Siège social aux États-Unis
Cisco Systems, Inc.
San Jose, Californie

Siège social en Asie-Pacifique
Cisco Systems (USA) Pte. Ltd.
Singapour

Siège social en Europe
Cisco Systems International
BV Amsterdam,
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et numéros de fax de nos bureaux sont indiqués sur le site Web Cisco, à l'adresse suivante : **www.cisco.com/go/offices**.

Rapport annuel Cisco 2013 sur la sécurité

Vivre dans le monde de « connectivité universelle » d'aujourd'hui.

Les cybercriminels profitent de l'angle d'attaque qui s'élargit rapidement dans le monde de « connectivité universelle » d'aujourd'hui, où les utilisateurs se servent de tout type d'appareil pour accéder à des applications professionnelles dans un environnement réseau utilisant des services cloud décentralisés. Le *Rapport annuel 2013 de Cisco® sur la sécurité* met en évidence les principales tendances des menaces mondiales en se basant sur des données réelles. Il fournit par ailleurs un aperçu et une analyse qui permettent aux entreprises et aux gouvernements d'améliorer leurs futures politiques en matière de gestion de la sécurité. Ce rapport associe les recherches d'experts aux renseignements de sécurité collectés par Cisco, en s'attachant à la collecte de données réalisée pendant l'année civile 2012.

Table des matières

Le réseau d'interconnexions entre les appareils, les environnements cloud et les applications

La connectivité « universelle » et l'Internet of Everything représentent des évolutions dont on observe le développement rapide dans le domaine des communications et de la collaboration. Il s'agit du réseau d'interconnexions existant entre les appareils, les environnements cloud et les applications.

Cette évolution était prévisible, mais les entreprises d'aujourd'hui ne sont peut-être pas prêtes à relever le défi d'un monde de connectivité universelle. En tout cas pas du point de vue de la sécurité.

« Si connectivité universelle pose problème, c'est essentiellement parce que nous arrivons rapidement à un point où les utilisateurs exercent de moins en moins leurs activités professionnelles via un réseau d'entreprise », affirme Chris Young, Vice-président senior du groupe Sécurité et secteur public de Cisco. « De plus en plus souvent, on observe que des appareils de tout type se connectent en tout lieu à une partie quelconque du réseau. Avec les appareils disposant d'un accès à Internet (smartphones et tablettes, par exemple), ils peuvent se connecter à des applications susceptibles de s'exécuter n'importe où, que ce soit dans un cloud SaaS (Software as a Service) public, dans un cloud privé ou dans un cloud hybride. »

Parallèlement, une autre évolution a commencé : la formation progressive de ce qu'on appelle « l'Internet of Everything », qui se définit comme la connexion intelligente :

- **des personnes :** réseaux sociaux, centres de population, communautés numériques ;
- **des processus :** systèmes, processus d'entreprise ;
- **des données :** Web, informations ;
- **des choses :** monde physique, appareils et objets.

« De plus en plus souvent, on observe que des appareils de tout type se connectent en tout lieu à une partie quelconque du réseau. Les appareils connectés à Internet (smartphones, tablettes et autres) tentent de se connecter à des applications qui peuvent être exécutées sur toutes les plates-formes. »

Chris Young, Vice-président senior du groupe Sécurité et secteur public de Cisco

« Si les connexions réseau sont déjà utiles et profitables aujourd'hui, elles vont devenir indispensables avec la croissance et la convergence des personnes, des processus, des données et des objets sur Internet. »

Nancy Cam-Winget, Ingénieur experte, Cisco

Basé sur l'Internet des objets (« Internet of Things »[1]), l'Internet of Everything apporte au réseau un niveau d'intelligence supérieur, grâce auquel la convergence, l'orchestration et la visibilité deviennent possibles entre des systèmes jusque-là disparates. Dans l'Internet of Everything, ce ne sont plus seulement des périphériques mobiles, des ordinateurs portables et des postes de travail qui se connectent ; en plus de cela, le nombre de connexions machine à machine (M2M) effectuées quotidiennement augmente rapidement. Il s'agit souvent d'objets que nous utilisons au quotidien et qui nous semblent aller de soi, mais que nous n'avons pas l'habitude de considérer comme étant connectées à Internet : l'installation de chauffage d'une maison, une éolienne ou une voiture, par exemple.

L'Internet of Everything n'est pas pour tout de suite, bien sûr, mais nous n'en sommes pas loin, quand on voit les problèmes que pose la connectivité universelle. Et si celui-ci pose des difficultés aux entreprises en matière de sécurité, il ouvre également la porte à de nouvelles perspectives. « Des choses prodigieuses vont devenir possibles grâce à l'Internet of Everything », déclare Nancy Cam-Winget, Ingénieur experte, Cisco. « Si les connexions réseau sont déjà utiles et profitables aujourd'hui, elles vont devenir indispensables avec la croissance et la convergence des personnes, des processus, des données et des objets sur Internet. Une fois mature, l'Internet of Everything créera de nouvelles capacités, permettra des expériences plus riches et offrira des possibilités inégalées de développement économique, pour les gouvernements que pour les entreprises et les particuliers. »

Les défis créés par le cloud en matière de sécurité

Comme les entreprises choisissent de plus en plus de gérer leurs systèmes par le biais du cloud, il devient encore plus difficile qu'auparavant d'assurer la sécurité d'un grand nombre d'applications, de périphériques et d'utilisateurs (que ce soit dans le contexte de la connectivité universelle ou de l'Internet of Everything). Les données rassemblées par Cisco permettent de conjecturer que le trafic mondial des data centers devrait être multiplié par quatre au cours des cinq prochaines années. C'est en matière de données présentes sur le cloud que la croissance devrait être la plus rapide et, en 2016, le trafic mondial sur le cloud devrait représenter près des deux tiers du trafic total des data centers.

Il est prévu que le trafic mondial des data centers soit multiplié par quatre au cours des cinq prochaines années. C'est en matière de données cloud que la croissance devrait être la plus rapide et, en 2016, le trafic mondial sur le cloud devrait représenter près des deux tiers du trafic total des data centers.

Avec les solutions fragmentées, telles que l'application de pare-feu à des emplacements variables en périphérie du réseau, il est impossible de garantir la sécurité des données qui sont continuellement transférées entre les appareils, les réseaux et les environnements cloud. Même au sein des data centers, qui hébergent désormais les données les plus précieuses des entreprises (les données massives ou « big data »), la virtualisation devient davantage la règle que l'exception. Les défis posés par la virtualisation et le cloud computing en matière de sécurité exigent de repenser les positions en ce qui concerne la gestion de la sécurité afin de tenir compte de ce nouveau paradigme : pour sécuriser le nouveau modèle économique, il faut modifier les anciens modes d'accès et de confinement, ainsi que les mécanismes de contrôle de la périphérie des réseaux.

Hyperconnexion des employés et confidentialité des données

Autre facteur de complication dans l'univers de la connectivité universelle : les jeunes, dont la mobilité est considérable. Ils considèrent qu'il doit leur être possible de travailler partout, grâce aux divers appareils disponibles à l'endroit où ils se trouvent. Ce *Rapport annuel 2013 de Cisco sur la sécurité* présente des conclusions du rapport *Cisco Connected World Technology 2012*, basé sur des recherches réalisées en 2011 relativement aux changements d'attitude des étudiants et jeunes professionnels du monde entier quant au travail, aux technologies et à la sécurité.

Autre facteur de complication dans l'univers de la connectivité universelle : les jeunes, dont la mobilité est considérable. Ils considèrent qu'il doit leur être possible de travailler partout, grâce aux divers appareils disponibles à l'endroit où ils se trouvent.

Dans cette dernière étude, axée sur la confidentialité, nous avons cherché à découvrir dans quelle mesure et à quelle fréquence, selon ces jeunes professionnels, une entreprise peut empêcher un employé de naviguer sur Internet pendant ses heures de travail. Elle nous a beaucoup éclairés sur leur attitude envers la sécurité. Dans l'étude du rapport *Cisco Connected World Technology 2012*, nous avons également cherché à établir si tous les utilisateurs continuent de se préoccuper activement de la confidentialité en ligne.

Analyse des données et tendances mondiales en matière de sécurité

Le *Rapport annuel 2013 de Cisco sur la sécurité* comprend une analyse approfondie des tendances du trafic de courriers indésirables et de programmes malveillants sur le Web, basée sur les

« Aujourd'hui, les menaces qui pèsent sur les gouvernements, les entreprises et les communautés connaissent des changements troublants. »

John N. Stewart, Vice-président senior et directeur de la sécurité de Cisco

recherches réalisées par Cisco. Alors qu'en général, les acteurs de « l'économie souterraine » ont concentré leurs efforts dans le développement de techniques de plus en plus sophistiquées au cours des dernières années, les recherches de Cisco indiquent clairement que les cybercriminels se contentent souvent de méthodes de base bien connues pour tromper les utilisateurs.

L'augmentation des attaques de déni de service distribué (DDoS) au cours de l'année dernière n'est qu'un exemple de la tendance « on reprend l'ancien et on recommence » du cybercrime. Pendant des années, les attaques DDoS (qui peuvent paralyser les prestataires de services Internet et interrompre le trafic en direction et en provenance de sites Web ciblés) n'ont pas été considérée comme prioritaires en matière de sécurité IT au sein de nombreuses entreprises. Toutefois, de récentes vagues d'attaques menées contre de prestigieuses entreprises (notamment des institutions financières américaines[2]) nous ont rappelé que toute menace de cybersécurité peut entraîner une interruption conséquente, voire des dommages irréparables, si l'organisation ne s'y est pas correctement préparée. Lorsque les entreprises établissent leurs plans de gestion de la continuité des activités, elles doivent donc réfléchir à la manière de réagir et à la stratégie de reprise à mettre en œuvre en cas d'interruption inopinée du réseau, que ce soit à cause d'une attaque DDoS contre l'entreprise ou parce qu'une usine de fabrication connectée à Internet est tout à coup hors ligne, ou encore à cause d'une attaque multiétages sophistiquée mise en œuvre par des criminels ; ou encore autre chose, que nous n'avons jamais vue auparavant.

« Les discussions autour de la sécurité IT ont souvent été inutilement alarmistes au cours des années antérieures, mais aujourd'hui, les menaces qui pèsent sur les gouvernements, les entreprises et les communautés connaissent des changements troublants », assure John N. Stewart, Vice-président senior et directeur de la sécurité de Cisco. « On ne peut plus considérer le cybercrime comme un phénomène agaçant ou comme un coût supplémentaire lié aux activités de l'entreprise. Nous nous approchons désormais d'un seuil critique, où les pertes économiques générées par le cybercrime risquent de surpasser les revenus générés grâce aux technologies de l'information. Pour limiter les dommages que le cybercrime inflige dans le monde, nous avons donc besoin de nouvelles idées et de nouvelles approches. »

La prolifération des terminaux

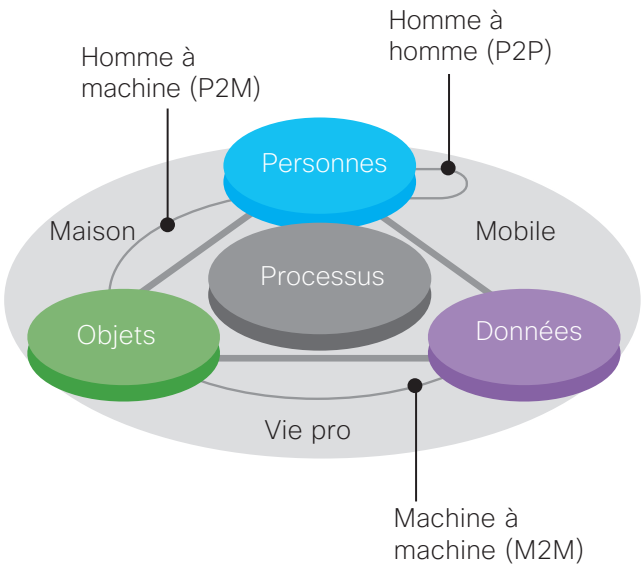
Comme nous évoluons vers un modèle de connectivité universelle, les appareils connectés à Internet sont de plus en plus nombreux : en 2012, ils sont devenus plus de 9 milliards.[3]

Aujourd'hui, moins de 1 % des objets du monde physique sont connectés. Il reste donc un vaste potentiel de « connexion du monde non connecté »[4]. Avec environ 50 milliards « d'objets » connectés à Internet aujourd'hui, le nombre de connexions devrait passer à 13 311 666 640 184 600 en 2020. Avec seulement un objet de plus connecté à Internet (50 milliards + 1), le nombre de connexions augmenterait alors de 50 milliards ![5]

Quant aux « objets » connectés à l'Internet of Everything, il peut s'agir aussi bien d'un smartphone que d'une installation de chauffage d'une maison, d'une éolienne ou d'une voiture. Dave Evans, Responsable des technologies futures au sein du groupe Internet Business Solutions, explique le concept de prolifération des terminaux de la manière suivante : « Bientôt, votre voiture sera connectée à l'Internet of Everything. Le nombre d'objets sur Internet augmentera alors de 1. Pensez maintenant aux nombreuses connexions que votre voiture pourrait établir : avec les autres voitures, les feux de circulation, votre domicile, le garagiste, les bulletins d'information météorologiques, les panneaux d'avertissement, voire la route elle-même. »[6]

> « Bientôt, votre voiture sera connectée à l'Internet of Everything. Le nombre d'objets sur Internet augmentera alors de 1. Pensez maintenant aux nombreux éléments auxquels votre voiture pourrait être connectée : les autres voitures, les feux de circulation, votre domicile, le personnel du service public, les bulletins d'informations météorologiques, les panneaux d'avertissement, voire la route elle-même. »
>
> David Evans, Responsable des technologies futuristes, Cisco

Figure 1 : Internet of Everything
L'Internet of Everything se définit comme la connexion intelligente des personnes, des processus, des données et des objets.



Dans l'Internet of Everything, ce qui compte le plus, ce sont les connexions. Pas leur nombre, mais leur type. C'est ça qui va être bénéfique pour les personnes, les processus, les données et les objets.

Dans l'Internet of Everything, ce qui compte le plus, ce sont les connexions. Pas leur nombre, mais leur type. C'est ça qui va être bénéfique pour les personnes, les processus, les données et les objets. Et finalement, le nombre de connexions supplantera le nombre d'objets.[7] L'explosion des nouvelles connexions qui commencent déjà à intégrer l'Internet of Everything est essentiellement dû au développement croissant d'appareils disposant d'une adresse IP, ainsi qu'à l'augmentation de la bande passante disponible dans le monde et à l'émergence d'IPv6. Les seuls risques de sécurité posés par l'Internet of Everything sont dus à la prolifération des terminaux disposant d'une connectivité universelle : si cette prolifération nous rapproche peu à peu d'un monde encore plus étroitement connecté, elle offre également de nouvelles opportunités d'incursion aux individus malveillants qui cherchent à tromper les utilisateurs ou à compromettre les réseaux ou les données. Les nouvelles connexions elles-mêmes représentent des risques, car elles permettent de transférer davantage de données, et ces données doivent être protégées en temps réel, y compris les données massives que les entreprises continueront de collecter, de stocker et d'analyser.

« Comme l'Internet of Everything est en train de prendre forme rapidement, les professionnels de la sécurité ont intérêt à commencer à réfléchir aux nouvelles stratégies à adopter, au lieu de se contenter d'assurer la sécurité des terminaux et de la périphérie du réseau, comme ils faisaient jusqu'à maintenant ».

Chris Young, Vice-président senior du groupe Sécurité et secteur public de Cisco

« Comme l'Internet of Everything est en train de prendre forme rapidement, les professionnels de la sécurité ont intérêt à commencer à réfléchir aux nouvelles stratégies à adopter, au lieu de se contenter d'assurer la sécurité des terminaux et de la périphérie du réseau, comme ils faisaient jusqu'à maintenant », explique Chris Young. « Il y aura trop d'appareils, trop de connexions et trop de types de contenus et d'applications. Et leur nombre ne fera que croître. Dans ce nouvel environnement, le réseau lui-même devient composant du paradigme de sécurité qui permet aux entreprises d'étendre leurs politiques et leurs stratégies de surveillance aux divers environnements. »

Le point sur le programme BYOD de Cisco

La prolifération des terminaux est un phénomène que Cisco connaît bien au sein de sa propre organisation qui emploie 70 000 personnes à travers le monde. Depuis l'officialisation des pratiques BYOD (Bring Your Own Device, utilisez votre propre appareil) voici deux ans, l'entreprise a observé une augmentation de 79 % du nombre d'appareils utilisés au sein de son organisation.

