n'importe quel autre site et signale l'URL à la marque de destination à titre d'URL suspecte à examiner.
- Les produits de sécurité et les logiciels d'accès libre attentifs à l'hameçonnage : serveurs de courriel, les dispositifs de sécurité modernes et les services en nuage utilisent des notifications sur les sites adresses IP, noms de domaines et mécanismes d'hameçonnage connus. Basés à la fois sur la correspondance directe et l'analyse euristique d'URL incluses dans le courriel ou transitant par le réseau de l'entreprise, les appâts d'hameçonnage et les « clics » peuvent être détectés à des fins de blocage, d'alerte et d'action.

3. Signalement

Le signalement des attaques d'hameçonnage sert à deux fins. Il peut aider les marques qui sont imitées à répondre à la menace et fournir une voie qui pourrait être utile à l'application de la loi. Une fois qu'une attaque par hameçonnage est détectée, il existe plusieurs avenues permettant de la signaler afin de protéger les membres de la communauté au sens large en les informant sur les appâts qu'ils risquent de recevoir ou des sites Web d'hameçonnage qu'il pourrait visiter. Les marques et les organisations imitées dans les appâts et les sites Web d'hameçonnage peuvent alerter leurs clients, leurs employés et leurs unités constitutives — les victimes les plus probables. Les individus qui s'aperçoivent d'un site d'hameçonnage peuvent également le signaler, et les marques victimes peuvent aider en assurant et promouvant une méthodologie simple que leurs clients ainsi que d'autres peuvent utiliser pour leur signaler tout hameçon.

Une fois qu'une organisation a appris être la cible d'une campagne d'hameçonnage, il est important d'attirer l'attention de l'écosystème antihameçonnage composé d'organisations de l'industrie, de fournisseurs et les répondeurs aux incidents. Cela peut être fait pour les attaques occasionnelles par hameçonnage en signalant l'attaque par le biais de l'un des sites répertoriés à la fin de cette section.

Pour faciliter autant que possible le signalement, de nombreuses marques ont créé des adresses de courriel faciles à retenir telles que « reportphishing@targetedbrand.tld ». Pour encourager le signalement, les marques devraient mettre en évidence sur leurs sites des informations sur la façon de signaler un hameçon et sont encouragées à rendre disponible cette information dans leurs interactions avec les clients.

La plupart des principales cibles d'hameçonnage utilisent des services de tiers spécialisés, à la base, dans le traitement de contenu en ligne illégal/indésirable, car ceux-ci ont établi des relations et des processus avec de principaux fournisseurs et des capacités de traduction et ont des enquêteurs qui se penchent sur les menaces au sein de leur personnel. Quelle que soit la méthode de signalement utilisée, la constatation et le signalement des attaques par hameçonnage dans les plus brefs délais peuvent aboutir à l'identification du criminel.

De nombreux serveurs compromis contiennent des fichiers journaux qui laissent une trace indiquant comment ils ont été piratés et comment le contenu criminel a été placé sur le serveur. Aussi, chaque site d'hameçonnage doit fournir au criminel un moyen de recevoir les informations

d'identification volées. Cela se fait généralement par courriel, mais peut également comporter la mise en place de dossiers secrets sur le serveur Web d'où sont volées les informations d'identification. L'analyse des sites d'hameçonnage identifiés peut aider à identifier, désactiver ou surveiller ces points d'exfiltration de données et peut mener à l'identification des criminels.

4. Enquêtes policières et d'entreprises

La plupart des enquêtes d'hameçonnage sont effectuées par la société dont la marque est imitée, ou par les fournisseurs de renseignements sur les menaces ou les organismes d'application de la loi agissant en leur nom.[28] Utilisant plusieurs des techniques décrites dans la section « Analyse et renseignements » ci-dessus, les enquêteurs peuvent identifier et recenser les victimes et calculer leurs pertes, mais aussi trouver le lien entre les nombreux sites d'hameçonnage créés par un même criminel ou lui apportant des bénéfices financiers.

Plutôt que d'essayer de résoudre chaque cas séparément, les sociétés sont encouragées à développer des relations avec les organismes d'enquête pour comprendre les meilleures méthodes d'échanger ces informations. Aux États-Unis, le programme InfraGard du FBI et l'équipe spéciale des services secrets américains pour les crimes électroniques sont des programmes qui aident à développer ces relations. Les centres nationaux, tels que le National Cyber Forensics & Training Alliance (NCFTA), offrent aussi des opportunités d'envisager des partenariats public-privé dans les enquêtes sur la cybercriminalité. Une collaboration avec ces organisations peut aider les marques à jouer un rôle dynamique en faveur du processus d'application de la loi. Le fait d'avoir souvent plusieurs marques victimes représentées dans une seule affaire a pour effet une réponse plus dynamique des organismes d'application de la loi, tout en assurant la « sécurité de la multitude » pour les marques victimes qui peuvent trouver regrettable d'être nommées au nombre des victimes.

5. Sensibilisation de l'utilisateur/la victime

Le McAfee Labs a signalé fin 2014 que l'hameçonnage demeure une tactique efficace pour infiltrer les réseaux d'entreprises. Leur étude a révélé que 80 % des utilisateurs commerciaux sont incapables de détecter les arnaques, et que leurs employés du service financier ou de ressources humaines assurent une performance en dessous de la moyenne. Vos employés peuvent répondre à un questionnaire sur l'hameçonnage ici : https://phishingquiz.mcafee.com.[29] Ces chiffrent montrent à quel point il est important que nos entreprises et nos programmes gouvernementaux continuent de dispenser les formations obligatoires régulières à leurs employés. Ceci fut l'une des recommandations du Federal Financial Institutions Examination Council (FFIEC). SANS (www.sans.org) contient également des informations sur l'exécution d'un programme antihameçonnage sur leur site Web SecuringTheHuman.[30]

Bien que la formation des utilisateurs soit plus difficile à effectuer, les entreprises aux prises avec de hauts taux d'hameçonnage sont invitées à sensibiliser leurs clients à chaque fois que l'opportunité se présente de communiquer avec eux, que ce soit par un ajout à la facture mensuelle, un avertissement spécial lorsque le client se connecte au système en ligne, ou par un message enregistré lorsqu'elles interagissent avec leurs clients par téléphone. Les sociétés s'inquiétant du fait que leur marque soit associée à la cybercriminalité peuvent au lieu de cela adopter un message anticipatif, tel que la campagne « Stop. Think. Connect. » ou déclarer leur soutien à efforts gouvernementaux de cybersensibilisation, tels que les semaines et mois annuels de sensibilisation à la cybersécurité que proposent les pays les plus développés.[31, 32] De nombreuses ressources sont disponibles dans le cadre de ces campagnes de sensibilisation publique qui peuvent être adoptées par les sociétés.

L'APWG encourage les entreprises à aider à la formation « *just-in-time (juste à temps)* » en adoptant comme page d'accueil celle de l'APWG sur la sensibilisation à l'hameçonnage. Les administrateurs de site Web qui retirent un site après avoir être piraté sont également encouragés à remplacer la page par la page d'accueil de l'APWG.[33] Plusieurs organisations ont mis au point d'excellentes pages de formation pour aider à sensibiliser leurs utilisateurs. Celles-ci comprennent Visa et Stay Safe Online :

http://www.visasecuritysense.com/en_US/phishing-attack.jsphttp://www.visasecuritysense.com/en_US/phishing-attack.jsp
https://www.staysafeonline.org/

La Commission fédérale américaine (FTC) alerte avec un trait d'humour les consommateurs aux risques liés à l'hameçonnage et représentant les stratagèmes d'hameçonnage standard par le biais de jeux en ligne et de vidéos YouTube.

- Jeux en ligne : http://www.onguardonline.gov/media/game-0011-phishing-scams, et
- Vidéo sur Youtube : https://www.consumer.ftc.gov/media/video-0006-phishy-home.

6. Participation de l'industrie :

Les organisations de partage d'informations telles que le FS-ISAC (*Financial Services Information Sharing Analysis Center*) et l'équipe des institutions financières du Canada pour la réponse aux incidents cybernétiques (*Canadian Financial Institutions' Computer Incident Response Team* - CFI-CIRT) sont également d'importance pour aider à traiter les crimes par hameçonnage multimarque.

La participation à des groupes de plaidoyer de l'industrie, tels que le Groupe de travail antihameçonnage (APWG)[34], le Groupe de travail anti abus pour la messagerie, les programmes malveillants et les mobiles (M[3]AAWG)[35], la *Online Trust Association* (OTA)[36], le *Merchant Risk Council* (MRC)[37], et le *Forum of Incident Response and Security Teams* (FIRST)[38] sont quelques-unes des organisations associatives portant sur la fraude en ligne et le cyberdélit. Les réunions de leurs membres, leurs publications, ainsi que leurs groupes d'intérêts spéciaux offrent de nombreux bénéfices aux marques victimes d'hameçonnage. L'APWG, à titre d'exemple, propose des capacités multiples pour le partage d'informations et le signalement à grande échelle des sites d'hameçonnage à ses organisations membres, ce qui le rend une ressource des plus précieuses pour les entités visées par des attaques d'hameçonnage.

RÉFÉRENCES

STATISTIQUES

- Rapports du Groupe de travail antihameçonnage sur les tendances d'hameçonnage et sur l'utilisation des noms de domaine
  http://www.antiphishing.org/resources/apwg-reports/

  [N.B. Sur demande écrite, l'APWG peut fournir des tableurs contenant les données sources de ses rapports de l'année courante jusqu'en 2006. Contact : secretarygeneral@apwg.org]http://www.apwg.org/reports/APWG_CrimewareReport.pdf
- Enquête mondiale sur l'hameçonnage du Groupe de travail antihameçonnage :
  http://docs.apwg.org/reports/APWG_Global_Phishing_Report_1H_2014.pdf

- Enquête sur les vulnérabilités du Web du Groupe de travail antihameçonnage http://www.apwg.org/reports/apwg_web_vulberabilities_survey_june_2011.pdfhttp://www.apwg.org/reports/apwg_web_vulberabilities_survey_june_2011.pdf
- Hameçonnage : combien y a-t-il qui prennent l'appât ? Gouvernement du Canada http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-eng.aspxhttp://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-eng.aspx

PROGRAMME À L'USAGE SPÉCIFIQUE DE L'UTILISATEUR

- Le Code de conduite antibot des fournisseurs de services Internet : http://www.m3aawg.org/abcs-for-ISP-code
- iCode.org — Association de l'industrie de l'Internet : https://icode.orghttps://www.ccc.go.jp/en_activity/index.html
- Centre consultatif anti réseau zombie — ECO (Allemagne) : https://www.botfrei.de/en/https://www.botfrei.de/en/
- STOP. THINK. CONNECT. http://www.stopthinkconnect.org
- Conseils au consommateur de l'APWG : http://www.antiphishing.org/resources/overview/
- Sensibilisation des consommateurs de l'APWG : http://www.antiphishing.org/resources/Educate-Your-Customers/ http://www.stopthinkconnect.org

SIGNALEMENT DE L'HAMEÇONNAGE :

Groupe de travail antihameçonnage :
http://www.antiphishing.org/report-phishing/
Courriel : reportphishing@apwg.org

Fournisseurs principaux de navigateurs et de services de courriel :
Google :https://www.google.com/safebrowsing/report_phish/https://www.google.com/safebrowsing/report_phish/
Microsoft :
www.microsoft.com/security/online-privacy/phishing-scams.aspx#Reporthttp://www.microsoft.com/security/online-privacy/phishing-scams.aspx - Report
Yahoo :
https://safety.yahoo.com/Security/IVE-BEEN-PHISHED.htmlhttps://safety.yahoo.com/Security/IVE-BEEN-PHISHED.html
https://safety.yahoo.com/Security/IVE-BEEN-PHISHED.html
Ressources pour les fournisseurs de sécurité en ligne :
http://www.phishtank.orghttp://www.phishtank.org
https://submit.symantec.com/antifraud/phish.cgihttps://submit.symantec.com/antifraud/phish.cgi
http://phishing.eset.com/reporthttp://phishing.eset.com/report
http://toolbar.netcraft.com/report_urlhttp://toolbar.netcraft.com/report_url
http://toolbar.netcraft.com/report_url
États-Unis :
Le Internet Crime and Complaint Center fournit un signalement centralisé des cybercrimes où des pertes ont eu lieu : www.ic3.gov/default.aspxhttp://www.ic3.gov/default.aspx
US-CERT propose également une adresse à laquelle tous les rapports d'hameçonnage peuvent être envoyés : https://www.us-cert.gov/report-phishinghttps://www.us-cert.gov/report-phishing

Courriel : phishing-report@us-cert.gov
Le système de signalement de spam de la Commission fédérale de commerce alimente la Consumer Sentinel Data Base, une base de données servant d'outil pour les enquêtes policières : UCE@ftc.gov
Canada :
« Centre de notification des pourriels » :
fightspam.gc.ca
Courriel : spam@fightspam.gc.ca
Centre antifraude du Canada :
www.antifraudcentre.ca/english/reportit-howtoreportfraud.htmlhttp://www.antifraudcentre.ca/english/reportit-howtoreportfraud.html
www.antifraudcentre.ca/francais/reportit-howtoreportfraud.htmlhttp://www.antifraudcentre.ca/francais/reportit-howtoreportfraud.html
L'Association des banquiers canadiens publie une liste des pages de signalement du spam de la plupart des banques canadiennes : www.cba.ca/en/consumer-information/42-safeguarding-your-money/91-email-fraud-phishing

Royaume-Uni :
Le National Fraud & Cyber Crime Reporting Centre permet de signaler la fraude, les tentatives de fraudes, ainsi que les arnaques en ligne ou les virus. Les consommateurs peuvent utiliser le lien ci-dessous pour signaler une fraude.
www.actionfraud.police.uk/report_fraud
L'Action Fraud Business Reporting Tool est un outil destiné aux professionnels de la sécurité compétents qui aurait besoin de signaler plusieurs cas de fraude chaque jour :
https://app03.actionfraud.police.uk/report/Account
Irlande :
https://www.botfrei.de/ie/ueber.html

Australie :
http://www.acma.gov.au/Citizen/Stay-protected/My-online-world/Spam/reporting-spam-i-acma
https://www.scamwatch.gov.au/content/index.phtml/tag/reportascam
https://report.acorn.gov.au/https://report.acorn.gov.au/
Courriel : report@submit.spam.acma.gov.au

Nouvelle-Zélande :
http://complaints.antispam.govt.nz/

France :
https://www.signal-spam.fr
Le CERT-LEXSI français, l'Europol, et les gouvernements des Pays-Bas et du Luxembourg proposent également un site pour le signalement de l'hameçonnage :
https://phishing-initiative.eu

MEILLEURES PRATIQUES COURANTES

- What To Do If Your Website Has Been Hacked (Que faire si votre site est piraté) http://www.apwg.org/reports/APWG_WTD_HackedWebsite.pdf
- Rapport consultatif sur les registres des sous-domaines http://www.apwg.org/reports/APWG_Advisory_on_Subdomain_Registries.pdf
- Recommendations sur les meilleures pratiques antihameçonnages destinées aux opérateurs de registres http://www.apwg.org/reports/APWG_RegistrarBestPractices.pdf
- Mesures pour protéger les services d'enregistrement de noms de domaine contre l'exploitation et le mauvais usage https://www.icann.org/en/system/files/files/sac-040-fr.pdf
- *M³AAWG Sender Best Communications Practices, Version 3.0* https://www.m3aawg.org/sites/default/files/document/M3AAWG_Senders_BCP_Ver3-2015-02.pdf
- Trust in Email Begins with Authentication (Rapport officiel du M3AAWG sur l'authentification du courriel) https://www.m3aawg.org/sites/default/files/document/M3AAWG_Email_Authentication_Update-2015.pdf
- M³AAWG /APWG Anti-Phishing Best Practices for ISPs and Mailbox Providers, Version 2.01 https://www.m3aawg.org/sites/default/files/M3AAWG_AWPG_Anti_Phishing_Best_Practices-2015-06.pdf

NOMS DE DOMAINE ET ADRESSES IP

Une variété d'activités malveillantes et illégales peut tirer parti des vulnérabilités du Système de noms de domaine (DNS) en raison de pratiques commerciales et de sécurité inefficaces des opérateurs de l'Internet qui se penchent sur l'infrastructure et les registres des noms de domaine, les bureaux d'enregistrement, les revendeurs et les fournisseurs de services d'anonymisation, ainsi que d'enregistrement fiduciaire. Une meilleure gestion par les opérateurs de réseau et de meilleures pratiques par les organisations qui gèrent les adresses IP et les noms de domaine, ou les organisations qui fournissent des services d'enregistrement de noms de domaine, peut atténuer ces menaces.

APERÇU DE LA TECHNOLOGIE

ADRESSES DE PROTOCOLE INTERNET (IP)

Chaque ordinateur sur Internet a une adresse IP qui sert à acheminer le trafic vers et à partir de cet ordinateur. Les adresses IP traditionnelles, dites adresses IPv4 sont constituées de nombres binaires codés sur 32 bits, exprimés par quatre nombres décimaux de la manière suivante 64.57.183.103. La première partie de l'adresse, dans ce cas précis 64.57.183, indique le réseau, et le reste de l'adresse, en l'occurrence 103, identifie un ordinateur particulier (« hôte ») sur le réseau. La division entre le réseau et l'hôte varie en fonction de la taille du réseau, donc l'exemple ci-dessus n'est que typique. Une version plus récente appelée IPv6 utilise un système d'adressage beaucoup plus large de 128 bits, exprimé par des blocs de chiffres séparés par deux points, tels que 2001:500:2F::F. Les adresses IPv4 ont été presque toutes attribuées, donc nous sommes maintenant à mi-chemin d'une transition progressive vers l'IPv6.

Pour que le trafic du réseau puisse s'écouler d'un ordinateur à un autre, par exemple, à partir de l'ordinateur d'un utilisateur vers les serveurs Web de Google ou vice-versa, le trafic sortant de

l'ordinateur s'écoule au moyen d'ordinateurs intermédiaires, appelés routeurs, vers sa destination.

Il y a environ 500 000 itinéraires de réseau visibles aux plus grands routeurs de l'Internet, appelés les routeurs principaux. (Le nombre total de réseaux est beaucoup plus élevé, car une route principale couvre généralement des dizaines de milliers de réseaux de clients.) Pour maintenir les tableaux de 500 000 itinéraires, les routeurs principaux utilisent le système *Border Gateway Protocol* (BGP) qui sert à échanger des informations, de sorte que les routeurs peuvent ajuster automatiquement les tableaux lorsque de nouveaux réseaux sont en ligne ou qu'un lien entre les réseaux échoue ou est en cours de réparation.

Un peu à la manière des numéros de téléphone, chaque adresse IP visible dans le monde doit être unique. Les fournisseurs de service Internet et les grandes entreprises obtiennent des blocs d'adresses directement à partir de registres Internet régionaux tels que ARIN qui attribuent les espaces IP pour les États-Unis, le Canada et certaines parties des Caraïbes, tandis que les petites entreprises et les particuliers utilisent des parties de blocs attribués à leurs fournisseurs de services Internet. Certaines adresses IP ne sont pas visibles dans le monde, par exemple 192.168.1.1 ou 10.0.0.51; elles sont analogues aux extensions de l'autocommutateur privé (*Private Branch Exchange* - PBX) dans un système téléphonique d'entreprise, accessible uniquement à partir du propre réseau de cette organisation.

LE SYSTÈME DES NOMS DE DOMAINE

Étant donné qu'il peut être difficile aux personnes de se souvenir des adresses IP et que celles-ci sont liées à des réseaux physiques, le Système des noms de domaine (DNS) est une base de données distribuée contenant des noms et permettant à une personne d'utiliser un nom comme www.google.com à la place de l'adresse IP correspondante 173.194.73.105 (pour IPv4) ou 2607:f8b0:4000:807::1012 (pour IPv6). Malgré sa taille énorme, le DNS offre une excellente performance grâce à des caches et des délégations. Parce qu'il serait impossible de stocker tous les noms en une seule base de données au sein du DNS, il est divisé en zones stockées sur des serveurs différents, mais reliées logiquement.

En principe, pour trouver l'adresse de www.google.com de Google, le logiciel de recherche DNS sur l'ordinateur d'un utilisateur, connu sous le nom d'un programme de résolution, contacte d'abord l'un des serveurs racines du DNS, qui réponds que pour tous les noms en .com, il faudra rechercher dans une liste de serveurs DNS qui ont des informations faisant autorité pour .com (dans ce cas, géré par Verisign). Ensuite, il contacte l'un des serveurs du .com, qui à son tour répond que pour tous les noms de google.com, il faudra rechercher dans la liste des serveurs DNS contenant l'information des noms google.com (gérés évidemment par Google). Enfin, il contacte l'un de ces serveurs DNS, qui fournit les adresses IP pour www.google.com.http://www.google.com./

Comme les utilisateurs d'Internet ont tendance à rechercher les mêmes noms à maintes reprises, chaque réseau et de nombreux ordinateurs individuels ont un cache qui se souvient des requêtes et des réponses DNS récentes, donc si quelqu'un utilisant le cache a récemment demandé www.google.com, les requêtes suivantes peuvent être répondues à partir du cache plutôt que d'aller vers les serveurs maitres. Ou si quelqu'un demande mail.google.com ou www.yahoo.com, le cache fournit les serveurs pour google.com (pour mail.google.com) ou les serveurs pour .com (pour www.yahoo.com), réduisant fortement le nombre de requêtes vers les serveurs maitres, et accélérant les réponses aux utilisateurs.

Comme il existe diverses façons par lesquelles les partis hostiles peuvent injecter de fausses

données DNS dans les caches et les ordinateurs individuels (certaines discutées ci-dessous), les extensions de sécurité du système des noms de domaine (DNSSEC) ajoutent des signatures cryptographiques sécurisées aux données renvoyées par les serveurs DNS, afin que les ordinateurs de l'utilisateur puissent vérifier la validité des signatures et veiller à ce que les données du DNS qu'ils utilisent soient valides et proviennent en fait de la bonne partie. Le DNSSEC se développe depuis 17 ans, mais n'a été significativement utilisé qu'au cours des dernières années. La gestion des clés du DNSSEC est complexe, et peut présenter un défi pour les responsables des serveurs du DNS.

EXPLOITATION DES VULNÉRABILITÉS DU DNS

Les plus graves exploitations de failles du DNS (Système des noms de domaine) sont les celles concernant les programmes de résolution, à travers lesquelles des cybercriminels introduisent des données faussées pour rediriger le trafic Web et autre à de fausses versions de sites Web populaires.

POLLUTION DE CACHE

La pollution du cache est une catégorie de ces exploitations qui consiste à utiliser les failles de sécurité pour introduire des données forgées dans les caches du DNS d'où elles sont fournies aux ordinateurs des victimes. Peu d'utilisateurs peuvent détecter les fausses informations du DNS utilisées par leurs ordinateurs. En conjuguant plusieurs exploitations, une personne malveillante peut présenter une réplique parfaite d'un site Web, d'un sceau de confiance, d'un logo, et afficher le nom de domaine correct dans la barre d'adresse du navigateur. Ceci peut se solder par un vol d'informations d'identification, l'accès à des ressources financières, la compromission de renseignements d'entreprise ou d'États, ou tout simplement une redirection vers des publicités pour des bénéfices financiers.

Les exploitations malveillantes de programme de résolution se produisent en entier chez une NSP (un fournisseur de services de noms tel que le serveur de nom de l'entreprise, ou un service DNS public comme OpenDNS ou Google DNS) et dans les systèmes des opérateurs de réseaux, sans besoin de compromettre l'ordinateur d'un utilisateur.

Lorsque le DNSSEC est correctement déployé par toutes les parties à une recherche de nom, y compris le titulaire de nom de domaine, le bureau d'enregistrement, et le NSP, il empêchera la pollution de cache ainsi que d'autres usages malveillants du DNS. Actuellement, le DNSSEC n'est que faiblement déployé, et n'est toujours pas considéré comme une défense fiable contre la pollution de cache. La défense actuellement déployée contre la pollution de cache est appelée *UDP Source Port randomisation*, mais cette défense a nécessité, en 2008, que tous les logiciels DNS soient mis à niveau.

