Rapport sur la cybersécurité

1er semestre 2014

Synthèse

Toute cyberattaque, quelle que soit son ampleur, résulte d'un maillon faible dans la chaîne de sécurité. Un maillon faible peut se présenter sous différentes formes : un logiciel obsolète, du code mal écrit, un site web abandonné, des erreurs de développement, un utilisateur à la confiance aveugle... Les adversaires sont déterminés à repérer la moindre faille et à l'exploiter pleinement.

Malheureusement pour les entreprises et les utilisateurs ciblés, les pirates ont vite fait de trouver ces faiblesses. Et, dans l'Internet of Everything en rapide évolution qui se base finalement sur les fondements de la connectivité au cœur de l'Internet des objets, cela ne risque pas de changer. En effet, puisque tout objet connecté à un réseau, de la voiture aux systèmes domotiques, présente une surface exposée exploitable, la tâche des pirates s'en trouvera encore simplifiée.

Les effets des cyberattaques donnent à réfléchir, aussi bien en termes de coûts et de pertes, qu'en termes de productivité et de réputation. Selon le Ponemon Institute, une brèche dans la protection des données coûte, en moyenne, 5,4 millions de dollars en 2014 (contre 4,5 millions en 2013). De plus, dans son rapport sur l'évaluation des coûts associés au cybercrime et au cyberespionnage ***(Estimating the Cost of Cyber Crime and Cyber Espionage),*** le Center for Strategic and International Studies estime, qu'aux États-Unis, ces pratiques représentent un manque à gagner annuel de 100 milliards de dollars pour l'économie et entraîne pas moins de 508 000 pertes d'emploi.[1]

PARTAGER LE RAPPORT SEMESTRIEL 2014 CISCO SUR LA CYBERSÉCURITÉ

Étudier et comprendre le risque

Aller à la section Étudier et comprendre le risque

Notre ***rapport semestriel sur la cybersécurité*** propose une analyse des menaces et des tendances. Les chercheurs de Cisco nous aident à identifier les nombreux types de failles qui existent dans les systèmes que nous utilisons, Internet y compris. En outre, ils nous expliquent comment y remédier afin d'en réduire le nombre et les effets. Principales conclusions :

Dans le cadre du projet « Inside Out » que nous menons actuellement, nous chercheurs ont étudié les requêtes DNS (ou plus précisément sur le processus de recherche de l'adresse IP associée à un nom de domaine) émanant des réseaux d'entreprise de certains de nos clients, en l'occurrence 16 multinationales. Ils ont dressé le constat suivant :

Près de 70 % des réseaux observés émettent des requêtes DNS pour le DNS dynamique (DDNS).

Plus de 90 % des réseaux observés émettent des requêtes DNS d'obtention de noms d'hôtes liés à la diffusion de programmes malveillants.

Plus de 40 % des réseaux observés émettent des requêtes DNS pour des sites et des domaines associés à des appareils fournissant des services tels que : VPN IPsec (Sécurité IP), VPN SSL (Secure Sockets Layer), protocole SSH (Secure Shell), protocole SFTP (Simple File Transfer Protocol), FTP et FTPS (FTP Secure).

Sur les 2 528 alertes publiées entre janvier et juin 2014, 28 ont été identifiées comme des vulnérabilités activement exploitées. Il s'agit de vulnérabilités prioritaires ou urgentes qui doivent être corrigées dans les plus brefs délais.

Même si l'on enregistre une diminution globale en 2013, le volume total de spam augmente à nouveau depuis le mois d'octobre dernier. Toutefois, tous les pays ne sont pas concernés.

Les tendances

Aller à la section sur les tendances

Au premier semestre 2014, le secteur de la chimie et de l'industrie pharmaceutique, qui est très rentable, se classe à nouveau dans le Top 3 des secteurs présentant un risque élevé d'attaques par programmes malveillants sur le web.

Le secteur de la presse et de l'édition a également enregistré un taux sensiblement plus élevé d'attaques par programmes malveillants sur le web, comparé aux observations précédentes.

2014 semble être une année active en matière d'attaques par déni de services (DDoS) via le protocole Network Time Protocol (NTP). L'une des attaques avec amplification NTP les plus importantes a été observée au cours du premier semestre 2014. Elle visait un client du fournisseur mondial de services DNS CloudFlare. En février, au plus fort de l'attaque, le trafic UDP (User Datagram Protocol) atteignait près de 400 Gbit/s.

Selon nos chercheurs, le nombre de kits d'exploits a chuté de 87 % depuis que le supposé créateur du très célèbre kit d'exploits Blackhole a été arrêté, en 2013.

Plusieurs kits d'exploits observés durant le premier semestre 2014 ont tenté de s'imposer sur le territoire autrefois dominé par le kit d'exploits Blackhole. Cependant, aucun véritable leader ne s'est encore démarqué.

Si les exploits visant les points de vente ont de plus en plus la cote auprès des cybercriminels, c'est pour plusieurs raisons :

Les terminaux de paiement étant de plus en plus souvent connectés à Internet, les criminels disposent d'un point d'accès aux réseaux d'entreprise.

En effet, de nombreuses entreprises ne sont pas conscientes du fait que les données relatives aux cartes de paiement sont des données sensibles et ne garantissent pas un niveau de sécurité suffisant.

Elles ont de plus en plus souvent recours à des fournisseurs pour la totalité ou une partie de leurs solutions de paiement, ce qui offre encore d'autres points d'entrée aux criminels.

Perspectives

Aller à la sections Perspectives

Les risques que l'Internet des objets est susceptible d'engendrer sur le plan de la sécurité et la raison pour laquelle les entreprises devraient adopter une approche proactive pour s'en protéger.

L'importance de l'utilisation de l'analytique prédictive et de l'apprentissage automatique dans l'identification des menaces difficiles à détecter sur le réseau.

La tendance, au sein des entreprises, à considérer la cybersécurité à la fois comme un risque stratégique et un processus métier.

Le besoin en solutions basées sur les plates-formes et axées sur la visibilité et les menaces qui couvrent toute la période englobant l'attaque (avant, pendant et après celle-ci) aident à combler les failles dans les systèmes de sécurité et réduisent la complexité inhérente à la disparité des produits.

Table des matières

Ce document contient des éléments qui peuvent être consultés et partagés.

Cliquez pour accéder à la fonctionnalité Rechercher dans Adobe Acrobat

Partager du contenu par e-mail ou via les médias sociaux

Logiciels recommandés :

Adobe Acrobat Version 7.0 et plus récente

L'Internet des objets : les nouvelles opportunités et les risques qui en découlent

Les analystes et visionnaires spécialistes des technologies définissent l'Internet des objets comme le réseau d'objets physiques auxquels on accède via Internet. Ces objets sont dotés d'une technologie intégrée qui leur permet d'interagir en fonction des états internes ou de l'environnement externe. En d'autres termes, le fait que les objets puissent capter et communiquer impacte la prise de décision dans son ensemble (comment, où et qui).[2]

Selon Cisco, l'Internet des objets devrait compter jusqu'à 50 milliards d'objets d'ici 2020.[3] Son impact sur la sécurité est déjà visible, car il accroît de manière exponentielle la taille de la surface exposée. Avec l'Internet des objets, la protection et la détection continues et généralisées ont davantage d'importance, les personnes, les processus et les données étant tous de plus en plus connectés.

Dans ce monde en constante évolution où l'informatique omniprésente et l'interactivité extrême sont les maîtres mots, tout objet connecté à un réseau présente une surface exposée que les pirates peuvent exploiter. Et même si leurs actions ne *sont encore* que pures spéculations, une chose est certaine : ils ont des projets, ils testent leurs idées et certains ont déjà réussi quelques attaques.