Le *Rapport annuel 2011 de Cisco sur la sécurité*[8] a d'abord analysé le développement du programme BYOD de Cisco, mis en œuvre dans le cadre de la transition actuelle de la société dans le but de devenir une « entreprise virtuelle ». Lorsque Cisco atteindra la dernière étape du programme BYOD, d'ici plusieurs années, la société sera de plus en plus indépendante des sites d'activités et des services, tout en préservant la sécurité de ses données.[9]

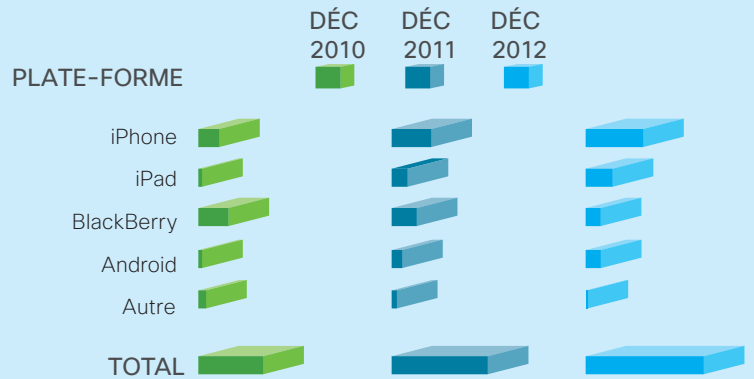
En 2012, Cisco a intégré la prise en charge d'environ 11 000 smartphones et tablettes à l'ensemble de l'entreprise, soit près de 1 000 nouveaux appareils connectés à Internet par mois. « À la fin de l'année 2012, l'entreprise comptait près de 60 000 smartphones et tablettes (dont un peu moins de 14 000 iPads) et tous étaient des appareils apportés par les employés », déclarait Brett Belding, directeur principal des services de mobilité chez Cisco. « La mobilité chez Cisco c'est maintenant le BYOD, point à la ligne. »

L'iPad d'Apple représente le type d'équipement ayant enregistré la plus forte augmentation en termes d'utilisation chez Cisco. « Quand on pense que ce produit n'existait même pas il y a trois ans, c'est fascinant ! », déclare Belding. « Désormais plus de 14 000 iPads sont utilisés chaque jour chez Cisco par nos employés pour réaliser diverses activités, aussi bien personnelles que professionnelles. Et ils utilisent les iPads en plus de leurs smartphones. »

Quant aux smartphones, le nombre d'iPhones d'Apple utilisés chez Cisco a presque triplé en deux ans pour atteindre presque 28 600. Les terminaux BlackBerry de RIM, Android de Google et Microsoft Windows sont également inclus dans le programme BYOD de Cisco. Les employés optent pour l'accès aux données de l'entreprise sur leur appareil personnel en échange de contrôles de sécurité. Par exemple, les utilisateurs qui souhaitent vérifier leur messagerie et leur agenda sur leur appareil doivent utiliser le profil de sécurité de Cisco qui recours à l'effacement des données à distance, le cryptage et la gestion de l'accès par mot de passe.

> « Aujourd'hui, nous prenons en charge plus d'appareils que jamais auparavant. Pourtant, nous n'avons jamais eu aussi peu de problèmes de prise en charge. À terme, nous espérons que l'employé pourra se connecter à l'aide de l'appareil de son choix, assurer lui-même sa mise en service en utilisant le moteur Cisco Identity Services Engine (ISE), et installer nos outils WebEx de collaboration, notamment Meeting Center, Jabber et WebEx Social. »
>
> Brett Belding, Responsable senior des services de mobilité IT chez Cisco

Figure 2 : Déploiement des appareils mobiles Cisco



Dès le départ, la prise en charge des médias sociaux a constitué un composant clé du programme BYOD chez Cisco. « Nous dépendons fortement de [la plate-forme de collaboration d'entreprise] WebEx Social en tant que plate-forme de prise en charge de notre stratégie BYOD, et cela a représenté pour nous un gain énorme », déclare Belding. « Le nombre d'appareils pris en charge n'a jamais été aussi élevé, et dans le même temps, le nombre de demandes d'assistance n'a jamais été aussi bas. Notre objectif est qu'un jour, un employé puisse simplement apporter l'appareil de son choix et assurer lui-même sa mise en service à l'aide de Cisco Identity Services Engine (ISE), puis configurer nos principaux outils de collaboration WebEx, notamment Meeting Center, Jabber et WebEx Social ».

La prochaine étape du BYOD chez Cisco, selon Belding, consiste à continuer à améliorer la sécurité en améliorant la visibilité et le contrôle de tous les appareils et de toutes les activités des utilisateurs, à la fois sur le réseau physique et sur l'infrastructure virtuelle, tout en améliorant l'expérience utilisateur. « Se soucier de l'expérience utilisateur est une approche essentielle dans l'informatisation des activités », déclare Belding. « Nous essayons d'appliquer ce concept à notre entreprise. Il le faut. Je pense que nous assistons aujourd'hui à une « informatisation » des utilisateurs. Nous n'en sommes plus au stade où ils nous demandaient : « Est-ce que je peux utiliser cet appareil pour travailler ? » Maintenant, le message, c'est : « Je comprends que vous devez préserver la sécurité de l'entreprise, mais n'interférez pas avec mon expérience utilisateur. »

Des services résidant dans divers clouds

Le trafic mondial des data centers augmente. Selon Cisco Global Cloud Index, le trafic mondial des data centers devrait se multiplier par quatre au cours des cinq prochaines années, avec un taux de croissance composé annuel de 31 % entre 2011 et 2016.[10]

Dans le cadre de cette prodigieuse évolution, le trafic de données cloud est celui qui connaît la croissance la plus rapide. Le trafic cloud mondial devrait se multiplier par six au cours des cinq prochaines années, avec un taux de croissance de 44 % entre 2011 et 2016. En fait, en 2016, le trafic cloud mondial constituera près des deux tiers du trafic total des data centers.[11]

Cette explosion du trafic cloud pose la question de la capacité des entreprises à gérer ces informations. Dans le cloud, les outils habituels de surveillance se brouillent : une organisation peut-elle placer des filets de sécurité autour de ses données cloud si le data center ne lui appartient pas et qu'elle ne le gère pas ? Comment appliquer les outils de sécurité (même les plus basiques, comme les pare-feu et les antivirus) lorsque la périphérie du réseau est indéfinissable ?

Malgré les nombreuses questions soulevées en matière de sécurité, de plus en plus d'entreprises adoptent le cloud. Et dans ce cas, il y a peu de chances qu'elles décident de revenir à un modèle de data center privé. Si le cloud offre de nombreuses opportunités aux

Le trafic cloud mondial devrait se multiplier par six au cours des cinq prochaines années, avec un taux de croissance de 44 % entre 2011 et 2016.

organisations (économies, amélioration de la collaboration entre les employés, productivité et réduction de l'empreinte carbone, par exemple), les entreprises qui choisissent de transférer leurs processus et données vers le cloud doivent également être prêtes à affronter les risques de sécurité suivants :

Hyperviseurs

Capable de créer et d'exécuter des machines virtuelles, ce type de logiciel peut conduire à des actions de piratage massives et à l'altération des données sur plusieurs serveurs, s'il est la cible d'une attaque. Les pirates disposent alors de la facilité de gestion et d'accès offerte par la virtualisation. Un hyperviseur pirate (attaqué par le biais d'une technique appelée « hyperjacking ») peut prendre le contrôle d'un serveur complet.[12]

Un hyperviseur pirate (contrôlé par le biais d'une technique appelée « hyperjacking ») peut prendre le contrôle d'un serveur complet.

Réduction des coûts d'entrée

La virtualisation a réduit les coûts d'entrée des prestations de services telles que les serveurs privés virtuels (VPS). Les anciens modèles de data center reposant sur des équipements matériels disparaissent, tandis qu'apparaissent de plus en plus d'infrastructures rapides, peu coûteuses et faciles d'accès pour les criminels. Par exemple, de nombreux services VPS proposés pour la vente immédiate (avec la possibilité de régler via Bitcoin ou tout système de paiement conçu pour limiter les possibilités de suivi) ont subi des attaques criminelles. Avec la virtualisation, les infrastructures sont désormais disponibles facilement, à un coût dérisoire. Avec peu ou pas de politique de régulation des activités.

« Dissociation » des applications virtualisées

Désormais, les applications virtualisées étant dissociées des ressources physiques qu'elles exploitent, il devient difficile d'aborder la sécurité selon une approche traditionnelle. Les prestataires de services IT s'efforcent de minimiser les coûts grâce à des offres très flexibles permettant de déplacer les ressources selon les besoins (ce qui est très différent des groupes de sécurité, où on cherchait à rassembler les services de sécurité prioritaire, pour les séparer des services qui pouvaient être moins sécurisés).

« La virtualisation et le cloud computing créent des problèmes tels que ceux qui sont générés par l'utilisation des appareils personnels dans un cadre professionnel (BYOD), mais tout le monde en est fou », assure Joe Epstein, ancien Président-directeur général de Virtuata, entreprise acquise par Cisco en 2012, qui propose des solutions innovantes de sécurisation des informations au niveau des machines virtuelles pour les environnements en cloud et les data centers. « Désormais, des applications et données de grande valeur se déplacent à travers tout le data center. Et les entreprises sont mal à l'aise avec la notion de charges de travail virtuelles. Dans un environnement virtuel, comment être certain que ce vous exécutez est fiable ? Pour l'instant, cela est impossible et cette incertitude est un frein essentiel à l'adoption du cloud. »

Mais M. Epstein signale qu'il devient de plus en plus difficile pour les entreprises d'ignorer la virtualisation et les environnements cloud. « Bientôt, le monde va tout partager », explique-t-il. « Tout va se virtualiser et être partagé. Il deviendra absurde d'exécuter uniquement des data centers privés. L'univers IT de demain s'appuiera sur les clouds hybrides. »

« La virtualisation et le cloud computing créent des problèmes similaires à ceux liés à l'utilisation des appareils personnels dans un cadre professionnel (BYOD), mais tous les utilisateurs réclament avec force le recours à ces technologies… Désormais, des applications et des données de grande valeur se déplacent à travers l'ensemble du data center. »

Joe Epstein, ancien Président-directeur général de Virtuata

Pour répondre aux difficultés grandissantes posées par les clouds et la virtualisation, il faut mettre en place une stratégie de gestion de la sécurité adaptative et réactive. Selon M. Epstein, la stratégie de sécurité doit être un élément programmable, intégré de façon transparente au fabric sous-jacent du data center. En outre, il ne faut pas rajouter celle-ci une fois la mise en œuvre terminée, mais au contraire l'intégrer dès la phase de conception.

La convergence entre utilisation personnelle et professionnelle

La génération Y dans l'entreprise

Les professionnels d'aujourd'hui (surtout les jeunes de la « génération Y ») exigent d'être libres d'accéder au Web non seulement au moment où ils le souhaitent et selon leur propre méthode de travail, mais aussi à l'aide de l'appareil de leur choix. Toutefois, ils ne veulent pas que leur employeur entrave cette liberté, situation qui peut créer des tensions pour les professionnels en charge de la sécurité.

Les deux tiers des personnes interrogées pour l'étude du rapport *Cisco Connected World Technology 2012* considèrent que les employeurs ne doivent pas contrôler les activités en ligne des employés sur les appareils fournis par l'entreprise. En résumé, ils pensent que les employeurs n'ont pas à s'occuper de cela. Seulement un tiers (34 %) des professionnels interrogés ont déclaré que ça ne les dérangeait pas que leur employeur surveille leurs activités en ligne.

Seulement une personne interrogée sur cinq a déclaré que son employeur contrôlait ses activités en ligne lors de l'utilisation des appareils de l'entreprise, tandis que 46 % ont indiqué que leur employeur n'exerçait aucun contrôle. Les conclusions de la dernière étude *Connected World* montrent également que la génération Y considère le contrôle des activités en ligne des employés comme une attitude particulièrement choquante (même quand il s'agit de professionnels qui travaillent dans des entreprises qui n'effectuent pas de tels contrôles).

Seulement une personne interrogée sur cinq a déclaré que son employeur contrôlait ses activités en ligne lors de l'utilisation des appareils de l'entreprise, tandis que 46 % ont indiqué que leur employeur n'exerçait aucun contrôle.

Outre les difficultés auxquelles les professionnels de la sécurité se voient confrontés, il semble exister une différence de point de vue entre ce que les employés croient être autorisés à faire avec les appareils fournis par leur entreprise et les politiques imposées par les services IT en matière d'usage personnel. Quatre personnes interrogées sur dix ont déclaré qu'elles ne sont censées utiliser les appareils fournis par l'entreprise que pour leurs activités professionnelles, tandis qu'un quart d'entre elles ont déclaré qu'elles étaient autorisées à employer les appareils de l'entreprise pour leurs activités extra-professionnelles. Toutefois, 90 % des professionnels IT interrogés ont déclaré qu'ils appliquent en effet des politiques qui interdisent d'utiliser les appareils fournis par l'entreprise pour les activités personnelles en ligne. 38 % reconnaissent cependant que les employés ne respectent pas ces politiques et utilisent les appareils de l'entreprise pour leurs activités personnelles. (Pour plus d'informations sur la façon dont Cisco aborde les défis liés au phénomène BYOD, consultez la page 16.)

Il semble exister une différence de point de vue entre ce que les employés croient être autorisés à faire avec les appareils fournis par leur entreprise et les politiques imposées par les services IT en matière d'usage personnel.

Confidentialité et génération Y

Selon le rapport *Cisco Connected World Technology 2012*, la génération Y semble avoir accepté le fait que la confidentialité des données personnelles est devenue une notion obsolète grâce à Internet. 91 % des jeunes consommateurs interrogés ont déclaré qu'ils pensaient que l'ère de la confidentialité était terminée et qu'ils ne pouvaient pas contrôler la confidentialité de leurs informations. Toutefois, un tiers des personnes interrogées ont indiqué qu'elles ne se préoccupaient pas des données personnelles les concernant qui sont enregistrées et stockées.

Par ailleurs, la génération Y est généralement convaincue que son identité en ligne est différente de son identité hors ligne. 45 % de ces personnes ont déclaré que leur identité est souvent différente selon leur activité, tandis que 36 % pensent qu'ils utilisent des identités complètement différentes. Seulement 8 % pensent que ces identités sont identiques.

En outre, les jeunes consommateurs sont convaincus que les sites Web respectent la confidentialité de leurs données privées. Souvent, ils préfèrent partager leurs données sur de grands sites de communautés ou des médias sociaux, où l'apparent anonymat ressenti au sein d'une multitude d'utilisateurs les met plus à l'aise. 46 % d'entre eux pensent que certains sites Web respectent la confidentialité de leurs informations, tandis que 17 % sont convaincus que la plupart des sites Web la respectent. Cependant, 29 % d'entre eux déclarent qu'ils n'ont pas confiance dans la capacité des sites Web à respecter la confidentialité de leurs données et s'inquiètent de la sécurité et du vol d'identité. Comparez cela à l'idée de partager vos données avec une société qui sait qui vous êtes et ce que vous faites.

« La génération Y arrive à présent sur le marché du travail avec de nouvelles pratiques et une attitude différente envers la gestion des informations et la sécurité y étant associée. Ces nouveaux acteurs du marché sont convaincus que la confidentialité est désormais obsolète, qu'elle va disparaître et que les entreprises doivent à présent fonctionner dans le cadre de ce paradigme. Pour les générations précédentes, le concept va être dur à avaler », explique Adam Philpott, Directeur, Vente de produits de sécurité EMEAR, Cisco. « Toutefois, il reste aux entreprises la possibilité d'offrir à leurs employés des formations sur la sécurité des informations, afin de leur expliquer les risques existants et de leur donner des conseils relatifs au partage de leurs informations et à l'exploitation des outils en ligne dans le cadre de la sécurité des données. »

« La génération Y arrive à présent sur le marché du travail avec de nouvelles pratiques et une attitude différente envers la gestion des informations et la sécurité y étant associée. Ces nouveaux acteurs du marché sont convaincus que la confidentialité est désormais obsolète, qu'elle va disparaître et que les entreprises doivent à présent fonctionner dans le cadre de ce paradigme. Pour les générations précédentes, le concept va être dur à avaler. »

Adam Philpott, Directeur, Ventes de produits de sécurité EMEAR, Cisco

Pourquoi les entreprises ont-elles besoin de sensibiliser le public à la désinformation des médias sociaux

Jean Gordon Kocienda
Analyste des menaces au niveau mondial, Cisco

Pour beaucoup d'entreprises, les médias sociaux ont constitué une aubaine : la possibilité d'être connectées directement avec les clients ou avec tout autre public via Twitter et Facebook a aidé de nombreuses organisations à améliorer la visibilité de leurs marques grâce aux interactions sociales en ligne.

Cette communication directe et rapide a toutefois un inconvénient : sur les médias sociaux, des informations incorrectes ou trompeuses peuvent se propager à une vitesse incroyable. Il n'est pas difficile d'imaginer un scénario dans lequel un terroriste coordonnerait des attaques à l'aide de tweets trompeurs, dans l'intention d'engorger des routes ou des lignes de téléphone, ou encore pour pousser des personnes à agir d'une façon qui pourrait s'avérer dangereuse. Ainsi, l'été dernier, le gouvernement de l'Inde a bloqué des centaines de sites Web et jugulé des textes[13], dans le but de restaurer le calme dans le nord-est du pays, après la publication de photos et de messages texte. À la suite de rumeurs, des milliers de travailleurs paniqués se sont ruées sur les trains et les bus.

Sur les médias sociaux, des campagnes de désinformation similaires ont également affecté les prix du marché. Un tweet Reuters détourné a ainsi signalé que l'Armée syrienne libre était tombée à Alep. Quelques jours plus tard, un fil Twitter a été piraté et un prétendu haut diplomate russe a déclaré que le Président syrien Bashar Al-Assad était mort. Avant que ces déclarations ne puissent être démenties, les prix du pétrole sont montés en flèche sur les marchés internationaux.[14]

Les professionnels de la sécurité doivent être attentifs aux médias sociaux et repérer ces publications rapides et préjudiciables, surtout quand elles ciblent l'entreprise. Ils doivent agir vite afin de protéger leurs réseaux des programmes malveillants, signaler toute tentative trompeuse d'hameçonnage aux employés, réacheminer les données et fournir des conseils aux employés en matière de sécurité. Les responsables de la sécurité ne veulent surtout pas signaler aux dirigeants des événements qui se révéleraient être des canulars.