Les logiciels du DNS, comme tous les logiciels de l'infrastructure de l'Internet, doivent être mis à niveau périodiquement pour corriger les défauts connus au fur et à mesure qu'ils sont découverts et réparés par le fournisseur de logiciel. Un contrôle minutieux est recommandé en tout temps pour détecter les conditions anormales de l'infrastructure en ligne, mais ce contrôle devient d'une importance capitale après chaque mise à jour de logiciel puisque la mise à jour pourrait corriger quelques défauts tout en introduisant d'autres.

La sécurité contextuelle mérite aussi d'être mentionnée. Si le logiciel de DNS était complètement exempt d'erreur, il serait toujours nécessaire de totalement sécuriser, mettre à jour et contrôler le système d'exploitation, y compris les systèmes de virtualisation ainsi que les routeurs, les

commutateurs, les pare-feux, et les systèmes de détection et de prévention d'intrusion. Le RFC 2196, le Manuel sur la sécurité des sites, donne un aperçu de ces questions.

MEILLEURES PRATIQUES :

1. Soutenir le déploiement mondial du DNSSEC afin de sécuriser la distribution des données du DNS. Ceci comprend la signature de toutes les zones d'autorité avec le DNSSEC, et permettre la validation par le DNSSEC dans tous les serveurs DNS récursifs.
2. Utiliser le TSIG (Protocole de signature de transaction du DNS) pour toutes les mises à jour du DNS en ligne, ainsi que pour les opérations de transfert de zone de serveur à serveur, pour assurer l'authenticité et l'autorisation.
3. Garder patché le logiciel de DNS jusqu'à la dernière version recommandée par le vendeur, et surveiller l'infrastructure du DNS à la recherche d'anomalies en tout temps, mais particulièrement après l'installation d'un correctif publié par le vendeur.
4. Fournir un document des meilleures pratiques en matière de politique de sécurité pour les programmes de résolution de DNS, afin de sensibiliser les responsables de réseaux et de systèmes.

PROGRAMMES MALVEILLANTS CIBLANT LE DNS

La méthode « DNS Changer » est une autre façon de falsifier les réponses du DNS. Ce programme malveillant modifie l'ordinateur de chaque victime afin que celui-ci change le programme de résolution de DNS qu'il utilise, substituant les programmes de résolution de DNS contrôlés par la personne malveillante à ceux du programme de résolution du FSI de l'utilisateur. La personne malveillante fournira ensuite, de manière sélective, des réponses falsifiées à chaque fois que cela lui apportera un revenu supplémentaire.

Le DNS Changer fonctionne non seulement sur les ordinateurs des utilisateurs, mais aussi sur les routeurs des maisons ou des petites entreprises. L'avantage qu'apporte pour la personne malveillante la modification des paramètres du routeur est que ce changement est susceptible de durer plus longtemps et de couvrir tous les ordinateurs, téléphones, iPad et autres appareils d'une maison ou d'un bureau - comprenant potentiellement tous les appareils de contrôle de la maison qui sont sans fil, tel que les thermostats, les caméras, les cadres photo, les réseaux sans fil et filaires, etc. Le routeur pourrait être à l'intérieur du modem fourni par le service à large bande ou un appareil externe acheté et installé par l'utilisateur.

Le FBI a travaillé avec le secteur privé pour priver les cybercriminels du DNS Changer de leurs ressources (et de leur liberté).[39] Les adresses IP utilisées par les programmes de résolution compromis ont été réacheminées vers des programmes de résolution précis pendant plusieurs mois, tandis que des groupes de bénévoles notifiaient les FSI et les utilisateurs touchés. Remarque : la stratégie de base utilisée par les criminels du DNS Changer fonctionnerait tout aussi bien s'ils l'essayaient à nouveau — toutes les vulnérabilités sous-jacentes nécessaires sont encore présentes dans l'équipement très populaire qui ne peut être mis à niveau par le vendeur.

La détection du trafic DNS mal orienté peut être effectuée au niveau du FSI en surveillant le trafic DNS des clients sortant vers des programmes de résolution autres que celui qu'ils fournissent. Il convient de noter qu'il est très fréquent pour les utilisateurs techniquement avancés — ou ceux qui

se sont volontairement abonnés à un service de DNS différent — d'acheminer ailleurs leur trafic de DNS. Une conception soignée des systèmes de détection est nécessaire pour éviter les faux positifs.

À l'avenir, les utilisateurs peuvent être amenés à passer au programme de résolution d'un acteur malveillant par piratage psychologique ou par incitation. À titre d'exemple, si les programmes de résolution du FSI doivent refuser l'accès à certains noms du DNS (tels que le contenu piraté ou autrement illégal), les utilisateurs peuvent répondre à des offres qui promettent un accès non censuré au DNS. Il existe bon nombre de raisons légitimes pour permettre aux utilisateurs de choisir leur service de résolution de DNS sans censure ni interférence.

MEILLEURES PRATIQUES :

1. Sensibiliser le public sur les dangers du changement de programme de résolution de DNS afin de limiter les attaques par piratage psychologique.
2. Encourager les opérateurs de réseau à diffuser de manière anonyme les caches DNS non locaux qui sont les plus recherchés dans leurs réseaux, afin d'identifier d'éventuels programmes de résolution de DNS malveillants.
3. Fournir les informations diffusées à tous les chercheurs anti abus approuvés pour aider à détecter les services ayant dupé les utilisateurs ou ayant falsifié des réponses du DNS et pour les distinguer des services légitimes de résolution de DNS.
4. Élaborer des indicateurs sur la base de ces données agrégées pour aider à identifier les cybercriminels et les traduire en justice, mettre à jour une liste noire des programmes de résolution frauduleux, et créer des initiatives de mitigation coordonnée comme celle qui a eu lieu pour lutter contre le DNS Changer.
5. Mettre en place des meilleures pratiques pour l'anonymisation, suffisant pour empêcher la connexion des utilisateurs originaux, leurs FSI, et l'activité DNS, afin d'éviter des représailles contre les utilisateurs qui contournent la censure, car cela ne ferait que mener les utilisateurs à utiliser des programmes de résolution de DNS plus difficiles à détecter, mais pouvant potentiellement être tout aussi compromis.

ATTAQUE PAR USAGE MALVEILLANT DES SERVICES D'ENREGISTREMENT DE NOMS DE DOMAINE

La facilité avec laquelle les cybercriminels peuvent enregistrer et utiliser de nouveaux domaines les aide à mener à bien leurs fraudes. La fourniture de fausses informations sur leur identité et l'usage fréquent de références financières volées rendent difficile l'identification des véritables propriétaires des noms de domaines qui sont utilisés pour commettre les fraudes. La charge de détecter l'utilisation malveillante des noms de domaine repose sur les épaules des chercheurs anti abus, souvent longtemps après le début de l'activité malveillante a commencé, et parfois même après sa fin. La charge de mitiger les domaines malveillants s'impose à chaque entreprise fournissant un accès Internet à des utilisateurs — soit par des requêtes visant à suspendre les activités malveillantes ou par la propagation souvent lente de listes rouges contenant ces domaines. Les listes rouges sont nécessaires parce que les demandes de redirection, de suspension ou de suppression des noms de domaines sont souvent ignorées.

Les cybercriminels exploitent des services d'enregistrement de domaine en utilisant des cartes de crédit volées pour enregistrer les domaines, en enregistrant rapidement de nombreux domaines

grâce à l'automatisation, en enregistrant des domaines par le biais de revendeurs ou de fournisseurs de services d'anonymisation et d'enregistrement fiduciaire qui ne sont pas réceptifs ou qui semblent permettre une activité malveillante, et en changeant souvent de domaines qu'ils peuvent utiliser quelques minutes, voire quelques secondes après les avoir enregistrés. Les chercheurs d'abus généralement ne peuvent surveiller les données d'enregistrement du DNS nouvellement enregistrées que par capture instantanée toutes les 24 heures. Les listes rouges ont besoin d'un certain temps avant de reconnaitre les domaines malveillants et ensuite propager l'information sur leur réputation après que l'acteur malveillant ait commis son acte de malveillance.

Les cybercriminels peuvent créer un sous-domaine sur la base des domaines qui leur appartiennent, tel que bankname.ssl-cgi.Cybercriminalsexample.com. Il n'y a aucune limite au nombre de noms pareils qu'ils peuvent créer — gratuitement. Duper les utilisateurs ne nécessite pas un nom de marque, mais juste quelque chose qui semble réaliste. Les noms comme secure-order.verified. exemple.com sont acceptés par la plupart des utilisateurs, car ils ressemblent à d'autres noms qu'ils ont souvent vus.

Certaines entités aident en fait à commettre des abus d'IP en créant des noms de domaine susceptibles d'induire en erreur les consommateurs. Ces services créent des noms de domaine qui imitent les marques délibérément en utilisant des fautes de frappe comme SEARZ avec la lettre « Z » au lieu de la lettre « S », ou PAYPA1 avec le chiffre « 1 » au lieu de la lettre « L ». Bien que ces domaines peuvent ne jamais servir à une campagne d'hameçonnage, ils existent par millions, donc il devient difficile pour les chercheurs d'abus de distinguer le *typosquattage* relativement inoffensif de la prochaine activité malveillante avant qu'elle ne se produise.

En outre, les attaquants détournent des noms de domaine à travers d'autres techniques, notamment :

- en compromettant les informations d'identification permettant au titulaire de nom de domaine d'accéder au panneau de commande du bureau d'enregistrement (en volant le mot de passe que les clients utilisent pour se connecter au site de gestion de leur domaine) ;
- en compromettant les systèmes du bureau d'enregistrement afin de voler l'ensemble ou une partie des mots de passe (appelé protocoles EPP ou codes d'autorisation) requis pour transférer des noms de domaine d'un bureau d'enregistrement à un autre ; et
- en compromettant les noms de serveurs , ou sa base de données DNS, afin de modifier sur place les données relatives au domaine de la victime, sans aucune redirection en amont.

MEILLEURES PRATIQUES :

1. Les opérateurs de registre de noms de domaine, tant pour les espaces des domaines génériques de premier niveau (gTLD) que pour ceux des domaines de premier niveau géographique (ccTLD), ainsi que les bureaux d'enregistrement avec lesquels ils traitent, devraient mettre en œuvre et superviser étroitement l'obligation de s'informer sur les clients « *Know your customer* » afin de prévenir les usages malveillants lors de l'attribution des domaines. Cela leur permettra de déterminer si et quand ils devraient éviter de traiter avec un opérateur de registre, un bureau d'enregistrement, un revendeur ou un fournisseur de services d'anonymisation et d'enregistrement fiduciaire.
2. Tous les opérateurs de registre, les bureaux d'enregistrement, les revendeurs et les fournisseurs de services d'anonymisation et d'enregistrement fiduciaire devraient

appliquer une authentification HTTPS obligatoire à facteurs multiples, pour réduire le risque de vol d'informations d'identification de compte client et mieux protéger les sessions transactionnelles de leurs clients.

3. Les opérateurs de registre et les bureaux d'enregistrement de noms de domaines devraient envisager des accords de coopération ou de protocoles d'accord avec les organisations de protection des consommateurs, tels que LegitScript et le Groupe de travail antihameçonnage (APWG). En établissant des niveaux prédéfinis de confiance, les rapports d'abus émanant de ces organismes peuvent être traités par les opérateurs de registre ou les bureaux d'enregistrement d'une manière beaucoup plus rapide et plus efficace, comme le programme de suspension de domaine malveillant de l'APWG.
4. Les opérateurs de registres et les bureaux d'enregistrement des noms de domaine devraient rechercher rigoureusement des cartes de crédit volées lors des enregistrements, pour empêcher l'enregistrement de domaines malveillants.
5. Faire appliquer des obligations juridiques (dans leurs propres juridictions nationales) et contractuelles que les fournisseurs de services d'enregistrement de domaine, y compris tous les opérateurs de registre, les bureaux d'enregistrement, les revendeurs et les fournisseurs de services d'anonymisation et d'enregistrement fiduciaire doivent respecter concernant l'action spécifique aux rapports d'abus.
6. En ce qui concerne les services d'anonymisation et d'enregistrement fiduciaire, il est urgent de mettre en œuvre et d'appliquer des programmes d'accréditation. Ceci permettra de clarifier les règles et les processus de traitement des requêtes visant à « relayer », transmettre des communications au client sous-jacent, et à « révéler », divulguer l'identité du client. Cela s'applique à tous les services d'anonymisation et d'enregistrement fiduciaire, indépendamment de savoir s'ils opèrent dans l'espace gTLD ou l'espace ccTLD et s'ils appartiennent, sont gérés ou exploités par un opérateur de registre ou un bureau d'enregistrement.
7. Les opérateurs de registre et les bureaux d'enregistrement, tant pour les espaces gTLD que pour les espaces ccTLD, devraient éviter de traiter avec des fournisseurs de service d'anonymisation et d'enregistrement fiduciaire n'ayant pas souscrit à un programme d'accréditation.
8. Avant de traiter les demandes d'enregistrement de nouveaux noms de domaine ou d'accepter les transferts de domaines entrants, les bureaux d'enregistrement et les opérateurs de ccTLD qui offrent des services d'enregistrement directement au public devraient valider la réputation de certains éléments des données d'enregistrement, tels que :
    a. les adresses de courriel utilisées par le titulaire de nom de domaine, par le titulaire du compte et tous les autres contacts du WHOIS,
    b. l'adresse IP à partir de laquelle les transactions sont demandées,
    c. les serveurs de noms que les clients souhaitent définir pour leur nom de domaine,
    d. l'adresse postale du titulaire de nom de domaine, et
    e. un échantillon statistiquement valable des noms de domaine déjà enregistrés par le même client.

    À titre d'exemple, un service de validation de réputation est fourni gratuitement par la Secure Domain Foundation et permet aux bureaux d'enregistrement et opérateurs de registres appropriés de décider de refuser la création de nouveaux noms de

domaine, ou d'accepter les transferts entrants, si des éléments de données ont une mauvaise réputation indiquant une activité malveillante récente.

9. Améliorer les algorithmes de réputation afin qu'ils comprennent l'âge du domaine : les domaines de plus d'un an sont moins susceptibles d'être « rejetés » ; certains services d'accréditation de courriel empêchent les clients d'utiliser des domaines de moins d'un mois ; et, examiner les domaines de moins d'une journée est actuellement un moyen efficace pour trouver les activités malveillantes.
10. Étant donné que les pirates de domaine utilisent des adresses IP généralement différentes de celles qu'utilisent les titulaires, les bureaux d'enregistrement et les revendeurs devraient assurer un suivi de l'activité du compte concernant les adresses IP. Si une nouvelle adresse IP accède au compte du client, le bureau d'enregistrement ou le revendeur devrait informer tant le titulaire de nom de domaine que le contact administratif de ce nom de domaine.
11. Continuer à améliorer les navigateurs et à sensibiliser l'utilisateur pour que ce dernier sache reconnaitre les signaux de navigateur quant aux certificats de validation approfondie (« barre verte ») et pour empêcher la confusion de sites qui utilisent des termes comme « sécurisé » ou « ssl ».
12. Apprendre aux sociétés comment envoyer des notifications à l'utilisateur qui soient difficiles à imiter pour dissuader l'hameçonnage et le piratage psychologique.
13. Pour les sites et les logiciels utilisant des listes rouges de domaines, encourager une approche multicouche avec une variété de types de listes rouges, y compris les méthodes de blocage préventives ainsi que les listes rouges réactives, dans le but d'améliorer l'efficacité du blocage.
14. Soutenir les projets DNS passifs comme Farsight Security Inc (FSI) Security Information Exchange (SIE) qui fournissent des alertes rapides aux chercheurs académiques et commerciaux sur les sous-domaines malveillants activement utilisés.
15. Pensez à utiliser des technologies de pare-feu DNS telles que Response Policy Zones (RPZ), un marché ouvert de multiconsommateur multifournisseur, qui fournit des recommandations de politique de résolution de DNS aux opérateurs DNS récursifs. (Voir http://dnsrpz.info/)

ATTAQUES DNS DE SERVEUR WEB ET AUTRE

Les cybercriminels exploitent la réputation des domaines légitimes en pénétrant de façon illégale leurs serveurs et en y déposant des fichiers malveillants qui infectent ensuite le domaine légitime de l'URL. (Cette technique est insensible aux listes de domaine rouges, à moins que celles-ci soient disposées à mentionner des domaines légitimes qui servent du contenu malveillant, bloquant ainsi un contenu légitime au même titre que le contenu malveillant.)

Les cybercriminels utilisent les redirections de domaine pour présenter tout d'abord un domaine de bonne réputation, et ensuite rediriger l'utilisateur vers le site de destination malveillant. Ces personnes utilisent plusieurs niveaux de redirection et récemment même la redirection vers des URL à adresses IP numériques plutôt que vers des noms de domaine.

Le succès de ces techniques repose sur les méthodes de détection inadéquates qui peuvent reconnaitre ces attaques uniquement lorsque l'utilisateur « agit comme le ferait une victime », en suivant les redirections. Malheureusement, certains commerçants compliquent davantage la menace en utilisant plusieurs niveaux de redirection pour suivre la réaction des clients au courriel

de markéting. Il est souvent fait mauvais usage des services de raccourci d'URL qui sont souvent utilisés pour rediriger d'un domaine bien connu comme bit.ly au site Web malveillant de cybercriminels. Un utilisateur a du mal à faire la différence entre les millions d'URL bit.ly légitimes utilisés pour raccourcir l'adresse Web longue des messages de Twitter, et ceux qui conduiront à des programmes malveillants ou, par exemple, une annonce pour la vente illégale de produits pharmaceutiques.

Récemment, l'ICANN elle-même a été victime d'un groupe de pirates informatiques qui ont pu accéder au compte d'enregistrement de domaine de l'ICANN sur Register.com. Les attaquants ont en l'occurrence modifié les paramètres DNS de plusieurs domaines (icann.net, iana-servers.com, icann.com et iana.com) et détourné le trafic des visiteurs vers un site Web défiguré.

MEILLEURES PRATIQUES :

1. Établir et maintenir un système qui bloque les domaines légitimes compromis servant un contenu malveillant, la notification rapide, l'approche retester et retirer, ainsi qu'une aide à l'amélioration de l'hygiène sécuritaire sur tous les serveurs Web d'un site exploité.
2. Encourager les services de raccourci d'URL à vérifier et revérifier toutes les redirections de la chaine pour chacune des redirections qu'ils fournissent et à collaborer avec de multiples fournisseurs de protection d'abus afin d'identifier de nouveaux responsables d'abus.
3. Mettre au point une sensibilisation et des ressources destinées à l'industrie et aux utilisateurs finaux, pour leur apprendre à identifier et éviter les raccourcis d'URL auxquels font défaut les mesures anti abus adéquates.
4. Améliorer l'efficacité des contrôles de réputation des URL, entre autres par le test des redirections, des tests qui semblent être un utilisateur réel pendant le test, et l'élaboration de politiques concernant la profondeur maximale des redirections, tout cela pour limiter le mauvais usage des services de raccourci d'URL et services de redirection d'URL vulnérables.

ATTAQUES D'ADRESSES IP

Les attaques des adresses IP sont classées en deux catégories générales : les courriels qui mentent au sujet de leur adresse IP (usurpation) et les réseaux utilisant des plages d'adresses IP qu'ils ne sont pas autorisés à utiliser (annonce « *rogue* »).

USURPATION D'ADRESSES IP

Chaque paquet de données envoyé sur Internet contient l'adresse IP « source » de l'ordinateur à partir duquel il a été envoyé et l'adresse de l'ordinateur vers lequel il est destiné. Il est possible pour un ordinateur hostile de mettre une fausse adresse source (usurpée) sur le trafic sortant. Pour les transactions dans lesquelles la destination renvoie des paquets vers l'adresse source, notamment le DNS, cela peut créer du trafic indésirable vers la véritable adresse qui a été usurpée. Il est facile d'envoyer de petites requêtes DNS donnant lieu à de grands résultats DNS, se soldant par un déni de service à l'adresse usurpée.

MEILLEURES PRATIQUES :

1. Les FSI et les réseaux de transit devraient filtrer le courriel entrant, assurer le suivi de la plage d'adresses assignée à chaque réseau client, et rejeter le trafic dont l'adresse source se trouve en dehors de la plage assignée, pour empêcher leurs clients d'envoyer du trafic avec des adresses usurpées. Ceci est généralement appelé BCP 38[40], du nom d'un document de

l'IETF sur les meilleures pratiques actuelles. Le BCP 84, un autre document de l'IETF sur les meilleures pratiques, recommande que les fournisseurs en amont de connectivité IP filtrent les paquets qui pénètrent leurs réseaux en provenance de clients en aval, et rejettent tous les paquets ayant une adresse source qui n'a pas été assignée à ce client.[41]

2. Encourager une pratique universelle de filtrage à la sortie pour tous les clients connectés ou les réseaux de pairs.

ANNONCES « *ROGUES* » (FAUSSES ANNONCES)

Chaque réseau peut annoncer via BGP ses propres plages d'adresses IP. Les réseaux hostiles peuvent annoncer des plages réseau qu'ils ne sont pas autorisés à utiliser. Cela peut entrainer le reroutage et le détournement de trafic à destination du réseau réel, ou il peut autoriser un trafic « furtif » en annonçant une plage d'adresses, en effectuant une attaque et puis en retirant l'annonce. À moins que les victimes soient au courant de l'annonce « *rogue* » (fausse annonce), ils s'en prendront au propriétaire légitime des adresses.

MEILLEURES PRATIQUES :

1. Les opérateurs de réseau devraient mettre en œuvre le filtrage à la sortie[42] (discuté ci-dessus), du BCP 84, qui recommande que les annonces BCP provenant de clients et de pairs soient limitées à une liste explicite de réseaux reconnus comme étant attribués à ce client ou ces pairs.
2. Les FSI devraient s'efforcer, dans la mesure du possible, de mettre en œuvre le BGPSEC (sécurité BGP) pour cryptographiquement protéger les annonces d'itinéraire et empêcher la publication de données non fiables.

VOL DE PLAGES D'ADRESSES

Aux débuts de l'Internet, les adresses étaient souvent attribuées de manière informelle et les dossiers incomplets. De ce fait, un considérable espace ancien d'adresses attribuées pourrait être obsolète, soit parce que les organisations ont oublié les adresses qu'elles avaient utilisées ou parce que ces entités n'existent plus. Les cybercriminels ont profité de ces adresses abandonnées par la falsification de documents ou le réenregistrement de domaines abandonnés utilisés dans les courriels, afin de prendre le contrôle de l'espace d'adressage ancien.