Les voitures, les appareils médicaux et même les interphones bébé ont tous récemment été la cible des pirates de l'Internet des objets, qui se consacrent maintenant à la recherche et au développement dans ce domaine.[4-6]

L'objectif ultime de l'Internet des objets est d'accroître l'efficacité opérationnelle, d'inspirer de nouveaux modèles commerciaux et d'améliorer la qualité de la vie. En connectant les objets du quotidien et en les intégrant dans un même réseau, nous profitons de leur capacité à combiner de simples données pour générer des informations utilisables. Cela signifie également que, potentiellement, une proportion bien plus importante d'informations personnelles et professionnelles seront stockées dans le cloud et y transiteront. Cette évolution implique la nécessité d'appliquer des mesures de sécurité adéquates destinées à protéger les données et d'élaborer des politiques de confidentialité visant à réglementer l'utilisation des données.

Dans le monde de l'Internet des objets, la confidentialité est une préoccupation de premier ordre. Et même si les utilisateurs prennent les précautions nécessaires pour sécuriser leurs informations et sont généralement plus méfiants, ils restent cependant vulnérables aux risques engendrés par des maillons faibles de la chaîne de sécurité indépendants de leur contrôle (voir la section La sécurité compromise des connexions cryptées, page 29). Lorsqu'un cybercriminel arrive au stade où il peut recouper des informations issues de différentes sources, par exemple d'un véhicule, d'un smartphone ou d'un système domotique, il possède alors des informations bien plus précises sur l'utilisateur que s'il exploitait les données d'un appareil, d'un système ou d'une application unique. Ces informations détaillées sur les utilisateurs, qu'elles portent sur leurs habitudes d'achat ou leur localisation géographique, permettent aux cybercriminels de lancer habilement des campagnes très ciblées et d'un niveau de sophistication jamais égalé.

Il peut sembler difficile à imaginer pour certains qu'un appareil portable aussi anodin qu'un moniteur d'activité physique ou qu'un système d'enregistrement vidéo puisse constituer un risque important ou susciter l'intérêt d'un pirate. Toutefois, puisque les systèmes embarqués pour voitures et autres appareils non standard s'apparentent de plus en plus aux plates-formes informatiques standard, ils sont potentiellement vulnérables aux mêmes menaces[7] que celles qui touchent les appareils standard.

Les plus grands fournisseurs du secteur connaissent bien les problèmes de sécurité susceptibles d'affecter les appareils de l'Internet des objets. Ils s'appuient donc sur leurs connaissances et sur leur expérience pour intégrer des fonctionnalités de sécurité dans l'architecture même de leurs produits. Les entreprises nouvelles doivent tenir compte des leçons apprises au cours des 20 dernières années par les acteurs du secteur de la cybersécurité pour ne pas reproduire les mêmes erreurs au fur et à mesure qu'elles innovent. La plupart des bonnes pratiques applicables à l'informatique générale s'appliquent également aux appareils de l'Internet des objets : par exemple, toujours installer la version la plus récente d'un logiciel. Mais dans le monde de l'Internet of Everything vers lequel nous conduit l'Internet des objets, la sécurité sera gérée en grande majorité par des systèmes et non par des utilisateurs. Et ce paramètre devra être pris en compte au moment de concevoir les technologies de sécurité spécifiques à ce nouvel environnement. Cela implique notamment de fournir un maximum de transparence aux utilisateurs afin qu'ils aient la garantie que la sécurité de leurs appareils de l'Internet des objets est gérée automatiquement ou qu'ils sachent à quel moment une action manuelle de leur part est nécessaire.

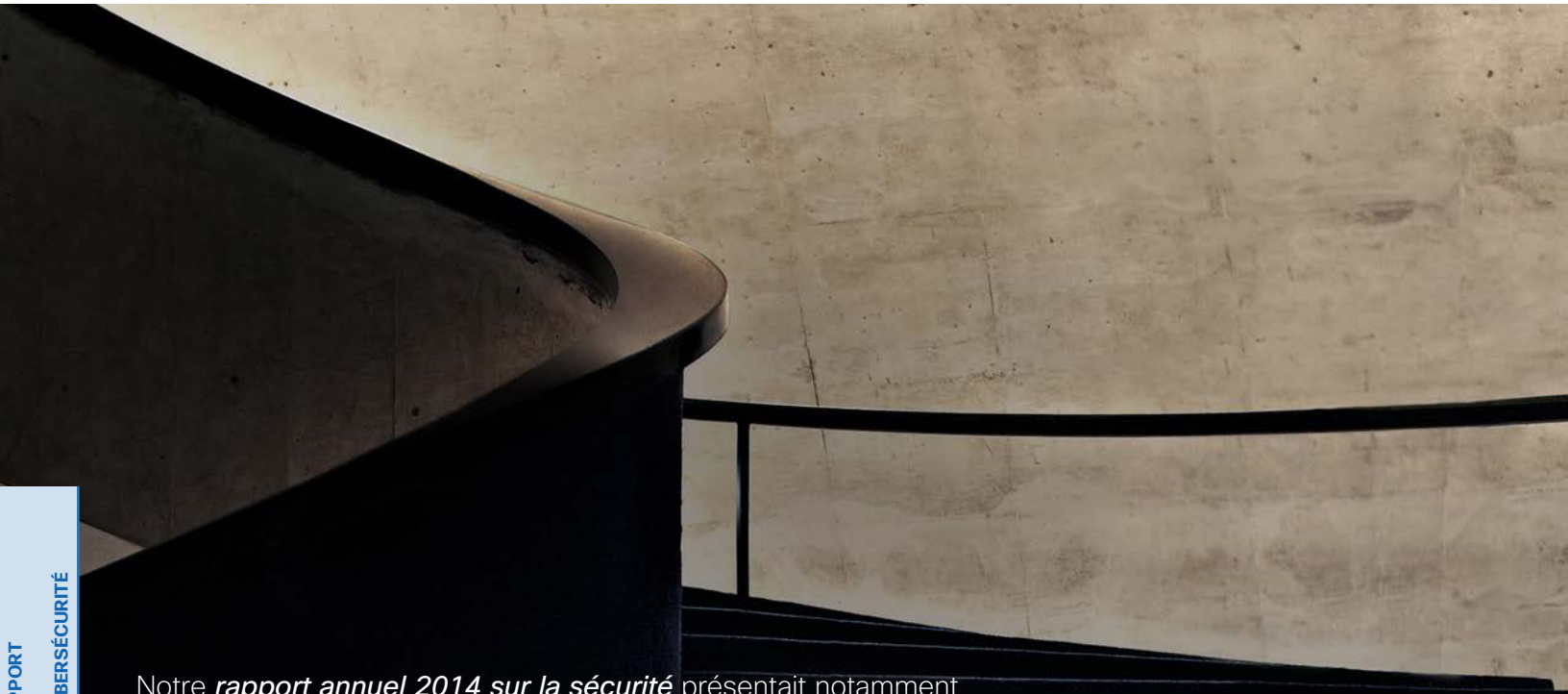
Le nombre de nouveaux appareils connectés ne cessera de croître, tout comme le nombre d'appareils connectés laissés à l'abandon et non gérés. À l'instar du nombre incalculable de sites web oubliés ou laissés à l'abandon (voir Vulnérabilités WordPress : qui est aux commandes ?, page 37), ces appareils, qui vont de l'électroménager, aux caméras de surveillance en passant par les imprimantes personnelles, constituent des maillons faibles de la chaîne de sécurité. Pour les hackers entreprenants, ils sont autant de portes franchissables qui peuvent mener tout droit au datacenter auxquels ils sont connectés.

Les capacités et les motivations des cybercriminels sont bien connues, et leur intérêt croissant pour l'Internet des objets s'inscrit dans une évolution naturelle. À la différence de l'époque où naissait Internet, nous avons du recul. Nous savons déjà par expérience que l'Internet des objets est source de risques et que des attaques cibleront les entreprises et les utilisateurs. Le plus grand risque, à l'heure actuelle, est de sous-estimer la virulence des attaques et la vitesse à laquelle l'environnement de l'Internet des objets et le monde de l'Internet of Everything se développent.