Pour éviter de tomber dans le panneau, la meilleure chose à faire est de vérifier que l'évènement est confirmé par diverses sources. À une certaine époque, les journalistes s'occupaient de cela, donc lorsque nous lisions ou écoutions les actualités, tout avait déjà été vérifié. Aujourd'hui, c'est différent : pour trouver des informations, beaucoup de journalistes s'appuient sur les mêmes tweets que ceux que nous pouvons lire. Si plusieurs personnes tombent dans le panneau, elles risquent de croire que l'événement se confirme, alors qu'il s'agit d'un tweet que l'on a fait suivre (retweet).

Dans le cas d'événements nécessitant une action rapide, le mieux est peut-être d'utiliser votre flair : si l'événement semble exagéré, réfléchissez-y à deux fois avant de le publier ou de le citer.[15]

Dans le cas des événements nécessitant une action rapide, le mieux est peut-être d'utiliser votre flair : si l'événement semble exagéré, réfléchissez-y à deux fois avant de le publier ou de le citer.

Les données massives

Un enjeu majeur pour les entreprises d'aujourd'hui

Dans les milieux professionnels, il n'est question que de données massives (« Big Data ») et de l'énorme potentiel représenté par l'analyse des énormes volumes de données générées, collectées et stockées par les entreprises.

Dans le rapport *Cisco Connected World Technology 2012*, nous avons étudié l'impact de la tendance de l'analyse des données massives sur les entreprises, notamment au sein des équipes IT. Selon les conclusions de l'étude, dans environ 74 % des entreprises de la planète, les données sont collectées et stockées, et les dirigeants appuient leurs décisions stratégiques sur l'analyse des données massives. En outre, 70 % des professionnels IT interrogés ont déclaré que les données massives vont constituer une priorité stratégique pour leur entreprise et les équipes IT au cours de la prochaine année.

Avec les diverses tendances qui évoluent et voient le jour dans le domaine des réseaux (mobilité, cloud, virtualisation, prolifération des terminaux, etc.), les volumes de données massives devraient devenir de plus en plus importants et offrir des capacités d'analyse de plus en plus grandes pour les entreprises. Mais les données massives suscitent certaines craintes quant à la sécurité. D'après les conclusions de l'étude *Connected World* 2012, un tiers des personnes interrogées (32 %) pensent que les données massives compliquent la gestion des contraintes de sécurité et la protection des données et du réseau, car les données sont trop nombreuses, de même que les moyens d'y accéder . En résumé, les données massives augmentent encore le nombre de vecteurs et d'angles d'attaque que les équipes de sécurité (et les solutions de sécurité) des entreprises doivent gérer.

Dans environ 74 % des entreprises de la planète, les données sont collectées et stockées, et les dirigeants appuient leurs décisions stratégiques sur l'analyse des données massives.

La Corée, l'Allemagne, les États-Unis et le Mexique ont les plus forts pourcentages de responsables informatiques estimant que l'exploitation des données massives pose des problèmes de sécurité.

Les professionnels IT interrogés convaincus que les données massives compliquent la gestion de la sécurité ont été les plus nombreux en Corée (45 %), en Allemagne (42 %), aux États-Unis (40 %) et au Mexique (40 %). Pour garantir la sécurité, plus des deux tiers (68 %) des professionnels IT interrogés pensent que l'ensemble de l'équipe IT devrait être impliqué dans la stratégie et les efforts visant à donner une place prépondérante à l'analyse des données massives au sein de l'entreprise. Gavin Reid, Directeur des recherches sur les menaces pour Cisco SIO (Security Intelligence Operations), l'affirme : « Les données massives ne compliquent pas la sécurité : elles la rendent possible ». Chez Cisco, nous recueillons et stockons 2,6 trillions d'enregistrements chaque jour. C'est ainsi que nous constituons la plate-forme qui nous permet de détecter et de contrôler les incidents. »

Des obstacles demeurent cependant en ce qui concerne l'adoption des solutions conçues pour aider les entreprises à mieux gérer et à valoriser l'exploitation de leurs données massives. Les personnes interrogées mettent en avant un budget insuffisant, le manque de temps à consacrer à l'analyse des données massives, des solutions inadaptées, un personnel IT insuffisant et l'absence du niveau requis d'expertise IT. Le fait que presque une personne interrogée sur quatre (23 %) ait évoqué le manque d'expertise et de personnel comme obstacle à l'exploitation efficace des données massives par leur entreprise montre la nécessité de voir arriver sur le marché davantage de professionnels devant être formés dans ce domaine.

Le cloud est également un facteur qui peut contribuer efficacement à l'exploitation des données massives selon 50 % des professionnels IT interrogés dans le cadre de l'étude *Connected World* de 2012. Ces derniers pensent que leurs entreprises doivent envisager la mise en œuvre et le déploiement de solutions cloud pour que l'exploitation des données massives représente une démarche intéressante. Ce sentiment

Des obstacles demeurent cependant en ce qui concerne l'adoption des solutions conçues pour aider les entreprises à mieux gérer et à valoriser l'exploitation de leurs données massives. Les personnes interrogées mettent en avant un budget insuffisant, le manque de temps à consacrer à l'analyse des données volumineuses, des solutions inadaptées, un personnel IT insuffisant et l'absence du niveau requis d'expertise IT.

domine en Chine (78 %) et en Inde (76 %), où plus de trois personnes interrogées sur quatre pensent que le cloud est une condition incontournable pour tout projet d'exploitation efficace des données massives. Par conséquent, dans certains cas, l'étude indique que l'intérêt pour la mise en œuvre de projets d'exploitation de données massives dépend de l'adoption du cloud.

Plus de la moitié des responsables informatiques interrogés ont également confirmé que les discussions à ce sujet au sein de leurs entreprises n'ont pas encore porté leurs fruits. Cela n'est pas surprenant étant donné que les acteurs du marché se demandent comment ils vont exploiter leurs données massives, les analyser et les utiliser de façon stratégique. Dans certains pays, cependant, les discussions concernant les données massives se traduisent par des décisions pertinentes sur les stratégies, la direction et les solutions à adopter. À cet égard, la Chine (82 %), le Mexique (67 %), l'Inde (63 %) et l'Argentine (57 %) font figure de leader. Plus de la moitié des personnes interrogées pour ces pays indiquent que les discussions à ce sujet dans leurs entreprises ont déjà bien progressé, qu'elles ont donné des résultats et qu'elles se sont traduites par des actions concrètes.

Trois responsables informatiques interrogés sur cinq dans le cadre de l'étude *Connected World de 2012* estiment que l'exploitation des données massives peut aider les pays et leurs économies à être plus compétitifs sur le marché mondial.

Dans certains pays les discussions portant sur l'exploitation des données massives se traduisent par des décisions pertinentes sur les stratégies, la direction et les solutions à adopter. À cet égard, la Chine, le Mexique, l'Inde et l'Argentine font figure de leaders. Plus de la moitié des personnes interrogées pour ces pays indiquent que les discussions à ce sujet dans leurs entreprises ont déjà bien progressé, qu'elles ont donné des résultats et qu'elles se sont traduites par des actions concrètes.

État des lieux concernant les attaques exploitant une faille de sécurité

Le danger guette là où l'on ne s'y attend pas

De nombreux professionnels de sécurité, et certainement un grand nombre d'utilisateurs en ligne, ont des idées préconçues sur les endroits où l'on risque le plus d'être la victime d'un programme malveillant sur le Web.

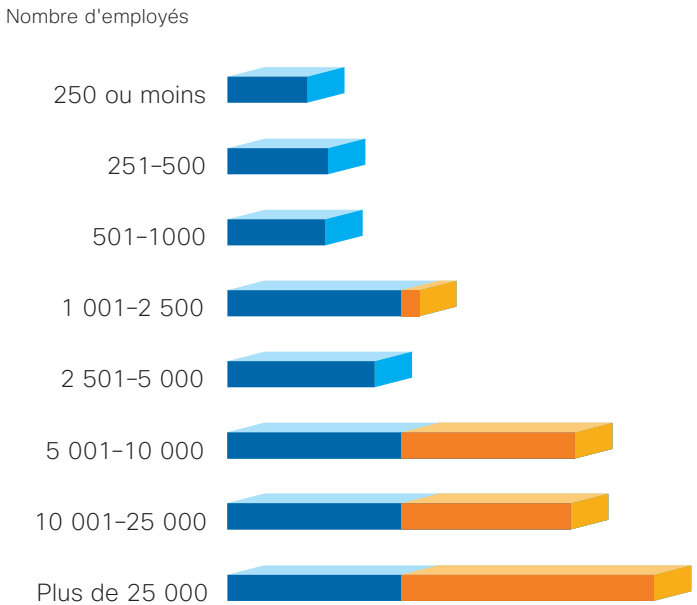
La croyance générale est que les sites qui favorisent les activités délictueuses, notamment les sites vendant des produits pharmaceutiques illégaux ou des contrefaçons de produits de luxe, risquent le plus d'héberger des programmes malveillants. Nos données révèlent une toute autre réalité. Ce ne sont pas sur les sites à caractère délictueux que les attaques de programmes malveillants sont les plus fréquentes.

« Les attaques de programmes malveillants se produisent sur tous les sites que l'on visite sur Internet, y compris ceux que l'on visite souvent même dans le cadre d'activités commerciales » , souligne Mary Landesman, spécialiste de la sécurité chez Cisco. « En fait, les sites commerciaux et industriels font partie de l'une des trois principales catégories de sites sur lesquels une attaque d'un programme malveillant risque le plus de se produire. Bien sûr, ces sites n'ont pas vocation à contenir une menace. » Les dangers sont souvent bien visibles. On les trouve par exemple dans des publicités en ligne qui sont distribuées sur des sites Web légaux. Ou ils sont le fait de hackers ciblant les utilisateurs selon les sites qu'ils visitent le plus.

De plus, les sites Web infectés par un programme malveillant sont répandus dans de nombreux pays et de nombreuses régions, pas seulement dans un ou deux pays, contrairement à l'idée selon laquelle les sites Web de certains pays risquent plus de contenir du contenu malveillant que d'autres. « Le Web est le mécanisme de prolifération le plus efficace à ce jour, bien plus que les vers et virus qui parviennent à atteindre et infecter un public de masse silencieusement et efficacement », estime

Le danger se trouve souvent exposé à la vue de tous dans des publicités en ligne piégées.

Figure 3 : Risque encouru selon la taille des entreprises
Les grandes entreprises encourent 2,5 fois plus de risques d'être exposé à des programmes malveillants sur le Web.



Toutes les sociétés, quelle que soit leur taille, sont exposées à des risques importants d'attaques par des programmes malveillants sur le Web. Chaque entreprise devrait se concentrer principalement sur la protection de son réseau et de sa propriété intellectuelle.

Landesman. « Les entreprises ont besoin d'une protection, même si elles bloquent les sites 'potentiellement à risque' avec des mesures supplémentaires d'inspection et d'analyse en profondeur. »

Attaques de programmes malveillants par taille d'entreprise

Les grandes entreprises (25 000+ employés) risquent 2,5 fois de plus que les petites entreprises d'être les victimes d'attaques de programmes malveillants. L'ampleur de ce risque peut s'expliquer par le fait que les plus grandes entreprises possèdent une propriété intellectuelle de plus grande valeur, et c'est pour cela qu'elles sont plus souvent la cible d'attaques.

Bien que les plus petites entreprises enregistrent moins d'attaques sur le Web par utilisateur, il n'en demeure pas moins que toutes les entreprises, quelle que soit leur taille, sont confrontées à ce risque qui est important. Chaque organisation devrait se concentrer principalement sur la protection de son réseau et de sa propriété intellectuelle.

Attaques de programmes malveillants par pays

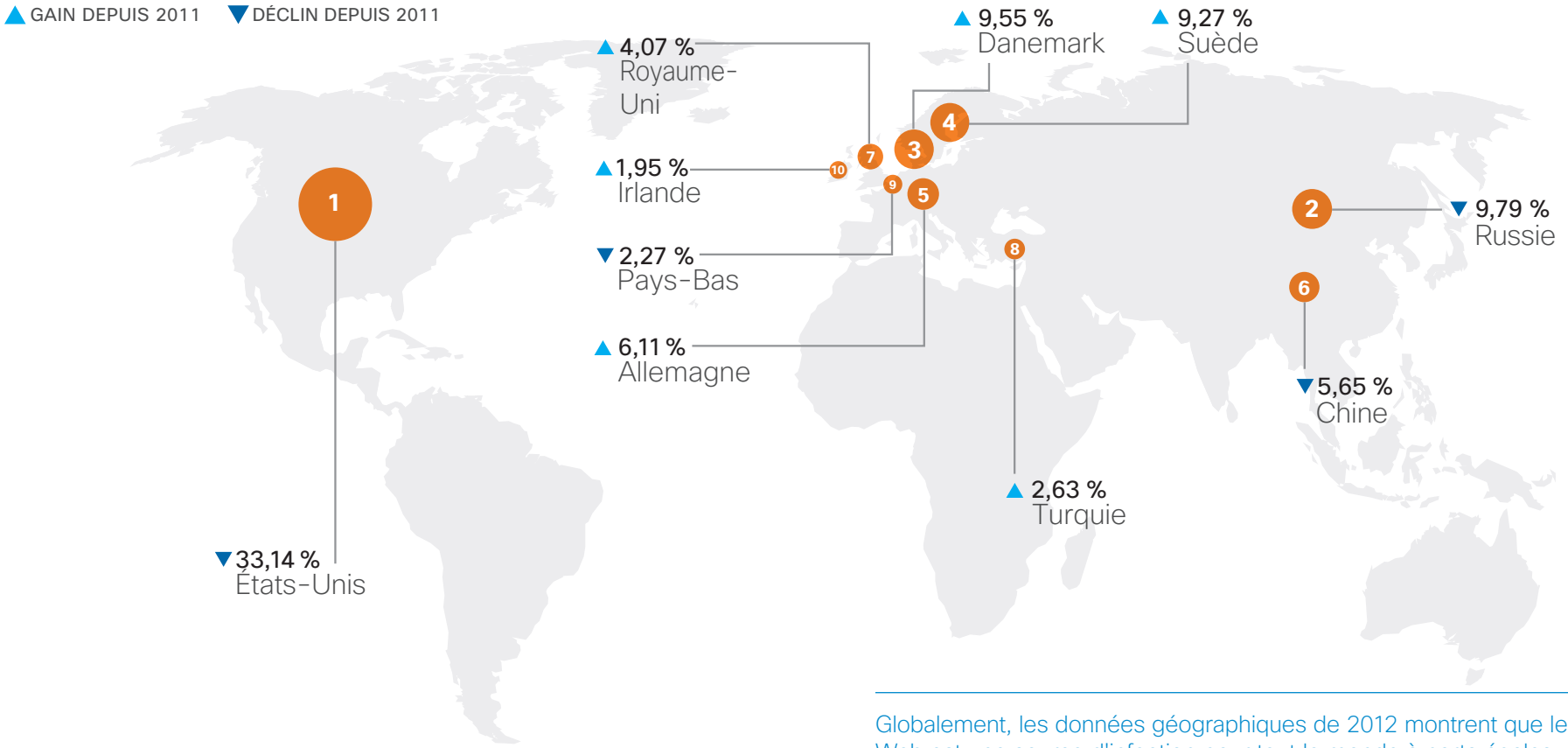
La recherche de Cisco montre un changement important dans les tendances mondiales d'attaques de programmes malveillants par pays en 2012. La Chine, qui était deuxième dans la liste des victimes en 2011 est descendue à la sixième place en 2012. Le Danemark et la Suède sont désormais troisième et quatrième respectivement. Les États-Unis sont toujours premiers en 2012, comme en 2011, avec 33 % de toutes les attaques par des programmes malveillants se produisant sur des sites Web hébergés aux États-Unis.

Les changements d'ordre géographique entre 2011 et 2012 reflètent les changements de détection des menaces et les habitudes des utilisateurs. Par exemple, le « malvertising », soit une technique visant à diriger les utilisateurs vers des publicités en ligne contenant un programme malveillant, a joué un rôle plus important dans les attaques sur le Web en 2012 qu'en 2011. A cet égard, il faut de nouveau souligner que les attaques de programmes malveillants se produisent le plus fréquemment sur des sites légaux et grand public qui ont été infectés ou qui contiennent à leur insu des publicités piégées. La publicité malveillante peut concerner n'importe quel site Web, quelle que soit son origine.

Globalement, les données géographiques de 2012 montrent que le Web est une source d'infection pour tout le monde à parts égales, contrairement à l'idée reçue selon laquelle seuls un ou deux pays seraient responsables de l'hébergement de sites Web à risques ou que certains pays seraient plus sûrs que d'autres. Enfin, la diffusion dynamique de contenu du Web 2.0 qui permet la monétisation de sites Web partout dans le monde, peut également contribuer à la propagation de programmes malveillants.