MEILLEURES PRATIQUES :

1. Les registres Internet régionaux devraient mettre en œuvre et suivre des procédures permettant de vérifier l'identité des propriétaires prétendus d'espaces anciens, pour empêcher les cybercriminels de contrôler cet espace d'adresses. ARIN, le RIR de l'Amérique du Nord, a des procédures détaillées pour cela.[43]

RÉFÉRENCES

- Wikipédia, Discussion sur le DNSSEC : http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
- RFC 2196, *Site Security Handbook*, B. Fraser, Ed., septembre 1997, http://www.rfc-editor.org/info/rfc2196
- RFC 4034 *Resource Records for the DNS Security Extensions*. R. Arends, R. Austein, M. Larson, D. Massey, S. Rose. mars 2005, http://www.rfc-editor.org/info/rfc4034
- RFC 4035 *Protocol Modifications for the DNS Security Extensions.* R. Arends, R. Austein, M. Larson, D. Massey, S. Rose. mars 2005, http://www.rfc-editor.org/info/rfc4035
- US CERT Vulnerability Note VU#800113, « Multiple DNS implementations vulnerable to cache poisoning », http://www.kb.cert.org/vuls/id/800113/
- Groupe de travail sur le virus DNS Changer, http://www.dcwg.org/http://www.dcwg.org/
- Brian Krebs, « A Case of Network Identity Theft », http://voices.washingtonpost.com/securityfix/2008/04/a_case_of_network_identity_the_1.html
- Open Resolver Project, http://openresolverproject.org/
- *M³AAWG Sender Best Communications Practices, Version 3.0* https://www.m3aawg.org/sites/default/files/document/M3AAWG_Senders_BCP_Ver3-2015-02.pdf
- FCC CSRIC III Working Group 4 reports on BGP Security Best Practices: http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf

MENACES MOBILES ET DE TÉLÉPHONIE

L'ENVIRONNEMENT MOBILE

Avec l'avènement du smartphone et les marchés d'applications pour Android, Apple, Windows, et BlackBerry, les consommateurs recourent de plus en plus à leurs appareils mobiles pour accéder aux comptes en ligne, faire des achats et effectuer d'autres transactions financières. Les smartphones représentent 70 % des quelques 1,85 milliard de téléphones mobiles vendus au monde en 2014[44], Android et iPhone étant les dispositifs les plus couramment utilisés actuellement. La tablette, à mi-chemin entre téléphone et ordinateur traditionnel, est également devenue un principal acteur de ce domaine. Les ventes au détail d'appareils mobiles, y compris de tablettes, sont passées de 11 % de l'ensemble du marché électronique en 2011[45] à 13 % en 2014[46]

Mondialement, il y a environ 3,7 milliards d'utilisateurs actifs de téléphones mobiles[47], dépassant 50 % de la population mondiale qui s'élève à 7,3 milliards,[48] et la plupart d'entre eux accèdent à l'Internet via leur téléphone mobile. Pendant le quatrième trimestre de 2014, les vendeurs ont expédié plus de 500 millions d'unités mobiles à travers le monde.[49]

MARCHÉS D'APPLICATIONS

À la différence du marché de logiciel PC où les principales applications sont développées par un certain nombre de fournisseurs connus et de confiance et où les utilisateurs sont moins susceptibles d'installer des applications provenant de sources moins fiables, l'écosystème des applications mobiles encourage les utilisateurs finaux à charger un grand nombre d'applications de faible cout, de fournisseurs plus petits et souvent moins dignes de confiance, y compris de sociétés composées d'une seule personne. Dans de nombreux pays, la plupart des applications proviennent des marchés d'applications dont la sécurité laisse à désirer, qui proposent des applications chargées de programmes malveillants. Dans d'autres pays, les utilisateurs peuvent être initialement limités au chargement d'applications uniquement auprès des vendeurs de systèmes d'exploitation de téléphone ou de marchés d'applications approuvés par leur opérateur ; toutefois, les utilisateurs peuvent substituer les paramètres pour pouvoir accéder à n'importe quel marché d'applications. Les fournisseurs principaux de systèmes d'exploitation de téléphone, y compris Google, Apple, Microsoft et RIM, exploitent des marchés d'application volumineux qui disposent d'une sécurité renforcée. Apple, par exemple, a 1,4 million d'applications dans son App Store, générant 25 milliards USD de ventes cumulées pour les développeurs d'applications et de jeux à ce jour. Cependant, étant donné l'ampleur des marchés d'applications, même les plus surs, il devient extrêmement difficile d'empêcher les logiciels malveillants d'être occasionnellement offerts. Comme le commerce électronique a migré vers l'environnement mobile, les mauvais acteurs et les fraudeurs ont vite fait de suivre.

MENACES PARTICULIÈRES ET MEILLEURES PRATIQUES

SÉCURITÉ DES MAGASINS D'APPLICATIONS

Les smartphones peuvent être compromis par l'installation de nouveaux logiciels, souvent obtenus d'un magasin contrôlé par le fabricant du système d'exploitation (OS) du téléphone. En 2014, Symantec a conclu que 17 % (plus que 160 000) de toutes les applications Android étaient effectivement des programmes malveillants déguisés[50]. Lors d'un examen des 100 applications de santé de l'App Store, 20 % transmettaient les informations d'identification de l'utilisateur sans les chiffrer, plus de la moitié (52 %) n'avaient pas de politiques de confidentialité visibles et, en

moyenne, chaque application contactait cinq domaines Internet (généralement une combinaison de services de publicité et d'analytique)[51].

Certains fournisseurs de systèmes d'exploitation et certains magasins d'application ont la possibilité de supprimer les applications malveillantes du téléphone de l'utilisateur si cette application a été obtenue à l'origine de leur magasin. D'autres applications malveillantes seront rejetées avant d'intégrer le magasin si elles violent les politiques de sécurité définies par ce magasin.

Apple a placé davantage de restrictions sur les applications et les développeurs avant de leur permettre un accès à l'App Store. Le magasin Google Play a une politique d'acceptation plus ouverte et repose plus sur le retrait des applications acceptées qui s'avèrent être malveillantes ou qui violent les politiques de leur magasin d'applications.

Lorsqu'un consommateur achète un smartphone, l'accès aux magasins d'applications officieux est généralement désactivé ; le téléphone est verrouillé et ne permet qu'un petit ensemble de magasins « officiels » d'applications (par exemple, ceux du fabricant du système d'exploitation et de l'opérateur mobile). Les appareils mobiles qui utilisent le système d'exploitation Android ont un paramètre appelé « Sources inconnues » avec une case à cocher pour autoriser l'installation d'applications provenant de sources externes au marché. L'utilisateur peut reconfigurer les téléphones Android pour permettre la connexion vers des magasins d'applications non officiels ou différents. Les appareils Apple nécessitent un processus de débridage ou « *jailbreaking* » plus difficile techniquement ; toutefois, pour les utilisateurs moins avertis, ce service de débridage est proposé à un prix modeste dans beaucoup de kiosques et de points de vente. Même pour accéder des magasins d'applications différents tels que le Amazon Appstore, cette case doit être probablement cochée. Malheureusement, le téléphone est ensuite ouvert aux installations provenant de sources inconnues, quelles qu'elles soient. Les utilisateurs peuvent alors être plus facilement poussés à installer des programmes malveillants. L'auteur de programmes malveillants se permet un laissez-passer sans surveillance chez tous les magasins d'application mobile officiels une fois que l'accès aux magasins officieux est activé.

Il y a aussi de nouvelles façons pour les fraudeurs d'échapper aux restrictions des magasins d'applications, même si le téléphone est configuré pour utiliser uniquement le magasin officiel. Les navigateurs d'appareil mobile peuvent être utilisés pour installer des applications mobiles HTML5, qui placent une icône sur l'écran d'accueil de l'appareil semblable à une application installée depuis le magasin d'applications. Les attaquants peuvent alors exploiter les vulnérabilités du navigateur stock qui est livré avec l'appareil mobile, ou de navigateurs alternatifs que l'utilisateur peut choisir d'installer. Les liens entre le navigateur et les fonctions natives de l'appareil tels que la caméra, le microphone, les transmetteurs téléphoniques et la géolocalisation peuvent être utilisés par un criminel pour obtenir des données à caractère personnel et les activités courantes de l'utilisateur de l'appareil mobile.

La connexion nom d'utilisateur/mot de passe utilisée par chaque appareil mobile pour accéder au magasin d'applications et autoriser les achats est un important point de vulnérabilité. Une fois en possession de ces informations d'identification, les criminels peuvent organiser les pertes financières et installer les espiogiciels. Les systèmes d'exploitation mobiles d'Apple et de Google nécessitent actuellement les mêmes noms d'utilisateur et mot de passe que les clés du magasin d'applications et les autres services, y compris les ordinateurs portables, le stockage de fichiers en nuage, les contacts, le calendrier et le courriel. Alors qu'un nom d'utilisateur et mot de passe auraient autrefois seulement permis à un attaquant d'accéder au compte de courriel de l'abonné, les

mêmes informations d'identification permettent maintenant d'accéder au magasin d'applications. Dans plusieurs cas, les criminels obtenant cette information clé effacent toutes les données se trouvant sur des ordinateurs portables et des téléphones d'utilisateurs. Un certain nombre de tiers offrent une protection antivirus pour certains téléphones et font l'effort de tester toutes les nouvelles applications du magasin à la recherche d'activités malveillantes ou d'une intention de nuire.

MEILLEURES PRATIQUES POUR L'INDUSTRIE ET LE GOUVERNEMENT RELATIVES AUX MAGASINS D'APPLICATIONS

1. « Neutralité de l'application » : permettre aux utilisateurs et opérateurs de réseaux ou d'autres parties dignes de confiance de spécifier explicitement des magasins d'applications supplémentaires « dignes de confiance », et peut-être un niveau de confiance associé à chacun. Cela permet aux consommateurs de choisir d'autres magasins d'applications de renom sans s'exposer à des téléchargements risqués d'applications provenant de sources inconnues.
2. Identifier les applications à potentiel malveillant par des balayages de sécurité rigoureux avant de leur permettre d'être proposés par le magasin au lieu de compter sur les plaintes qui n'arriveront que par la suite.
3. Fournir des avertissements, des contrôles et des informations aux utilisateurs afin de réduire l'occurrence d'incidents où des utilisateurs seraient dupés et amenés à suivre des instructions malveillantes pour contourner les mesures sécuritaires.
4. Améliorer les politiques de sécurité des mécanismes de réinitialisation du mot de passe pour empêcher les criminels d'obtenir des informations d'identification du magasin d'applications ne leur appartenant pas.
5. Les appareils peuvent être verrouillés pour n'accéder qu'au magasin d'applications officiel comme mesure pratique anticoncurrentielle. Alors que ce modèle protège les consommateurs, il les invite aussi à employer des solutions de contournement qui introduisent des failles de sécurité (p. ex., le débridage, le « *rooting [accès au root)*] » ou le déverrouillage des appareils). Les politiques qui permettent ou aident au verrouillage des magasins d'applications devraient être évaluées au regard des failles de sécurité que peut créer le déverrouillage.
6. Encourager les magasins d'applications à s'abonner à des centres d'analyse des menaces de réseaux zombie/en ligne, afin qu'elles puissent bénéficier des analyses, alertes et rapports provenant de ces centres. Les applications malveillantes sont alors détectées, signalées et supprimées le plus rapidement possible.
7. Fournir des mécanismes permettant aux utilisateurs de signaler des applications potentiellement malveillantes.

PROGRAMMES MALVEILLANTS MOBILES

Des applications malveillantes, appelées programmes malveillants mobiles, existent pour les appareils utilisant les systèmes d'exploitation Android, iOS, Windows Phone, Symbian (Nokia) et BlackBerry. Actuellement, la majorité des programmes malveillants mobiles ciblent la plateforme Android dans les régions qui utilisent abondamment des marchés d'applications non officielles.

La plupart des programmes malveillants sont une application utile ou semblent l'être, et sont distribués sur les sites Web ou via des magasins d'applications non officielles. Souvent, les promoteurs des programmes malveillants altèreront des applications légitimes corrompues en insérant un code « cheval de Troie ». Les utilisateurs pourront ainsi installer ces applications modifiées, ignorant qu'elles contiennent du code malveillant. Les criminels utilisent de plus en plus la publicité numérique comme véhicule pour propager des programmes malveillants ; ceci est connu est connu sous le nom de *malvertising*, ou publicité malveillante. En outre, 2014 a vu l'émergence du ver SMS qui se propage par SMS en siphonnant le carnet d'adresses des appareils infectés.[52] Les destinataires sont dupés et amenés à cliquer le lien malveillant contenu dans le SMS qui les mène au code malveillant exploitant une faille de sécurité. S'ils installent ce code-là, alors leurs contacts recevront le même SMS malveillant, ce qui rend ce vecteur d'attaque très viral.

Un programme malveillant typique exécute des actions qui génèrent des revenus pour les attaquants. Les systèmes de monétisation directe entrainent une perte financière directe à la victime et comprennent des applications malveillantes qui peuvent effectuer des fonctions très variées, y compris : l'envoi de messages SMS surtaxés à un court-code enregistré par les attaquants ; le téléchargement au paiement de contenu ; le clic sur des liens payants au clic ; l'appel de numéros de téléphone payant ; l'interception d'informations d'identification bancaire en ligne ; et la demande de rançon pour déverrouiller les appareils des victimes. Les attaquants peuvent également générer des revenus indirectement par la collecte des numéros de téléphone pour le spam de SMS, la collecte des données de l'appareil et de l'utilisateur pour le markéting, l'affichage de publicités, la vente d'espiogiciels commerciaux et l'utilisation de l'appareil infecté pour extraire des cryptomonnaies. En outre, les applications d'espiogiciels commerciaux permettent à une partie de surveiller une personne d'intérêt et de recueillir les données de l'appareil et de l'utilisateur, telles que les messages SMS, les courriels, l'emplacement et le trafic téléphonique.

Voici des exemples notoires de programmes malveillants pour Android, BlackBerry et iOS.

Piratage Oleg Pliss (2014) : L'attaque Oleg Pliss attaque par un compte iCloud compromis pour bloquer les utilisateurs de leurs iPhone.

Slocker.A (2014) : Le Slocker.a est s. Ce « rançongiciel » chiffre les fichiers de données de l'utilisateur d'un appareil Android puis exige un paiement pour la clé de déchiffrement.

SMScapers (2013 – à ce jour) : Ce programme malveillant se présente sous l'apparence d'une application pornographique disséminée par affichage publicitaire mobile. Elle facture des frais aux utilisateurs sans le faire explicitement en envoyant un SMS à un numéro court surtaxé et supprime la notification par SMS s'y rapportant. La campagne a principalement ciblé le Royaume-Uni, mais l'application de la règlementation pertinente a contribué à une forte baisse de cette activité. La campagne a été répartie sur vingt entités juridiques différentes, ajoutant donc à la complexité du processus de mise en vigueur. Cette campagne est toujours active dans 15 autres pays[5354].

Worm.Koler (2014 - à ce jour) : En 2014, le nombre des rançongiciels a augmenté et plusieurs échantillons ont vu le jour, parmi lesquels ScareMeNot, ScarePackage et ColdBrother. Aux États-Unis, Worm.Koler

s'est propagé par SMS aux contacts se trouvant dans le carnet d'adresses des téléphones infectés. Ce code malveillant bloque les victimes et les empêche d'accéder à leur appareil par un faux avertissement du FBI indiquant qu'un contenu illégal a été trouvé sur leur appareil. Ils sont ensuite encouragés à payer une amende pour éviter des accusations criminelles et débloquer leurs appareils.

DeathRing (2014 - à ce jour): DeathRing principalement cible l'Asie ; ce programme malveillant tente d'hameçonner les données sensibles des victimes en affichant des SMS au contenu fallacieux. Le vecteur d'attaque est unique, car ce programme malveillant semble être préinstallé, suggérant que ses auteurs ont pu s'infiltrer dans la chaine d'approvisionnement à un certain moment.

MEILLEURES PRATIQUES DE L'INDUSTRIE ET DU GOUVERNEMENT POUR LA PROTECTION CONTRE LES PROGRAMMES MALVEILLANTS MOBILES

1) Sensibiliser les consommateurs en utilisant des annonces d'intérêt public, des pages Web, des brochures et d'autres médias aux fins suivantes :
   a) obtenir des applications seulement de marchés d'application proposant des fournisseurs de confiance et effectuant des vérifications des applications ou des développeurs, ou directement des fournisseurs bien connus de l'application ;
   b) examiner et comprendre les écrans d'autorisation, les accords de licence d'utilisateur final, les politiques de confidentialité et les conditions de l'accord lors de l'installation de nouvelles applications ;
   c) maintenir les restrictions de sécurité par défaut de l'appareil et ne pas le débrider (le débridage est discuté plus en détail ci-dessous) ;
   d) installer la localisation à distance et verrouiller le logiciel pour faciliter la récupération et la protection des données dans les téléphones perdus ou volés. Par exemple, IMEI (International Mobile Equipment Identity) est un code de 15 — ou 17— chiffres qui distingue de manière unique un appareil. Le code IMEI peut permettre à un réseau GSM ou UMTS (Universal Mobile Telecommunications Service) de bloquer les appels d'un téléphone égaré ou volé ;
   e) installer et exécuter un logiciel de sécurité mobile sur tous les appareils ;
2) élaborer des moyens pour le signalement des applications suspectes, et encourager les consommateurs à adopter cette pratique ;
3) encourager, automatiser et faciliter la sauvegarde des données du téléphone sur un nuage ou un support de stockage personnel (par exemple, un PC) ;
4) évaluer l'utilisation de solutions de sécurité mobiles telles que les navigateurs sécurisés, des solutions de gestion des périphériques mobiles (MDM), les sandboxes mobiles d'entreprise et les applications de prévention des pertes de données pour minimiser le risque d'infection et l'impact en résultant.

   Un excellent exemple de sensibilisation des consommateurs sur les meilleures pratiques mobiles a été créé par Ofcom et se trouve ici : http://consumers.ofcom.org.uk/files/2014/1394750/using-apps-safely-and-securely.pdf

MENACES MIXTES

Les appareils mobiles sont maintenant utilisés dans le processus d'authentification multifacteur pour la connexion à des comptes de grande valeur. Un exemple d'une menace mixte d'authentification à 2 facteurs serait un utilisateur visitant un site financier sur leur ordinateur de bureau et se connectant avec un nom d'utilisateur et un mot de passe comme par le passé. Mais maintenant, la banque exige une nouvelle étape pour que l'utilisateur ait accès à son compte : la réception d'un appel ou d'un message texte sur leur téléphone portable avec un code que l'utilisateur saisira dans le navigateur Web de l'ordinateur de bureau. Cette étape supplémentaire a été ajoutée parce que les ordinateurs de bureau de tant d'utilisateurs sont infectés de programmes malveillants ayant fait passer le mot de passe bancaire aux criminels. Les criminels se sont révélés persistants en attaquant chaque nouvelle méthode de protection. Ils auront désormais besoin de compromettre à la fois le mot de passe financier de l'utilisateur, puis son téléphone cellulaire, et être en mesure de relier les deux.

Cela rend les téléphones une cible encore plus précieuse pour les criminels qui souhaiteront les compromettre et les contrôler. Ce contrôle peut être physique si le téléphone a été volé, ou accompli à distance avec un logiciel d'espionnage d'appareil mobile. De toute façon, les menaces mixtes nécessitent plus d'efforts de la part des criminels et sont susceptibles de cibler des comptes ou des systèmes de plus grande valeur.

Les applications pour appareil mobile sont également utilisées comme générateurs de jetons, comme les codes de six chiffres que nous voyions uniquement sur les clés physiques émises individuellement pour les appareils à authentification à deux facteurs tels que le Google Authenticator et Amazon AWS virtuel MFA.

Selon la position des criminels, ils peuvent être en mesure d'observer le contenu du trafic sortant et entrant de certains appareils mobiles et recueillir les codes d'authentification. Tel est le cas des codes envoyés par courriel, que certaines banques offrent en option. Le trafic SMS (message texte des appareils mobiles) n'est pas chiffré.

L'absence d'un cadre pour partager des informations concernant les menaces mixtes peut elle-même être considérée comme une menace ; il permet à un grand nombre de codes malveillants qui pourraient être supprimés d'exploiter des failles de sécurité. Il est nécessaire de concevoir et de mettre en œuvre des stratégies et des cadres impliquant des entités techniques, politiques, judiciaires et policières dans plusieurs pays.

MODIFICATION DES APPAREILS MOBILES

Un certain nombre de fabricant d'équipement d'origine (OEM) et d'opérateur de réseaux mobiles établissent des environnements d'informatique mobile sécurisés afin de maintenir la stabilité et la sécurité des appareils et assurer une expérience positive à l'utilisateur. Dans de nombreux cas, la modification de ces environnements crée des failles de sécurité pouvant exposer les informations de l'utilisateur, permettant le vol de service sous la forme d'appels téléphoniques non autorisés ou de messages texte, permettant le contrôle à distance des ressources du périphérique telles que les microphones ou les caméras pour écouter ou voir à l'insu de l'utilisateur, ou permettant à un adversaire d'effectuer une longue liste d'activités non autorisées diverses.

De nombreuses techniques existent pour modifier le matériel et le logiciel d'un appareil, mais les trois modifications les plus connues sont le « débridage », le « rooting », et « le déverrouillage ».

DÉBRIDER UN APPAREIL

Le débridage ou « *jailbreaking* » est un processus permettant à un individu de remplacer les contrôles intégrés d'un appareil. Le fabricant peut utiliser des contrôles OEM pour appliquer des autorisations d'application, protéger des zones critiques du système de fichiers d'un appareil, forcer des applications à authentifier le dispositif, appliquer une certaine complexité aux mots de passe, ainsi que d'autres fonctions de gestion et d'administration.

Pourquoi débride-t-on un appareil ? L'une des raisons tient au fait que, même avec des centaines de milliers d'applications mobiles disponibles, certaines personnes voudraient des versions modifiées ou personnalisées des applications mobiles. Dans certains cas, une application modifiée peut couter moins cher que l'application officielle (mais peut bafouer le droit d'auteur) ; cependant, l'application moins couteuse peut également contenir du contenu malveillant.

Exemple : Zeus Mitmo (Man in the middle/mobile)

Zeus est un cheval de Troie qui cible les machines Windows et tente de voler des informations bancaires via l'enregistrement des touches du navigateur et la récupération de formulaire. Les mécanismes de prolifération typiques de Zeus étaient les activités de téléchargement furtif et les tentatives d'hameçonnage amenant l'utilisateur à naviguer vers un site malveillant. Il a été identifié vers 2007 et a reçu de nombreuses mises à jour qui l'ont rendu plus sophistiqué, la plus récente le rend capable d'attaquer l'espace mobile. Cette mise à jour bénéficie au programme malveillant Zeus, car de nombreuses entreprises, y compris des institutions financières, utilisent maintenant le SMS comme second vecteur d'authentification, donc être en possession du nom d'utilisateur et mot de passe en ligne ne suffit plus au processus de vol d'identité. L'évolution de ce vecteur de menace établit une variante prévue par un gang Zeus : infecter l'appareil mobile et renifler tous les messages SMS qui lui sont livrés. Le scénario est décrit ci-dessous.

- L'attaquant vole à la fois le nom d'utilisateur et le mot de passe en ligne en utilisant un programme malveillant (ZeuS 2.x).
- L'attaquant infecte l'appareil mobile de l'utilisateur en le forçant à installer une application malveillante soit par SMS ou via des programmes malveillants se faisant passer pour une application bancaire ou de productivité légitime.
- L'attaquant se connecte avec les informations d'identification volées en utilisant l'ordinateur de l'utilisateur en tant SOCKS/proxy et effectue une opération spécifique qui nécessite une authentification SMS.
- Un SMS est envoyé à l'appareil mobile de l'utilisateur avec le code d'authentification. Le programme malveillant en cours d'exécution dans l'appareil transmet le SMS à un autre terminal contrôlé par l'attaquant.
- L'attaquant saisit le code d'authentification et achève l'opération.

Les pirates utilisent ensuite ces informations pour contrôler les comptes bancaires des victimes et effectuer des transferts non autorisés vers d'autres comptes, les acheminant généralement par des comptes contrôlés par des réseaux mules.

ROOTING D'UN APPAREIL

Le débridage permet à un utilisateur de remplacer des contrôles, élève l'accès de l'utilisateur pour lui conférer des privilèges d'accès au root, et finalement accorde à l'utilisateur tous les privilèges du système d'exploitation. Le « rooting » d'un appareil accorde à un utilisateur les privilèges les plus élevés d'un système d'exploitation.

Pourquoi exécuter un « rooting » d'un appareil ? En plus du chargement d'applications personnalisées ou non autorisées et le contournement des contrôles, l'accès au root permet à un utilisateur d'altérer les composants et les fonctionnalités du système d'exploitation d'un périphérique ou le remplacer entièrement. Certains systèmes d'exploitation d'appareils mobiles sont basés sur une forme d'UNIX avec des ensembles réduits de commandes ; les utilisateurs altérant le système d'exploitation peuvent libérer du stockage en éliminant les fonctions ne sont pas nécessaires à la plupart des utilisateurs d'appareils mobiles. Le « rooting » d'un appareil pourrait également permettre à un utilisateur de charger des commandes additionnelles comme il le souhaite.