Étudier et comprendre le risque

Nos chercheurs ont analysé l'ensemble des données de sécurité collectées au cours du premier semestre 2014, ensemble le plus vaste jamais exploité. Nos experts travaillent sans relâche sur les menaces nouvelles, comme le trafic de programmes malveillants. Leurs analyses permettent d'avoir une indication du comportement à venir des cybercriminels et aident à détecter les menaces.

La mutation des menaces : lorsque le risque vient de l'intérieur



Notre ***rapport annuel 2014 sur la sécurité*** présentait notamment les conclusions d'un projet mené par nos experts et intitulé « Inside Out ». Son but était d'examiner les résolutions DNS provenant de l'intérieur des réseaux d'entreprise.[8]

Nos spécialistes ont découvert que du trafic malveillant était présent dans 100 % des réseaux analysés.[9]

D'après leurs observations, les chercheurs ont pu établir que les réseaux d'entreprise du groupe étudié avaient certainement été infiltrés depuis un certain temps et que l'infiltration première n'avait pas été détectée.

Dans ce rapport, nous présentons d'autres conclusions du projet « Inside Out ». Ces informations sont basées sur l'analyse des données collectées sur une sélection de réseaux de clients depuis le début de l'année 2014. Nos spécialistes ont examiné en détail les réseaux de 16 multinationales qui, à elles toutes, ont géré plus de 4 000 milliards de dollars d'actifs et généré un chiffre d'affaires supérieur à 300 milliards de dollars en 2013. Cette analyse a permis de mettre en lumière trois points essentiels qui ont montré un lien entre ces géants mondiaux et le trafic malveillant.

Requêtes DDNS

La menace

Le DDNS (Dynamic DNS) est un système habituellement utilisé à des fins légitimes, plus spécifiquement par les particuliers qui doivent pouvoir convertir un nom de domaine complet (FQDN) statique, serveuraccueil.fai.com par exemple, en un nombre ou un groupe d'adresses IP attribués de façon dynamique par leur fournisseur de services Internet (FAI).

Malheureusement, à l'instar de nombreuses technologies et de fonctionnalités conçues au départ à des fins légitimes, le DDNS est très prisé des pirates informatiques, car il permet à des mécanismes d'attaque tels que les botnets d'échapper à la détection et à la destruction. Des volumes inhabituellement élevés de requêtes de domaines émises via des fournisseurs de services DDNS, nom-services.com par exemple, peuvent être le signe d'une compromission d'un réseau d'entreprise. Même si la plupart et parfois la totalité des requêtes de fournisseurs DDNS d'une entreprise sont légitimes, il est indispensable de les valider afin de confirmer leur légitimité.

Conclusions

Près de 70 % (66,67 % pour être exact) de requêtes client observées en 2014 dans le cadre du projet « Inside Out » émettaient des requêtes DNS pour des services DDNS. (Remarque : selon nos spécialistes, ce pourcentage devrait augmenter au fur et à mesure que le nombre de réseaux analysés s'accroît. Cisco vient juste de classer cette nouvelle catégorie en tant qu'indicateur de compromission [IOC, indicator of compromise]. L'IOC désigne un événement ou un élément, souvent subtil, qui lorsqu'il est corrélé avec d'autres IOC sur un même système, indique une probable compromission.) Comme nous l'avons déjà évoqué, cela ne signifie en aucun cas que tous ces clients ont été la cible de logiciels malveillants utilisant des fournisseurs DDNS. Toutefois, Cisco a recommandé à ces clients d'analyser plus en détail les requêtes DDNS pour s'assurer qu'elles étaient réellement utilisées à des fins professionnelles.

Requêtes de sites associés à des programmes malveillants MiTB

La menace

Palevo, SpyEye et Zeus appartiennent à une famille de programmes malveillants qui intègre une fonctionnalité MiTB (man-in-the-browser). Les recherches DNS portant sur des hôtes compromis par Palevo, Zeus et SpyEye présentent un risque sérieux. Ces botnets se propagent via la messagerie instantanée, les réseaux peer-to-peer (P2P) et les médias amovibles. Ils sont utilisés pour des attaques par déni de service distribué (DDoS) visant à voler des informations à l'instant même où elles sont saisies dans des formulaires. Palevo, Zeus et SpyEye revêtent une importance particulière, car ils sont spécifiques d'une classe de programmes malveillants qui ciblent notamment les informations financières saisies dans des formulaires en ligne à partir de navigateurs fonctionnant sous Windows.

Conclusions

Sur plus de 90 % (93,75 %) des réseaux observés en 2014, des redirections vers des sites web hébergeant des programmes malveillants ont été détectées. Il a été notamment établi que ces réseaux émettent des requêtes DNS pour des noms d'hôtes dont l'adresse IP de résolution est considérée comme vecteur des malwares Palevo, Zeus ou SpyEye ou infectée par ces derniers.

Requêtes DNS d'obtention de noms de domaine complet, de sites et d'hôtes associés à des protocoles administratifs

La menace

Des entités malveillantes peuvent utiliser des canaux de communication ou des protocoles de transfert de données sécurisés et cryptés pour couvrir leurs traces lorsqu'ils volent des informations, comme les VPN Ipsec (IP Security) et SSL (Secure Sockets Layer) et les protocoles SSH (Secure Shell), SFTP (Simple File Transfer Protocol), FTP et FTPS (FTP Secure). Les entreprises doivent par conséquent contrôler et valider régulièrement ces communications. Couverts par ces canaux, les cybercriminels peuvent exfiltrer les données sur les sites piégés sans être détectés.

Conclusions

Plus de 40 % (43,75 %) des réseaux de clients observés en 2014 émettent des requêtes DNS vers des sites et des domaines associés à des appareils fournissant des services impliquant notamment VPN IPsec et SSL et les protocoles SSH, SFTP, FTP et FTPS.

Nos chercheurs ont établi un instantané des vulnérabilités et des compromissions possibles des données à partir des recherches DNS émanant de réseaux d'entreprise. Nos experts en cybersécurité ont analysé les informations issues de listes de blocage et ont observé des tendances dans les compromissions de systèmes informatiques, les vulnérabilités visant des secteurs d'activité spécifiques, et les facteurs géopolitiques pouvant nuire aux acteurs concernés et altérer les informations ciblées. Nous remettons aux clients qui participent au projet Inside Out un *rapport sur les cybermenaces externes*.

Les tendances géopolitiques à surveiller

Selon nos experts en cybersécurité, les événements géopolitiques en Europe orientale et au Proche-Orient sont à l'origine de nouvelles cybertendances qui accroissent les risques pour les entreprises, les gouvernements et autres organisations, sans oublier les utilisateurs, et ce, partout dans le monde :

L'instabilité politique en Ukraine a entraîné une série d'attaques par déni de service distribué (DDoS) et de défigurations de sites web apparemment calculées pour soutenir les actions sur le terrain. Les troubles en Crimée et à Kiev ont dévoilé des activités d'espionnage sophistiquées sur les réseaux ukrainiens au moyen de programmes malveillants (appelés Ouroboros ou Snake), qui sévissait déjà depuis des mois voire des années.

Au Proche-Orient, la prise de secteurs entiers du nord et de l'ouest de l'Irak par l'État islamique en Irak et au Levant (EIIL) est accompagnée d'une campagne sur les médias sociaux prônant des opérations de sabotage et la guerre psychologique.

L'avenir est incertain. Les profondes divisions ethniques et religieuses s'accroissent dans une partie du monde qui est déjà à la pointe dans l'utilisation de cyberattaques commanditées ou non par un état. Au second semestre 2014, des élections présidentielles tendues en Turquie et les élections de mi-mandat aux États-Unis, ainsi que le retrait prévu des forces militaires en Afghanistan, risquent d'avoir des répercussions sur le cyberespace mondial.