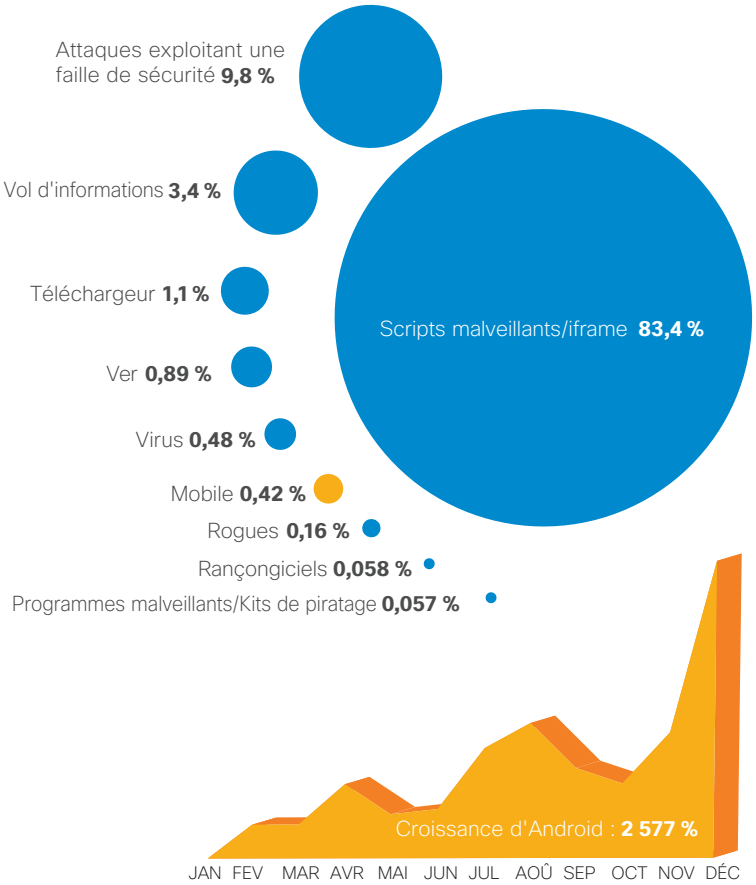
Figure 4 : Programmes malveillants provenant du Web par pays

Un tiers de l'ensemble des programmes malveillants du Web est issu de domaines hébergés aux États-Unis.



Globalement, les données géographiques de 2012 montrent que le Web est une source d'infection pour tout le monde à parts égales, contrairement à l'idée reçue selon laquelle seuls un ou deux pays seraient responsables de l'hébergement de sites Web à risques ou que certains pays seraient plus sûrs que d'autres.

Figure 5 : Principaux types de programmes malveillants du Web
Le nombre de programmes malveillants du Web sur Android a augmenté de 2 577 % en 2012. Pourtant, les programmes malveillants destinés aux appareils mobiles ne représentent qu'un faible pourcentage de l'ensemble des programmes malveillants rencontrés sur le Web.



Bien sûr, il y a une différence distincte entre l'endroit où une attaque peut se produire et où l'auteur de l'attaque est hébergé. Dans le « malvertising », par exemple, les attaques se produisent en général sur des sites Web légaux et réputés qui contiennent des publicités de sites tiers. Cependant, le programme malveillant peut, quant à lui, être hébergé sur un domaine complètement différent. Les données de Cisco étant principalement basées sur les endroits où les attaques ont lieu, elles ne donnent aucune indication sur l'origine des programmes malveillants qui en sont les auteurs. Par exemple, la popularité croissance des médias sociaux et des sites de divertissement au Danemark et en Suède, et les risques inhérents d'infection par des publicités malveillantes, sont largement responsables de l'augmentation des attaques sur des sites hébergés dans ces pays, mais cela ne fournit aucune indication sur l'origine des programmes malveillants qui en sont la cause.

Principaux types de programmes malveillants sur le Web en 2012

Les programmes malveillants sur Android se sont répandus beaucoup plus rapidement que les autres types de programmes malveillants sur le Web. Une tendance importante, étant donné, qu'Android est désormais majoritaire sur le marché mondial des appareils mobiles. À cet égard, il faut souligner que même si les attaques sur appareils mobiles représentaient seulement 0,5 % de toutes les attaques sur le Web en 2012, 95 % de ces attaques se sont produites avec des appareils dotés d'Android. En outre, 2012 a vu l'émergence du premier botnet Android détecté, indiquant que la prolifération de programmes malveillants sur les appareils mobiles en 2013 doit être surveillée.

Bien que certains experts affirment que les attaques sur Android représentent « la plus grande menace » et que les équipes de sécurité des entreprises doivent y porter toute leur attention en 2013, les données réelles montrent le contraire. Comme nous l'avons évoqué précédemment, les attaques de programmes malveillants Web sur appareils mobiles représentent moins d'1 % du total des attaques, rien à voir avec le scénario catastrophe que certains mettent en avant. L'impact de la prolifération des appareils personnels utilisés dans les entreprises ne doit pas être surestimé, mais les entreprises doivent principalement concentrer leur attention sur des menaces telles que les pertes accidentelles de données, en veillant à ce que les employés installent uniquement des applications provenant de circuits de distribution officiels et approuvés. Si les utilisateurs choisissent des applications provenant d'autres sources, ils doivent s'assurer avant de les télécharger qu'ils en connaissent l'auteur et que celui-ci est fiable mais aussi que leur code n'a pas été altéré.

Si l'on examine l'ensemble des attaques de programmes malveillants, il n'est pas surprenant de constater que les scripts et les iFrames malveillants représentaient 83 % des attaques en 2012. Un chiffre relativement similaire à celui des années

précédentes, mais cela mérite de s'intéresser à cette tendance. Ces types d'attaques sont souvent liées à l'action d'un code malveillant inséré sur des pages Web « de confiance », que les utilisateurs visitent quotidiennement et qui permet aux pirates de tromper leur vigilance sans qu'ils s'en rendent compte.

Les attaques exploitant une faille de sécurité arrivent ensuite au second rang, représentant 10 % du nombre total des attaques de programmes malveillants provenant du Web au cours de l'année dernière. Cependant, ces chiffres résultent principalement de l'endroit où les attaques en bloc ont lieu et non de la concentration réelle des attaques exploitant une faille de sécurité sur le Web. Par exemple, les 83 % d'attaques par scripts et iFrames masqués malveillants sont des attaques en bloc qui s'exécutent bien avant qu'une attaque exploitant une faille de sécurité n'ait lieu. Par conséquent, ce chiffre peut réduire artificiellement le nombre d'attaques exploitant une faille de sécurité observées.

Les attaques exploitant une faille de sécurité demeurent une cause importante d'infection sur le Web, et leur présence continue souligne la nécessité pour les éditeurs de logiciels d'adopter des mesures de sécurité exemplaires dans les cycles de vie de leurs produits. Les entreprises doivent se concentrer sur la sécurité dans le cadre du processus de conception et de développement de leurs produits, avec une détection des failles en amont et des cycles d'application de correctifs réguliers et au bon moment.

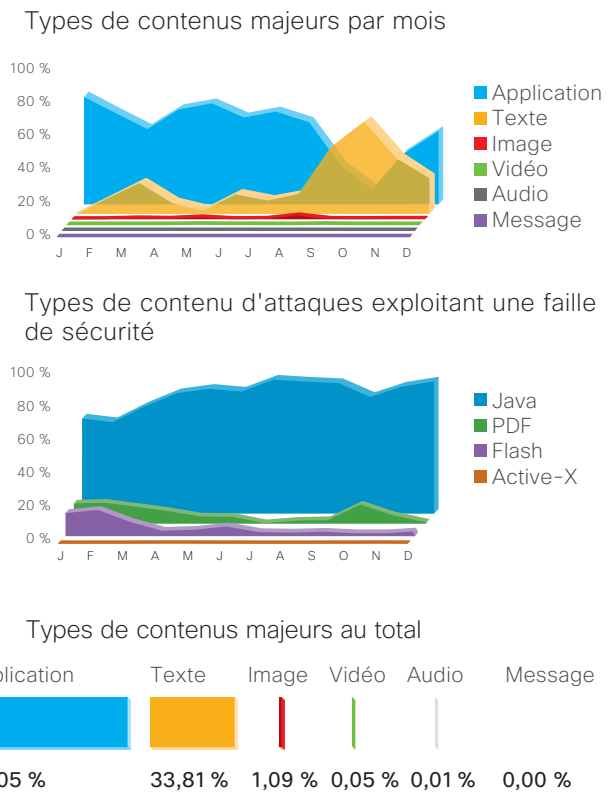
Les entreprises et les utilisateurs doivent aussi être conscients des risques de sécurité inhérents à l'utilisation de produits qui ne sont plus pris en charge par leurs fabricants. Il est également essentiel que les entreprises mettent en œuvre un processus de gestion des risques de sécurité et que les utilisateurs mettent régulièrement à jour leur matériel et leurs logiciels.

Les programmes de vol d'informations font partie des cinq types principaux d'attaque, avec 3,5 % du nombre total d'attaques sur le Web en 2012, viennent ensuite les programmes de téléchargement (1,1 %) et les vers (0,8 %). Une fois encore, ces chiffres indiquent où les attaques en bloc se produisent, en général à l'endroit où se cachait le script ou l'iFrame malveillant. Par conséquent, ces chiffres n'indiquent pas le nombre réel de programmes de vol d'informations, de téléchargement ou de vers qui se propagent via le Web.

Principaux types de contenu malveillant

Les créateurs de programmes malveillants cherchent constamment à optimiser leur retour sur investissement en recherchant le meilleur moyen d'atteindre le plus grand nombre de victimes potentielles avec le moins d'efforts possible. Pour y parvenir, ils tirent parti des technologies multiplateformes lorsqu'ils le peuvent. Dans cette optique, les boîtes à outils de diffusion d'attaques exploitant une faille de sécurité émettent celles-ci dans un ordre spécifique, jusqu'à ce qu'une attaque atteigne son but. La forte

Figure 6 : Principaux types de programmes malveillants du Web en 2012
Les attaques exploitant une faille de sécurité Java ont représenté 87 % de toutes les attaques de ce type sur le Web.

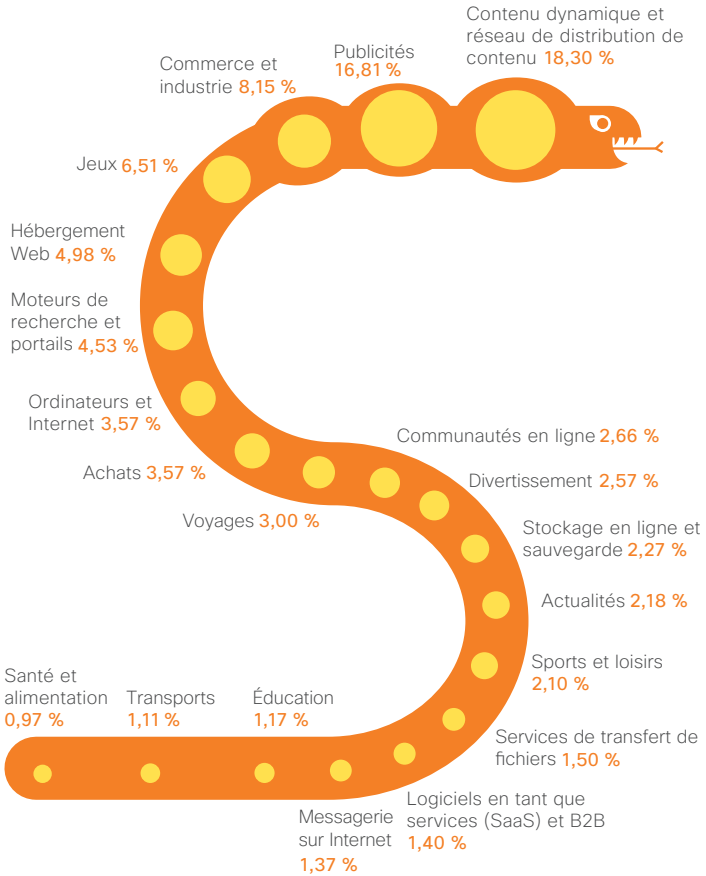


La forte concentration d'attaques exploitant une faille de sécurité Java montre que les vulnérabilités liées à l'environnement Java font prioritairement l'objet de tentatives de la part des auteurs d'attaques en raison du taux de réussite rencontré.

Figure 7 : Principales catégories de sites

Les sites d'achats en ligne hébergent 21 fois plus de contenus malveillants par rapport aux sites de diffusion de logiciels contrefaits.

Remarque : la catégorie des « contenus dynamiques » est en tête de la liste de Cisco des principaux sites susceptibles d'être infectés. Cette catégorie inclut les systèmes de diffusion de contenus tels que les statistiques Web, des analyses de site, et d'autres contenus tiers non publicitaires.



concentration d'attaques exploitant une faille de sécurité Java montre que les vulnérabilités liées à l'environnement Java font prioritairement l'objet de tentatives de la part des auteurs d'attaques en raison du taux de réussite rencontré. En outre, avec plus de 3 milliards d'appareils exécutant Java,[16] cette technologie donne l'opportunité aux hackers d'élargir le champ de leurs attaques à plusieurs plates-formes.

Deux autres technologies multiplateformes, PDF et Flash, arrivent en deuxième et troisième place dans l'analyse de Cisco sur les principaux types de contenu diffusés dans les programmes malveillants. Bien qu'Active X continue à être exploité, les analystes de Cisco ont constaté une baisse de l'utilisation de cette technologie pour la diffusion de programmes malveillants. Cependant, comme cela a été mentionné concernant Java, les nombres plus faibles de certains types d'attaques exploitant une faille de sécurité reflètent principalement l'ordre dans lequel les attaques sont menées.

L'examen des contenus malveillants effectué par Cisco révèle que presque deux fois plus de programmes malveillants sont basés sur des images que sur des vidéos autres que Flash. Cependant, cela est en partie dû à la manière dont les navigateurs traitent les types de contenu déclarés et aux moyens employés par les pirates pour manipuler ces contrôles en déclarant des types de contenu erronés. En outre, les systèmes de commande et de contrôle malveillants transmettent souvent des informations de serveur via des commentaires cachés dans des fichiers image ordinaires.

Principales catégories de sites infectés

Comme le montrent les données de Cisco, l'idée selon laquelle les infections se produisent en général sur des sites « à risque », par exemple ceux qui distribuent des logiciels contrefaits, est fausse. L'analyse de Cisco indique que la grande majorité des attaques sur le Web se produit sur des sites légaux et grand public. En d'autres termes, la majorité des attaques se produit dans des endroits que les utilisateurs en ligne visitent le plus et qu'ils pensent être sûrs.

Les publicités en ligne arrivent en deuxième place dans la liste des catégories de site en ligne avec 16 % du nombre total d'attaques par programmes malveillants. La publicité syndiquée est un moyen courant de monétiser les sites Web. Ainsi une publicité malveillante diffusée de cette manière peut avoir des effets dramatiques.

La vaste majorité des attaques de programmes malveillants sur le Web se produit lors de la visite de sites Web grand public. En d'autres termes, la majorité des attaques se produit dans des endroits que les utilisateurs en ligne visitent le plus et qu'ils pensent être sûrs.

Les cybercriminels ont bien étudié les habitudes de navigation modernes pour infecter le plus de monde possible sur le Web.

Plus loin dans la liste, les sites commerciaux et industriels (notamment des sites d'entreprises, de ressources humaines et de services de transport) sont à la troisième place. Les sites de jeux en ligne arrivent à la quatrième place, suivi par les sites d'hébergement Web et les moteurs de recherche qui occupent respectivement la cinquième et la sixième places. Les 20 principales catégories de sites Web sur lesquels des attaques sont possibles ne figurent pas parmi les sites en général considérés comme potentiellement à risque. Parmi les sites sur lesquels des attaques sont possibles, il y a en fait un mélange équilibré comprenant des types de sites populaires et légaux tels que les sites d'achat en ligne (8ème place), les sites d'informations (13ème place), les logiciels sous forme de services (SaaS) et les applications entreprise-à-entreprise (16ème place).

Les cybercriminels ont bien étudié les habitudes de navigation modernes pour infecter le plus de monde possible sur le Web. Les créateurs de programmes malveillants suivent les utilisateurs à la trace. Ils infectent directement les sites Web considérés comme fiables ou par le biais de réseaux de distribution tiers.

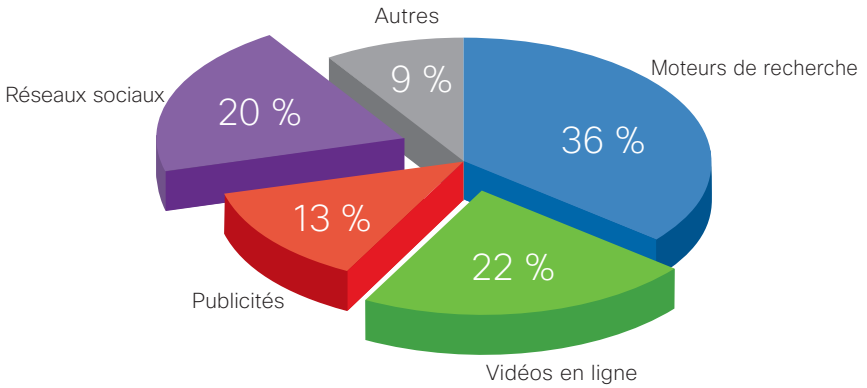
Applications populaires les plus sollicitées

Les changements observés dans les habitudes des utilisateurs en ligne élargissent le champ d'action des cybercriminels pour lancer des attaques exploitant une faille de sécurité. Les entreprises de toutes tailles ont de plus en plus recours aux médias sociaux et à la vidéo en ligne ; la plupart des grandes marques sont présentes sur Facebook et Twitter et beaucoup d'entre elles intègrent des médias sociaux dans leurs produits. Ces destinations Web, qui attirent un public massif et sont acceptées dans les règles des entreprises, représentent autant de nouvelles opportunités pour diffuser des programmes malveillants.