DÉVERROUILLAGE D'UN APPAREIL

Les opérateurs de réseaux mobiles (ORM) peuvent subventionner les ventes de téléphones cellulaires en vertu d'un contrat qui nécessite l'utilisation du réseau de l'ORM pour une certaine période. Pour aider à prévenir la fraude et le vol, les ORM utilisent souvent un moyen technique appelé « verrouillage » pour limiter l'utilisation du téléphone à leur propre réseau. Un appareil peut généralement être déverrouillé en saisissant un « code de déverrouillage » unique fourni par l'ORM sur demande ou à la satisfaction d'un engagement contractuel. Les consommateurs peuvent également trouver ou acheter un code de déverrouillage en ligne. En obtenant le code à partir de sources tierces, les utilisateurs courent le risque de perdre des informations personnelles ou d'avoir des logiciels malveillants installés par un fournisseur non digne de confiance.

MEILLEURES PRATIQUES POUR LES PARTICULIERS EN CE QUI CONCERNE LA MODIFICATION DES APPAREILS MOBILES :

1. Le débridage, le rooting et le déverrouillage des appareils ne sont pas recommandés pour ceux qui cherchent un appareil normal et stable, ainsi que le soutien OEM à long terme, car ces méthodes peuvent introduire des vulnérabilités à l'insu de l'utilisateur.
2. N'utilisez pas des services de déverrouillage « tiers » non officiels.

MEILLEURES PRATIQUES POUR L'INDUSTRIE ET LES GOUVERNEMENTS EN CE QUI CONCERNE LA MODIFICATION DES APPAREILS MOBILES :

1. Mettre au point et promouvoir l'information et la sensibilisation des consommateurs sur les risques découlant de la modification des appareils mobiles.
2. Créer des protections plus fortes pour empêcher les utilisateurs de passer outre l'OEM.
3. Appliquer la loi de manière adéquate contre les promoteurs de l'usage abusif des plateformes mobiles.

MENACES À LA BANDE DE BASE

Il existe plusieurs classes de menaces à la bande de base. Certains pourraient comprendre la création d'un réseau GSM (Système mondial de communications mobiles) illicite qui inciterait les appareils à se connecter. D'autres peuvent impliquer des attaques dans le cadre desquelles des messages spécialement conçus tentent d'exploiter les failles de sécurité des appareils mobiles. Avec la croissance de la recherche à moindre cout et des installations GSM criminelles, ces menaces se sont multipliées.

Traditionnellement, l'exploitation d'un réseau GSM nécessitait un investissement important, ce qui rendait difficiles les recherches en dehors des grandes institutions et limitait la découverte et l'exploitation des attaques de réseau. À titre d'exemple, pour usurper un réseau GSM, un attaquant devrait exploiter une station de transmission de base (BTS). Lorsque la technologie GSM a été appliquée, les attaques de réseau contre les appareils finaux ne posaient pas vraiment de problème, donc les téléphones n'étaient pas tenus d'authentifier les réseaux auxquels ils s'attachaient. Récemment toutefois, le logiciel libre et à données ouvertes tel que OpenBTS a permis à quiconque de créer son propre réseau GSM à une fraction du cout de l'équipement de classe opérateur, ce qui rend les études sur la sécurité du GSM à portée des chercheurs et des criminels de la sécurité.

Attaques de la bande de base
Un attaquant exploitera une fausse station de transmission de base (BTS) dans les environs de la station mobile (MS) cible. La fausse BTS transmet des messages d'information du système annonçant la disponibilité d'un réseau auquel la station mobile cible serait disposée à se connecter. Comme le principal critère pour la réception du réseau est la force du signal, l'attaquant peut forcer la MS à se connecter à la fausse station de base par simple transmission d'un signal plus fort que celui de la station de base légitime. Cela ne se produira pas instantanément, mais le processus peut être accéléré à l'aide d'un brouilleur GSM brouillant sélectivement la fréquence de la station BTS légitime. Ce scénario est fort similaire à celui qui est utilisé par les identificateurs de l'identité internationale d'abonné mobile (IMSI). **Le GSM ne fournissant pas toujours une authentification mutuelle, il n'y a pas de protection contre de fausses BTS.**

MEILLEURES PRATIQUES DE L'INDUSTRIE ET DU GOUVERNEMENT POUR LA PROTECTION CONTRE LES MENACES AUX BANDES DE BASE :

Au fur et à mesure que les opérateurs adoptent de nouvelles technologies (par exemple, 3G et 4G / LTE), les appareils devraient être obligés à authentifier l'infrastructure de l'opérateur à laquelle ils s'attachent.

1. Les fournisseurs de services peuvent collaborer avec les fabricants des appareils pour avertir les utilisateurs lorsque l'appareil ouvre une session qui n'utilise pas l'authentification mutuelle. Ceci permettra d'alerter l'utilisateur à ce vecteur de menace potentiel.

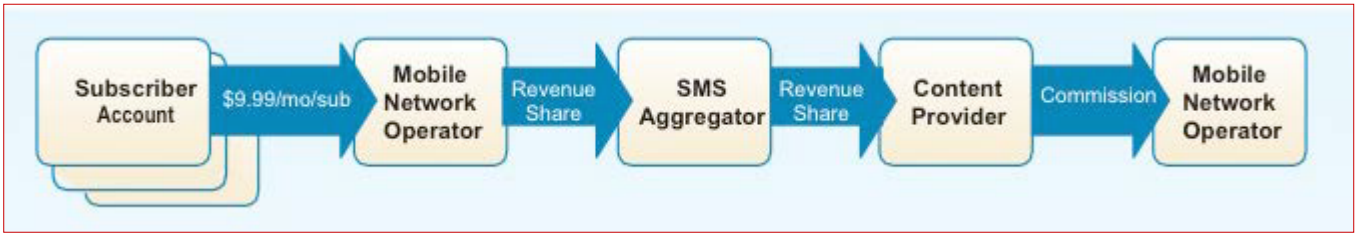
ABUS DES SERVICES SURTAXÉS

Offerts normalement en tant que services pour les applications vocales et de texte, et facturés au compte cellulaire prépayé ou postpayé d'un abonné, les services surtaxés comprennent les services d'horoscope par appel payant unique ou récurrent, les dons de bienfaisance aux catastrophes, les

crédits de jeu, les services de conseil et de chat, les conseils d'amour mensuels par SMS, et un large éventail d'autres formules.

MODÈLE COMMERCIAL DU TAUX MAJORÉ :

Le désir de créer un vaste écosystème d'applications qui offre de nombreux avantages pour le développeur a conduit à des environnements complexes et des factures interminables proposant différents modèles de partage des revenus comme le service typique d'abonnement SMS prémium à 9,99 USD/mois, criminellement exploitable (illustré ci-dessous).



Dans cet exemple, un opérateur de réseau mobile permet à des « agrégateurs SMS » indépendants d'obtenir le routage d'un bloc de « codes courts » (numéros de téléphone typiquement composés de 4 à 7 chiffres pouvant être acheminés au sein d'une partie du réseau de téléphonie mondiale). L'agrégateur SMS vend ensuite une connectivité SMS mobile à deux sens au propriétaire de l'application horoscope à titre de fournisseur de contenu. Le fournisseur de contenu paie une commission par abonnement à une société de publicité affiliée. Les parties adjacentes peuvent n'être que faiblement liées.

Les parties et les relations se compliquent progressivement vers le côté droit de ce diagramme. Dans un certain nombre de cas, les fournisseurs de contenu permettent des relations mal authentifiées en ligne seulement avec les affiliés de la publicité pour faciliter le déni plausible de leur spam ou de celui de leurs affiliés. Des mécanismes de paiement presque anonymes tels que les transferts aux banques étrangères, l'argent virtuel d'Internet non règlementé ou les mécanismes de paiement en ligne réduisent les obstacles et permettent au spam de faciliter la fraude.

Les arnaques par service surtaxé se produisent depuis des années, mais le taux de pénétration croissant des services mobiles, l'évolution des données mobiles, et l'établissement d'un écosystème mondial de la cybercriminalité ont mené à des attaques plus nombreuses et plus variées. La fraude peut se produire à presque n'importe quelle étape des processus de service ou de paiement, en dupant l'utilisateur et l'amenant à utiliser un service ou à s'y abonner, ou un affilié exigeant un faux

Programmes malveillants des tarifs majorés

Phonepay Plus, le régulateur de services surtaxés du Royaume-Uni, a imposé des amendes de 330 000 £ en décembre 2014 à trois compagnies différentes après avoir découvert qu'elles utilisaient les programmes malveillants mobiles pour imposer des frais aux utilisateurs de téléphones Android. Le programme malveillant était contenu dans des applications qui se téléchargeaient automatiquement sans le consentement de l'utilisateur lorsque celui-ci visitait certains sites pornographiques spécifiques. Une fois ces programmes installés, les consommateurs pourraient déclencher par inadvertance un abonnement en cliquant n'importe où sur l'écran. L'application envoie ensuite des messages texte cachés surtaxés afin que le propriétaire ne voie aucun enregistrement de ces messages dans son journal téléphonique.

abonnement, ou encore en installant des programmes malveillants mobiles qui subrepticement envoient des messages à des services à taux majoré à l'insu de l'abonné.

Un code malveillant courant par lequel un fraudeur exploite une faille de sécurité consiste à établir un numéro pour un service surtaxé et faire un appel vocal d'une sonnerie ou à envoyer un SMS à une victime dans l'espoir de l'inciter à répondre. Ceci amène l'appelant à utiliser un service d'appel payant à son insu ou sans son consentement. Les abonnements non autorisés, le « cramming » au conseil d'amour surtaxé ou d'autres services de messages texte par des affiliés ou des fournisseurs de contenu ont tous été courants.

Cela a causé de nombreux agrégateurs SMS à mettre en œuvre une vérification secondaire, impliquant généralement un message de confirmation ou l'échange de PIN entre l'abonné SMS et l'agrégateur SMS. Mais même ceux-ci ont été exploités ; par exemple, le programme malveillant GGTracker d'Android envoie un abonnement par SMS ainsi que le message SMS de confirmation sans la connaissance des abonnés.[55]

L'usurpation d'identité de l'abonné via l'accès non autorisé aux réseaux de signalisation ou des codes malveillants cryptographiques est encore une méthode permettant de commettre des fraudes du tarif majoré.

MEILLEURES PRATIQUES DE L'INDUSTRIE ET DU GOUVERNEMENT POUR LA PROTECTION CONTRE LES ARNAQUES DES TARIFS MAJORÉS :

La fraude du tarif majoré est similaire à d'autres genres de cyberdélit, donc elle est abordée de manière appropriée par un certain nombre de techniques courantes, y compris l'autoprotection, la sensibilisation du consommateur ainsi que les mesures de lutte contre les programmes malveillants et de protection des consommateurs

De nombreux opérateurs mobiles ont mis en place un service de signalement qui permet aux abonnés de signaler un SMS de spam en envoyant des messages à un code court (par exemple, 7726 qui est l'orthographie du mot « spam »). Beaucoup de gouvernements et d'organismes d'application responsables du spam par SMS dans certains pays ont établi leurs propres numéros de signalement comme le 1909 en Inde, le 33700 en France et le 0429 999 888 en Australie.

Les mesures spécifiques de protection contre les arnaques de tarif majoré comprennent la défense précoce, les actions de partenaires et la confirmation supplémentaire.

1. **Plaintes au TSP ou régulateurs :** Encourager les consommateurs à déposer leurs plaintes. Ces plaintes permettent aux TSP d'identifier la source des menaces et de mettre en place des mécanismes de défense qui permettent la détection précoce, avant que des fonds ne soient transférés. En intégrant des clauses anti abus dans leurs conditions générales et en les appliquant, les TSP et les plateformes de services surtaxés peuvent arrêter le paiement aux criminels avant qu'il ne se produise. Le TSP est averti à un stade précoce par les plaintes et applique ses conditions générales, freinant la rentabilité du criminel. De même, les plaintes aux régulateurs et aux organismes d'application de la loi fournissent d'amples renseignements pouvant se traduire par l'application de la loi contre les fraudeurs.
2. **Actions de partenaires concernant les relations et les paiements :** La fraude tient à l'extraction de fonds vers un emplacement caché ou irrécupérable. Les parties peuvent se protéger en exigeant l'identification complète, la qualification et l'authentification des

autres parties, grâce à des mécanismes de paiement réputés ou en retardant le paiement pour une période suffisante.

3. **Confirmations supplémentaires :** Comme bon nombre des exploits impliquent un « cramming » ou la falsification de communications entre les parties adjacentes de la chaine de paiement, les notifications et les confirmations entre les parties plus réputées peuvent empêcher les fraudes ou les identifier rapidement. Des exemples de cela peuvent inclure un agrégateur SMS ou un opérateur de réseau mobile confirmant l'abonnement avec l'abonné plutôt que de compter uniquement sur des affirmations du côté en aval du flux de paiement.

SPAM MOBILE

Le scénario suivant décrit une activité antispam internationale récente et montre le rôle essentiel de la collaboration internationale, en particulier la collaboration interopérateur, qui est indispensable à la défense des réseaux et des abonnés contre les abus.

L'opérateur A et l'opérateur B se trouvent dans des pays différents ; les deux pays ont de nombreux locuteurs d'une même langue. Le spam provenant du réseau de l'opérateur A constitue la majorité du spam entrant dans le réseau de l'opérateur B. L'opérateur A surveille le spam dans son réseau par le biais d'un signalement de spam basé sur des codes courts et de l'analyse du journal du serveur de messagerie. L'opérateur B dispose également d'un signalement de spam basé sur des codes courts, mais ne collecte pas les numéros d'origine des messages signalés comme du spam. L'opérateur B effectue toutefois une analyse automatisée antispam sur le trafic des messages. Le réseau de l'opérateur B recueille par conséquent des informations sur les sources du spam et son contenu.

Les opérateurs A et B ont appris séparément l'existence du spam provenant du réseau de l'opérateur A et reçu par l'opérateur B. L'opérateur A bloque les spammeurs qu'il identifie sur son réseau, mais uniquement s'il a reçu un certain volume de rapports de spam contre un numéro source donné. Ainsi, tant qu'un spammeur du réseau de l'opérateur A envoie son spam uniquement à des numéros à l'extérieur du réseau de l'opérateur A, il peut envoyer infiniment de spam aux abonnés de l'opérateur B, parce que :

a) Les abonnés de l'opérateur A ne signaleront jamais de spam, sa condition pour déclencher l'arrêt ; et

b) Il n'y a pas de pratiques de partage d'informations permettant de contrecarrer les spammeurs internationaux.

Étant donné l'absence de données partagées entre les opérateurs, les spammeurs peuvent fonctionner tout à fait librement dans un certain pays s'ils s'appliquent à envoyer leur spam aux abonnés d'autres opérateurs plutôt qu'aux abonnés du réseau sur lequel ils ont leurs comptes.

MEILLEURES PRATIQUES DE L'INDUSTRIE ET DU GOUVERNEMENT POUR LA PROTECTION CONTRE LE SPAM MOBILE :

Dialogue et partage de données : Les spammeurs exploitent les vulnérabilités des fournisseurs de services, en matière de politiques anti abus, aux défenses et aux connaissances. Depuis que le spam est apparu en 1993 jusqu'à ce jour où le spam représente environ 90 % de la totalité du trafic courriel sur Internet, une des principales leçons apprises de la prolifération du spam de courriel est la suivante : lorsque les participants à l'écosystème partagent leurs informations, ils changent la

donne pour les spammeurs. Le dialogue et le partage des données interopérateur, auxquels participent des facilitateurs tiers tels que les concepteurs de technologies et les organes de l'industrie, sont indispensables pour protéger l'écosystème mobile du spam et des spammeurs qui migrent des outils et techniques aiguisés sur Internet depuis plus d'une décennie vers l'univers mobile ouvert, de plus en plus basé sur les IP, et déjà connecté à l'échelle planétaire.

Alors que les points de données suivants ne sont pas critiques pour la collaboration entre les fournisseurs de services, ils sont utiles pour déjouer les spammeurs et peuvent être capturés via le signalement de spam :

Éléments des données :	**Remarques**
Le numéro mobile à l'origine du spam	Le MSISDN (numéro unique associé à l'appareil de l'abonné) ou le IMSI (numéro unique de la carte SIM)
Le nombre de rapports reçus signalant du spam	nécessite la collecte et la corrélation des rapports
Le nombre d'individus ayant signalé du spam	Utile sans être critique
Réseau de l'expéditeur du Spam	Résultant de la recherche

Il convient de noter qu'aucun des éléments de données identifiés ci-dessus ne fournit d'informations personnellement identifiables sur la personne ayant signalé le spam. Les informations recueillies ne concernent que le numéro étant signalé comme expéditeur de spam.

Comme dans l'exemple des opérateurs A et B ci-dessus, le partage de données concernant les éléments ci-dessus permet de combattre le spam tant à l'intérieur d'un pays qu'au-delà des frontières nationales.

Le partage interopérateur à l'international de données sélectionnées à partir de rapports signalant le spam comporte des avantages ainsi que des risques. Les avantages comprennent la possibilité d'adopter des mesures correctives pour les plaintes volontaires des abonnés. Le dialogue antispam et le partage de données entre les opérateurs facilitent les efforts que déploient ceux-ci pour surveiller de façon suivie leurs propres règles de bon usage, les affiner et les appliquer. Enfin, le partage de données peut fournir des preuves corroborantes qui appuient les décisions de fermeture prises par les opérateurs et qui contribuent au travail des organes d'application des lois et de règlementation. La collaboration internationale interopérateur aux fins de ces objectifs compliquera la tâche des spammeurs mobiles qui cherchent à se dissimuler.

En revanche, des préoccupations quant à la vie privée, la sécurité et l'aspect juridique doivent être examinées dans la mise en œuvre d'une quelconque collaboration internationale dans cet espace. À l'heure actuelle, ces préoccupations font obstacle à la collaboration transfrontalière. Certains ont cependant relevé que les préoccupations au sujet de la vie privée sont dénuées de fondement, puisque 1) le signalement de spam est volontairement communiqué par les abonnés, 2) il n'est pas indispensable d'inclure des informations personnelles identifiables (PII) lors du partage de données sur les plaintes, et 3) l'inclusion du contenu du message lors du partage de données sur les

plaintes n'est pas essentielle. (Partager le contenu du message peut augmenter le risque de partage accidentel des PII des déclarants ou de personnes autres que le spammeur. Toutefois, le contenu des messages de spam signalés comme tels peut être utile à l'identification et au blocage du spam.)

En résumé, le partage international interopérateur de certains éléments des données change la donne pour les spammeurs qui auront moins d'endroits où se cacher. Le partage des données nécessitera un dialogue et un consensus sur les données à partager ainsi que sur les modalités de ce partage entre les participants de l'écosystème.

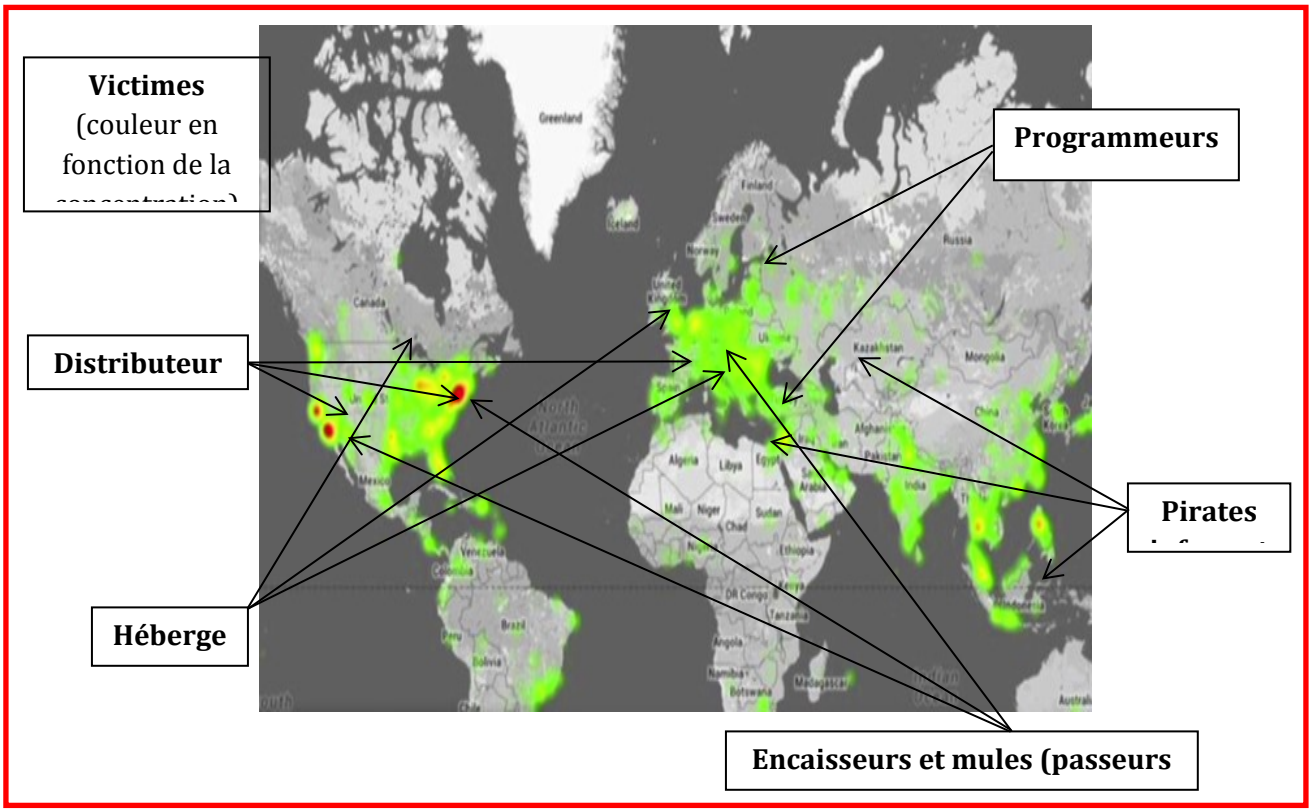
L'industrie devrait également s'efforcer d'informer le personnel d'application de la loi dès qu'elle s'aperçoit d'un comportement illégal dans ses réseaux et systèmes. La coordination avec les forces de l'ordre, sur l'aspect criminel aussi bien que sur le côté règlementaire, permet souvent d'identifier la source de la menace et de décourager d'autres activités pareilles.

CROISSANCE DES ABUS TRANSFRONTALIERS

Alors que les pays se penchent sur les attaques et menaces internes, les attaquants portent leur attention ailleurs pour identifier et exploiter les vulnérabilités internationales. Par exemple, la campagne nord-américaine de spam « iPad/iPhone gratuit » visait initialement les États-Unis. Les opérateurs canadiens et américains ont mis en place des défenses techniques bloquant le spam envoyé à leurs abonnés. Les attaquants ont rapidement découvert cela et ont commencé à envoyer du spam par SMS aux abonnés canadiens à partir de téléphones américains, éludant ainsi les défenses. Des cas similaires existent en ce qui concerne la fraude, l'hameçonnage, les programmes malveillants et les espiogiciels. Dans la plupart des cas (par exemple, la défense contre le spam et les programmes malveillants), il s'est avéré nécessaire d'arrêter l'abus à la source, car les pays de réception peuvent ne pas pouvoir identifier l'abus caché à l'intérieur du volume élevé du flux de communication. Comme l'Internet, les réseaux de communications mobiles sont mondiaux et nécessitent une approche internationale en matière de défense internationale et une collaboration internationale.

CONSIDÉRATIONS INTERNATIONALES

Les cybercriminels marquent une nette préférence pour les environnements transnationaux. Par exemple, un vendeur illégal de pilules en ligne résidant aux États-Unis pourrait envoyer des courriels publicitaires non sollicités à partir d'un ordinateur infecté au Brésil, redirigeant les acheteurs potentiels vers un site Web dont le nom de domaine est russe (tout en hébergeant physiquement ce site en France). Le paiement des commandes par carte de crédit peut être traité par une banque en Azerbaïdjan, les commandes expédiées directement de l'Inde, et les bénéfices canalisés vers une banque à Chypre. Ce faisant, les criminels savent qu'un certain nombre de facteurs compliqueraient toute enquête officielle concernant leurs crimes en ligne, réduisant le risque de se faire prendre. Ces facteurs comprennent notamment le manque de coopération, les différences entre les juridictions, ainsi que le cout des enquêtes internationales.