PARTAGER LE RAPPORT SEMESTRIEL 2014 CISCO SUR LA CYBERSÉCURITÉ

Exploitation de failles sur le web : Java toujours en tête

Les attaques qui exploitent le langage de programmation Java restent majoritaires selon les indicateurs de compromission surveillés par Cisco® FireAMP, la solution avancée de détection de programmes malveillants. Au cours du premier semestre 2014, ces attaques ont continué à progresser à un rythme impossible à maîtriser.

PARTAGER LE RAPPORT SEMESTRIEL 2014 CISCO SUR LA CYBERSÉCURITÉ

FIGURE 1

Répartition des compromissions d'applications, premier semestre 2014

SOURCE : Cisco® FireAMP[10]

Les exploitations de failles Java totalisaient 91 % des IOC en novembre 2013, selon le ***rapport annuel 2014 Cisco sur la cybersécurité.*** Ce chiffre a légèrement augmenté pour atteindre 93 % en mai 2014. Ces attaques sont particulièrement prisées des cybercriminels en raison de leur retour sur investissement élevé et de l'ubiquité du langage Java. (Pour plus d'informations sur les problèmes liés à Java et pour obtenir des conseils pour y remédier, consultez notre ***rapport annuel 2014 sur la cybersécurité***[11]***).***

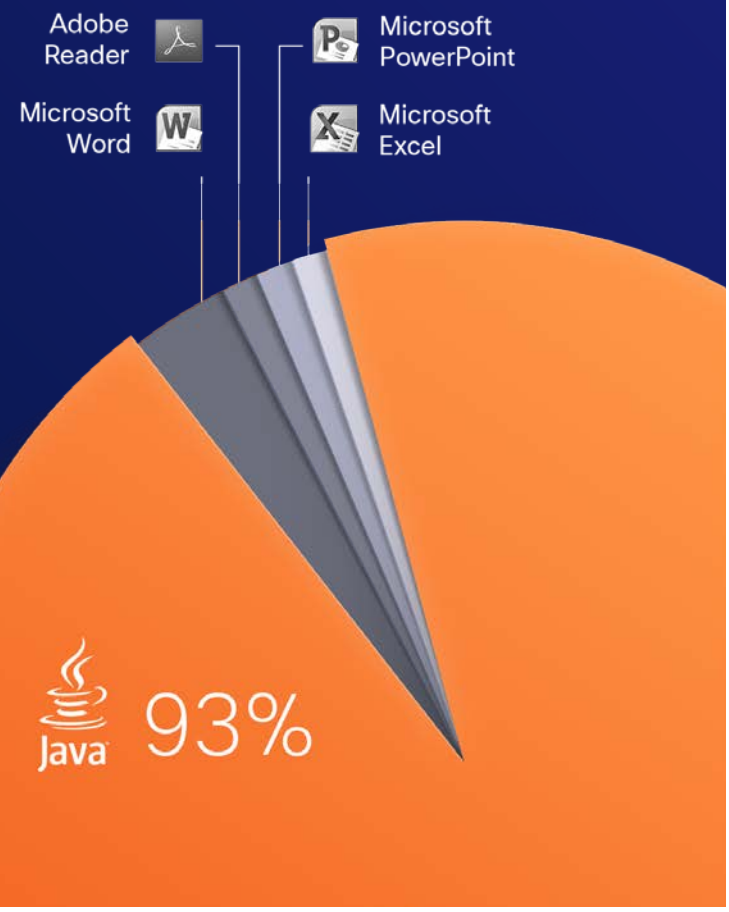


FIGURE 2

Détections de programmes malveillants exploitant Java sur le web (janvier-mai 2014)

SOURCE : Cisco Cloud Web Security

Les programmes malveillants exploitant Java sur le web représentaient, en mars 2014, 10 % de l'ensemble des programmes malveillants détectés sur le web.

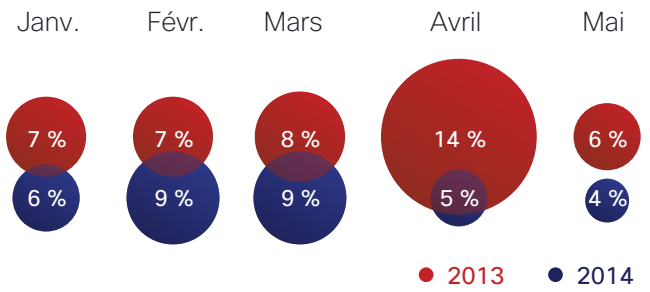


FIGURE 3

Exploitations de failles Java, PDF et Flash détectées (janvier-mai 2014)

SOURCE : Cisco Cloud Web Security

Java, Flash et Adobe PDF sont les principaux vecteurs utilisés par les cybercriminels.

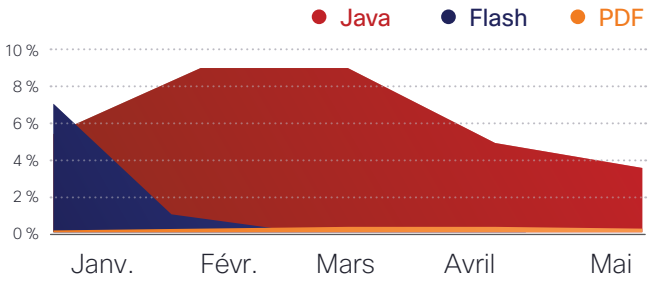
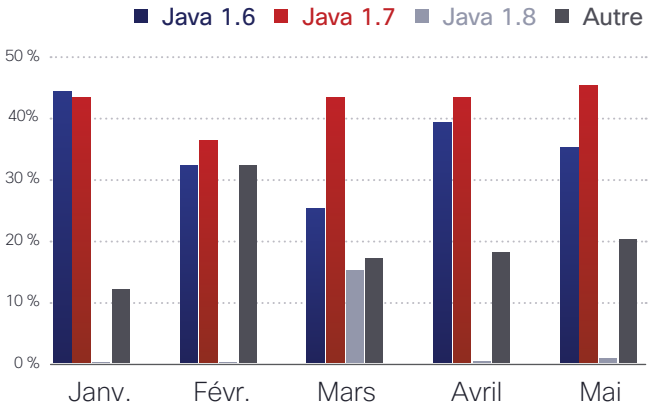


FIGURE 4

Détection d'attaques Java par version (janvier-mai 2014)

SOURCE : Cisco Cloud Web Security

Les cybercriminels continuent à exploiter avec succès les anciennes versions de Java, en particulier Java 6 et 7. Mars a connu un pic de détections d'attaques par programmes malveillants avec Java 8, c'est-à-dire lors de la sortie de la nouvelle version de Java. Cependant, les attaques exploitant Java 8 ont considérablement baissé dès le mois d'avril et sont restées à un faible niveau en mai. Avec l'augmentation des kits d'exploits qui ont recours principalement à d'autres vecteurs que Java, notamment Microsoft Silverlight, il semble que les cybercriminels abandonnent Java 8 (qui dispose de contrôles de sécurité plus efficaces) pour se tourner vers d'autres logiciels plus propices aux attaques.



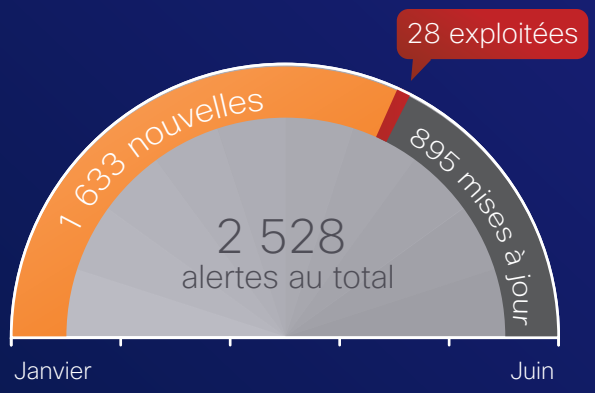
Les vulnérabilités : les exploits les plus courants

FIGURE 5

Statistiques relatives aux alertes (janvier-juin 2014)

SOURCE : Cisco Intellishield®

Du 1er janvier 2014 au 30 juin 2014, Cisco a publié des milliers d'alertes sur les vulnérabilités connues qui lui ont été communiquées par divers fournisseurs. Bien que ce chiffre soit impressionnant, les vulnérabilités les plus critiques représentent seulement 1 % de toutes les alertes enregistrées. Sur les 2 528 nouvelles alertes répertoriées au cours de cette même période, 28 vulnérabilités seulement ont été activement exploitées peu de temps après la publication des rapports, selon notre étude.