Selon les données de Cisco Application Visibility and Control (AVC), la grande majorité (91 %) des demandes Web est répartie entre les moteurs de recherche (36 %), les sites vidéo en ligne (22 %), les réseaux publicitaires (13 %) et les réseaux sociaux (20 %).

Les entreprises de toutes tailles ont de plus en plus recours aux médias sociaux et à la vidéo en ligne ; la plupart des grandes marques sont présentes sur Facebook et Twitter et beaucoup d'entre elles intègrent des médias sociaux dans leurs produits.

Figure 8 : Applications populaires par nombre de clics
Les médias sociaux et la vidéo en ligne modifient la façon dont les employés passent leur temps au travail et s'exposent à de nouvelles vulnérabilités.



Si une corrélation est établie entre les données sur les principaux sites Web visités sur Internet et la catégorie des sites Web les plus dangereux, les sites que les utilisateurs visitent le plus, tels que les moteurs de recherche, sont ceux sur lesquels ils risquent le plus d'être victimes d'un programme malveillant.

Si une corrélation est établie entre les données sur les principaux sites Web visités sur Internet et la catégorie des sites Web les plus dangereux, les sites que les utilisateurs visitent le plus, tels que les moteurs de recherche, sont ceux sur lesquels ils risquent le plus d'être victimes d'un programme malveillant. Cette corrélation montre une fois encore que les créateurs de programmes malveillants recherchent à optimiser leur retour sur investissement. Par conséquent, ils vont concentrer leurs efforts sur les endroits attirant le plus d'utilisateurs et où ces derniers sont le plus vulnérables.

Lorsque l'horreur gothique donne naissance aux programmes malveillants

par Kevin W. Hamlen
professeur associé, Département informatique de l'université du Texas à Dallas

Le camouflage des programmes malveillants est une menace à laquelle les spécialistes de la sécurité risquent de plus en plus d'être confrontés. Alors que la plupart des programmes malveillants utilisent un mécanisme de mutation simple ou d'obscurcissement pour se transformer et être plus difficiles à étudier par rétro-ingénierie, les programmes malveillants à auto-camouflage sont encore plus furtifs, car ils fusionnent avec logiciels ciblés déjà présents sur chacun des systèmes qu'ils infectent. Cela leur permet d'échapper aux mécanismes de défense qui recherchent des anomalies (un code d'exécution décompacté ou crypté par exemple), qui contiennent souvent des programmes malveillants plus conventionnels.

La technologie la plus récente en matière de programme malveillant à auto-camouflage, appelée comme il se doit Frankenstein[17] est un produit de notre recherche cette année dans le centre d'études et de recherche sur la cybersécurité (Security Research and Education Center) de l'Université du Texas à Dallas. Comme le scientifique fou du roman d'horreur de Mary Shelley écrit en 1818, « le programme malveillant Frankenstein » crée des mutants en volant des morceaux de code des autres logiciels qu'il rencontre et assemble ces morceaux de code pour créer des variantes de lui-même. Chaque mutant Frankenstein est alors composé entièrement de logiciels sans anomalie, à l'aspect inoffensif. Il effectue des opérations d'extraction ou de cryptage non suspectes de code d'exécution et a accès à un pool extensible de transformations de code qu'il s'est approprié lors de sa rencontre avec d'autres programmes.

Pour donner vie à ses créations, Frankenstein utilise un ensemble de techniques tirées de la théorie de la compilation et de l'analyse des programmes. Les fichiers binaires des victimes sont analysés pour y rechercher des courtes séquences d'octets pouvant être décodées en séquences d'instructions utiles appelées *gadgets*. Un interprète de séquences déduit ensuite les effets sémantiques possibles de chaque gadget détecté. Une recherche à rebours est ensuite appliquée pour détecter des séquences de gadget qui, lorsqu'elles sont exécutées dans l'ordre, exécutent le comportement nuisible du contenu du programme malveillant.

Comme le scientifique fou du roman d'horreur de Mary Shelley écrit en 1818, « le programme malveillant Frankenstein » crée des mutants en volant des morceaux de code des autres logiciels qu'il rencontre et assemble ces morceaux de code pour créer des variantes de lui-même.

Chaque séquence détectée est enfin assemblée pour former un nouveau mutant. En pratique, Frankenstein détecte plus de 2 000 gadgets par seconde, ce qui peut représenter plus de 100 000 gadgets à partir des fichiers binaires de deux ou trois victimes en moins de cinq secondes. Avec un tel pool de gadgets à leur disposition, les mutants produits ont rarement besoin de partager des séquences d'instructions communes. Par conséquent, chaque mutant semble unique.

D'une manière générale, notre recherche suggère que les programmes malveillants de nouvelle génération risquent de plus en plus d'abandonner les mutations simples basées sur le cryptage et l'empaquetage en faveur de mécanismes d'obscurcissements binaires *métamorphiques* comme ceux utilisés par Frankenstein. Ces obscurcissements sont faciles à mettre en œuvre. Ils permettent une propagation rapide et empêchent l'identification des programmes malveillants lors des phases d'analyse statique de la plupart des moteurs de détection. Pour contrer cette menace, il faudra déployer certaines des technologies utilisées pour développer Frankenstein, notamment des analyses statiques basées sur la sémantique et non syntaxiques, l'extraction de fonctions et des signatures sémantiques dérivées de l'apprentissage machine[18] au lieu d'analyses purement manuelles.

D'une manière générale, notre recherche suggère que les programmes malveillants de nouvelle génération risquent de plus en plus d'abandonner les mutations simples basées sur le cryptage et l'empaquetage en faveur d'obscurcissements binaires métamorphiques comme ceux utilisés par Frankenstein.

Cet article mentionne une recherche soutenue en partie par l'agence National Science Foundation (NSF) (subvention n° 1054629) et l'agence Air Force Office of Scientific Research (AFOSR) (subvention FA9550-10-1-0088) aux États-Unis. Les opinions, constatations, conclusions ou recommandations exprimées sont celles de l'auteur et ne reflètent pas nécessairement celles de l'agence NSF ou de l'agence AFOSR.

[17] Vishwath Mohan et Kevin W. Hamlen. "Frankenstein: Stitching Malware from Benign Binaries." Dans *Proceedings of the USENIX Workshop on Offensive Technologies (WOOT)*, pp. 77-84, août 2012.

[18] Mohammad M. Masud, Tahseen M. Al-Khateeb, Kevin W. Hamlen, Jing Gao, Latifur Khan, Jiawei Han et Bhavani Thuraisingham. "Cloud-based" Malware Detection for Evolving Data Streams. *ACM Transactions* on Management Information Systems (TMIS), *2*(3), octobre 2011.

Analyse des vulnérabilités et des menaces en 2012

Le graphique sur les catégories de failles de sécurité et de menaces montre une augmentation importante du nombre de menaces. En 2012 le nombre de menaces a augmenté de 19,8 % par rapport à 2011. Cette nette augmentation des menaces impose aux entreprises de mettre en permanence à jour leurs systèmes de gestion des failles de sécurité et de leur appliquer les correctifs les plus récents, surtout avec l'adoption d'environnements virtuels.

Les entreprises doivent également répondre à l'augmentation croissante de l'utilisation de logiciels tiers et ouverts (Open Source) inclus dans leurs produits et présents dans leurs environnements. « Une seule faille dans des solutions tierces ou ouvertes (Open Source) peut avoir un impact sur un large éventail de systèmes dans l'environnement. Il est alors très difficile d'identifier ces systèmes pour les mettre à jour ou de leur appliquer des correctifs », déclare Jeff Shipley, Directeur de la recherche et des opérations de sécurité chez Cisco.

Concernant les types de menaces, les plus courantes sont les menaces de gestion des ressources, ce qui inclut en général les failles relatives au déni de service, les menaces liées à la validation d'informations notamment par injection SQL et les erreurs de type exécution de script inter-site, ainsi que les dépassements de mémoire tampon qui se traduisent par un déni de service. La prépondérance de menaces similaires aux années précédentes, combinée à la nette augmentation des menaces, indique que le secteur de la sécurité doit trouver le moyen de mieux détecter et traiter ces failles de sécurité.

Le graphique Évaluation de l'urgence des alertes Cisco IntelliShield illustre le niveau d'activité menaçante associée à des failles de sécurité spécifiques. L'augmentation importante de l'urgence de niveau 3 indique qu'un plus grand nombre de failles sont exploitées. Cela est probablement dû au nombre croissant de révélations des mécanismes des attaques exploitant une faille de sécurité communiquées publiquement par des chercheurs ou des outils de test, et à l'incorporation de ces mécanismes dans les boîtes à outils de création d'attaques. Ces deux facteurs augmentent le nombre d'attaques disponibles qui sont utilisées par les hackers et les groupes criminels.

Le graphique Évaluation de la gravité des alertes Cisco IntelliShield illustre le niveau d'impact des attaques exploitant une faille de sécurité. L'évaluation de la gravité indique également une augmentation sensible des menaces de niveau 3 pour les mêmes raisons indiquées précédemment concernant la disponibilité des outils de création d'attaques.

Figure 9 : Classements des critères d'urgence et de gravité

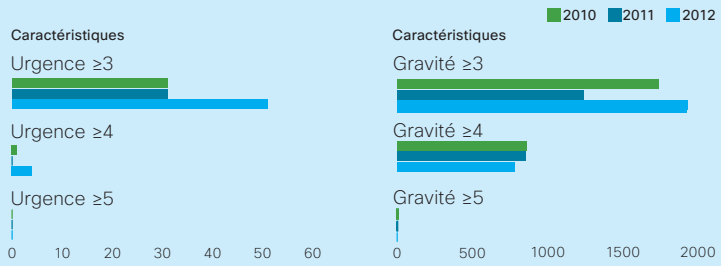
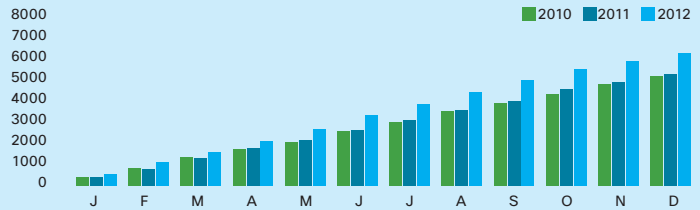


Figure 10 : Catégories de menaces et de vulnérabilités

	Nombre d'alertes mensuelles en 2010				Nombre d'alertes mensuelles en 2011				Nombre d'alertes mensuelles en 2012			
	Total	Réamp	Nouveau		Total	Réamp	Nouveau		Total	Réamp	Nouveau	
Janvier	417	259	158	417	403	237	166	403	552	344	208	552
Février	430	253	177	847	400	176	224	803	551	317	234	1103
Mars	518	324	194	1364	501	276	225	1304	487	238	249	1590
Avril	375	167	208	1740	475	229	246	1779	524	306	218	2114
Mai	322	174	148	2062	404	185	219	2183	586	343	243	2700
Juin	534	294	240	2596	472	221	251	2655	647	389	258	3347
Juillet	422	210	212	3018	453	213	240	3108	514	277	237	3861
Août	541	286	255	3559	474	226	248	3582	591	306	285	4452
Septembre	357	167	190	3916	441	234	207	4023	572	330	242	5024
Octobre	418	191	227	4334	558	314	244	4581	517	280	237	5541
Novembre	476	252	224	4810	357	195	162	4938	375	175	200	5916
Décembre	400	203	197	5210	363	178	185	5301	376	183	193	6292
	5210	2780	2430		5301	2684	2617		6292	3488	2804	



« Une seule faille dans des solutions tierces ou ouvertes (Open Source) peut avoir un impact sur un large éventail de systèmes dans l'environnement. Il est alors très difficile d'identifier ces systèmes pour les mettre à jour ou de leur appliquer des correctifs. »

Jeff Shipley, Directeur de la recherche et des opérations concernant la sécurité chez Cisco

Des menaces évolutives

Nouvelles méthodes, types d'attaques identiques

Tous les moyens sont bons pour lancer des attaques exploitant une faille de sécurité IT aujourd'hui, tant que la méthode sélectionnée est efficace.

Cela ne signifie pas que les acteurs dans l'économie parallèle ne continuent pas à créer des outils et des techniques toujours plus sophistiqués pour notamment infecter les ordinateurs des utilisateurs, infecter les réseaux et voler des données sensibles. En 2012, on a pu constater un retour aux « bonnes vieilles méthodes » pour trouver de nouveaux moyens de perturber ou de contourner les protections de sécurité des entreprises.

Les attaques DDoS en sont un parfait exemple. Plusieurs institutions financières aux États-Unis ont été la cible privilégiée par deux campagnes importantes et conjointes lancées par des groupes d'hacktivistes étrangers au cours des six derniers mois de 2012 (pour une analyse détaillée, consultez la section Tendances des dénis de service distribué pour 2012). Certains experts en sécurité avertissent que ces événements ne sont qu'un début et que « les hacktivistes, les réseaux de crime organisé et même des États-nations seront les auteurs »[19] de ces attaques à l'avenir, qu'ils travaillent seuls ou en groupe.

« Nous constatons une tendance dans les dénis de service distribué (DDoS), avec des pirates qui introduisent davantage de contexte à propos de leur site cible afin de donner une importance encore plus grande à la panne », affirme Gavin Reid, Directeur de la recherche sur les menaces pour les opérations SIO (Security Intelligence Operations) chez Cisco. « Au lieu de provoquer une attaque SYN, le déni DDoS tente désormais de manipuler une application spécifique au sein de l'organisation, ce qui peut éventuellement provoquer une série de dommages en cascade en cas d'échec. »

En 2012, on a pu constater un retour aux « bonnes vieilles méthodes » pour trouver de nouveaux moyens de perturber ou de contourner les protections de sécurité des entreprises.

« Même contre un adversaire moyennement sophistiqué, les techniques de pointe en matière de sécurité réseau sont souvent dépassées. »

Gregory Neal Akers, Vice-président senior du groupe de recherche de sécurité avancée chez Cisco

Alors que les entreprises pensent qu'elles sont suffisamment protégées contre la menace DDoS, il est plus que probable que leur réseau ne serait pas en mesure de faire face au type d'attaques DDoS incessantes et intensives comme celles auxquelles nous avons assisté en 2012. « Même face à un adversaire ingénieux, mais de niveau moyen, l'état actuel de la sécurité du réseau est souvent nettement dépassé », prévient Gregory Akers Neal, Vice-président principal du groupe Advanced Security Initiatives chez Cisco.

Une autre tendance observée au sein de la communauté de cybercriminalité tourne autour de la « démocratisation » des menaces. Nous constatons de plus en plus fréquemment que les outils et les techniques, de même que les renseignements nécessaires pour exploiter les vulnérabilités, sont « largement partagés » dans l'économie souterraine aujourd'hui. « Les techniques ont beaucoup évolué », confirme M. Akers. « Nous assistons maintenant à une plus grande spécialisation et une plus grande collaboration entre les acteurs malveillants. Nous avons affaire à une véritable chaîne de la menace : quelqu'un développe un bogue, quelqu'un d'autre développe le programme malveillant, une autre personne conçoit le composant d'ingénierie sociale, et ainsi de suite. »

Créer des menaces puissantes qui les aideront à accéder à de grandes quantités de ressources précieuses en provenance du réseau ; voilà l'une des raisons pour laquelle les cybercriminels mettent souvent en commun leur savoir-faire. Mais, comme pour toute organisation bien réelle qui sous-traite des tâches, l'efficacité et les économies de coûts figurent parmi les principaux moteurs de l'approche de création d'une menace dans la communauté de cybercriminalité. Les « talents indépendants » recrutés pour ces tâches font généralement de la publicité pour vanter leurs compétences et rémunèrent la vaste communauté de cybercriminalité via des marchés secrets en ligne.

Attaques par amplification et réflexion

Les attaques par amplification et réflexion DNS [20] utilisent des résolveurs récursifs ouverts du système de noms de domaines (DNS) ou des serveurs DNS faisant autorité pour augmenter le volume du trafic d'attaques transmis à une victime. En usurpant[21] les messages de demande DNS, ces attaques dissimulent leur véritable source et envoient des requêtes DNS qui retournent des messages de réponse de 1 000 à 10 000 % plus grands que les messages de demande DNS envoyés. Ces types de profils d'attaque sont couramment observés lors des attaques DDoS[22].

Les organisations participent à leur insu à ces attaques en laissant des résolveurs récursifs ouverts sur Internet. Mais elles peuvent détecter les attaques à l'aide de divers outils[23] et des technologies de télémétrie de flux[24] et elles peuvent les empêcher en sécurisant[25] leur serveur DNS ou en limitant le taux[26] des messages de réponse DNS.

Tendances des dénis de service distribué pour 2012

L'analyse suivante est dérivée du référentiel ATLAS d'Arbor Networks, qui comprend des données recueillies à partir d'un certain nombre de sources de 240 FAI partout dans le monde, sur le pic de trafic de 37,8 Tbit/s.[27]

La taille des attaques continue à augmenter

Globalement, la taille moyenne des attaques a augmenté au cours de l'année passée. Il y a eu une augmentation de 27 % dans le débit des attaques (de 1,23 Gbit/s en 2011 à 1,57 Gbit/s en 2012) et une augmentation de 15 % du débit de paquets par seconde utilisés dans les attaques (de 1,33 Mp/s en 2011 à 1,54 Mp/s en 2012).