JURIDICTION ET COOPÉRATION INTERNATIONALE

Les agents chargés d'appliquer la loi ne disposent pas de pouvoirs illimités. En particulier, un agent chargé d'appliquer la loi dans une ville ou un pays donné n'aura normalement aucune compétence lui permettant d'exiger la production de documents ou d'arrêter un criminel au-delà de sa propre juridiction. Les enquêtes transfrontalières exigent une coopération internationale entre les services de police nationaux et internationaux, un processus pouvant impliquer des procédures officielles d'une complexité redoutable, nécessitant par ailleurs du temps et des ressources. Les complications associées à ces processus peuvent retarder les enquêtes, voire rendre certaines enquêtes impossibles.

COUVERTURE STATUTAIRE ET PRÉCÉDENT EN COMMON LAW

Une activité illégale dans un pays peut ne pas être illégale ailleurs. Certains pays ne disposent pas de lois, par exemple, concernant le courrier électronique indésirable et n'ont pas non plus criminalisé la diffusion de programmes malveillants. Sur d'autres territoires, le système judiciaire pourrait ne pas pouvoir répondre à un flux régulier de nouvelles drogues chimiquement différentes tout en étant équivalentes. Dans d'autres cas, une loi pourrait exister en théorie sans que le pays n'ait jamais reconnu coupables dans le cadre d'une poursuite judiciaire ceux qui contreviennent à cette loi. Chacune de ces conditions est un obstacle à l'application de la loi et à la collaboration.

Exemple : Arnaque du centre d'appels indien

Quelque 60 000 personnes au Royaume-Uni se sont récemment retrouvées victimes de l'arnaque du centre d'appels indien et du prêt Internet de plusieurs millions de livres sterling. Les enquêteurs estiment que le nombre de personnes victimes de l'arnaque des prêts fait de cette fraude la plus grande jamais exécutée au Royaume-Uni. À son paroxysme, plus de 1000 personnes par jour ayant légitimement demandé des crédits en blanc auprès de banques et de sociétés de financement recevaient des appels non sollicités de centres d'appels à New Delhi — environ 100 personnes étaient dupées par jour et amenées à s'inscrire et payer des frais de traitement garantissant le prêt fictif. Selon la police indienne, au moins 10 millions de livres sterling ont été soutirées aux victimes.

COUT DES ENQUÊTES INTERNATIONALES

Tous les aspects du travail à l'échelle internationale coutent aux organismes d'application de la loi bien plus que lorsque ceux-ci se consacrent à des affaires strictement locales. Lorsqu'un enquêteur a besoin de se rendre dans un pays étranger, le cout des billets d'avion et divers déplacement pourrait être substantiel. Il se peut que des organismes à court d'argent ne puissent tout simplement pas se permettre de se pencher sur des affaires qui présentent des aspects transfrontaliers.

Paradoxalement, alors qu'il peut s'avérer couteux pour un agent d'application de la loi de travailler sur un crime comportant une dimension internationale, les cybercriminels sont souvent capables de se procurer d'autre pays, vis Internet, un bien ou un service illégal. Par exemple, un auteur de programme malveillant d'un pays économiquement défavorisé serait disposé à écrire un programme malveillant qui entrainerait des dommages s'élevant à plusieurs millions pour quelques centaines de dollars. Ces conditions incitent fortement les cybercriminels à travailler dans un environnement transfrontalier, et un grand nombre d'entre eux le fait.

MEILLEURES PRATIQUES POUR L'INDUSTRIE ET LES GOUVERNEMENTS EN CE QUI CONCERNE DES QUESTIONS SPÉCIFIQUES AU CONTEXTE TRANSFRONTALIER :

1. **Collaboration :** La collaboration est au cœur de la défense internationale efficace. Tout d'abord, les parties gouvernementales et non gouvernementales dans les pays touchés doivent prendre conscience de la question. Il est nécessaire ensuite de concevoir et de mettre en œuvre des stratégies et des cadres impliquant des entités techniques, politiques, judiciaires et policières dans plusieurs pays. Les principaux défis à la réalisation de la collaboration nécessaire consistent entre autres à identifier le bon ensemble de forums et d'obtenir une participation appropriée.
2. **Échange de données sur les menaces/abus** Il est nécessaire d'échanger des informations au sujet des menaces et des abus pour surmonter les obstacles transfrontaliers. Bien qu'une communication humaine soit requise, l'ampleur et la portée des abus (par exemple, les milliards de courriels indésirables et de messages d'hameçonnage envoyés chaque jour) exigent l'adoption d'une approche mécanisée. Là encore, pour réussir à mettre en œuvre un cadre international mécanisé, celui-ci doit tenir compte des obstacles à la mise en œuvre et l'adoption généralisées, y compris la fragmentation parmi de nombreux systèmes disparates ; les divers besoins fonctionnels de différents pays (dont les obstacles juridiques et les questions techniques/technologiques) ; et les besoins particuliers de différents opérateurs. Un système d'échange d'information sur les abus devrait également soutenir les modèles pair-à-pair et de serveurs centralisés et identifier à la fois les formats et les protocoles de transfert.
3. **Formation :** Afin de reconnaitre les menaces mobiles et d'y répondre, les professionnels et les forces d'application de la loi doivent rester informés des nouvelles tendances et menaces.

MENACES DE LA TÉLÉPHONIE VOCALE

ENVIRONNEMENT DE LA TÉLÉPHONIE VOCALE

Les consommateurs disposent de nombreuses options en ce qui concerne les appels vocaux téléphoniques : filaires, sans fil, d'autres sources (par exemple, ordinateur). Ces appels peuvent traverser le réseau téléphonique public commuté (RTPC) via multiplexage temporel (MRT), protocole voix sur IP (VoIP), ou une combinaison du MRT et de la VoIP. La téléphonie Internet fait référence à l'intégration des services téléphoniques dans les réseaux informatiques. Le processus convertit essentiellement les signaux vocaux analogiques qui étaient traditionnellement envoyés par le circuit filaire en signaux numériques. Ces signaux sont transmis via Internet et ensuite reconvertis en signaux vocaux analogiques.

Le nombre d'abonnés au téléphone fixe dans le monde a culminé en 2006 et ne fait que diminuer depuis. Par exemple, les abonnés au téléphone fixe comptaient un peu moins de 1,11 milliard en 2014, en baisse comparativement à 1,14 milliard en 2013. Simultanément, le nombre d'abonnés au mobile-cellulaire augmente partout dans le monde et s'approche rapidement du nombre d'habitants sur terre. Les abonnements cellulaires mobiles ont atteint presque 7 milliards vers la fin de 2014, ce qui correspond à un taux de pénétration de 96 %, mais les taux de croissance étaient à leur plus bas (2,6 mondialement), indiquant que le marché se rapproche à grands pas de son niveau de saturation.

Le protocole d'accès au réseau (SIP) est un protocole de communication pour la signalisation et le contrôle des sessions de communication multimédia. Il est couramment utilisé dans les applications VoIP ou de téléphonie Internet.

Le multiplexage temporel (MRT) est un procédé de transmission et de réception de signaux indépendants sur une voix de signal commune par des commutations synchronisées à la fin de chaque ligne de transmission.

À la fin de 2014, le nombre d'abonnements haut débit mobile avait atteint 2,3 milliards dans le monde, environ 5 fois ce qu'il était six ans plus tôt (en 2008). Les abonnements mobiles à large bande comptaient 2,1 milliards en 2013. La pénétration du haut débit fixe ne cesse de croitre, bien que lentement (à 4,4 % mondialement en 2014). Comme les services deviennent plus abordables, l'utilisation du haut débit fixe a connu un essor et vers 2013, il avait environ 700 millions d'abonnements haut débit fixes, correspondant à un taux de pénétration mondial de 9,8 %.

Le nombre d'internautes dans le monde aura atteint quelque 3 milliards vers la fin de l'année 2014, en hausse comparativement à 2,7 milliards de personnes en 2013.[56]

Avec la croissance généralisée de la téléphonie Internet, il est vital que l'infrastructure à l'appui de cette technologie demeure sécurisée et disponible. Même un « temps d'arrêt » négligeable a le potentiel de couter aux entreprises des millions de dollars en pertes de revenus et en problèmes de service clientèle.

LES MENACES À LA VOIP :

Cette section une simple taxonomie des menaces à la téléphonie vocale, couvrant les questions qui affectent les systèmes des communications unifiées (CU) et vocales ainsi que les meilleures pratiques pour la prévention et l'élimination de ces menaces. Cette section met l'accent sur la téléphonie vocale, mais ces menaces peuvent affecter d'autres formes de communication, y compris la vidéo et la messagerie. Ces menaces touchent principalement les entreprises, mais peuvent aussi affecter les fournisseurs de services, les petites entreprises et les consommateurs.

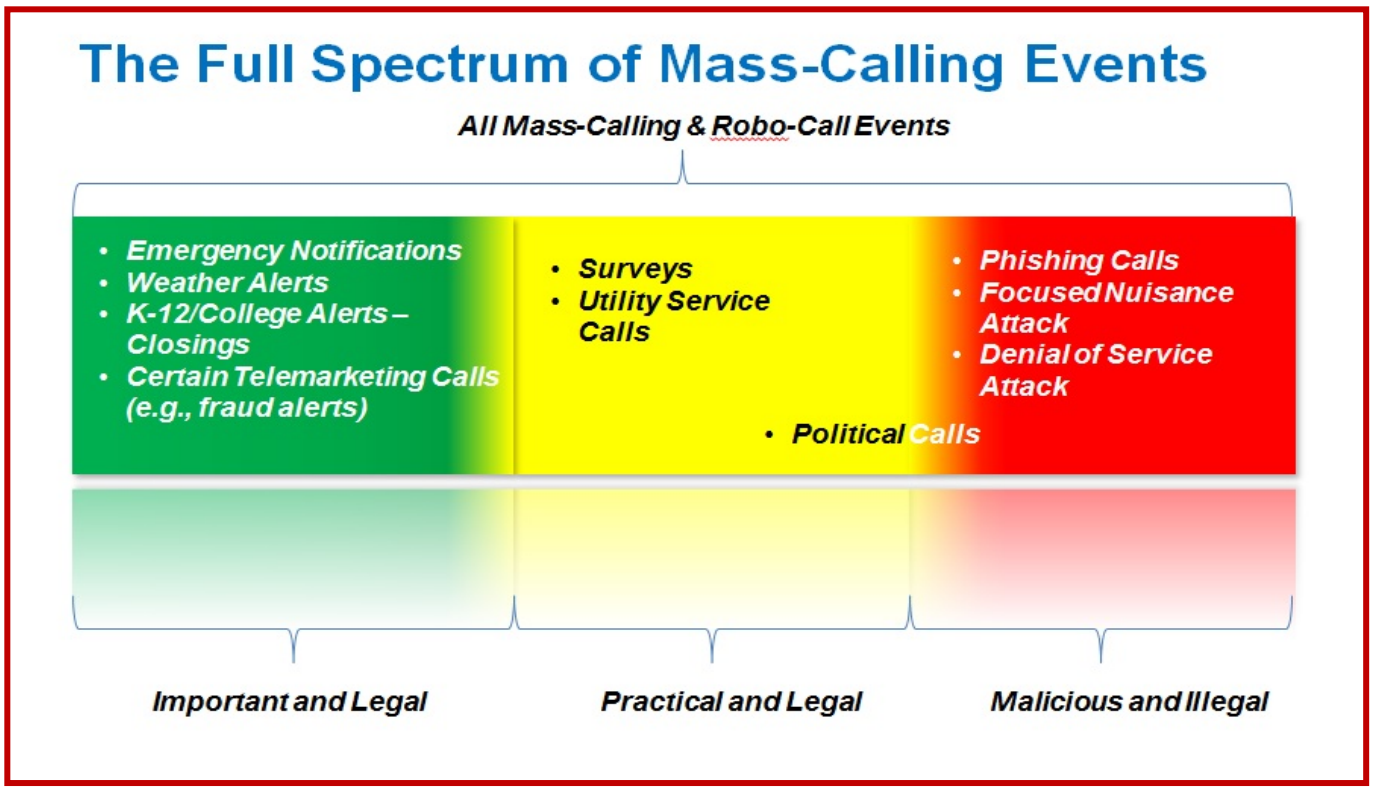
Les arnaques par sonnerie unique : Des consommateurs de services sans fil reçoivent des appels automatisés de numéros de téléphone avec des indicatifs régionaux usurpant des numéros nationaux, mais qui en fait sont des numéros de téléphone internationaux payants à l'appel. Ces appels automatisés généralement déconnectent après une sonnerie, ne donnant pas le temps au consommateur de répondre à l'appel, l'incitant ainsi à rappeler le numéro. Les clients qui rappellent génèrent du trafic supplémentaire à ces opérateurs étrangers, et l'arnaqueur peut recevoir une partie des frais de terminaison (ou peut-être du service surtaxé) que le fournisseur de services étranger perçoit de l'opérateur du client des services sans fil.

AUTOMATE D'APPEL

L'automate d'appel est un système téléphonique capable de faire automatiquement des appels vocaux. Il constitue une forme d'abus de plus en plus problématique pour les services vocaux. Il est généralement utilisé pour effectuer des appels à des fins de vente, de markéting ou de sondage. Par exemple, lorsqu'un sondage d'opinion ou un autre type de sondage est mené, le message préenregistré peut demander à la personne qui décroche d'appuyer sur un chiffre correspondant à la réponse prédéfinie de leur choix. Il est également couramment utilisé pour les notifications d'urgence, les annonces ou les rappels. Les agents de la sécurité publique y recourent fréquemment via le système appelé système de notification des situations d'urgence. L'automate d'appel est toutefois aussi couramment utilisé pour arnaquer les consommateurs ou à d'autres fins illicites.

Aux États-Unis par exemple, les automates d'appels touchent particulièrement les clients du téléphone fixe, souvent ciblés par les télévendeurs malhonnêtes et les fraudeurs.[57] Les automates d'appels se plaçaient en haut de la liste de plaintes reçues par le FTC en 2014. Les opérateurs ont récemment commencé à recevoir un nombre croissant de plaintes provenant des clients de services sans fil également. Par exemple, l'arnaque « par sonnerie unique » visait récemment à inciter les clients des services sans fil à composer par inadvertance des numéros internationaux payants.[58] Les appels d'hameçonnage visant spécifiquement à accéder aux informations personnelles et financières, souvent appelés « vishing » ou hameçonnage vocal, sont également fréquents.

Les automates d'appels sont aussi fréquemment utilisés pour submerger à la fois les clients des services filaires et sans fil lors d'attaques par déni de service de téléphonie (TDoS) en créant des évènements d'appels en masse qui empêcheraient les appels légitimes d'aboutir.



MEILLEURES PRATIQUES CONTRE LES AUTOMATES D'APPEL :

Les opérateurs ou les fournisseurs tiers peuvent offrir des outils et des solutions pour lutter contre les automates d'appels. Il n'existe pas de solution miracle, cependant, pouvant éliminer tous les appels automatisés indésirables ou illégaux.

Pots de miel : Un « pot de miel » est un piège tendu pour détecter, détourner ou contrecarrer les tentatives d'utilisation non autorisée d'un réseau ou d'un système. Généralement, les pots de miel imitent un ordinateur, des données ou un site du réseau, mais ils sont réellement isolés, protégés et surveillés. Ils sont construits spécifiquement pour servir d'appât aux attaquants. Une fois l'appât mordu, les acteurs malveillants peuvent être suivis et surveillés.

Collecte de données et analytique : L'information est un outil puissant pour la prévention des automates d'appels Les fournisseurs peuvent identifier et analyser des modèles d'appels suspects pour identifier des automates d'appels illicites, notamment en collectant l'information relative au flux normal du trafic dans un réseau donné et en les combinant à des analytiques afin d'identifier des modèles d'appels suspects en fonction du volume des appels, leur routage, leur destination, leur durée et le pourcentage d'appels complétés. Se basant sur cette information, ils peuvent établir des listes noires servant à bloquer les appels provenant de certains numéros, ou des listes blanches qui définissent les appels pouvant être reçus. Une fois qu'un modèle d'automate d'appel est identifié, les opérateurs de réseaux et les organismes d'application de la loi peuvent utiliser des techniques permettant de retracer l'origine des appels pour identifier les coupables et les poursuivre.

Équipement destiné aux abonnés : Les opérateurs et les fournisseurs tiers offrent tous les deux des outils permettant de gérer les appels entrants. Les types d'équipements les plus courants comprennent :

- ***Identification de l'appelant :*** L'identification de l'appelant affiche le numéro qui appelle. Les clients peuvent utiliser cette technologie bien connue pour filtrer les appels provenant de sources inconnues. Les services et appareils de blocage d'appel reposent sur les informations d'identification de l'appelant transmises avec les appels entrants pour bloquer les appels des numéros qui se trouvent sur une liste noire.
- ***Appareils CAPTCHA[59]*** **:** font passer certains appels par des menus conçus pour exclure les appelants non humains.[60]
- ***Applications :*** les clients sans fil peuvent télécharger une variété d'applications qui utilisent la fonctionnalité d'identification de l'appelant pour rejeter ou filtrer les appels provenant de numéros de téléphone que les applications identifient comme suspects sur la base de diverses techniques telles que les algorithmes approvisionnés par la foule ou les listes noires.[61] Les utilisateurs peuvent également tirer parti des fonctionnalités intégrées de leurs smartphones qui leur permettent de gérer quels appels auront une sonnerie et lesquels n'en auront pas.
- ***Identification de clés publiques/privées*** : ce système est en cours d'élaboration et vise à authentifier l'appelant ou l'adresse de réseau associée à l'appelant.

Régimes de règlementation : De nombreux agents de commercialisation ont utilisé la téléphonie pour promouvoir des campagnes de markéting. La plupart des listes des abonnés auto-exclus (*Do Not Call*) interdisent les appels automatisés à moins que le consommateur n'ait consenti à recevoir de tels appels de l'entité appelante. En outre, l'agacement des consommateurs à cause des sollicitations non désirées a entrainé un certain nombre de pays à règlementer tous les appels commerciaux, certaines juridictions appliquant l'option d'inclusion « automatique » (par exemple, l'Allemagne, l'Autriche et Israël) et de nombreux appliquant l'option d'exclusion « automatique » (certains volontaires ; certains obligatoires). Dans des pays tels que l'Australie, les États-Unis et le Canada, les listes nationales d'abonnés auto-exclus sont complétées parallèlement par des lois qui règlementent les télévendeurs, qui comprennent couramment des règles concernant l'heure d'appel, l'identification de l'appelant (CLI) et certaines divulgations obligatoires.

Les sanctions peuvent être importantes, et avec les dommages potentiels à la réputation, elles ont grandement contribué à garantir que les entreprises citoyennes aient des politiques et des procédures qui assurent leur conformité.

Le réseau international visant à protéger les consommateurs d'appels indésirables dans le cadre du Plan d'action de Londres a établi un forum annuel et des téléconférences périodiques pour discuter de questions courantes et émergentes concernant la gestion, à l'échelle mondiale, des appels non sollicités de télémarkéting ainsi que des opportunités de collaboration dans l'application de la loi.

Normes de l'industrie : Les fournisseurs de services, les organes de normalisation de l'industrie et les organismes d'application de la loi ont travaillé en collaboration et chacun de son côté pour mitiger ces types d'appels illégaux. Les fournisseurs de services et les entités privées soit élaborent soit on déjà des services et des fonctionnalités permettant aux consommateurs de gérer les appels automatisés illégaux[62] et devraient continuer à élaborer et à appliquer ces normes.

Les fournisseurs de services devraient également envisager d'améliorer le bureau de service à la clientèle ou leurs autres centres recevant des appels, l'accès en ligne des clients, ainsi que les centres de réparations et les services d'assistance technique, et devraient informer leur personnel sur les fonctions liées à l'identification de l'appelant, les utilisations légitimes de la mystification de l'identité de l'appelant et les usurpateurs d'identité malveillants actuellement connus.

Certains fournisseurs peuvent envisager la création d'un bureau spécifiquement dédié aux appels malveillants ou des équipes de sécurité qui se penchent sur de telles questions. Les clients qui continuent à s'inquiéter après leur contact avec le bureau de service clientèle ou les ressources en ligne peuvent être renvoyés à ce groupe pour une assistance supplémentaire selon les processus spécifiques des fournisseurs de services. Les clients peuvent être invités à partager les informations pertinentes telles que les dates et les heures des appels mystifiés, ainsi que d'autres détails appropriés pour enquêter sur les appels. Les bureaux des appels malveillants ou les équipes de sécurité peuvent contribuer par un travail précieux à apaiser ces préoccupations, tels que :

- la fourniture et la surveillance d'équipements de localisation d'appel pour les services téléphoniques du client,
- le suivi, la traduction et l'identification des sources d'appel par l'intermédiaire de systèmes de commutation de central et de surveillance et d'analyse de réseau,
- l'utilisation de systèmes de facturation, d'adresse et de gérance informatique pour identifier les sources de l'appel lorsque cela est possible,
- le travail direct avec les fournisseurs de services interurbains, locaux, sans fil et autres fournisseurs de communication, ainsi qu'avec les bureaux des appels malveillants,
- la collaboration avec les organismes d'application de la loi pour la publication des informations relatives aux parties identifiées, et
- la communication, au nom des clients, avec les parties identifiées et, le cas échéant, résoudre des problèmes pouvant aller des appels de menaces ou de harcèlement aux appels automatisés et générés par ordinateur, l'usurpation, les rafales de télécopies et tout autre type d'appel malveillant identifié par les clients.

Application de la loi : Alors que le système de la conformité règlementaire peut venir à bout des appels non sollicités provenant d'entreprises légitimes, il ne constitue pas un moyen suffisant pour dissuader ceux qui cherchent à duper le public. Le seul moyen pour venir à bout de ces acteurs et de leurs abus demeure souvent une capacité répressive assez importante. Certains pays ont adopté une attitude agressive contre l'utilisation de la téléphonie, soit par le biais du VoIP ou d'autres moyens, pour induire en erreur les consommateurs. La poursuite judiciaire en vertu des lois de protection du consommateur, à la fois dans le cadre de procédures civiles et pénales, a conduit à de fortes amendes ainsi qu'à des peines d'emprisonnement. Pour résoudre complètement le problème du télémarkéting frauduleux, il est essentiel que les organismes d'application de la loi, l'industrie et les régulateurs continuent à retrouver et traduire en justice les fraudeurs dont l'usurpation d'identité d'appelant et les automates d'appels se sont traduits par des fraudes à des centaines de millions de dollars à l'échelle mondiale.

ATTAQUES PAR DÉNI DE SERVICE DE TÉLÉPHONIE (TDOS)

Le TDoS est une attaque qui vise à désactiver le système de téléphone d'une personne morale ou d'une fonction publique. En saturant un numéro de téléphone de l'extérieur, ou même la totalité des canaux de communication de l'entité, les attaquants peuvent rapidement désactiver tous les appels

entrants et sortants. Les attaques TDoS sont très semblables aux attaques par déni de service (DDoS) sur des sites spécifiques du Web. Les attaquants bénéficient en prenant comme otage le système de téléphone et en perturbant ce système jusqu'à ce que la victime paie une somme spécifiée.

Pour lancer une attaque TDoS, l'attaquant doit avoir accès à plusieurs canaux de communication ou à plusieurs comptes de protocole d'accès aux réseaux (SIP) (habituellement piratés). Il utilise alors des automates d'appel pour contacter simultanément et de manière répétée un ou plusieurs des numéros de téléphone de la victime. Les « outils » ou les « kits » pour les attaques TDoS sont facilement disponibles sur Internet. Il est également très facile de commander une telle attaque par des personnes sans scrupules. Ce type d'attaque est généralement effectué pour perturber, extorquer des fonds ou dissimuler une fraude.