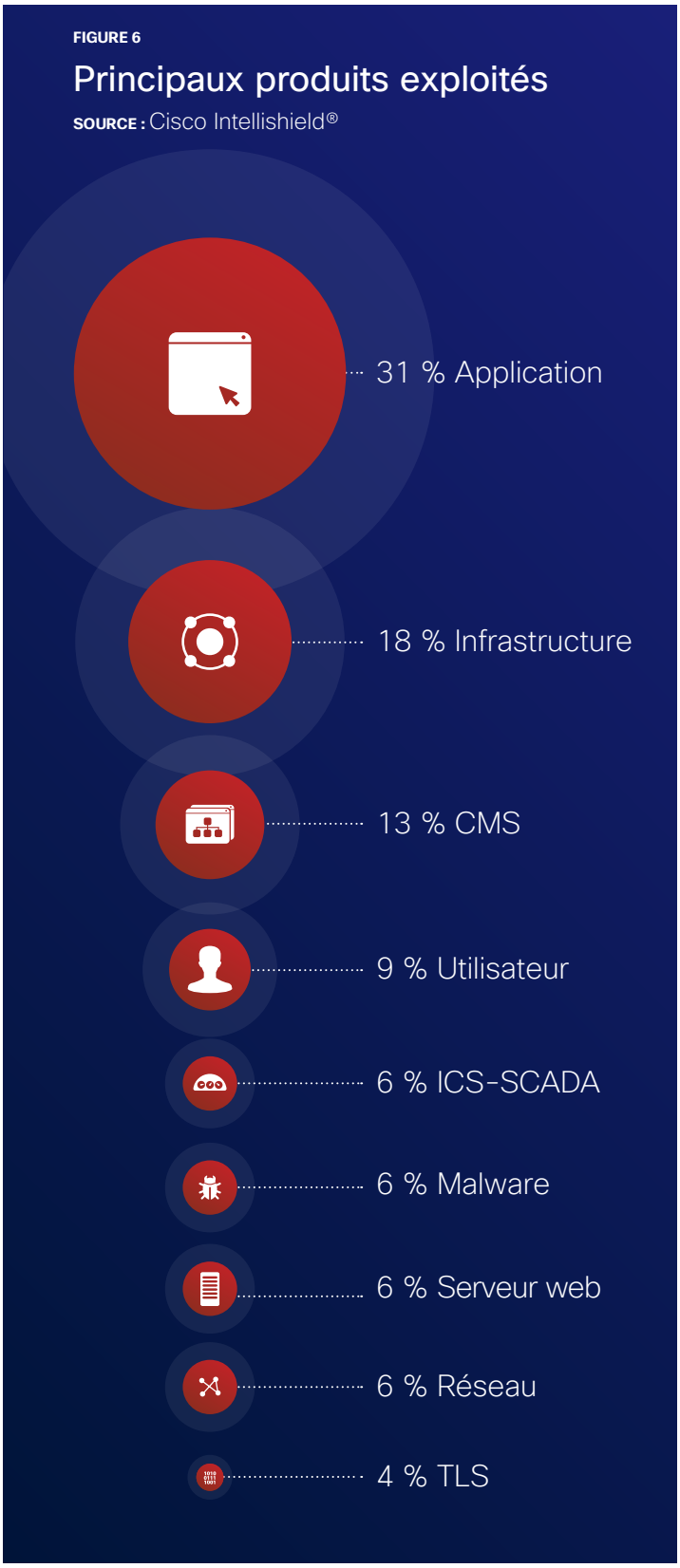
Les cybercriminels visent les vulnérabilités courantes ou « maillons faibles » qu'ils sont capables d'exploiter facilement après une phase de « recherche et de développement » efficace. Les exploits qui sont parvenus à leurs fins sont ensuite incorporés à des kits d'exploits vendus dans l'économie souterraine. Les plus populaires contiennent notamment des programmes malveillants exploitant les langages de programmation Java et Silverlight. (Voir les sections Exploitation de failles sur le web : Java toujours en tête à la page 15 et Kits d'exploits : l'ouverture à la concurrence à la page 33.)

Sur la base des rapports sur les vulnérabilités publiés, les professionnels de la cybersécurité et la presse spécialisée soulignent l'importance des vulnérabilités de type « zero-day », car il semble urgent d'apporter une réponse à cette menace critique. Cependant, les entreprises doivent lutter en priorité contre les quelques vulnérabilités que les cybercriminels exploitent le plus. Un plus grand nombre de processus de routine peuvent suffire pour remédier à d'autres vulnérabilités.

FIGURE 6

Principaux produits exploités

SOURCE : Cisco Intellishield®



Les entreprises doivent donc disposer d'un « processus d'application de correctifs d'urgence » fonctionnant en association avec leurs processus d'application de correctifs habituels. En remédiant rapidement aux vulnérabilités les plus urgentes, les autres vulnérabilités peuvent être intégrées dans le processus d'application de correctifs et de maintenance activé régulièrement. La gestion des risques est par conséquent plus performante. Cette approche est en effet plus efficace que de tenter d'installer tous les correctifs ou de ne les installer seulement que lors des périodes de maintenance planifiées. Pour que les correctifs d'urgence soient efficaces, il faut disposer d'informations fiables sur les menaces les plus urgentes.

La Figure 6 montre les principaux produits que les cybercriminels ont exploités au cours du premier trimestre de 2014. La Figure 7 décrit certaines des vulnérabilités les plus souvent exploitées, selon le système d'évaluation standardisé de la criticité des vulnérabilités CVSS (Common Vulnerability Scoring System).