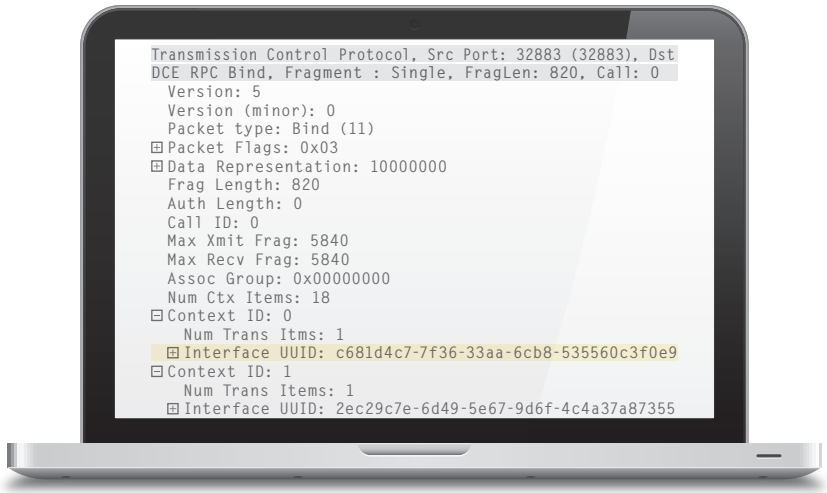
Origine des attaques

Les trois principales sources d'attaque enregistrées, après avoir supprimé 41 % des sources sans attribution dues à l'anonymisation des données, sont la Chine (17,8 %), la Corée du Sud (12,7 %) et les États-Unis (8,0 %).

Attaques de plus grande taille

La taille de l'attaque la plus volumineuse enregistrée a été estimée à 100,84 Gbit/s et l'attaque a duré environ 20 minutes (la source de l'attaque est inconnue due à l'anonymisation des données). La taille la plus volumineuse correspondante enregistrée en (p/s) a été estimée à 82,36 Mp/s et l'attaque a duré environ 24 minutes (la source de l'attaque est inconnue due à l'anonymisation des données).

Figure 11 : Fuites IPS (Intrusion Prevention System) analysées en direct



Le service Cisco Security Research and Operations gère plusieurs laboratoires de programmes malveillants afin d'observer le trafic malveillant « à l'état naturel ». Des programmes malveillants sont volontairement introduits dans le laboratoire afin de s'assurer que les dispositifs de sécurité sont efficaces ; les ordinateurs sont également laissés intentionnellement vulnérables et exposés à Internet.

Militarisation des techniques de fraude modernes

Les cybercriminels mettent constamment au point de nouvelles techniques pour contourner les dispositifs de sécurité. Les chercheurs de Cisco sont à l'affût des nouvelles techniques et de la « militarisation » de techniques bien connues.

Le service Cisco Security Research and Operations gère plusieurs laboratoires de programmes malveillants afin d'observer le trafic malveillant « à l'état naturel ». Des programmes malveillants sont volontairement introduits dans le laboratoire afin de s'assurer que les dispositifs de sécurité sont efficaces ; les ordinateurs sont également laissés intentionnellement vulnérables et exposés à Internet.

Au cours de l'un de ces tests, le système de prévention des intrusions (IPS) de Cisco a détecté une attaque d'appel de procédure à distance Microsoft (MSRPC) bien connue. Une analyse minutieuse a déterminé que l'attaque faisait appel à une tactique inédite de fraude dans le but de contourner les dispositifs de sécurité.[28] Cette fraude consistait à envoyer plusieurs identificateurs de contexte de liaison au sein de la demande de liaison initiale. Ce type d'attaque peut contourner les protections sauf si le système IPS surveille et détermine les identificateurs corrects.

Les cybercriminels mettent constamment au point de nouvelles techniques pour contourner les dispositifs de sécurité. Les chercheurs de Cisco sont à l'affût des nouvelles techniques et de la « militarisation » de techniques bien connues.

ÉTUDE DE CAS

Opération Ababil

En septembre et octobre 2012, Cisco et Arbor Networks ont suivi une campagne d'attaques DDoS ciblée et particulière grave, baptisée « Opération Ababil », laquelle visait les institutions financières basées aux États-Unis. « Les attaques DDoS étaient préméditées, ciblées, annoncées avant les faits et exécutées à la lettre. Les auteurs de l'attaque ont réussi à rendre plusieurs sites financiers majeurs inaccessibles aux clients légitimes pendant plusieurs minutes et, dans les cas les plus graves, pendant des heures. Au cours de ces événements, plusieurs groupes ont revendiqué la responsabilité de ces attaques ; au moins un groupe prétendait dénoncer la législation relative aux droits d'auteur et à la propriété intellectuelle aux États-Unis. D'autres ont justifié leur implication comme réponse à une vidéo publiée sur YouTube et jugée offensante pour certains musulmans.

Du point de vue de la cybersécurité, l'opération Ababil est remarquable car elle a tiré profit d'applications Web et de serveurs d'hébergement communs qui sont aussi populaires que vulnérables. Autre fait marquant et inhabituel dans cette opération, ces attaques simultanées, réalisées avec une bande passante élevée, ont été perpétrées à l'encontre de plusieurs entreprises d'un même secteur (financier).

Comme c'est souvent le cas dans le secteur de la sécurité, on a encore fait du neuf avec du vieux.

Le 18 septembre 2012, les « Cybercombattants de Izz ad-Din al-Qassam » ont publié un message sur le site Pastebin [29] pour exhorter les Musulmans à cibler les grandes institutions financières et les plates-formes de commercialisation de matières premières. Les menaces et les cibles spécifiques ont fait l'objet d'une couverture médiatique à l'échelle du monde entier et se sont poursuivies pendant quatre semaines consécutives. Chaque semaine, de nouvelles menaces avec de nouvelles cibles ont été suivies d'actions aux dates et aux heures fixées. Au bout de la cinquième semaine, le groupe a cessé de désigner des cibles, mais il a fait comprendre que les campagnes se poursuivraient. Comme promis, les campagnes ont repris de plus belle en décembre 2012, ciblant une fois encore plusieurs institutions financières importantes aux États-Unis.

La phase 2 de l'opération Ababil a également été annoncée sur le site Pastebin.[30] Au lieu de recourir à des machines infectées, diverses applications Web PHP, y compris le système de gestion de contenu Joomla, ont servi de robots collecteurs principaux dans la campagne. En outre, de nombreux sites WordPress, qui utilisent souvent le module d'extension obsolète TimThumb, ont été touchés à la même époque. Les auteurs d'attaques s'en prenaient souvent à des serveurs non maintenus à jour, qui hébergeaient ces applications et y chargeaient des environnements Web PHP dans le but de déployer d'autres outils d'attaque. Cependant, le concept de « commande et contrôle » ne s'appliquait pas de la manière habituelle ; les auteurs d'attaques se connectaient aux outils, soit directement soit par le biais de scripts, de serveurs proxys et de serveurs intermédiaires. Lors des cyberévénements de septembre et octobre 2012, un large éventail de fichiers et d'outils basés sur PHP ont été utilisés, et non pas seulement le fameux « itsoknoproblembro » (aka « Brobot ») dont on a beaucoup parlé. Dans la seconde phase de l'activité, des outils d'attaque mis à jour tels que Brobot v2 ont également été utilisés.

L'opération Ababil a déployé une série d'outils à travers différents vecteurs pour propager des attaques de la couche application sur HTTP, HTTPS et DNS, avec un trafic d'attaque volumétrique sur une variété de protocoles TCP, UDP, ICMP et IP. L'analyse de Cisco a montré que la majorité des paquets étaient envoyés vers le port TCP/UDP 53 (DNS) ou 80 (HTTP). Tandis que le trafic sur le port UDP 53 et le port TCP 53 et 80 représente normalement le trafic valide, les paquets destinés au port UDP 80 constituent une anomalie qui n'est pas couramment utilisée par les applications.

Un rapport détaillé sur les modèles et les charges utiles de la campagne de l'opération Ababil est disponible dans le document Cisco Event Response consacré aux attaques par déni de service distribué sur les institutions financières.[31]

Leçons tirées

Alors qu'ils font partie intégrante de tout portefeuille de sécurité de réseau, les dispositifs de pare-feu et IPS reposent sur une inspection d'état du trafic. Les techniques ciblant la couche application utilisées dans la campagne de l'opération Ababil sont facilement venues à bout de ces tables d'état et, dans plusieurs cas, ont conduit à leur échec. La technologie de veille permettant de limiter les attaques DDoS était la seule contre-mesure efficace.

Les services de sécurité gérés et les fournisseurs d'accès à Internet ont montré leurs limites. Lors d'une attaque DDoS classique, le principe de sagesse qui prévaut consiste à faire face aux attaques volumétriques dans le réseau. Dans les cas de campagnes ciblant la couche application qui sont déployées au plus près de la victime, celles-ci doivent être traitées au niveau du data center ou à la « périphérie client ». Du fait que plusieurs entreprises étaient ciblées en même temps, les centres d'épuration de réseau ont été mis à rude épreuve.

Il est essentiel de maintenir les composants et les logiciels à jour sur les dispositifs de limitation des attaques DDoS. Les déploiements moins récents ne sont pas toujours en mesure de faire face aux nouvelles menaces. Il est également important de disposer de la capacité adéquate aux bons endroits. Être en mesure de limiter les effets d'une attaque de grande ampleur est inutile si le trafic ne peut pas être canalisé vers l'emplacement où la technologie a été déployée.

Même si la limitation des attaques DDoS sur le cloud ou en réseau implique généralement une capacité de bande passante beaucoup plus élevée, les solutions sur site offrent un meilleur temps de réaction face à ces attaques et elles permettent un contrôle et une visibilité de meilleure qualité. Combiner les deux permet d'obtenir une solution plus complète.

Conjointement aux technologies DDoS en cloud et en réseau, et dans le cadre de la caution obtenue pour les événements de l'opération Ababil, Cisco a défini des techniques de détection et de limitation dans le bulletin Identifying and Mitigating the Distributed Denial of Service Attacks Targeting Financial Institutions Applied Mitigation (Limitation appliquée à l'identification et la réduction des attaques de déni de service distribué ciblant les institutions financières).[32] Ces techniques incluent l'utilisation du filtrage tACL (Transit Access Control List), l'analyse des données NetFlow et le mécanisme uRPF (unicast Reverse Path Forwarding). Par ailleurs, il existe un certain nombre de bonnes pratiques qui doivent être régulièrement révisées, testées et mises en œuvre afin d'aider les entreprises à se préparer et à réagir aux événements du réseau. Pour disposer d'une bibliothèque de ces bonnes pratiques, accédez au site des Ressources tactiques Cisco SIO[33] et des Meilleures pratiques en matière de sécurité pour les prestataires de services.[34]

Le courrier indésirable, plus présent que jamais

Les volumes de courriers indésirables continuent de décliner dans le monde, selon une étude de Cisco, mais l'expédition de courriers indésirables reste un outil incontournable pour de nombreux cybercriminels, qui y voient un moyen efficace et rapide d'exposer les utilisateurs à des programmes malveillants et de faciliter un grand nombre d'escroqueries.

Cependant, malgré l'idée reçue selon laquelle les programmes malveillants sont généralement déployés dans les pièces jointes au courrier électronique, l'étude de Cisco indique que peu d'expéditeurs de courriers indésirables aujourd'hui s'appuient sur cette méthode ; au contraire, ils se tournent vers des liens malveillants dans le contenu du courrier électronique en tant que mécanisme de diffusion beaucoup plus efficace.

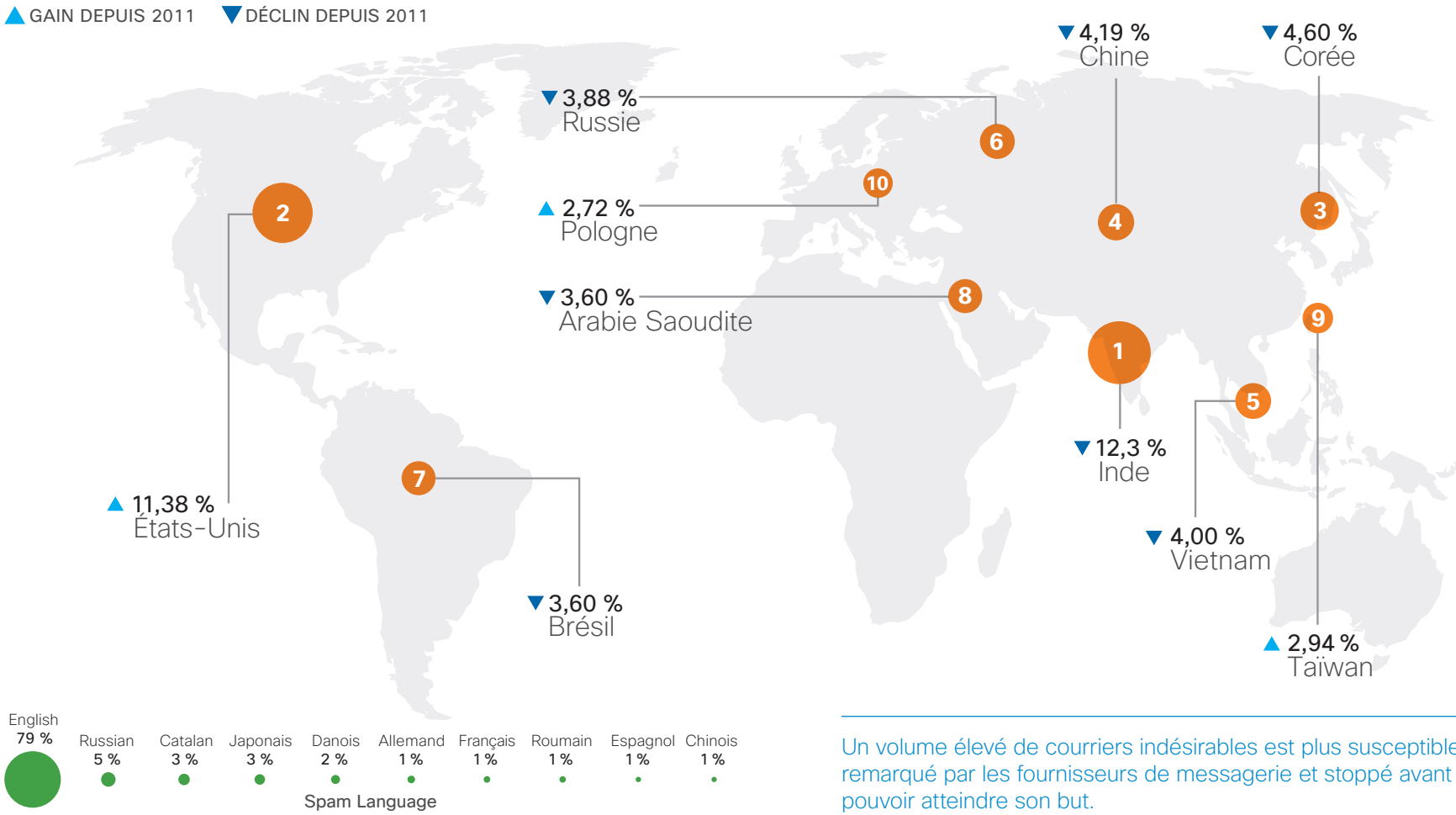
Le courrier indésirable est aussi moins « dispersé » que par le passé, la majorité des expéditeurs de courriers indésirables préférant cibler des groupes spécifiques d'utilisateurs avec l'espoir de générer des rendements plus élevés. Les produits pharmaceutiques de marque, les montres de luxe et les événements tels que les périodes de déclaration fiscale font partie de la liste des principaux thèmes que les expéditeurs de courriers indésirables choisissent de promouvoir le plus dans leurs campagnes. Au fil du temps, les expéditeurs de courriers indésirables ont appris que le meilleur moyen d'attirer les clics et les achats, et donc de générer un profit, consiste à tirer parti de marques contrefaites ou à profiter d'événements actuels qui ont l'attention de groupes importants d'utilisateurs.

Tendances du trafic de courriers indésirables au niveau mondial

Depuis les démantèlements de réseaux de botnets à grande échelle en 2010, les grands volumes de courrier indésirable ne sont pas aussi efficaces qu'ils l'étaient autrefois, et les expéditeurs de courriers indésirables ont appris et changé leurs tactiques. Il existe une nette évolution vers des campagnes plus petites et mieux ciblées, basées sur des événements mondiaux et des sous-ensembles spécifiques d'utilisateurs. Les gros volumes de courriers indésirables sont aussi plus susceptibles d'être détectés par les fournisseurs de messagerie et stoppés avant d'avoir pu atteindre leur but.

Figure 12 : Tendances du trafic de courriers indésirables au niveau mondial

Les volumes de courriers indésirables dans le monde ont diminué de 18 %, et la plupart des expéditeurs respectent les « horaires des banques » le week-end.



Un volume élevé de courriers indésirables est plus susceptible d'être remarqué par les fournisseurs de messagerie et stoppé avant de pouvoir atteindre son but.

En 2012, on a découvert plusieurs exemples d'expéditeurs de courriers indésirables qui surfaient sur l'actualité et les événements mondiaux, parfois même sur des tragédies humaines, pour abuser les utilisateurs.

En 2011, le volume total de courriers indésirables au niveau mondial a diminué de 18 %. On est loin de la chute spectaculaire du volume observée en 2010 suite aux démantèlements de réseaux de botnets, mais la tendance à la baisse représente néanmoins un signe encourageant.