MEILLEURES PRATIQUES CONTRE LA TDOS :

Passerelle de couche d'application : Il est important que les entreprises de toutes tailles sécurisent leurs systèmes VoIP et de téléphonie. Les systèmes VoIP sont comme tout autre système du réseau informatique et nécessitent donc une protection contre les mêmes classes de cyberattaques que d'autres serveurs de réseau. Tandis que les anciens pare-feux peuvent avoir du mal à gérer correctement les exigences particulières des systèmes VoIP, de nombreux équipements de sécurité modernes ont des passerelles de couche d'application (ALG) spécialement conçues pour gérer des protocoles spécifiques à la VoIP. Certains de ces ALG peuvent même fournir des fonctionnalités de sécurité spécifiques pour VoIP, telles que la prévention des attaques DHA (*Directory Harvest Attack*) ou des attaques DoS au niveau du réseau.

Protection des services essentiels
Le Comité directeur sur l'interconnexion du CRTC (CDCI) a examiné la question des attaques par déni de service de téléphonie au sein des groupes de travail sur le réseau et les services d'urgence et a suggéré de meilleures pratiques visant la protection des systèmes essentiels.

http://www.crtc.gc.ca/public/cisc/nt/NTCO0570.docx

Signalement aux organismes d'application de la loi : Les attaques TDoS peuvent éventuellement désactiver les principales infrastructures critiques, y compris les services d'urgence, les hôpitaux et les premiers intervenants. Ceci peut soulever des questions de sécurité nationale et devrait donc être confié à l'organisme d'application de loi concerné dès qu'une attaque est détectée.

Blocage/signalement sélectif des appels (*09)
Les codes de service en mode vertical, tel que le *09, devraient être définis par l'industrie pour permettre au consommateur de lancer facilement la capture automatique et l'analyse des informations du réseau concernant des appels non sollicités. Ce système fonctionne en permettant à un consommateur qui reçoit un appel non sollicité de télémarkéting ou de fraude entre autres de raccrocher le téléphone et d'appuyer sur le *09 pour signaler l'information complète de l'appel à l'opérateur, aux organismes d'application de la loi et aux régulateurs, et aussi de bloquer automatiquement les futurs appels en provenance de ce numéro.[63]

USURPATION D'APPEL

L'usurpation de l'identité de l'appelant est une méthode qui consiste à falsifier les informations de la personne à l'origine de l'appel. Alors que cette activité n'est pas une attaque en soi, elle est couramment utilisée pour masquer l'identité d'un attaquant ou pour rendre les attaques plus efficaces. Par le biais de cette usurpation, les fraudeurs ciblent des consommateurs avec des appels

qui semblent provenir de la zone du consommateur, de son code d'appel ou d'une source de confiance. Certains appelants ont utilisé des numéros associés avec des organismes gouvernementaux et ont emprunté l'identité de fonctionnaire dans des arnaques liées aux taxes et à l'immigration. La source de ces appels se trouve souvent sur un autre continent, ce qui complique davantage la recherche et l'arrêt des fraudes.

MEILLEURES PRATIQUES POUR LA PRÉVENTION CONTRE L'USURPATION D'APPEL :

Législation relative à la lutte contre la fraude : en général, il devrait être universellement illégal de transmettre des informations d'identification d'appelant trompeuses ou inexactes dans l'intention de frauder, de causer du tort ou d'obtenir indument quelque chose de valeur.[64]

Aux États-Unis par exemple, le Truth in Caller ID Act de 2010 interdit l'usurpation ou la falsification délibérée d'un numéro de téléphone ou d'un nom relayé comme identification de l'appelant visant à déguiser l'identité de l'appelant à des fins *nuisibles ou frauduleuses*. [65] Ce type de définition permet l'utilisation de l'usurpation d'identité à des fins non trompeuses, telles que l'utilisation par un médecin du numéro du bureau lorsqu'il appelle de sa ligne privée.

Sensibilisation du consommateur : La confiance des consommateurs dans le système téléphonique est en péril avec l'augmentation de l'usurpation d'identité d'appelant et les appels automatisés. Pour protéger les consommateurs contre les fraudes et autres méfaits qui reposent sur l'utilisation abusive de la plateforme téléphonique, les organismes publics ont lancé des campagnes de sensibilisation. La Commission fédérale de commerce (FTC), par exemple, a publié des mises en garde sur ses sites Web ainsi que des blogues, et fait une promotion de leurs efforts d'application de la loi afin de sensibiliser le consommateur aux automates d'appels et à l'usurpation d'identité d'appelant.[66] Encourager une plus grande sensibilisation des consommateurs sur l'utilisation de l'usurpation d'identité peut aider à réduire les dommages pouvant résulter de la fraude expliquée par le biais de cette technique. Les efforts de sensibilisation du consommateur devraient également mieux faire connaitre les différents outils que les consommateurs peuvent utiliser pour se protéger contre les appels non sollicités.

HÉBERGEMENT ET SERVICES EN NUAGE (CLOUD)

L'hébergement et les services en nuage constituent l'un des plus importants changements récents des technologies de l'information. Les sociétés sont enthousiasmées par la possibilité d'un meilleur contrôle du frais de capital, d'une agilité accrue et de la suppression de l'infrastructure informatique complexe. Les préoccupations concernant la sécurité et la perte du contrôle direct découragent toutefois l'adoption et la croissance de cette nouvelle technologie.

Les menaces en lignes et mobiles sont à la hausse pour les services d'hébergement et en nuage. Selon un récent article paru dans « The Economist », le marché mondial des services d'informatique en nuage devrait atteindre 176 milliards USD en 2015. Ce montant représente toujours une petite portion du total des dépenses en TI, mais les dépenses en services d'hébergement et de nuage augmentent rapidement. Actuellement, la plupart des autres parties de l'industrie dont stagnantes ou même en déclin, mais il est prévu que d'ici 2017, les dépenses en nuage atteignent un total de 240 milliards USD par an.[67]

La présente section catégorise les types d'hébergement et définit les domaines particulièrement préoccupants. Elle dresse le portrait des menaces actuelles à l'environnement en ligne hébergé ou

en nuage, et donne un aperçu des méthodes d'élimination employées dans le traitement de ces questions critiques.

TYPES D'HÉBERGEMENT

Les hébergeurs Internet facilitent l'opération de l'Internet mondial et démêlent les tenants et aboutissants qui le font fonctionner. Leur taille varie de celle d'une entreprise individuelle à celle des entreprises Internet internationales connues mondialement. Le fait que les fournisseurs d'infrastructures Internet sont relativement anonymes les différencie des autres aspects de l'Internet. Ces entreprises opèrent en général dans les coulisses, facilitant l'utilisation de l'Internet pour des entreprises aussi diverses qu'une teinturerie locale ou une banque mondiale.

FORMES D'INFRASTRUCTURES INTERNET

Pour mieux comprendre le marché des services d'infrastructure Internet, il faut envisager les formes sur lesquelles repose le fournisseur de services pour assurer ses services à l'utilisateur final. Ces formes fondamentales se composent de trois éléments :

- **Bâtiment** : Le bâtiment, communément appelé un centre de traitement de données, est la composante physique fondamentale d'un fournisseur d'infrastructure Internet. Il peut appartenir au fournisseur d'infrastructure ou être exploité par une tierce partie. Ce bâtiment abrite les routeurs et les commutateurs qui se connectent à l'Internet ainsi que les serveurs — physiques et virtuels — hébergeant du contenu, des données et des applications.
- **Serveur physique :** Le serveur physique vit dans une armoire ou sur une baie de serveur dans un centre de traitement de données. C'est dans ce serveur physique que le contenu et les applications sont stockés et sécurisés.
- **Serveur virtuel :** Le serveur virtuel est une partition virtualisée d'un serveur physique. Il agit et fonctionne tout comme un serveur physique avec une différence marginale dans la performance. Un seul serveur peut littéralement contenir jusqu'à des dizaines de serveurs virtuels.

Les hébergeurs Internet peuvent généralement être classés dans l'une de cinq catégories principales :

i. Hébergement mutualisé
ii. Hébergement standard sur serveur dédié
iii. Hébergement infogéré sur serveur dédié
iv. Infrastructure en nuage
v. Colocation

CATÉGORIES D'INFRASTRUCTURES INTERNET

Hébergement mutualisé : L'hébergement mutualisé désigne un espace partagé sur un serveur physique sans isolation entre les utilisateurs et sans affectation définie des ressources. Les ressources limitées d'un serveur physique sont partagées — souvent inégalement — parmi tous les clients qui y sont hébergés. Les fournisseurs peuvent littéralement accueillir des centaines de clients sur un seul serveur.

L'hébergement mutualisé est couramment utilisé pour publier le contenu statique ou dynamique de sites Web. Les plateformes de blogues comme WordPress et les applications simples de commerce

électronique sont souvent hébergées dans ces espaces mutualisés et sont dotées d'une installation automatisée.

Les organisations disposant de ressources très limitées utilisent également l'hébergement mutualisé pour communiquer et établir une présence sur Internet. L'hébergement mutualisé existe généralement à l'extrémité inférieure du marché de l'infrastructure. Les usagers types de cette catégorie sont les consommateurs, les petites entreprises, les bureaux à domiciles et les blogueurs.

Hébergement standard sur serveur dédié : Un fournisseur d'infrastructure fournissant un hébergement standard sur serveur dédié généralement loue des serveurs dédiés physiques (parfois dénommés serveurs « Bare Metal ») ou des serveurs virtuels logés dans les bâtiments du centre de traitement de données du fournisseur de l'infrastructure. Les clients louent en général les ressources du serveur sur une base contractuelle fixe.

Les clients de l'hébergement standard sur serveur dédié ont un accès au root sur le serveur et le plus souvent se gèrent eux-mêmes. Le fournisseur d'infrastructure fournit un soutien de base et gère certaines tâches de gestion limitées telles que la maintenance du matériel, les sauvegardes et l'installation du système d'exploitation et du logiciel du serveur Web.

Le serveur appartient au fournisseur qui le loue au client. Le client n'a pas affaire à un cycle de rafraichissement TI. Il peut tout simplement se déplacer vers un autre serveur qui correspond à ses besoins. Normalement, il ne paie pas pour le renouvèlement du matériel ou n'a aucune obligation de rester sur le serveur qu'il a loué.

L'hébergement standard sur serveur dédié est conçu pour accueillir les configurations et les charges de travail relativement simples. Les petites entreprises utilisent généralement un hébergement standard sur serveur dédié pour éviter d'acheter et d'installer des actifs informatiques.

Hébergement infogéré sur serveur dédié : L'hébergement infogéré sur serveur dédié s'applique tant aux serveurs physiques dédiés qu'aux serveurs virtuels. Il existe de nombreuses similitudes entre l'hébergement standard sur serveur dédié et l'hébergement infogéré sur serveur dédié, la principale différence étant que le client paie pour un tout autre niveau de soutien administratif et technique. Ces différences sont dues à la fois à l'augmentation de la taille et à la complexité du déploiement de l'infrastructure. Le fournisseur d'infrastructure intervient pour prendre en charge la majeure partie de la gestion.

L'hébergement infogéré sur serveur dédié implique un large éventail de compétences et de capacités dans les domaines de l'administration des systèmes, de la gestion des bases de données, de la sécurité, du suivi, de la gestion des journaux, de la récupération d'urgence et de la sauvegarde. Les services de gestion peuvent même s'étendre pour couvrir la couche d'application, bien que cela est rare en dehors de la plupart des applications d'entreprise. Un déploiement type d'hébergement infogéré disposera d'un certain nombre de dispositifs additionnels, y compris des bases de données, des serveurs Web et d'applications, des pare-feux et des équilibrages de charge. Au lieu d'un stockage local, les clients utilisent u réseau un système lié au réseau ou des réseaux de zone de stockage. Ils achèteront également des services de sauvegarde et de réplication ou mettront en place des scénarios de récupération d'urgence. Certains fournisseurs d'infrastructures ajoutent à leur offre standard des services-conseils qui vont bien au-delà de la couche de services gérés standard.

Quand il s'agit d'hébergement infogéré sur serveur dédié, la relation d'hébergement se limite en général à un petit nombre des applications qui existent réellement au sein de l'entreprise. L'hébergement infogéré sur serveur dédié est, à bien des égards, utilisé comme une extension d'un centre de traitement de données local.

Ce type d'hébergement est conçu pour accueillir les configurations et les charges de travail relativement larges et complexes. Il est utile également lorsque les organisations ont besoin de capacités très spécifiques et spécialisées telles que la sécurité et la conformité. L'hébergement sur serveur dédié est une solution qui évite l'achat et l'installation d'actifs informatiques et permet de réaliser des économies de couts. Ce moyen permet également de réduire la charge du personnel informatique interne et de libérer des ressources.

Infrastructure en nuage : L'infrastructure en nuage est essentiellement une forme plus souple et évolutive de l'hébergement sur serveur virtuel. L'élément clé de l'infrastructure en nuage est la disponibilité des ressources. La taille d'un serveur peut être augmentée ou réduite, soit sur-le-champ ou dans un laps de temps très court. Ainsi, au lieu d'un ensemble fixe de ressources, l'utilisateur final peut ajuster la capacité de l'infrastructure en fonction de la demande (ou son absence). Typiquement, le service en nuage est consommé à l'heure, mais il commence à être facturé progressivement à la minute, permettant ainsi une consommation fondée sur l'utilité.

L'hébergement en nuage est également très résilient et ne présente aucun point de défaillance. Ses ressources sont mobiles et peuvent basculer automatiquement vers un autre hôte physique. Elles peuvent être redémarrées partout et à tout moment avec le bon ensemble d'outils et de capacités. Cette flexibilité permet au nuage de s'intégrer dans des environnements hybrides de n'importe quel centre de traitement de données, qu'il soit externalisé ou local.

Colocation : La colocation est la fourniture de la capacité du centre de traitement de données pour les organisations ayant besoin d'un lieu hors site pour abriter ou « colocaliser » des serveurs, du stockage ou un équipement de réseautage qui leur appartient et qu'ils gèrent. Les éléments de base de la colocation sont l'espace, la source d'énergie, le système de refroidissement et la connectivité Internet. Dans le modèle de colocation, le client a accès à une zone désignée d'un bâtiment où il installe l'équipement qu'il possède ou qu'il a loué. De nombreux fournisseurs de colocation offrent une gestion à distance et des services de surveillance. Certains fournisseurs louent l'équipement aux clients.

La réalité de l'industrie de l'infrastructure Internet peut devenir plus complexe, car les segments des services d'infrastructure continuent à se brouiller. Par exemple, la ligne entre le niveau d'hébergement standard et le niveau infogéré est de moins en moins claire en ce sens que les fournisseurs s'élargissent pour proposer des services à valeur ajoutée à mesure qu'ils s'orientent vers des services haut de gamme. Il en va de même pour la ligne entre l'hébergement sur serveur dédié — en parlant de serveur virtuel — et l'infrastructure en nuage. Un certain nombre d'offres d'hébergement sur serveur virtuel ressemblent aux infrastructures en nuage. Ils pourraient ne pas avoir toutes les caractéristiques du nuage, mais ils en présentent assez pour brouiller la ligne et créer des zones floues.

PANORAMA DES MENACES

Voici une liste des types d'abus les plus fréquemment observés chez les hébergeurs et les fournisseurs de services en nuage. Cette liste ne prétend pas être complète et changera invariablement avec le temps.

- **Spam (sortant)** : Le spam est tout courriel commercial indésirable ou non sollicité. Les fournisseurs doivent s'assurer que les utilisateurs finaux suivent les meilleures pratiques les plus récentes du M3GTAA concernant les expéditeurs.[68] Les hébergeurs Internet devront également s'abonner à autant de rapports de boucle de rétroaction qu'il leur est possible de traiter.
- **« Spamvertising » (redirections et charges utiles hébergées)** : Le spamvertising se produit lorsqu'un utilisateur final de l'hébergeur engage une tierce partie pour annoncer sa présence sur le Web. La plupart des plaintes de spam résultent des utilisateurs finaux qui envoient des courriels à des clients potentiels pour vanter de manière excessive un produit ou un service. Les fournisseurs recevant une de ces plaintes en sont très probablement au courant, soit en tant qu'expéditeur du courriel ou hôte du site faisant l'objet du courriel.
- **Hameçonnage sortant (hébergement et entrant pour des informations d'identification de client)** : L'hameçonnage se produit principalement lorsque le compte d'un utilisateur final est compromis, pratiquement toujours à la suite de scripts obsolètes que les utilisateurs finaux ont exécutés. Un site d'hameçonnage est un site frauduleux qui prétend être une entreprise légitime, comme une banque, une société de carte de crédit ou PayPal, et qui demande à l'individu de saisir des informations confidentielles. Les hameçonneurs obtiennent alors tout ce dont ils ont besoin pour frauder l'individu. (Voir la section Hameçonnage et piratage psychologique pour de plus amples informations.)
- **Pages piratées ou défigurées (hébergées côté client) :** Bien que les plaintes d'hameçonnage se classent souvent dans cette catégorie, les comptes piratés ne seront pas tous utilisés à des fins d'hameçonnage. Certains peuvent simplement être défigurés et les données des utilisateurs finaux endommagées ou détruites. Souvent, les pirates injecteront également un code malveillant ou téléchargeront des bots ajustés de manière à causer des problèmes supplémentaires comme l'exploitation de sites, les téléchargements furtifs ou la redirection vers d'autres contenus malveillants. Les tiers et les organismes d'application de la loi analysent ces évènements et fournissent des informations sur la façon de réparer les sites piratés. La plupart des comptes sont compromis en raison de systèmes de gestion du contenu non actualisés par les utilisateurs finaux pour des installations telles que Joomla ou WordPress.
- **Matériel pédopornographique (hébergé côté client)** : Pour le traitement approprié de ces questions, veuillez consulter le document du M^{3}AAWG sur les meilleures pratiques courantes concernant la manière de disposer du matériel pédopornographique (https://www.m3aawg.org/sites/default/files/document/M3AAWG_Disposition_CAM-2015-02.pdf).
- **Questions relatives aux droits d'auteur et à la propriété intellectuelle/marques commerciales (hébergées côté client) :** Pour consulter en ligne la loi américaine sur les droits d'auteur, voir http://www.copyright.gov/reports/studies/dmca/dmca_executive.html. D'autres régimes de droits d'auteur sont applicables dans d'autres juridictions.

- **Déni de service distribué ou autre trafic hostile sortant :** Les fournisseurs de service en nuage ou les hébergeurs Internet peuvent avoir de meilleures protections que les petites entreprises individuelles, mais ils courent également des risques plus élevés d'attaques DDoS que d'autres entreprises en ligne parce qu'ils ont, en effet, agrégé l'ensemble des risques de leurs clients. Une attaque sur un client peut affecter les autres et potentiellement toute l'opération d'hébergement en raison d'une forte dépendance sur l'infrastructure partagée.
- **Les abonnements malveillants :** Les pirates informatiques construisent des réseaux zombies en utilisant uniquement des essais gratuits ou des comptes gratuits « *freemium* » sur des services d'hébergement d'application en ligne. Ces pirates utilisent ensuite un processus automatisé pour générer des adresses électroniques uniques et s'abonner à des comptes gratuits en masse pour un assemblage de réseau zombie en nuage composé de milliers d'ordinateurs.

PRINCIPAUX DOMAINES DE PRÉOCCUPATION

Installations CRM vulnérables/dépassées

Étant donné qu'il existe plus de 67 millions de sites WordPress, ce qui représente 23 % de tous les sites du monde[69] —et que les éditeurs utilisent la plateforme pour créer des blogues, des sites d'information, des sites d'entreprise, des magazines, des réseaux sociaux, des sites sportifs, et autre, —il n'est pas surprenant qu'un grand nombre de criminels en ligne décident d'obtenir leur accès à travers ce système de gestion de contenu (CMS). Par exemple, Drupal, une plateforme CMS en croissance rapide, a été ciblée en 2014 par l'intermédiaire d'un logiciel tiers installé sur l'infrastructure du serveur de Drupal.org.

Ce n'est pas uniquement la popularité de ces sites qui les rend des cibles intéressantes. Un grand nombre de sites sur ces serveurs, bien qu'actifs, ont été abandonnés par leur propriétaire. Il y a probablement des millions de blogues abandonnés et de domaines achetés restés inactifs, et il est très possible qu'un certain nombre de ces sites ait été corrompu par les cybercriminels. Les experts de Cisco en matière de sécurité prédisent que le problème ne fera qu'empirer avec le nombre croissant des personnes qui sur les marchés émergents de l'Internet à travers le monde établissent un blogue ou un site Web et le délaissent.

L'utilisation généralisée de plug-ins conçus pour étendre les fonctionnalités d'un CMS et pour alimenter des vidéos, des animations et des jeux, se révèle également bénéfique aux cybercriminels cherchant à obtenir un accès non autorisé aux plateformes. Pour aggraver ce problème, de nombreux plug-ins sont laissés ne sont pas actualisés par leurs auteurs, forçant ceux qui les utilisent et en dépendent à ne pas mettre à jour leur installation au prix de perdre des clients ou des fonctionnalités de leur site. De nombreux CMS compromis observés par les chercheurs de Cisco en 2013 remontent à des plug-ins écrits dans le langage de script PHP, conçus mal et de manière non sécurisée.

Les statistiques recueillies par la société de sécurité Sucuri montrent un total de 3143 vulnérabilités WordPress, dans 15 catégories différentes.[70] Avec cette masse de vulnérabilités, les consommateurs de WordPress ont commencé à garder leur logiciel à jour, mais plus de 30 % des sites WordPress utilisent toujours la version 3 ou une version précédente[71], laissant ces sites exposés à l'exploitation des parties malveillantes.

Attaques DDoS :
Parce que les attaques DDoS ont longtemps été considérées comme « de l'histoire ancienne » en termes de techniques cybercriminelles, de nombreuses entreprises étaient persuadées que leurs mesures de sécurité pouvaient les protéger de manière adéquate. Cette confiance a été ébranlée en 2012 et 2013 par des attaques DDoS à grande échelle, dont l'opération Ababil qui a ciblé plusieurs institutions financières, probablement à des fins politiques.

Les chefs de file de l'industrie ont mis en garde contre les attaques DDoS qui, selon eux, devraient être une préoccupation majeure en matière de sécurité pour les organisations du secteur public et privé, car les campagnes futures devraient être encore plus importantes. Les organisations, en particulier celles d'un secteur industriel considéré comme une cible de premier choix telle que les services financiers et l'énergie, ou celles ayant un intérêt dans un tel secteur, doivent faire preuve d'une vigilance exceptionnelle. Entre 2010 et 2013, l'ensemble des interruptions imprévues dues à des attaques DDoS ont augmenté de 2 % à 13 %.[72] En fait, une comparaison des quatrièmes trimestres de 2013 et 2014 a montré que les attaques DDoS ont augmenté de 90 %, soulignant que les attaques ne font qu'augmenter.[73] Le cout total moyen de ces interruptions a également augmenté, passant de 613 000 USD à 822 000 USD en ce même laps de temps. [74]

Certaines attaques DDoS ont pris une tournure inquiétante. Elles ont été utilisées pour détourner l'attention d'autres activités illicites, telles que la fraude électronique. Ces attaques peuvent submerger le personnel bancaire, et empêcher le transfert d'être notifié au client et empêcher les clients de signaler la fraude. Les institutions financières sont rarement en mesure de recouvrer leurs pertes financières. Une telle attaque a eu lieu le 24 décembre 2012 et ciblé le site Web d'une institution financière régionale en Californie ; elle a permis de détourner l'attention des responsables de la banque du piratage du compte en ligne de l'un des clients rapportant aux voleurs plus de 900 000 USD.

L'expertise de plus en plus pointue dans la compromission des serveurs d'hébergement ne fera que rendre plus facile aux cybercriminels de lancer des attaques DDoS et de voler les organisations ciblées. En opérant une partie de l'infrastructure de l'Internet, les acteurs malveillants peuvent profiter d'une largeur de bande massive, et se préparer ainsi à lancer un certain nombre de campagnes puissantes. C'est déjà une réalité : en aout 2013, le gouvernement chinois a signalé que la plus grande attaque DDoS à laquelle elle a dû faire face a bloqué l'accès chinois à l'Internet pendant environ quatre heures.