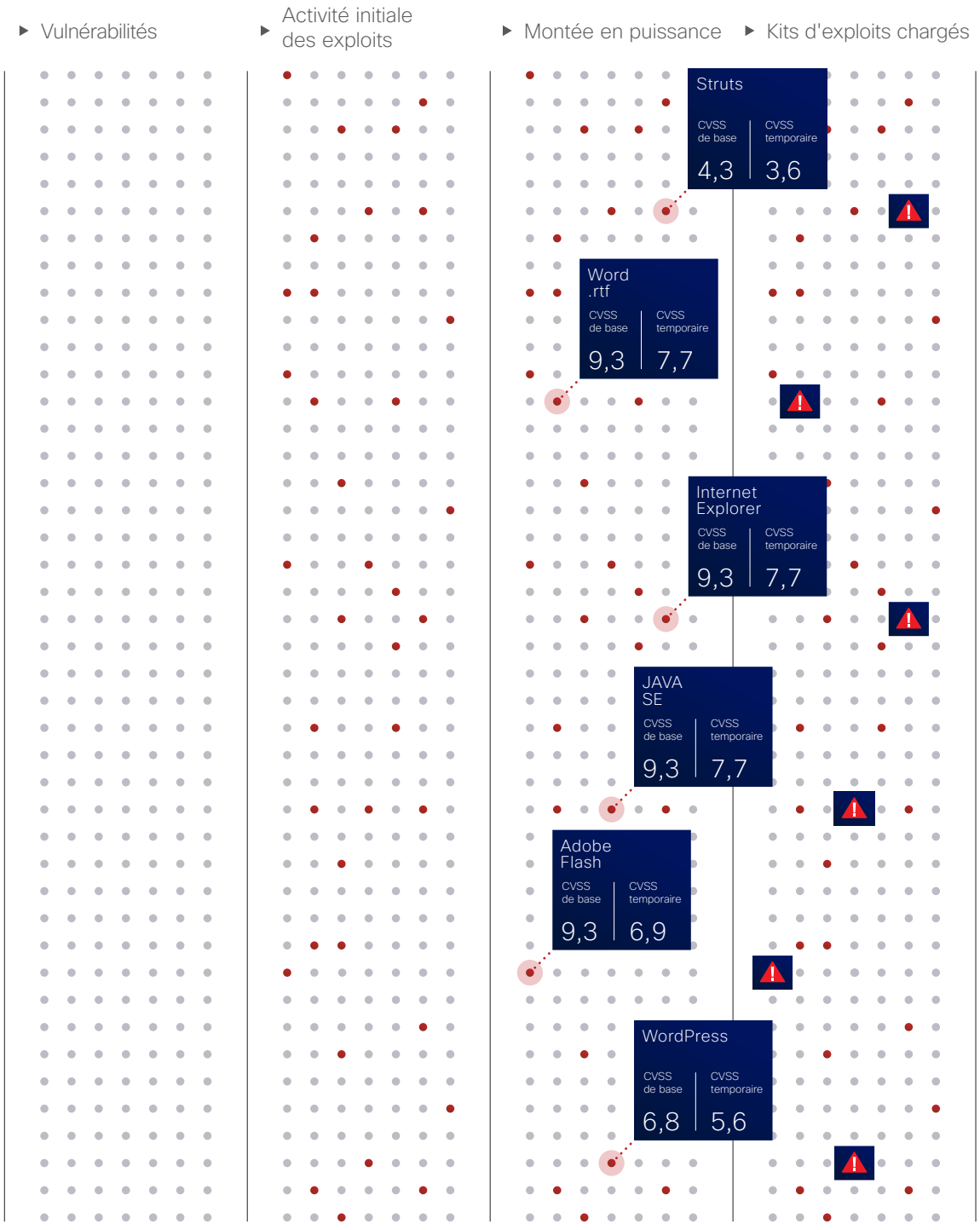
Le score « Urgence » dans le graphique CVSS est utile, car il indique que ces vulnérabilités sont activement exploitées, ce qui correspond aux scores « Temporel » indiquant des exploits actifs. En outre, en analysant la liste des produits exploités, les entreprises peuvent déterminer quels produits utilisés doivent être surveillés et faire l'objet de correctifs.

Notons que les vulnérabilités illustrées à la Figure 7 sont celles montrant des signes d'activité malveillante au cours de la période observée. La majorité de ces vulnérabilités n'ont pas encore été diffusées dans l'économie souterraine, c'est-à-dire qu'elles n'ont pas été intégrées dans les kits d'exploits à la vente.

FIGURE 7

Vulnérabilités les plus souvent exploitées

SOURCE : Cisco Intellishield®



Heartbleed n'est pas la seule cause d'inquiétude

Certaines entreprises n'ont pas été exposées à Heartbleed, une vulnérabilité logicielle présente dans la bibliothèque de cryptographie OpenSSL, car elles utilisaient une ancienne version de OpenSSL exempte de cette vulnérabilité.[12] La vulnérabilité permet d'exploiter une implémentation de l'extension TLS (Transport Layer Security) (RFC6520) heartbeat et de récupérer des clés privés ou des d'informations confidentielles lors de communications cryptées avec le protocole TLS.[13]

Cependant, ces entreprises doivent tenir compte du fait qu'entre janvier et avril 2014, il a été établi que 16 vulnérabilités TLS et de validation de certificat *n'étaient* pas liées à Heartbleed.

Ces vulnérabilités peuvent les exposer à des risques. Nos experts en cybersécurité conseillent également à tous les utilisateurs d'agir comme s'ils avaient été exposés à Heartbleed, et de prendre les mesures qui conviennent, à savoir modifier leurs mots de passe ou fermer leurs comptes Internet.[14]

Depuis la découverte de Heartbleed, d'autres failles dans le logiciel OpenSSL ont été découvertes par le projet OpenSSL (OpenSSL.org). Certaines d'entre elles peuvent permettre à un cybercriminel de créer une condition de déni de service, ou dans certains cas, d'empêcher l'exécution du code de ce logiciel.[15] Certaines de ces failles ont été longtemps négligées : par exemple, la vulnérabilité dite d'injection CCS, découverte par un spécialiste de la cybersécurité au Japon, est une faille de sécurité qui existe depuis 16 ans dans le logiciel OpenSSL. Elle permet à un cybercriminel d'intercepter et de décrypter les données cryptées transitant sur Internet.[16]

Le rapport sur les risques par secteur : une augmentation inhabituelle pour certains secteurs

Au cours du premier semestre 2014, l'industrie pharmaceutique et chimique, un secteur générant de gros profits, figure une fois de plus parmi les trois secteurs les plus touchés par des programmes malveillants. Il était n° 1 en 2013.[17] L'industrie aéronautique figure également dans les cinq secteurs les plus touchés, à la troisième place.[18] Cela n'est pas surprenant étant donné la valeur de la propriété intellectuelle détenues par les entreprises aéronautiques.

Le secteur de la presse et de l'édition occupe la première place du podium. Il enregistre un nombre plus élevé que la normale de détections d'attaques par programmes malveillants sur le web par rapport à la tendance observée précédemment par nos spécialistes en cybersécurité qui compilent ces données depuis 2008.

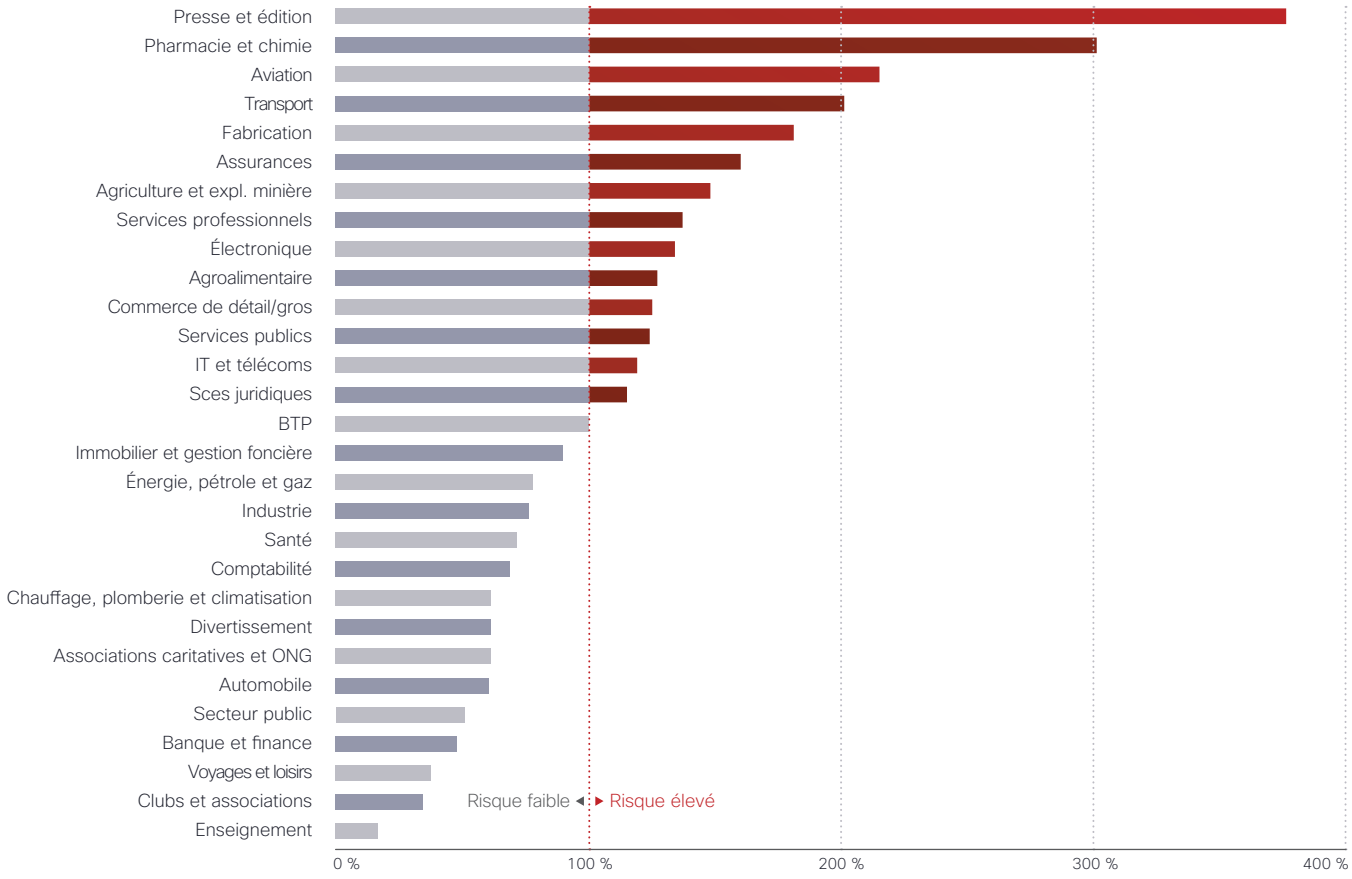
L'augmentation des attaques détectées dans le secteur de la presse et de l'édition est probablement due aux exploits et tentatives d'escroquerie réalisés par des cybercriminels qui profitent d'événements importants tels que les Jeux olympiques d'hiver de Sotchi ou les Oscars, et des faits marquants de l'actualité, comme le mystère du vol 370 de la Malaysia Airlines ou l'accident du ferry en Corée du Sud. Leurs escroqueries sont conçues de manière à cibler le « maillon faible » humain, c'est-à-dire les utilisateurs qui, attirés par les gros titres, sont redirigés en quelques clics vers des sites hébergeant des programmes malveillants.