Les expéditeurs de courriers indésirables continuent leurs recherches en vue de réduire leurs efforts tout en maximisant l'impact. Selon l'étude de Cisco, les volumes de courriers indésirables chutent de 25 % les week-ends, lorsque les utilisateurs se détournent un peu de leurs e-mails. Les volumes de courriers indésirables atteignent leurs plus hauts niveaux le mardi et le mercredi, avec une moyenne de 10 % supérieure à celle des autres jours de la semaine. Ce regain d'activité au milieu de la semaine et la baisse des volumes le week-end permettent aux expéditeurs de courriers indésirables de vivre « une vie normale ».

Cela leur donne également le temps de mettre au point des campagnes sur mesure en fonction des événements ayant lieu dans le monde au début de la semaine et qui vont les aider à générer un taux de réponse supérieur à leurs campagnes.

En 2012, on a découvert plusieurs exemples d'expéditeurs de courriers indésirables qui surfaient sur l'actualité et les événements mondiaux, parfois même sur des tragédies humaines, pour abuser les utilisateurs. Pendant l'ouragan Sandy, par exemple, les chercheurs de Cisco ont identifié une arnaque massive de manipulation des marchés d'actions reposant sur une campagne de courriers indésirables. Utilisant un message électronique pré-existant qui invitait la population à investir dans une action cotée en cents et axée sur l'exploration de ressources naturelles, les expéditeurs de courriers indésirables ont commencé à ajouter des titres accrocheurs concernant l'ouragan Sandy. L'un des aspects inhabituels de cette campagne est que les expéditeurs de courriers indésirables ont utilisé des adresses IP uniques pour envoyer un lot de courriers indésirables, et qu'ils n'ont pas activé ces adresses depuis.

Origine du courrier indésirable

En matière de courrier indésirable au niveau mondial, certains pays gardent leur place habituelle, tandis que d'autres changent radicalement leur classement. En 2012, l'Inde conserve sa place de premier pays d'origine de courriers indésirables dans le monde, tandis que les États-Unis passent de la sixième à la deuxième place entre 2011 et 2012. Pour compléter la liste des cinq premiers pays émetteurs de courriers indésirables, citons la Corée (troisième place), la Chine (quatrième place) et le Vietnam (cinquième place).

Dans l'ensemble, la majorité des expéditeurs de courriers indésirables concentrent leurs efforts sur la création de messages indésirables dans les langues parlées par les populations qui utilisent le plus le courrier électronique de manière régulière. Selon l'étude de Cisco, la première langue utilisée dans les messages de courrier indésirable en 2012 était l'anglais, suivie du russe, du catalan, du japonais et du danois. Fait notable, il existe des divergences entre l'endroit où le courrier indésirable est envoyé et les langues qui sont utilisées dans les messages correspondants ; par exemple, si l'Inde demeure le premier pays émetteur de courriers indésirables en 2012, les dialectes locaux n'ont pas modifié le classement des 10 premières langues utilisées dans les courriers indésirables envoyés depuis l'Inde. La même observation vaut pour la Corée, le Vietnam et la Chine.

Figure 13 : Origines des courriers indésirables
L'Inde reste en tête en termes de volumes d'échange de courriers indésirables et les États-Unis remontent en flèche en deuxième position.

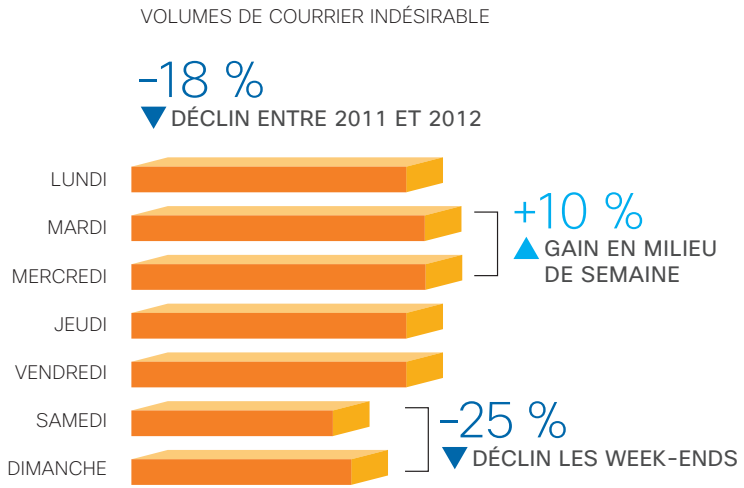


Figure 14 : Pièces jointes aux e-mails

Seuls 3 % des courriers indésirables comportent une pièce jointe contre 25 % des e-mails valides, mais la taille des pièces jointes aux courriers indésirables est plus importante de 18 %.

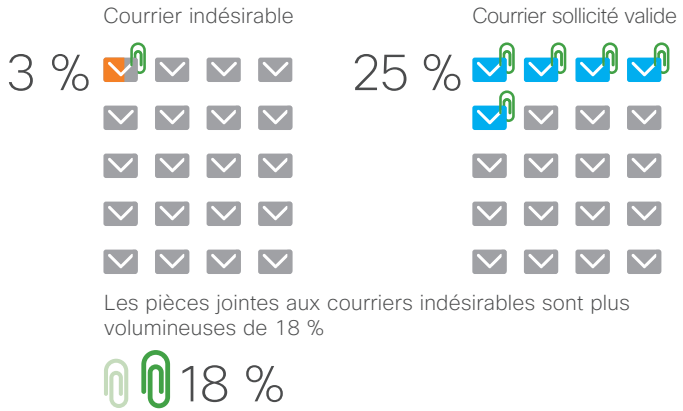
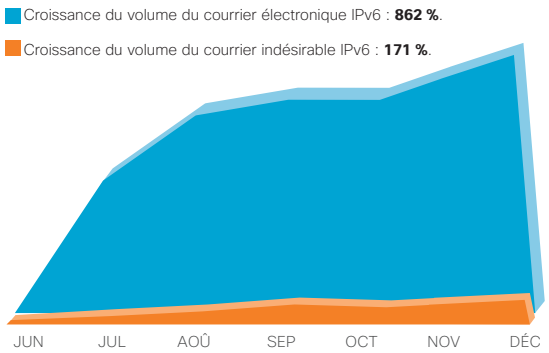


Figure 15 : Courriers indésirables IPv6

Alors que le trafic de messagerie IPv6 ne représente qu'un pourcentage infime du trafic global, il augmente à mesure qu'un plus grand nombre d'utilisateurs de messagerie migrent vers une infrastructure IPv6.



Pièces jointes aux e-mails

Le courrier indésirable a longtemps été considéré comme un mécanisme de diffusion de programmes malveillants, surtout en présence d'une pièce jointe. Cependant, une étude récente de Cisco sur l'utilisation de pièces jointes aux e-mails dans des campagnes de courrier indésirable montre que cette perception n'est peut-être qu'un mythe.

Seulement 3 % du courrier indésirable total comporte une pièce jointe, par comparaison aux 25 % de courrier électronique valide. Et, dans les rares cas où un message de courrier indésirable inclut effectivement une pièce jointe, celle-ci est en moyenne 18 % plus volumineuse qu'une pièce jointe classique qui serait incluse à un courrier électronique valide. Par conséquent, ces pièces jointes sont facilement repérables.

Dans le règne de la messagerie moderne, les liens sont rois. Les expéditeurs de courriers indésirables conçoivent leurs campagnes dans le but de convaincre les utilisateurs de visiter des sites Web où ils peuvent acheter des produits ou des services (souvent douteux). Une fois sur le site, les informations personnelles des utilisateurs sont recueillies, souvent à leur insu, ou sont utilisées frauduleusement d'une manière ou d'une autre.

Comme le révèle l'analyse sur les « marques usurpées » dont il est question plus loin dans cette section, la majorité du courrier indésirable provient de groupes qui cherchent à vendre un groupe très spécifique de marchandises de marque, qu'il s'agisse de montres de luxe ou de produits pharmaceutiques, lesquels sont des contrefaçons dans la plupart des cas.

Courrier indésirable IPv6

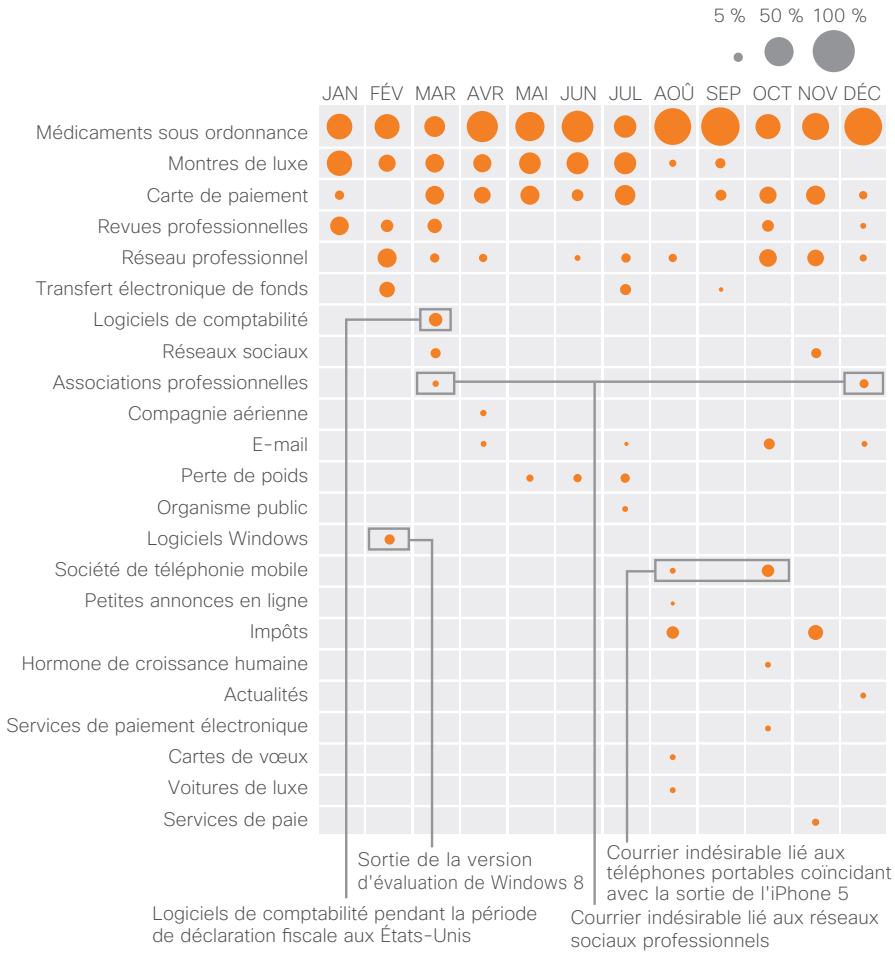
Alors que le trafic de messagerie IPv6 ne représente qu'un pourcentage infime du trafic global, il augmente à mesure qu'un plus grand nombre d'utilisateurs de messagerie migrent vers une infrastructure IPv6.

Cependant, alors que les volumes globaux de courriers électroniques se développent à un rythme rapide, ce n'est pas le cas avec le courrier indésirable IPv6. Ceci suggère que les expéditeurs de courriers indésirables s'abstiennent de consacrer du temps et de l'argent pour migrer vers la nouvelle norme Internet. Il n'existe aucun besoin impératif pour les expéditeurs de courriers indésirables, et pas ou peu d'avantages matériels, de provoquer un tel changement à l'heure actuelle. Comme les adresses IPv4 sont épuisées et que les appareils mobiles et la communication M2M génèrent une croissance explosive de la technologie IPv6, attendez-vous à ce que les expéditeurs de courriers indésirables mettent à niveau leurs infrastructures et intensifient leurs efforts.

Dans le règne de la messagerie moderne, les liens sont rois. Les expéditeurs de courriers indésirables conçoivent leurs campagnes pour convaincre les utilisateurs de visiter des sites Web où ils peuvent acheter des produits ou des services. Une fois sur le site, les informations personnelles des utilisateurs sont recueillies, souvent à leur insu, ou sont utilisées frauduleusement d'une manière ou d'une autre.

Figure 16 : Usurpation de marques

Les expéditeurs de courriers indésirables ciblent les produits pharmaceutiques et les montres de luxe, ainsi que les périodes de déclaration fiscale.



Marques usurpées

Avec les courriers indésirables de marques usurpées, les expéditeurs de courriers indésirables utilisent des organisations et des produits pour envoyer leurs messages dans l'espoir que les utilisateurs en ligne cliqueront sur un lien ou effectueront un achat. La majorité des marques usurpées sont des médicaments délivrés sur ordonnance, tels que les médicaments contre l'anxiété et les analgésiques. En outre, les marques de montres de luxe représentent une couche permanente de « bruit » qui assure une certaine cohérence tout au long de l'année.

L'analyse de Cisco montre que les expéditeurs de courriers indésirables sont également experts lorsqu'il s'agit de corréler leurs campagnes à des événements d'actualité. De janvier à mars 2012, les données de Cisco montrent un pic de courriers indésirables concernant les logiciels Windows, ce qui a coïncidé avec la sortie du système d'exploitation Windows 8. De février à avril 2012, lors de la période d'envoi des déclarations d'impôts aux États-Unis, l'analyse montre une augmentation brutale du nombre de courriers indésirables liés aux logiciels de comptabilité.

De janvier à mars 2012, puis de nouveau entre septembre et décembre 2012, ce qui correspond au début et à la fin de l'année, le courrier indésirable relatif aux réseaux professionnels a fait une entrée remarquée, peut-être parce que les expéditeurs de courriers indésirables savent que les gens commencent souvent leur recherche d'emploi au cours de ces périodes de l'année.

Résultat, les expéditeurs de courriers indésirables sont là pour l'argent, et au fil des ans, ils ont appris que le meilleur moyen d'attirer les clics et les achats consistait à offrir des produits pharmaceutiques et des marchandises de luxe, et à corréler leurs attaques à des événements vers lesquels une grande partie du monde a les yeux tournés.

De septembre à novembre 2012, les expéditeurs de courriers indésirables ont mené une série de campagnes en se faisant passer pour des compagnies de téléphonie mobile, ce qui coïncide avec la sortie de l'iPhone 5.

Résultat, les expéditeurs de courriers indésirables sont là pour l'argent, et au fil des ans, ils ont appris que le meilleur moyen d'attirer les clics et les achats consistait à offrir des produits pharmaceutiques et des marchandises de luxe, et à corréler leurs attaques à des événements vers lesquels une grande partie du monde a les yeux tournés.

Gestion de la vulnérabilité : un fournisseur ne doit pas se contenter d'une énumération ambivalente[35]

La manière dont un fournisseur divulgue les problèmes de sécurité liés à ses produits représente l'aspect le plus visible de ses pratiques de gestion des vulnérabilités. Chez Cisco, des avis consultatifs de sécurité[36] font l'objet d'études et sont publiés par l'équipe chargée de traiter les incidents liés à la sécurité des produits (PSIRT, Product Security Incident Response), un groupe d'experts en sécurité de premier plan qui comprennent que la protection des clients Cisco et celle de la société doivent aller de pair.

« Les avis consultatifs de sécurité font état de nos plus graves problèmes de sécurité des produits et sont généralement la première preuve publique d'une vulnérabilité des produits Cisco », explique Russell Smoak, directeur de la section Security Research and Operations chez Cisco. « En tant que tel, il est essentiel qu'ils soient un moyen de communication efficace qui aide les clients à prendre des décisions éclairées et à gérer les risques auxquels ils sont exposés. Outre les techniques de pointe de limitation des risques[37] dont nous faisons bénéficier nos clients afin d'exploiter les capacités de leur équipement Cisco existant, nous sommes en mesure de fournir autant de détails que possible pour apporter une réponse rapide et en toute confiance. »

La gestion des vulnérabilités, cependant, commence beaucoup plus tôt dans le cycle de vie d'une vulnérabilité et peut s'étendre au-delà de la divulgation initiale. « L'amélioration continue des pratiques de gestion des vulnérabilités est impérative pour pouvoir suivre le rythme de l'environnement de sécurité en pleine mutation, en raison de l'évolution des menaces ainsi que des nouveaux produits et technologies », assure M. Smoak.

En d'autres termes, un fournisseur qui ne parvient pas à évoluer avec des technologies de lutte contre les menaces, et qui ne révèle pas les menaces, risque de se retrouver à la traîne. Par exemple, une innovation des outils de gestion des vulnérabilités internes de Cisco a eu lieu dans le domaine des logiciels d'offres groupées de tiers. Un logiciel tiers est un code inclus dans le produit d'un fournisseur, mais qui n'a pas été écrit par le fournisseur lui-même ; il s'agit généralement d'un logiciel commercial tiers ou d'un logiciel ouvert (Open Source).

Cisco tire parti des outils sur mesure qui utilisent les données de vulnérabilité de Cisco IntelliShield[38] pour informer les équipes de développement de produit lorsqu'un problème de sécurité qui provient d'un logiciel tiers peut avoir un impact sur un produit Cisco. Cet outil, le gestionnaire d'alerte interne de Cisco, a considérablement amélioré la capacité de gérer les problèmes de sécurité qui ont pour origine un code non écrit par Cisco.

> Un fournisseur qui ne parvient pas à évoluer avec des technologies de lutte contre les menaces, et qui ne révèle pas les menaces, risque de se retrouver à la traîne.

L'amélioration des pratiques de divulgation des problèmes de sécurité devrait être, elle aussi, constante. Début 2013, Cisco commencera à utiliser un nouveau type de document, les avis de sécurité de Cisco (Cisco Security Notice), afin de divulguer des problèmes de sécurité de niveau faible à moyen liés aux produits. Ces avis permettront d'améliorer l'efficacité de la communication autour des questions de sécurité qui ne sont pas jugées suffisamment graves pour justifier d'avis consultatifs de sécurité de Cisco. Ces documents seront disponibles publiquement et indexés selon un indicateur d'exposition et de vulnérabilité commun (CVE) afin d'améliorer la visibilité.