Même les spammeurs utilisent des attaques DDoS pour riposter aux organisations qui, à leur avis, bloquent leur accès aux revenus. En mars 2013, l'organisation à but non lucratif Spamhaus (qui assure un suivi des spammeurs et a créé la liste rouge Spamhaus, un répertoire d'adresses IP suspectes) a fait l'objet d'une attaque DDoS qui a temporairement bloqué son site Web et ralenti le trafic Internet du monde entier. Les assaillants seraient prétendument des associés du CyberBunker, un hébergeur néerlandais avec des conditions d'utilisation permissives, et du STOPhaus, qui a publiquement exprimé son aversion envers les activités de Spamhaus. L'attaque DDoS a eu lieu après que Spamhaus, dont le service est largement utilisé, a fait figurer CyberBunker sur sa liste noire.

Serveurs mal configurés dans des environnements non gérés :
Avec l'arrivée des services en nuage, les utilisateurs ont la possibilité de créer et de configurer un environnement de serveur complet en une fraction du temps qui leur aurait fallu pour le matériel physique. Cela a permis aux utilisateurs de créer facilement leur propre infrastructure avec peu ou aucune connaissance sur le fonctionnement des systèmes qu'ils mettent en place. Bien que ce

changement a permis aux utilisateurs de faire plus qu'ils ne faisant avant, il a imposé de nouveaux défis dans la prévention et l'arrêt des abus qui ciblent ces systèmes.

La plupart des serveurs virtualisés et non gérés ne sont pas entretenus avec la vigilance déjà en place dans le monde du matériel physique géré. Les systèmes et les programmes d'exploitation ne sont pas correctement mis à jour (ou pas du tout) pour traiter par des correctifs les vulnérabilités et failles de sécurité. Les autorisations sont rarement modifiées ou sont fixées de manière qui autorise chaque personne ayant accès au serveur à introduire des modifications, laissant un serveur ouvert au monde extérieur et susceptible aux activités malveillantes.

Certains programmes utilisent des méthodes de communication entrantes et sortantes qui, à moins d'être correctement configurées, rend un serveur susceptible de servir d'outil dans des attaques de DDoS par réflexion, d'identification SSH, d'injection SQL et autres, pouvant bloquer les systèmes ciblés pour une période de temps considérable. En outre, ces erreurs de configuration permettent aux parties malveillantes d'accéder à des sites ou des informations hébergés sur le serveur, avec pour résultat un vol de données, des sites d'hameçonnage et l'hébergement de programmes malveillants.

La surveillance de ces systèmes mal configurés et leur mise à jour est une tâche monumentale pour les hébergeurs de ces serveurs donc peu est fait concernant ces systèmes avant qu'ils ne soient compromis.

MEILLEURES PRATIQUES

Prévention :

1) **Vérifier les clients avant qu'ils ne causent de problèmes :** Les hébergeurs Internet sont à la merci des pires pratiques de leurs clients. Les fournisseurs doivent prendre les devants en mettant en place un processus de vérification qui identifie les clients malveillants avant que ceux-ci n'entreprennent leurs activités abusives. Des efforts ciblant les clients qui seraient de bons candidats pour la société d'hébergement sont une autre façon de préserver la sécurité de l'environnement d'hébergement.
2)

3) **Exiger que les clients gardent les logiciels à jour :** le refus de garder à jour le logiciel, le matériel ou le support physique au sein de l'environnement est l'une des principales causes d'abus dans l'espace d'hébergement. Le contrat des clients devrait préciser que ceux-ci feront tout leur possible pour garder leurs systèmes à jour.

4) **Former et sensibiliser le personnel en contact direct avec les clients en matière de sécurité :** Les équipes en contact direct avec les clients, telles que le soutien à la clientèle, les ventes et le markéting, ne rencontrent pas au quotidien les problèmes qui constituent la norme pour les équipes de sécurité et de lutte contre les abus. Ces équipes devraient recevoir une formation pour savoir quand ils devraient informer un client ou un prospect que ses pratiques ne respectent pas les conditions et les règles de bon usage du système, ils sont de suite, et où ils devraient s'efforcer de fournir un environnement.
5) **Prévenir les abus à la périphérie du réseau :**
   a) Envisager des systèmes de détection d'intrusion (IDS) par le matériel.
   b) Utiliser les balayages des logiciels pour les analyses de sécurité et les pare-feux.
   c) Promouvoir l'utilisation de pare-feux basés sur le Web.
   d) Utiliser une approche différentielle à l'attribution des droits pour les clients importants.

e) Conclure des contrats avec les clients pour assurer la sécurité.
f) Maximiser le contact avec la clientèle et protéger l'identité des clients.
g) Encourager le client à utiliser des mots de passe forts.
h) Appliquer les meilleures pratiques sur les réseaux IPv6 : L'IPv6 offre tant d'adresses tant qu'il n'y a aucun besoin — et aucune raison — de partager une adresse IP unique entre plusieurs clients. La meilleure pratique consiste à attribuer à chaque client un espace d'adressage IPV6 /64 distinct. Même sur le plus petit système physiquement partagé, chaque client et chaque site doit disposer d'une adresse unique. Cela facilite la recherche des sources d'abus, permet aux victimes de bloquer le client fautif sans bloquer tout le reste du monde sur un même hôte, et le cas échéant facilite la suspension et le renouvèlement du service au besoin.
i) Les hébergeurs Internet doivent maintenir rigoureusement en interne leurs systèmes et pratiques de sécurité. Toutes les mesures préconisées ci-dessus sont inutiles si des acteurs malveillants parviennent à deviner les mots de passe qu'utilise le personnel du fournisseur. Les hébergeurs Internet doivent satisfaire les normes de conformité PCI.

Détection et identification :

1) **Utiliser des identifiants de clients confidentiels :** Les hébergeurs devraient créer un identificateur unique pour chaque client spécifique. Cet identificateur ne doit être évident qu'à l'hébergeur et devrait sembler inintelligibles aux tiers. Ceci protège l'identité du client tout en permettant à l'hébergeur d'hébergement d'identifier simplement et efficacement ses clients.

2) **Établir des comptes de rôle pour les domaines du réseau :** Les rôles établis par les RFC ainsi que les comptes de courriel considérés comme pratique courante devraient être créés pour chaque domaine et le domaine de client mis en service sur un réseau.

3) **Maintenir un SWIP et des IP exacts dans les enregistrements WHOIS :** Les hébergeurs Internet devraient maintenir des inscriptions claires et précises auprès de leur registre Internet régional (RIR) en ce qui a trait à l'attribution des espaces IP, y compris chaque sous-allocation supérieure à /27 clients. Ces inscriptions WHOIS devraient comprendre les comptes de rôle fonctionnel en vue du signalement d'abus.

4) **Mettre en place une télémétrie interne qui signale l'état du réseau :** En voici quelques exemples,
   a) autoanalyse du réseau,
   b) analyseur de trafic, et
   c) contrôle du filtre antispam sortant.

5) **Simplifier le signalement d'abus :** Les hébergeurs Internet doivent fournir des moyens aux membres du public afin que ceux-ci puissent soumettre des rapports signalant tout abus qu'ils perçoivent comme émanant du réseau en question. Les hébergeurs doivent ensuite accuser réception de ces rapports et prendre les mesures appropriées. Les hébergeurs Internet doivent garder des canaux de communication redondants pour remplacer tout canal défaillant.
   a) Courriel,
   b) Téléphone,
   c) Message instantané (chat),
   d) Systèmes de billets,
   e) Rapport sur l'état du site Web, et
   f) Présence sur les réseaux sociaux.

6) **Répondre rapidement aux plaintes :** Chaque soumission devrait avoir un accusé de réception automatique (AUTO-ACK) contenant assez de précision pour distinguer la soumission en question d'autres soumissions du plaignant. L'accusé de réception devrait inclure la plainte initiale, un numéro du billet original et toute autre information pouvant assurer à l'utilisateur que la plainte a été reçue et sera suivie.

7) **Envisager la désignation de reporters de confiance :** Les déposants des plaintes pourraient être déterminés à ce qu'elles soient de haute qualité ou de haute priorité Ces sources peuvent être internes comme elles peuvent être externes. Il convient de prévoir une voie de service de style prioritaire, tout en maintenant des niveaux de priorité spécifiés. Par exemple, un contact chez une liste noire de noms de domaine dont l'usage est répandu pourrait être désigné comme reporter approprié des priorités, même si une plainte de spam de cette source demeure évidemment moins importante qu'une attaque DDoS ayant lieu en même temps.

8) **Mettre en place des boucles de rétroaction (FBL) et des rapports automatisés :** Les consommateurs s'abonnant aux données FBL aident à éviter les listes DNSBL, limiter les dommages aux réputations et permettre au personnel de traiter de manière proactive avec les clients abusifs et abusés (compromis).

9) **Mettre en place des indicateurs de comparaison :** Établir des indicateurs systématiques qui seront utilisés par les hébergeurs Internet permet à ces hébergeurs ainsi qu'aux organismes d'application de la loi d'identifier l'abus et de comparer efficacement les données de l'ensemble de l'industrie.[75]

Élimination :
Les priorités en matière d'élimination fournissent aux hébergeurs Internet et aux clients des lignes directrices pour la solution des problèmes. Les recommandations concernant la priorité accordée aux plaintes doivent tenir compte de la sévérité et de la gravité de l'abus ainsi que de la portée de la question. En outre, la source du rapport et la sévérité du tort à la réputation de l'hébergeur Internet et du client doivent être prises en considération. Une campagne de spam massive pourrait être plus importante que la présence d'un réseau zombie inactif. Il devrait y avoir une évaluation au cas par cas des questions pouvant altérer le niveau de priorité pour un fournisseur donné ou un client donné.

Réagir rapidement aux questions de haut-niveau/prioritaires :
La majorité des plaintes reçues par un hébergeur ne nécessitent qu'un accusé de réception. Certains cas, cependant, tels que les plaintes de haut niveau, les demandes de retrait de site ou de retrait de la liste noire, nécessitent une réponse supplémentaire. Il faut contacter tout d'abord le client ou l'organe qui signale pour l'informer que le problème est en cours de traitement. Ils devraient être contactés à nouveau lorsque le problème est résolu. Les communications multiples ne s'avèrent nécessaires que si des questions persistantes ou exceptionnelles existent.
Communiquez de manière proactive lorsque des évènements se produisent à l'échelle de l'industrie ou de la compagnie.

Dans l'éventualité d'une compromission ou d'une vulnérabilité sérieuse qui pourrait exposer de multiples clients ou un groupe particulier de clients à des risques, un plan de communication devrait être élaboré visant à les informer du problème et à leur fournir des instructions générales sur la manière de le résoudre. Si la violation comprend un accès à des données personnelles, vous devez connaitre vos obligations en vertu des exigences régionales ou nationales, y compris la

portée de votre avis aux personnes touchées et votre notification des autorités appropriées chargées d'appliquer la loi. Ces communications doivent être envoyées en temps opportun. En outre, le personnel de soutien devrait être informé du problème et avoir les directives leur permettant de résoudre l'affaire avec les clients qui ont besoin d'aide.

S'occuper efficacement des clients difficiles :

1) Confirmer la validité de la plainte.
2) Informer le client d'une compromission. Inclure des instructions vérifiées destinées à aider le client dans la résolution du problème.
3) Fournir au client les Conditions générales pertinentes et les règlements gouvernementaux applicables pouvant avoir été violés et ayant causé la notification de violation ou de suspension de service. Ce faisant, l'accord avec le client est intact. La notification du client protège l'hébergeur Internet des questions éventuelles liées au client ou à un plaignant externe pouvant donner lieu à une contestation judiciaire.
4) Accorder un délai au client afin qu'il puisse remédier au problème ou, si un accord est en place, laisser au fournisseur le temps de résoudre la question lui-même.
5) Confirmer que la plainte a été résolue.
6) Clore l'incident. Au besoin, notifier la partie ayant soumis le rapport que le problème a été résolu. Suspendre le service des clients n'ayant pas répondu.

HARCÈLEMENT EN LIGNE

Pas un jour ne passe sans que les médias traditionnels et en ligne ne signalent une certaine forme de harcèlement en ligne. Bien qu'il puisse varier d'un harcèlement agaçant à des questions de vie ou de mort, il est clair que le problème du harcèlement en ligne va augmenter en fréquence au fur et à mesure que les services Internet deviennent de plus en plus disponibles mondialement. Ce phénomène peut aller d'embarrassants et cruels messages ou photos en ligne, des menaces en ligne, du harcèlement psychologique, des commentaires négatifs, au harcèlement permanent par courriel, sites Web, réseaux sociaux et messages textes.

Chaque groupe d'âge est vulnérable au harcèlement en ligne, qui représente un problème croissant dans les écoles, sur les campus universitaires, et même sur le lieu du travail. Le harcèlement en ligne est devenu un problème parce que l'Internet offre un anonymat attrayant aux agresseurs, étant donné qu'il est difficile de remonter à la source de l'intimidation. Malheureusement, rumeurs, menaces et photos peuvent être diffusées sur Internet très rapidement.

Il y a eu des tentatives de viabilité variable pour règlementer[76] et même rédiger une loi[77, 78]qui se penche sur certains aspects de la question, mais ce domaine a été dans l'ensemble à la fois omniprésent et en attente d'un examen supplémentaire et de l'élaboration de meilleures pratiques.

Le texte suivant fournit une liste des différentes formes de harcèlement en ligne ; il est suivi de quelques conseils simples permettant d'éviter le harcèlement.

Catfishing — un faux profil est configuré sur des sites et des réseaux sociaux pour attirer une victime potentielle dans une relation en ligne puis lui soutirer de l'argent.

Harcèlement par petites annonces (Craigslist) — des annonces sont créées qui prétendent qu'une personne recherche une relation sexuelle brutale ou d'autres types de comportement atypique et les réponses sont acheminées vers le numéro de téléphone du domicile de la victime ou son courriel.

La cyberintimidation – essentiellement un cyberharcèlement permanent, mais porte plus sur des enfants et adolescents harcelés en ligne par d'autres étudiants via des sites Web, des réseaux sociaux, des forums de discussion, du courriel ou par des applications pour smartphone et des SMS.

Le cyberharcèlement — quand le harceleur en ligne a été appelé à arrêter et continue à contacter la victime en ligne, de manière répétitive. Il peut prendre bien des formes — courriel, commentaires et messages publiés sur un site Web, forums de discussion, SMS, commentaires et messages via des applications de smartphone, etc.

Doxing – découvrir les données personnelles d'une personne et les révéler en ligne, y compris l'adresse domiciliaire, le numéro de téléphone du domicile, le numéro de cellulaire, le lieu et numéro de téléphone du travail, les informations des parents, etc.[79]

Emprunt d'identité — lorsqu'un utilisateur crée des profils ou des comptes en se servant d'un autre nom, photos et données d'identification, puis emprunte l'identité de cette personne. Ceci peut être utilisé pour discréditer la victime, ou dans certains cas comme un premier pas vers des activités frauduleuses visant un gain financier. Par exemple, en volant des photos et des informations d'un profil de réseaux sociaux et en créant un nouveau profil, un acteur malveillant peut se lier d'amitié avec des parents et des amis de la victime et les contacter dans le cadre d'une formule « voyageur coincé à l'étranger »[80] par lequel la personne prétend avoir voyagé quelque part et perdu son portefeuille. Les amis proches sont les plus susceptibles de tomber pour cette arnaque et envoyer de l'argent parce qu'ils croient que le profil truqué est réel.

Mobbing — lorsqu'un groupe d'utilisateurs en ligne cible un ou plusieurs individus et comme un « gang » harcèle et traque la victime ou les victimes pour forcer l'individu contre son gré de quitter l'Internet, l'expulser de son école ou lui faire perdre son emploi. [81]

Outing — divulguer l'orientation sexuelle (réelle ou alléguée) d'une personne, qu'elle soit homosexuelle, lesbienne, transgenre, ou partager en ligne des informations sur ses fétiches, conditions médicales, etc., sans permission.

Vol d'identité en ligne — vol de données personnelles à des fins d'usurpation d'identité ou de vente, donc il peut être utilisé pour obtenir frauduleusement des cartes de crédit ou d'autres instruments financiers, comme des crédits et des hypothèques.

Critique de vengeance — afficher des critiques fausses ou extrêmement épineuses sur des sites comme ripofferport.com. Celles-ci peuvent également prendre la forme de la publication, sur des sites comme thedirty.com, d'informations à caractère personnel portant des jugements catégoriques.

Porno de vengeance — le partage sur des sites Web et des forums en ligne de photos ou vidéos sexuellement explicite, sans le consentement de la partie concernée. Comme avec d'autres méthodes de harcèlement en ligne, la plupart des auteurs essaient de garder l'anonymat tout en mettant en ligne la porno de vengeance via la création de comptes de courriel gratuits ou de faux profils pour écrire au sujet de leurs victimes.

Textopornographie — consiste à envoyer en ligne des photos ou des vidéos sexuellement explicites via des applications telles que Snapchat, Instagram, Vine ou des sites Web tels que Facebook. Bien que la textopornographie en elle-même n'est pas harcèlement en ligne, elle peut le devenir si les photos sont envoyées à des destinataires réticents ou si le destinataire à son tour les redistribue.

Swatting — un faux appel téléphonique vers les autorités pour inciter une intervention armée, normalement par une équipe SWAT[82]. Cela prend parfois la forme d'une fausse menace de bombe ou d'un faux signalement de prise d'otages armée.

Trolling — les utilisateurs en ligne qui tentent de polémiquer par des commentaires intentionnellement tangentiels ou agressivement impolis. Cette catégorie peut comprendre les trolls embauchés, notamment les individus associés à des campagnes politiques peuvent être payés

pour enflammer les discussions ou publier des points de vue ridiculement empoisonnés de leurs adversaires pour les discréditer.

Meilleures pratiques pour limiter le harcèlement en ligne [83]:

Limitez où vous postez vos informations personnelles : Soyez conscient des personnes pouvant accéder à vos informations de contact ou à des informations sur vos intérêts, vos habitudes ou votre emploi pour minimiser votre exposition aux agresseurs. Ceci pourrait limiter votre risque de tomber victime et rendre, le cas échéant, l'identification de l'agresseur plus facile.

Évitez d'aggraver la situation : Une réponse hostile est susceptible de provoquer un agresseur. Selon les circonstances, pensez à ignorer la question. Souvent, la cyberintimidation et les agresseurs s'appuient sur la réaction de leurs victimes. Si vous ou votre enfant recevez des messages électroniques non désirés, que ce soit des SMS, des messages textes ou

Courriel, envisagez le changement de votre adresse électronique. Le problème pourrait disparaitre. Si vous continuez à recevoir des messages sur votre nouveau compte, vous aurez un solide dossier en faveur d'une action en justice.

Documentez la cyberintimidation : Notez toute activité en ligne (courriels, pages Web, messages sur les réseaux sociaux, etc.), y compris les dates pertinentes et l'heure. Conservez de ce registre une version électronique ainsi qu'une copie imprimée.

Signalez la cyberintimidation aux autorités compétentes : Si vous ou votre enfant êtes harcelé ou menacé, signalez l'activité correspondante aux autorités locales. Votre police locale ou nationale est souvent un bon point de départ. Il existe une distinction entre la liberté d'expression et les délits punissables. Les autorités chargées d'appliquer la loi et les procureurs peuvent vous aider à démêler les implications juridiques. Il conviendrait également de le signaler aux responsables de l'école qui peuvent avoir des politiques distinctes pour faire face à une activité impliquant les étudiants.

Contrôlez votre présence en ligne : Lorsque ces options sont disponibles, configurez les paramètres de confidentialité et de sécurité sur les sites Web de manière à ce qu'ils conviennent à votre niveau de confort pour le partage d'information. Par exemple, modifiez les paramètres de vos réseaux sociaux afin de limiter la visibilité des messages aux « amis seulement ». Vous avez le droit de limiter la manière de partager vos informations.

Utilisez des mots de passe forts et des questions d'identification : N'utilisez pas les mêmes mots de passe sur plusieurs sites. Si vous avez du mal à vous souvenir des mots de passe, utilisez un gestionnaire de mot de passe tel que iPassword (Agilebits) et utilisez l'authentification à deux facteurs, si possible sur les réseaux sociaux et les comptes de courriel. Si vous publiez des informations personnelles comme votre école élémentaire et le nom de jeune fille de votre mère sur les réseaux sociaux, utilisez des réponses différentes pour les questions d'identification que peut vous demander votre institution financière, afin que les réponses ne soient pas facilement devinées. Aussi, plutôt que d'utiliser des renseignements personnels réels, pensez à choisir une phrase

absurde que vous pouvez mémoriser et utilisez-la pour toutes ces questions (par exemple, le nom de jeune fille de votre mère : Batman).

Plus sûr pour moi, plus sûr pour tous : Ce que vous faites en ligne peut affecter tout le monde — à la maison, au travail et tout autour du monde. La pratique de bonnes habitudes en ligne sert les intérêts de la communauté numérique mondiale.

Sensibiliser votre communauté : De nombreuses ressources disponibles aident à décourager la cyberintimidation. Fournies par les autorités gouvernementales : [84]

CONCLUSION

Ces dernières années, l'environnement des menaces en ligne et mobile a changé radicalement, ciblant un large éventail de particuliers, d'entreprises et de réseaux. L'émergence de nouvelles technologies permet d'élaborer des attaques plus sophistiquées en exploitant les vulnérabilités d'un large éventail de plateformes, de canaux et de services.

Les méthodes traditionnelles de lutte contre les menaces en ligne, avec un logiciel antivirus, des pare-feux et des campagnes de sensibilisation constituent toujours une partie importante de la défense. Les programmes malveillants et réseaux zombies apparus depuis quelques dernières se sont transformés pour éviter d'être détectés et éliminés. Pour répondre à ces menaces nouvelles et émergentes et les combattre, la communauté internationale doit prendre des mesures supplémentaires dans l'écosystème de l'Internet, et élaborer dans le cadre d'une collaboration, des approches multilatérales à volets multiples.

Le présent rapport présente les meilleures pratiques recommandées aux consommateurs, à l'industrie et aux gouvernements pour lutter contre les menaces en ligne et mobiles. Ces recommandations proposent entre autres aux consommateurs de savoir anticiper en sécurisant leurs propres appareils ; aux fournisseurs de services d'appliquer les technologies et pratiques recommandées en matière de sécurité le plus tôt possible ; aux gouvernements d'assurer la mise en place d'environnements règlementaire et législatif modernes et leur application et d'œuvrer avec les organisations internationales afin de soutenir les efforts collaboratifs.

Elles représentent un ensemble d'outils permettant de contrôler les menaces en ligne, mobiles et de téléphonie vocale. Cependant, les menaces décrites dans le présent rapport sont juste un aperçu de l'environnement des menaces sévissant aujourd'hui. Au fur et à mesure que changent les activités en ligne, que l'utilisation de l'informatique mobile s'intensifie, et que les internautes et les entreprises modifient leurs réponses et leurs moyens de défense face aux menaces existantes, ces menaces évolueront et s'adapteront pour exploiter de nouvelles vulnérabilités et poursuivre de nouvelles cibles.

La mise en pratique de ces recommandations nécessite une approche multilatérale concertée. À cette fin, les auteurs de ce rapport encouragent fortement l'OCDE ainsi que d'autres organisations internationales à se joindre au M^{3}AAWG et au LAP et à collaborer avec les organisations régissant et administrant les infrastructures Internet. En outre, afin d'anticiper l'évolution de l'environnement des menaces, toutes les organisations concernées devraient commencer à participer plus activement au suivi des menaces et à la mise en œuvre de nouvelles mesures pour y remédier au besoin.

GLOSSAIRE

- **Fraude 419 :** nommée ainsi en référence au Code pénal nigérian chapitre 38, section 419 portant sur la fraude. « Quiconque aura, par des moyens frauduleux et dans l'intention de frauder, obtenu d'une autre personne toute chose susceptible d'être volée, ou incite une personne à livrer à quiconque une chose susceptible d'être volée, est coupable d'une infraction grave et passible d'une peine d'emprisonnement de trois ans ». Il s'agit des notoires courriels nigérians venant de princes ou d'autres schémas nécessitant l'avance d'une somme d'argent en échange de richesses incommensurables à la fin de la procédure.

- **Fraude au paiement à l'avance :** Les courriels proposent entre autres un acompte et le paiement excessif de services offerts. La forme la plus courante de cette fraude demande l'envoi de l'acompte à une tierce partie. Lorsque la tierce partie aura encaissé ce paiement, le paiement original s'avère être faux et il est rétracté du solde bancaire de la victime.