Les sites de presse et d'édition, quelle que soit leur taille, peuvent attirer un nombre important de visiteurs du monde entier, et ce, aussi bien le grand public que des entreprises. En outre, ils tirent leurs profits en grande partie de la publicité. Pour cette raison, il est probable que les publicités frauduleuses soient en partie responsables de l'augmentation des attaques par des programmes malveillants sur le web dans le secteur de la presse et de l'édition au cours du premier semestre de 2014. (Voir Publicités frauduleuses : un perturbateur de la cyberéconomie, page 35.)

FIGURE 8

Risques présentés par les programmes malveillants sur le web par secteur, premier semestre 2014

SOURCE : Cisco Cloud Web Security



Pour déterminer la fréquence des détections de programmes malveillants propres à un secteur, les spécialistes de la cybersécurité de Cisco comparent le taux de fréquence moyen pour toutes les entreprises qui ont recours au service Cisco Cloud Web Security au taux de fréquence médian pour toutes les entreprises d'un secteur donné qui ont recours à ce même service. Une fréquence supérieure à 100 % pour un secteur témoigne d'un risque supérieur à la normale de détection de programmes malveillants transmis sur le web, tandis qu'un taux inférieur à 100 % indique un risque moindre. Par exemple, une entreprise qui présente une fréquence de 170 % est exposée à 70 % de risques en plus que la valeur médiane. À l'inverse, une entreprise dont la fréquence est de 70 % est exposée à 30 % de risques en moins que la médiane.

Détection de programmes malveillants par région

Pour la première fois, nos spécialistes de la cybersécurité présentent des données relatives aux détections de programmes malveillants par secteur d'activité et selon la région. Les trois régions en question sont AMER (Amérique du Nord, Amérique centrale et Amérique latine), APJC (Asie-Pacifique, Chine, Japon et Inde) et EMEAR (Afrique, Europe et Proche-Orient).

Dans la zone AMER (voir Figure 9), l'aéronautique est nettement plus exposée aux détections de programmes web malveillants que les autres secteurs.

Le PIB a une influence sur les risques par secteur d'une région. En règle générale, plus les biens, les services ou la propriété intellectuelle ont de la valeur, plus le risque de détections y est élevé.

Un secteur spécifique peut également être sous-représenté dans les zones où il est peu développé. C'est une raison pour laquelle le risque « de la fourche à la fourchette » touche traditionnellement les entreprises des secteurs agricoles, agroalimentaires et des transports. C'est probablement également la raison pour laquelle le secteur de l'agroalimentaire a connu le plus grand nombre de détections de programmes web malveillants dans la zone EMEAR. Les épisodes de sécheresse et d'inondation ainsi que l'agitation politique que cette région a récemment connus ont mis à mal les infrastructures et ont entraîné des pénuries de ressources de base.

Détection et compromission

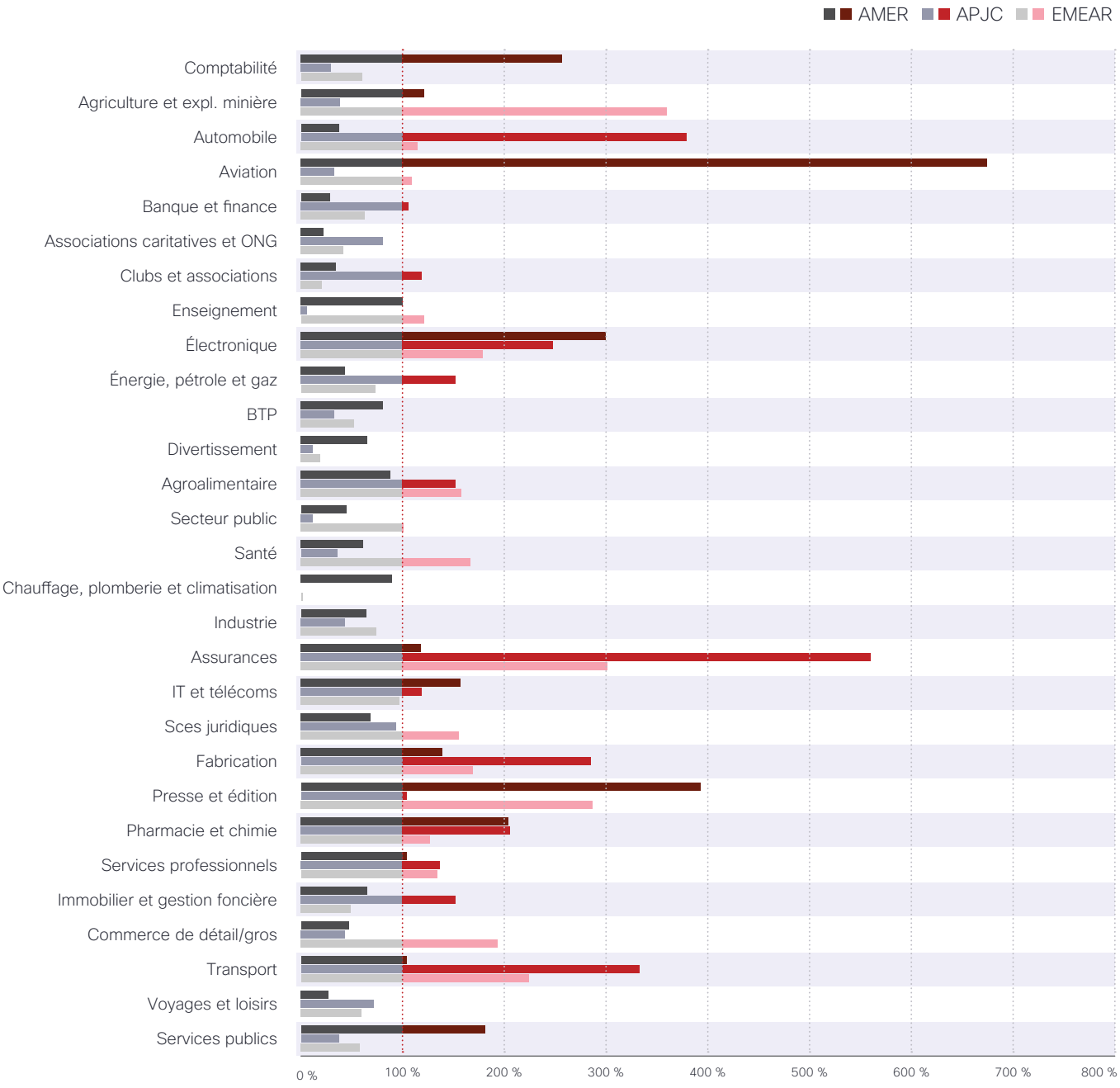
Une « détection » correspond à un blocage de programme malveillant. Contrairement à une « compromission », un utilisateur n'est pas infecté lors d'une détection, car aucun fichier binaire n'est téléchargé.