Pour améliorer encore davantage la façon de traiter les informations continuelles relatives aux questions de sécurité, les fournisseurs (dont Cisco) ont commencé à inclure les formats CVRF (Common Vulnerability Reporting Framework)[39] et OVAL (Open Vulnerability Assessment Language)[40] dans leurs communiqués. Ces nouvelles normes aident les utilisateurs à évaluer en toute confiance les vulnérabilités sur différentes plates-formes et technologies ; les normes sont capables d'évoluer grâce au format lisible par machine. Selon M. Smoak, « veiller à ce que nos clients disposent des outils dont ils ont besoin pour évaluer correctement les menaces qui pèsent sur leurs réseaux permet de réduire les risques et de hiérarchiser les tâches nécessaires pour sécuriser leurs infrastructures. »

Pour l'année à venir, si vous souhaitez obtenir des mises à jour supplémentaires, une analyse approfondie sur les tendances en matière de sécurité, ainsi que des informations sur les dernières publications de Cisco liées à la sécurité de l'entreprise, visitez le site Web Cisco Security Reports.
www.cisco.com/go/securityreport

Pour avoir un avis actualisé de la part de spécialistes de Cisco concernant un large éventail de questions de sécurité, visitez le blog de Cisco traitant de la sécurité.
blogs.cisco.com/security

Les perspectives en matière de sécurité en 2013

Le contexte actuel des menaces ne se résume pas à un problème causé par des utilisateurs incultes qui visitent des sites malveillants ; de même, le problème ne peut pas être résolu en bloquant des sites Web considérés comme « nuisibles ».

Ce rapport a démontré comment les auteurs d'attaques sont devenus de plus en plus ingénieux, en choisissant les sites, les outils et les applications qui risquent le moins d'être soupçonnés, et que les utilisateurs visitent. Les menaces modernes sont capables d'infecter un vaste public, et ce, silencieusement et efficacement, quel que soit le secteur industriel, la taille de l'entreprise ou le pays. Les cybercriminels tirent profit d'une surface d'attaque en pleine expansion dans l'univers actuel de la connectivité universelle, dans lequel les individus accèdent au réseau de leur entreprise à l'aide de tout type d'appareil.

À mesure que les infrastructures nationales stratégiques, les entreprises et les marchés financiers mondiaux poursuivent leur transition vers le cloud computing et la connectivité mobile, il est nécessaire d'opter pour une approche de la gestion de la sécurité intégrée et multicouche afin de protéger l'Internet of Everything en plein développement. « Les pirates et les cybercriminels profitent du fait que chaque entreprise du secteur privé ou public dispose de son propre programme de sécurité IT », explique John Stewart. « Oui, nous participons à des conférences et nous restons en contact les uns avec les autres, mais en matière de sécurité IT, nous avons vraiment besoin de passer d'une démarche individuelle à une approche fondée sur une veille en temps réel et une réponse collective. »

Construire une meilleure infrastructure de sécurité ne signifie pas créer une architecture plus complexe, bien au contraire. Il s'agit de faire travailler

Les menaces modernes sont capables d'infecter un vaste public, et ce, silencieusement et efficacement, quel que soit le secteur industriel, la taille de l'entreprise ou le pays.

l'infrastructure et les éléments qui la composent ensemble, avec plus d'intelligence pour détecter et limiter les menaces. Avec l'adoption rapide du phénomène BYOD (apporter son appareil personnel au travail), la réalité qui consiste pour un utilisateur à travailler avec plusieurs appareils, ainsi que la croissance des services cloud, l'ère de la gestion des fonctions de sécurité sur chaque terminal est terminée. « Nous devons adopter une approche holistique de la sécurité qui nous permet de surveiller les menaces sur tous les vecteurs, de l'e-mail à Internet en passant par les utilisateurs eux-mêmes », déclare Michael Covington, gestionnaire produit pour Cisco SIO. « L'intelligence en matière de menace doit être élevée au-dessus des plates-formes individuelles afin d'obtenir une perspective au niveau du réseau. »

Alors que les menaces ciblent de plus en plus les utilisateurs et les organisations à travers différents vecteurs, les entreprises ont besoin de recueillir, stocker et traiter toutes les activités du réseau liées à sécurité afin de mieux comprendre la portée et l'ampleur des attaques.

Le réseau de demain est un réseau intelligent qui doit assurer, par le biais d'une infrastructure de collaboration, une meilleure sécurité que précédemment grâce à la somme de ses composants individuels.

Ce niveau d'analyse peut ensuite être augmenté en fonction du contexte de l'activité du réseau afin de prendre des décisions de sécurité précises et opportunes. Comme les auteurs d'attaque deviennent plus ingénieux, les entreprises doivent concevoir des fonctionnalités de sécurité dans le réseau dès le départ, avec des solutions qui mettent en commun les informations sur les menaces, la politique de sécurité et les contrôles applicables dans tous les points de contact sur le réseau.

À mesure que les pirates deviennent plus ingénieux, les outils utilisés pour contrecarrer leurs efforts doivent également devenir plus sophistiqués. Le réseau fournissant une structure commune pour la communication entre les plates-formes, il servira également de moyen de protéger les appareils, les services et les utilisateurs qui ont l'habitude de l'utiliser pour échanger des contenus sensibles. Le réseau de demain est un réseau intelligent qui doit assurer, par le biais d'une infrastructure de collaboration, une meilleure sécurité que précédemment grâce à la somme de ses composants individuels.

À propos de Cisco Security Intelligence Operations (SIO)

Gérer et sécuriser les réseaux distribués et souples d'aujourd'hui est devenu un défi de plus en plus ardu.

Les cybercriminels en ligne continuent à exploiter la confiance des utilisateurs dans les applications et les appareils grand public, augmentant ainsi le risque pour les entreprises et leurs employés. La sécurité traditionnelle, qui repose sur la superposition des produits et l'utilisation de multiples filtres, ne suffit pas à assurer une protection contre la dernière génération de programmes malveillants qui se répandent rapidement, visent des cibles globales et utilisent de multiples vecteurs pour se propager.

Cisco conserve une longueur d'avance sur les toutes dernières menaces grâce aux capacités d'analyse des menaces en temps réel intégrées de Cisco SIO (Security Intelligence Operations). Cisco SIO est le plus vaste écosystème de sécurité cloud au monde, dans lequel plus de 75 térabits de flux de données en temps réel provenant des solutions Cisco déployées de messagerie électronique, de services Web, de pare-feu et de système de prévention des intrusions (IPS) sont analysés chaque jour.

Cisco SIO regroupe les données de tous les vecteurs de menace et les analyse en utilisant à la fois des algorithmes automatisés et des traitements manuels afin de déterminer les modes de propagation des menaces. Cisco SIO classifie ensuite ces menaces et crée des règles utilisant plus de 200 paramètres. Les chercheurs en sécurité analysent également les informations liées à des événements de sécurité qui pourraient avoir une incidence importante sur les réseaux, les applications et les appareils. Des règles sont transmises de façon dynamique aux dispositifs de sécurité Cisco déployés toutes les trois à cinq minutes.

Cisco SIO représente le plus grand écosystème de sécurité en cloud du monde, dans lequel plus de 75 térabits de flux de données dynamiques de la messagerie électronique Cisco déployée, du Web, du pare-feu, et des solutions IPS sont analysés chaque jour.

L'équipe Cisco SIO publie également des recommandations sur les meilleures pratiques en matière de sécurité, ainsi que des conseils techniques pour repousser les attaques. Cisco s'engage à fournir des solutions de sécurité complètes à la fois intégrées, opportunes, globales et efficaces, offrant ainsi une sécurité holistique à toutes les entreprises à travers le monde. Grâce à Cisco, les entreprises peuvent ainsi consacrer moins de temps à la recherche de menaces et de failles et se concentrer davantage sur une approche proactive de la gestion de la sécurité.

Pour obtenir des informations sur la veille avec alerte précoce, l'analyse des menaces et des vulnérabilités et les solutions éprouvées de limitation des risques de Cisco, visitez le site : **www.cisco.com/security**.

Méthodologie

L'analyse présentée dans ce rapport est fondée sur les données collectées à partir de diverses sources mondiales anonymes, y compris des solutions Cisco de messagerie électronique, de services Web, de pare-feu et de système de prévention des intrusions. Ces plates-formes sont en première ligne pour protéger les réseaux des clients contre les contenus malveillants et les intrus. Outre ces mécanismes de protection du client présents sur site, Cisco recueille également des données à partir d'un déploiement mondial de capteurs dont les fonctions consistent notamment à piéger les courriers indésirables et à parcourir le Web pour rechercher activement de nouveaux types de programmes malveillants.

Grâce à ces outils et aux données recueillies, la gigantesque couverture de réseau de Cisco donne aux systèmes SIO et aux chercheurs un aperçu d'un très grand échantillonnage des activités aussi bien légitimes que malveillantes sur Internet. Aucun fournisseur de sécurité ne dispose d'une visibilité totale de tous les contenus malveillants. Les données présentées dans ce rapport reflètent le point de vue de Cisco sur la situation actuelle du paysage des menaces et montrent nos efforts visant à normaliser les données et à refléter les tendances mondiales basées sur les données disponibles au moment de ce rapport.

Cisco recueille des données à partir d'un déploiement mondial de capteurs dont les fonctions consistent notamment à piéger les courriers indésirables et à parcourir le Web pour rechercher activement de nouveaux types de programmes malveillants.

Cisco Security IntelliShield Alert Manager Service

Le service Cisco Security IntelliShield Alert Manager offre une solution complète et économique, proposant des technologies de veille de sécurité indépendantes des fournisseurs et dont les entreprises ont besoin pour identifier, empêcher et limiter les attaques IT. Ce service d'alertes de menaces et de vulnérabilités personnalisable et basé sur le Web permet au personnel de sécurité d'accéder à des informations opportunes, précises et crédibles concernant les menaces et les vulnérabilités pouvant affecter leurs environnements. IntelliShield Alert Manager permet aux entreprises d'investir moins d'efforts dans la recherche de menaces et de vulnérabilités et de se concentrer davantage sur une approche proactive de la sécurité.

Cisco offre une période d'essai gratuite de 90 jours pour le service Cisco Security IntelliShield Alert Manager. En souscrivant à cette période d'essai, vous bénéficiez d'un accès complet au service, y compris aux outils et aux alertes de menaces et de vulnérabilités.

Pour en savoir plus sur le service Cisco Security IntelliShield Alert Manager, consultez la page : **https://intellishield.cisco.com/security/alertmanager/trialdo?dispatch=4**.

Pour plus d'informations

Service Security Intelligence Operations de Cisco
www.cisco.com/security

Blog sur la sécurité de Cisco
blogs.cisco.com/security

Services de gestion à distance Cisco
www.cisco.com/en/US/products/ps6192/serv_category_home

Produits de sécurité Cisco
www.cisco.com/go/security

La sécurité d'entreprise Cisco Organisation de programmes de sécurité d'entreprise de Cisco
www.cisco.com/go/cspo

[1] « The Internet of Things », de Michael Chui, Markus Löffler et Roger Roberts, *McKinsey Quarterly*, mars 2010 : www.mckinseyquarterly.com/The_Internet_of_Things_2538.

[2] « Cisco Event Response: Distributed Denial of Service Attacks on Financial Institutions », 1 octobre 2012 : www.cisco.com/web/about/security/intelligence/ERP-financial-DDoS.html.

[3] Groupe Cisco Internet Business Solutions.

[4] « The World Market for Internet Connected Devices–2012 Edition », communiqué de presse, IMS Research, 4 octobre 2012 : http://imsresearch.com/press-release/Internet_Connected_Devices_Approaching_10_Billion_to_exceed_28_Billion_by_2020&cat_id=210&type=LatestResearch.

[5] Groupe Cisco Internet Business Solutions.

[6] « Internet of Everything: It's the Connections That Matter », de Dave Evans, Blog Cisco, 29 novembre 2012 : http://blogs.cisco.com/news/internet-of-everything-its-the-connections-that-matter/.

[7] Groupe Cisco Internet Business Solutions.

[8] Rapport annuel 2011 de Cisco sur la sécurité, décembre 2011 : www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf.

[9] « Remote Access and BYOD: Enterprises Working to Find Common Ground with Employees », *Rapport annuel 2011 de Cisco sur la sécurité*, décembre 2011, p. 10 : www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf.

[10] « Cisco Global Cloud Index: Forecast and Methodology, 2011-2016 » : www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud_Index_White_Paper.html.

[11] Ibid

[12] « A Deep Dive Into Hyperjacking », de Dimitri McKay, SecurityWeek, 3 février 2011 : www.securityweek.com/deep-dive-hyperjacking.

[13] India Asks Pakistan to Investigate Root of Panic », de Jim Yardley, The New York Times, 19 août 2012 : www.nytimes.com/2012/08/20/world/asia/india-asks-pakistan-to-help-investigate-root-of-panic.html?_r=1&.

[14] « Twitter Rumor Sparked Oil-Price Spike », de Nicole Friedman, WSJ.com, 6 août 2012 : http://online.wsj.com/article/SB10000872396390444246904577573661207457898.html.

[15] À l'origine, cet article a été publié sur le blog de sécurité Cisco : http://blogs.cisco.com/security/sniffing-out-social-media-disinformation/

[16] Java.com : www.java.com/en/about/.

[17] Vishwath Mohan et Kevin W. Hamlen. *Frankenstein: Stitching Malware from Benign Binaries*. Extrait de Proceedings of the USENIX Workshop on Offensive Technologies (WOOT), p. 77-84, août 2012.

[18] Mohammad M. Masud, Tahseen M. Al-Khateeb, Kevin W. Hamlen, Jing Gao, Latifur Khan, Jiawei Han et Bhavani Thuraisingham. Cloud-based Malware Detection for Evolving Data Streams. ACM Transactions on Management Information Systems (TMIS), 2(3), octobre 2011.

[19] « DDoS Attacks: 2013 Forecast, Experts Say Recent Hits Only the Beginning », de Tracy Kitten, BankInfoSecurity.com, 30 décembre 2012 : http://ffiec.bankinfosecurity.com/ddos-attacks-2013-forecast-a-5396.

[20] « Maliciously Abusing Implementation Flaws in DNS », *DNS Best Practices, Network Protections, and Attack Identification*, Cisco.com : www.cisco.com/web/about/security/intelligence/dns-bcp.html#3.

[21] « IP Spoofing », de Farha Ali, Lander University, disponible sur Cisco.com : www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-4/104_ip-spoofing.html.

[22] « Distributed Denial of Service Attacks », de Charalampos Patrikakis, Michalis Masikos et Olga Zouraraki, Université technique nationale d'Athènes (NTUA), The Internet Protocol Journal - Volume 7, numéro 4. Disponible à l'adresse : www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html.

[23] « DNS Tools », The Measurement Factory: http://dns.measurement-factory.com/tools.

[24] Pour en savoir plus sur les outils DNS, consultez DNS-OARC (https://www.dns-oarc.net/oarc/tools) et The Measurement Factory (http://dns.measurement-factory.com/tools/index.html).

[25] « Secure BIND Template Version 7,3 07 Aug 2012 », de TEAM CYMRU, cymru.com : www.cymru.com/Documents/secure-bind-template.html.

[26] « Response Rate Limiting in the Domain Name System (DNS RRL) », RedBarn.org : www.redbarn.org/dns/ratelimits.

[27] Les données d'Arbor Networks ATLAS sont tirées de « pots de miel » déployés dans les réseaux des fournisseurs de services du monde entier ; des recherches sur les contenus malveillants de l'ASERT ; et d'un flux d'heure en heure de données anonymes basées sur une corrélation SNMP, NetFlow et BGP. Les données anonymes fournies par les clients prestataires de services chez Arbor Peakflow sont collectées et observées par ATLAS pour fournir une vue détaillée des modèles de trafics et de menaces sur Internet.

[28] « IPS Testing », Cisco.com : www.cisco.com/web/about/security/intelligence/cwilliams-ips.html.

[29] « Bank of America and New York Stock Exchange under attack unt [sic] », Pastebin.com, 18 septembre 2012 : http://pastebin.com/mCHia4W5.

[30] « Phase 2 Operation Ababil », Pastebin.com, 18 septembre 2012 : http://pastebin.com/E4f7fmB5.

[31] "Cisco Event Response: Distributed Denial of Service Attacks on Financial Institutions" : www.cisco.com/web/about/security/intelligence/ERP-financial-DDoS.html.

[32] Identifying and Mitigating the Distributed Denial of Service Attacks Targeting Financial Institutions *Applied Mitigation Bulletin* : http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=27115.

[33] « Ressouces techniques SIO (Security Intelligence Operations) », Cisco.com : http://tools.cisco.com/security/center/intelliPapers.x?i=55.

[34] « Service Provider Security Best Practices », Cisco.com : http://tools.cisco.com/security/center/serviceProviders.x?i=76.

[35] Anagramme avec l'aimable autorisation de anagramgenius.com.

[36] Cisco Security Advisories : http://cisco.com/go/psirt.

[37] Cisco Applied Mitigation Bulletins, Cisco.com : http://tools.cisco.com/security/center/searchAIR.x.

[38] Cisco Intellishield Alert Manager Service : www.cisco.com/web/services/portfolio/product-technical-support/intellishield/index.html.

[39] CVRF, ICASI.com : http://www.icasi.org/cvrf.

[40] OVAL, Oval International : http://oval.mitre.org/.