- **Protocole de passerelle frontière** (**Border Gateway Protocol-BGP) :** le protocole chargé des décisions du routage de base sur le réseau Internet. Il gère un tableau des réseaux IP ou « préfixes » qui désigne l'accessibilité des réseaux au sein du système autonome.[1]

- **Caches :** conservent les informations récemment utilisées dans un endroit plus rapidement accessible. Par exemple, un navigateur Web utilise un cache pour conserver sur votre disque dur l'information concernant les pages Web récemment visitées. L'accès au disque dur de votre ordinateur étant beaucoup plus rapide que l'accès à l'Internet, la mise en cache des sites peut accélérer considérablement votre navigation Web. [2]

- **Déni de service distribué (DDoS) :** attaque informatique visant à inonder un système cible ou autrement perturber sa capacité de recevoir des informations et d'interagir avec tout autre système. Par exemple, il s'agirait d'envoyer soit un seul soit un grand nombre de messages non sollicités vers un serveur ou un réseau afin d'empêcher son fonctionnement.

- **Téléchargements furtifs :** téléchargement involontaire de logiciels sur Internet. Un utilisateur peut autoriser un téléchargement sans en comprendre les conséquences, comme un programme exécutable falsifié, ou le téléchargement peut s'effectuer entièrement à l'insu de l'utilisateur.[3]

- **Fournisseur de services de courriel :** entreprise spécialisée dans la prestation de services de courriel à d'autres entreprises. Ces services peuvent comprendre la collecte et le maintien des listes d'adresses électroniques, l'envoi de courriels en masse aux adresses figurant dans les listes, l'élimination des adresses qui rebondissent, et le traitement des plaintes et des signalements d'abus découlant des envois de courriels en masse.

- **Pare-feu :** matériel ou logiciel installé sur un ordinateur pour contrôle l'accès entre un réseau privé et un réseau public comme l'Internet. Un pare-feu est conçu pour fournir une protection en empêchant tout accès non autorisé à l'ordinateur ou au réseau.

- **Global System for Mobile Communication (GSM) :** ensemble de normes mis au point par l'ETSI (European Telecommunications Standard Institut) pour décrire les protocoles de la seconde génération (2G) de réseaux cellulaires numériques de la téléphonie mobile. [4]

- **Filtrage d'accès au réseau (*ingress filtering*) :** technique utilisée pour s'assurer que les **Error! Hyperlink reference not valid.** entrants proviennent réellement de réseaux d'où ils prétendent provenir en bloquant les adresses IP fausses. [5]

- **Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN) :** coordonne les identificateurs uniques, y compris le système des noms de domaine (DNS), l'adressage du protocole Internet (IP), l'attribution de l'espace, l'affectation d'identificateurs de protocole, la gestion du système des noms de domaine génériques (gTLD) et des noms de domaine de codes de pays (ccTLD) de premier niveau ainsi que les fonctions de gestion du système de serveurs racines.

- **Mule :** personne qui transfère de l'argent ou des marchandises volées d'un pays à l'autre, soit en personne, soit via un service de courrier ou par voie électronique. Les mules en ligne existent généralement à la suite de l'hameçonnage ou des arnaques par programme malveillant[7]

- **Nœud :** dans le contexte de la transmission des données, un nœud d'un réseau de transmission physique peut soit être un équipement de terminaison de circuits de données (ETCD) tel qu'un modem, un hub, un pont ou un commutateur ; soit un équipement terminal de traitement de données (ETD) tel qu'un appareil de téléphone numérique, une imprimante ou un ordinateur hôte, ou par exemple un routeur, une station de travail ou un serveur.

- **JavaScript :** langage de script permettant aux auteurs de concevoir des pages Web interactives.

- **Hameçonnage :** tentative d'obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité ou de voler des numéros de carte de crédit ou de coordonnées bancaires à des fins frauduleuses. Par exemple, un message électronique semblerait provenir de la banque du destinataire pour l'inviter à se rendre sur un site Web et confirmer les détails de compte, mais plutôt le redirige vers un site Web falsifié où les renseignements personnels sont recueillis.

- **SMShing — hameçonnage via SMS ou message texte :** lien qui mène à un site Web frauduleux est envoyé par SMS, ou message qui demande au destinataire de composer un numéro de téléphone où l'attaque de piratage psychologique se poursuivra.

- **Usurpation** : prendre délibérément l'identité d'une autre personne physique ou morale, généralement afin de faire croire qu'un courriel ou un appel provient d'une source autre que sa véritable source.

- **Domaines de premier niveau (TLD) :** les TDL sont le plus haut niveau hiérarchique du système des noms de domaine de l'Internet et constitue la dernière partie du nom de domaine. À titre d'exemple, dans le nom de domaine www.example.com, le domaine de premier niveau est .com. La responsabilité de la gestion des domaines de premier niveau est déléguée à des organisations spécifiques par la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN), qui gère l'Autorité chargée de la gestion de l'adressage sur Internet (IANA) et la zone racine du DNS.

- **Typosquattage :** se fonde sur des erreurs de frappe que commet l'internaute lorsqu'il saisit les adresses de sites Web dans le navigateur En commettant une faute de frappe ou d'orthographe dans le nom de domaine, l'internaute sera dirigé vers un autre site, le site pirate du cybersquatteur. L'internaute ayant atteint le site du typosquatteur, il aura l'impression de se trouver sur le vrai site Web par le biais de logos, de format et de contenu copiés ou similaires.[8]

- **VoIP** : l'acheminement des conversations vocales sur Internet. Il ne s'agit pas d'un appel téléphonique, effectué du téléphone de maison ou de bureau et passant par le réseau téléphonique public commuté.

- **Vishing — hameçonnage par voix sur IP :** la victime reçoit un appel habituellement via une fonctionnalité VoIP courante qui permet d'usurper un numéro d'appelant. L'appel en question demande à la victime de se rendre sur un site Web ou d'appeler un numéro de téléphone où l'attaque par piratage psychologique se poursuivra. Les schémas courants comprennent le « Support technique Microsoft », des problèmes d'impôts impayés, ou encore « vous serez arrêté si vous ne payez pas une amende ».

- **Injection Web :** type de code malveillant exploitant une faille de sécurité par lequel l'attaquant ajoute un code à la fenêtre de saisie d'un formulaire électronique interactif pour accéder aux ressources ou modifier les données. Les fenêtres de saisie sont généralement destinées à l'authentification de l'utilisateur, mais la plupart de ces formulaires interactifs n'ont aucun mécanisme en place pour bloquer la saisie d'autres éléments que les noms et les mots de passe. À moins que de telles précautions soient prises, un attaquant peut utiliser les fenêtres de saisie pour envoyer leur propre requête à la base de données, s'autorisant ainsi à télécharger la base de données entière ou à interagir d'autres manières illicites. [9]

RÉFÉRENCES

1. http://en.wikipedia.org/wiki/Border_Gateway_Protocol
2. http://www.techterms.com/definition/cache
3. http://en.wikipedia.org/wiki/Drive-by_download
4. http://en.wikipedia.org/wiki/GSM
5. http://www.expertglossary.com/security/definition/ingress-filtering
6. http://www.icann.org/en/about/welcome
7. http://en.wikipedia.org/wiki/Money_mule
8. http://en.wikipedia.org/wiki/Typosquatters
9. http://searchsoftwarequality.techtarget.com/definition/SQL-injection

ENDNOTES

[1]DCWG, http://www.dcwg.org/
[2] Conficker Working Group, http://www.confickerworkinggroup.org/
[3] WinFixer, Wikipédia, http://en.wikipedia.org/wiki/WinFixer
[4] Symantec, 2015 Internet Security Threat Report, Volume 20, http://www.symantec.com/security_response/publications/threatreport.jsp
[5] McAfee, McAfee Labs 2014 Threats Predictions, http://www.mcafee.com/ca/resources/reports/rp-threats-predictions-2014.pdf
[6] Centre de téléchargement Microsoft, http://www.microsoft.com/en-us/download/details.aspx?id=44937
[7] Secunia, http://secunia.com/vulnerability_scanning/personal/
[8] PCMag, « The Best Password Managers for 2015 », http://www.pcmag.com/article2/0,2817,2407168,00.asp; PCMag, « You Can't Remember Good Passwords, So You Need a Password Manager », http://securitywatch.pcmag.com/security-software/332153-you-can-t-remember-good-passwords-so-you-need-a-password-manager
[9] PCMag, "The Best Free Antivirus for 2015", http://www.pcmag.com/article2/0,2817,2388652,00.asp
[10] Groupe de travail de génie Internet (IETF), « Recommendations for the Remediation of Bots in ISP Networks », http://tools.ietf.org/html/rfc6561
[11] Aquilina, James, Eoghan Casey, and Cameron Malin, Malware Forensics: Investigating and Analyzing Malicious Code, Elsevier, Inc., 2008.
[12] Safe Code, http://www.safecode.org
[13] M[3]AAWG, « ABCs for ISPs », https://www.m3aawg.org/abcs-for-ISP-code
[14] Agence de sécurité nationale, Guides de configuration de la sécurité (Security Configuration Guides), http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml
[15] National Vulnerability Database, « National Checklist Program Repository », http://web.nvd.nist.gov/view/ncp/repository
[16] Verizon, 2014 Data Breach Investigations Report, http://www.verizonenterprise.com/DBIR/2014/
[17] *Ibid.*
[18] APWG, Rapport sur les tendances de l'hameçonnage (APWG Phishing Attack Trends Reports), https://apwg.org/resources/apwg-reports/
[19] APWG, Enquête mondiale sur l'hameçonnage 1H2014 : utilisation des noms de domaine et tendances pour l'année (APWG Global Phishing Survey 1H2014: Trends and Domain Name Use), http://docs.apwg.org/reports/APWG_Global_Phishing_Report_1H_2014.pdf
[20] RSA, "2014 Cybercrime Roundup", www.emc.com/collateral/fraud-report/h13929-rsa-fraud-report-jan-2015.pdf
[21] Le Centre d'études stratégiques et internationales, Rapport 2014 de McAfee sur le cout global de la cybercriminalité (2014 McAfee Report on the Global Cost of Cybercrime), http://csis.org/event/2014-mcafee-report-global-cost-cybercrime
[22] O'Connor, Fred, PCWorld, « Monetising Medical Data is Becoming the Next Revenue Stream for Hackers », 21 mars 2015
[23] IT Governance, « 123 Million Health Care Records Breached so far this Year », 26 mars 2015, http://www.itgovernanceusa.com/blog/123-million-health-care-records-breached-so-far-this-year/
[24] Sender Policy Framework, « Project Overview », http://www.openspf.org/
[25] DKIM.org, http://dkim.org/
[26] ICANN, http://www.icann.org/
[27] DMARC, http://dmarc.org
[28] Dans la plupart des pays occidentaux, les institutions financières rembourseront aux consommateurs les pertes dues à des fraudes qui ont été faites par l'intermédiaire de l'institution financière.
[29] McAfee, "McAfee Labs Report Highlights Success of Phishing Attacks with 80% of Business Users Unable to Detect Scams", 4 septembre, 2014, http://www.mcafee.com/us/about/news/2014/q3/20140904-01.aspx
[30] SANS, « Mettre en place un programme antihameçonnage efficace (*Building an Effective Phishing Program*) », http://www.securingthehuman.org/media/resources/presentations/STH-Presentation-PhishingYourEmployees.pdf
[31] Stop. Think. Connect., « Ressources », www.stopthinkconnect.org/resources/
[32] StaySafeOnline.org, « *National Cyber Security Awareness Month* (mois national de la sensibilisation à la cybersécurité) », https://www.staysafeonline.org/ncsam/
[33] APWG, « *How to Redirect a Phishing Site Web Page to the APWG.ORG Phishing Education Page* », http://phish-education.apwg.org/r/how_to.html
[34] Groupe de travail antihameçonnage (APWG), apwg.org
[35] Groupe de travail antiabus pour la messagerie, les programmes malveillants et les mobiles, m3aawg.org
[36] Online Trust Alliance, otalliance.org
[37] Merchant Risk Council, merchantriskcouncil.org
[38] Forum of Incident Response and Security Teams, first.org

[39] FBI, « *DNS Changer Malware* » 9 novembre 2011, http://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf
[40] RFC Editor, « Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing », mai 2000, http://www.rfc-editor.org/info/bcp38
[41] RFC Editor, « Ingress Filtering for Multihomed Networks », mars 2004, http://www.rfc-editor.org/info/bcp84 https://www.arin.net/policy/nrpm.html
[42] RFC Editor, « Ingress Filtering for Multihomed Networks », mars 2004, http://www.rfc-editor.org/info/bcp84 43 https://www.arin.net/policy/nrpm.html
[44] Counterpoint, « Market Monitor: Handset and Spartphone Markets Q4 2014 », le 29 janvier 2015, http://www.counterpointresearch.com/marketmonitor2014q4
[45] The Realtime Report, « Mobile Commerce: Online Retail Sales from Mobile Devices Double in Last Year », 3 mai 2012, http://therealtimereport.com/2012/05/03/mobile-commerce-online-retail-sales-from-mobile-devices-double-in-last-year/
[46] Corra, « Mobile Shopping Trends by Device », 3 février 2015, http://corra.com/mobile-ecommerce-trends-2015
[47] GSMA Intelligence, « Global Data », https://gsmaintelligence.com/
[48] Worldometers, "Current World Population", http://www.worldometers.info/world-population/
[49] IDC, Llamas, Ramon, Anthony Scarsella, William Stofega, « Worldwide Mobile Phone 2015-2019 Forecast and Analysis », avril 2015, http://www.idc.com/getdoc.jsp?containerId=prUS23455612 (abonnement requis)
[50] Symantec, « Internet Security Threat Report », avril 2015, volume 20, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA- internet-security-threat-report-volume-20-2015-social_v2.pdf
[51] *Ibid.*
[52] Adaptive Mobile, "Selfmite: Attack Using SMS Worm to Increase Pay-Per-Install Income", 25 juin, 2014, http://www.adaptivemobile.com/blog/selfmite-worm
[53] Australie, Bulgarie, Belgique, France, Allemagne, Ghana, Grèce, Irlande, Kenya, Pays-Bas, États-Unis, Afrique du Sud, Espagne, Suède, Suisse
[54] Lookout, « Rapport 2014 sur les menaces à la sécurité mobile, » https://www.lookout.com/img/resources/Consumer_Threat_Report_Final_French_1.14.pdf
[55] **-** Bibat, Aerol, "GGTracker Malware Hides as Android Market", Android Authority, 21 juin, 2011 http://www.androidauthority.com/ggtracker-malware-hides-as-android-market-17281/
[56] ICT, « Statistics », http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
ICT, « ICT Facts and Figures, The World in 2014 », http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf
[57] Comparez par example: 47 U.S.C. § 227(b)(1)(A)(iii) avec 47 U.S.C. § 227(b)(1)(B) and 47 U.S.C. § 227(b)(2)(B)
[58] FCC, "'One Ring' Phone Scam," available at http://www.fcc.gov/guides/one-ring-wireless-phone-scam**.**
[59] CAPTCHA est l'abréviation de « *Completely Automated Public Turing test to tell Computers and Humans Apart* », le test public de Turing complètement automatique ayant pour but de différencier les humains des ordinateurs.
[60] Voir à titre d'exemple, T-Lock Call Blocker — Version N2, http://hqtelecom.com/callblocker?gclid=CMmt_raT6cECFc1_MgodhnEAWg ; page du produit CPR Call Blocker, http://www.cprcallblocker.com/purchase.html ; Digitone Call Blocker Plus, http://www.digitone.com ; et Sentry Dual Mode Call Blocker, http://www.plugnblock.com/?gclid=CJmKkbaT6cECFSFgMgodJRIAGA ; Privacy Corp Caller ID Manager, http://www.privacycorps.com/products/.
[61] Weisbaum, Herb, « Want to get rid of those $#%@ robocalls? There's an app for that, » http://www.cnbc.com/id/101758815#.
[62] Alliance for Telecommunications Industry Solutions, « Next Generation Interconnection Interoperability Forum (NGIIF) Auto Dialers Reference Document, » https://www.atis.org/docstore/product.aspx?id=26137
[63] NANPA, Vertical Service Codes, Code Definitions, http://www.nanpa.com/number_resource_info/vsc_definitions.html
[64] Allocution préparée par la Commission fédérale de commerce et présentée au sous-comité sur la protection du consommateur, la sécurité des produits et l'assurance du Comité du Commerce, de la Science et de Transport du Sénat américain, « Stopping Fraudulent Robocall Scams: Can More Be Done? », Washington DC, 10 juillet 2013 (« audition au Sénat »), http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=c1eec086-3512-4182-ae63-d60e68f4a532&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=7&YearDisplay=2013
[65] *Truth in Caller ID Act*, 47 U.S.C. § 227(e) ; cf. 16 C.F.R. Part 310.4(a)(8).
[66] Commission fédérale de commerce, « Robocalls Gone Wrong », https://www.consumer.ftc.gov/media/video-0027-robocalls-gone-wrong
[67] The Economist, « The Cheap, Convenient Cloud, » le 18 avril 2015, http://www.economist.com/news/business/21648685-cloud-computing-prices-keep-falling-whole-it-business-will-change-cheap-convenient?fsrc=scn/tw/te/pe/ed/thecheapconvenientcloud

[68] M[3]AAWG, "M[3]AAWG Sender Best Common Practices, Version 3, mis-à-jour février 2015," https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf
[69] http://w3techs.com/technologies/history_overview/content_management/all/y
[70] https://wpvulndb.com/statistics
[71] http://w3techs.com/technologies/details/cm-wordpress/all/all
[72] http://www.emersonnetworkpower.com/documentation/en-us/brands/liebert/documents/white%20papers/2013_emerson_data_center_cost_downtime_sl-24680.pdf Page 13
[73] http://www.stateoftheinternet.com/resources-web-security-2014-q4-internet-security-report.html
[74] http://www.emersonnetworkpower.com/documentation/en-us/brands/liebert/documents/white%20papers/2013_emerson_data_center_cost_downtime_sl-24680.pdf Page 14
[75] Noroozian, A. et al., « Developing Security Reputation Metrics for Hosting Providers, http://www.tudelft.nl/fileadmin/Faculteit/TBM/Onderzoek/Publicaties/hosting-metrics.pdf
[76] Le patron de Twitter s'engage à enrayer les trolls et l'abus : http://www.theguardian.com/technology/2015/feb/26/twitter-costs-dealing-abuse-harassing-dick-costolo
[77] Le suicide de Rehtaeh Parsons : https://en.wikipedia.org/wiki/Suicide_of_Rehtaeh_Parsons
[78] Granby, Québec, Le Canada s'emploie à imposer des amendes aux personnes insultant la police en ligne : http://www.cbc.ca/news/canada/montreal/granby-moves-to-fine-people-insulting-police-on-social-media-1.3045816
[79] *« 4chan Bullies Fitness Guru Scooby Off YouTube With Doxxing and Threats »*: http://newmediarockstars.com/2013/07/4chan-bullies-fitness-guru-scooby-off-youtube-with-doxxing-and-threats-video/
[80] *« How I got caught up in a 'stranded traveller' phishing scam »*: http://www.theguardian.com/money/2013/nov/13/stranded-traveller-phishing-scam
[81] *« How One Stupid Tweet Blew Up Justine Sacco's Life: »* http://www.nytimes.com/2015/02/15/magazine/how-one-stupid-tweet-ruined-justine-saccos-life.html?_r=0
[82] *« The World Has No Room For Cowards: »* http://krebsonsecurity.com/2013/03/the-world-has-no-room-for-cowards/
[83]Stay Safe Online, https://www.staysafeonline.org/stay-safe-online/for-parents/cyberbullying-and-harassment
[84] Du CTF des États-Unis, https://www.consumer.ftc.gov/articles/0028-cyberbullying ;
Nigéria, http://www.mamalette.com/parenting-3/cyber-bullying-nigerian-parents-need-know/;
ACMA, http://www.cybersmart.gov.au/Schools/Cyber%20issues/Cyberbullying.aspx;
GRC, http://www.rcmp-grc.gc.ca/cycp-cpcj/bull-inti/index-eng.htm ;
Service Policière de l'Afrique du Sud, http://www.saps.gov.za/child_safety/teens/cyber_bullying.php;

Comité Directeur

Andre Leduc, Manager, National Anti-Spam Coordinating Body, Industry Canada

Alyson Hawkins, Policy Analyst, Industry Canada

Christina Adam, Policy Analyst, Industry Canada

Jerry Upton, Executive Director, Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)

Lisa Foley, Policy Analyst, Industry Canada

Neil Schwartzman, Executive Director, CAUCE.org

Contributeurs

Alex Bobotek, Lead, Mobile Messaging Anti-Abuse Strategy and Architecture, AT&T

Amy Hindman, Principal Engineer, Verizon

Betsy Broder, Counsel for International Consumer Protection, Federal Trade Commission

Bruce Matthews, Manager, Anti-spam Team, Australian Communications & Media Authority

Carlo Catajan, iCloud Mail & iMessage Anti-Abuse, Apple Inc.

Carlos Alvarez, Sr. Manager, Security Engagement, SSR Team, ICANN

Chris Boyer, Assistant Vice President, Global Public Policy, AT&T

Christian Dawson, President, ServInt and Chairman, i2Coalition

David Jevans, Chairman, Anti-Phishing Working Group (APWG)

Eric Freyssinet, Ministère de l'intérieur, France

Foy Shiver, Deputy Secretary-General, APWG

Francis Louis Tucci, Manager, Network Repair Bureau, Verizon Wireless

Frank Ackermann, M³AAWG Public Policy Committee Co-chair

Gary Warner, Director of Research in Computer Forensics, University of Alabama at Birmingham

Jay Opperman, General Manager, CSP, Damballa

Jayne Hitchcock, President, WOAH

Jeff Williams, Dell SecureWorks

Jessica Malekos Smith, Student, UC Davis School of Law

John Levine, President, CAUCE.org

Jonathan Curtis, Norse Corporation

Justin Lane, Anti-Abuse Manager, Endurance International

Karen Mulberry, ISOC

Lee Armet, Senior Investigator, TD Bank Group

Mary Retka, Director, Network Policy, CenturyLink

Matthew Bryant, Ofcom

Matthew C Stith, Manager, Anti-abuse, Rackspace Hosting

Michael Hammer, American Greetings

Michael O'Reirdan, Comcast Fellow

Patrick Tarpey, Ofcom

Paul Vixie, CEO, Farsight Security

Peter Merrigan, Government of New Zealand

Phil Shih, Structure Research

Richard Feller, Hedgehog Hosting

Rod Rasmussen, President and CTO, Internet Identity (IID)

Sanjay Mishra, Distinguished Member of Technical Staff, Verizon

Sara Roper, Manager Information Security, CenturyLink

Sid Harshavat, Symantec

Steven Champeon, Enemieslist

Terry Zink, Program Manager, Microsoft

TR Shaw, SURBL

Venkata Atluri, Associate Professor, Alabama A&M University

Participants

Adam Panagia, Adria Richards, Alexander Falatovich, April Lorenzen, Autumn Tyr-Salvia, Bill Wilson, Bulent Egilmez, Chris Lewis, Dave Crocker, David Dewey, David Levitt, Donald McCarthy, Donald Smith, Dylan Sachs, Eric Chien, Franck Martin, Hein Dries-Ziekenheiner, Jacek Materna, Jack Johnson, Jared Mauch, Jean Marie Norman, John Cunningham, Julia Cornwell McKean, Kaio Rafael, Karmyn Lyons, Ken Simpson, Lucas Moura, Mark Collier, Matteo Lucchetti, Michael Shoukrey, Mustaque Ahamad, Nabeel Koya, Nitin Lachhani, Olivier Caleff, Patricia B. Hsue, Paul Ebersman, Peter Cassidy, Raymond Choo, Richard Clayton, Richard Gane, Rudy Brioche, Sid Harshavat, Steve Jones, Steven M. Wernikoff, Suresh Ramasubramanian, Toni Demetriou, Trent Adams, Will Clurman