Dans la zone APJC, le secteur des assurances, suivi des secteurs pharmaceutiques, de la chimie et de l'électronique sont les plus exposés. Les récentes catastrophes (tremblement de terre dévastateur, tsunami et accident nucléaire au Japon en 2011) ont entraîné un resserrement du marché des assurances, ce qui explique probablement pourquoi ce secteur est devenu une cible idéale. Et comme il fournit des services à de très grandes multinationales, les cybercriminels s'attaquent aux compagnies d'assurance afin de récupérer des informations sensibles sur leurs clients ou de s'introduire dans leurs réseaux et data centers.

FIGURE 9

Risque de détection par secteur et par région

SOURCE : Cisco Cloud Web Security



Les cinq principaux risques par secteur et par région

La Figure 10 présente la répartition des cinq principaux risques par secteur pour chaque région : AMER, APJC et EMEAR. Les balises iFrame et les scripts malveillants dominent dans tous les secteurs représentés, même si les cybercriminels des trois zones semblent s'appuyer fortement sur l'exploitation des failles de sécurité pour cibler certains secteurs. Dans la zone APJC, ils utilisent fréquemment les escroqueries, le hameçonnage et la fraude au clic pour abuser de la confiance des utilisateurs dans le secteur des transports et notamment du transport maritime.

Certains tentent même de cibler les cinq principaux secteurs à risque des trois zones avec des techniques faisant appel à des rançonneurs/faux logiciels de sécurité ou à des virus et des vers. Les attaques par programmes malveillants ciblant les terminaux mobiles sont également relativement faibles dans toutes les régions.

Les résultats illustrés ici sont principalement basés sur les données de détections d'attaques de programmes web malveillants de la solution Cisco de sécurisation du cloud, plutôt que sur les types de menaces sur le web.

PARTAGER LE RAPPORT SEMESTRIEL 2014 CISCO SUR LA CYBERSÉCURITÉ

FIGURE 10

Risque d'attaques par secteur

SOURCE : Cisco Cloud Web Security

Actualité des spams : la corde sensible de plus en plus sollicitée

Les créateurs de spams ont toujours employé des techniques de supercherie pour convaincre les destinataires d'ouvrir leurs messages et de cliquer sur les liens qu'ils contiennent, qui les dirigent généralement vers des programmes malveillants ou des sites web compromis. Les fausses livraisons de colis ou les problèmes de règlement d'impôts urgents sont des subterfuges courants, mais les professionnels de la sécurité observent aujourd'hui une nouvelle tendance : les spams qui visent à susciter l'émotion des destinataires.

Ces spams invoquent généralement des événements de la « vraie vie » comme le traitement d'une maladie grave ou une chance de rémission, ou encore des événements malheureux, comme un risque d'expulsion ou de faillite. Ces deux types de spam sont plus susceptibles d'inciter le destinataire à cliquer sur les liens qu'ils contiennent plutôt qu'un message concernant une livraison urgente.

Les spams qui jouent sur les émotions exploitent un maillon faible courant dans la chaîne de protection : l'utilisateur qui, même s'il est conscient des risques, est enclin à réagir à un message qui peut lui permettre d'atténuer les souffrances d'autrui.

Comme pour toute campagne de lutte contre le spam, le principal moyen de contenir les spams qui jouent sur les émotions est d'employer une technologie de blocage actualisée de manière dynamique.

Des spammeurs de plus en plus agiles changent de tactiques pour mieux parvenir à leurs fins

Les spammeurs contrecarrent rapidement les derniers moyens mis en place pour bloquer leurs messages. Ils adaptent le texte, les images et les noms de domaine afin de contourner les filtres. Et lorsqu'un message perd en efficacité, ils le transforment à nouveau.

Nos chercheurs surveillent l'évolution des types de spam et de message afin de vous informer des nouvelles tactiques employées par les spammeurs qui cherchent à infiltrer les réseaux ou à voler des informations. Ils doivent parfois mettre à jour des dizaines de fois les avertissements relatifs à un certain type de spam, comme un faux avis de paiement électronique, à mesure que les spammeurs adaptent leur tactique.

Le volume mondial de spams augmente deux fois plus vite que la normale, mais connaît un fort déclin dans certains pays

FIGURE 11

Volume mondial de spams (janvier 2014 à mai 2014)

SOURCE : Cisco Threat Intelligence Platform

Après un déclin global en 2013, le volume de spams augmente depuis octobre dernier. D'après nos recherches, ce volume a maintenant atteint son plus haut niveau depuis fin 2010. De juin 2013 à janvier 2014, entre 50 et 100 milliards de messages ont été envoyés par mois. Depuis mars 2014, on constate un pic de plus de 200 milliards de messages par mois, soit deux fois plus que les volumes habituels.[19]

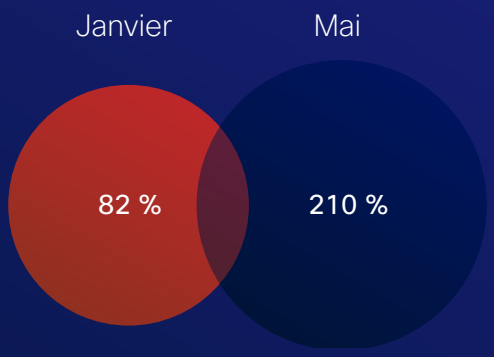
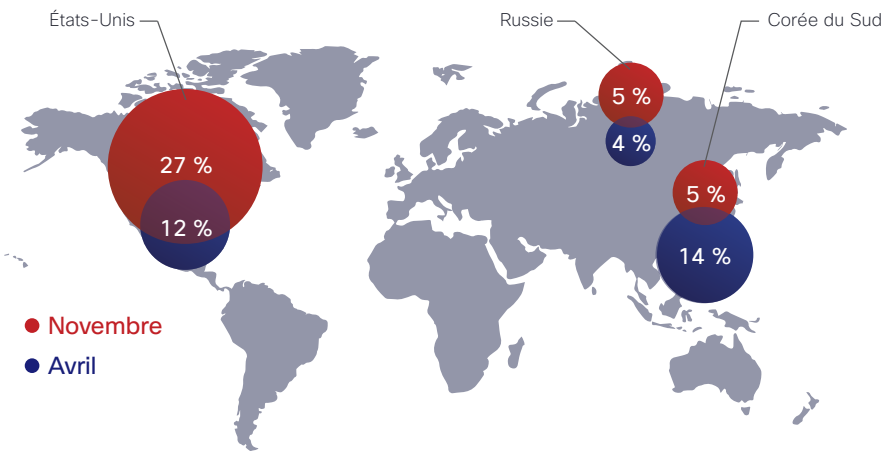


FIGURE 12

Tendances en volume par pays (novembre 2013 à avril 2014)

SOURCE : Cisco Threat Intelligence Platform

Malgré l'augmentation du volume de spams dans le monde, tous les pays ne sont pas logés à la même enseigne. En effet, la Russie et les États-Unis connaissent une forte chute des volumes de spams depuis novembre 2013. Parallèlement, la Corée du Sud connaît une recrudescence de courriers indésirables, par rapport aux 10 autres pays principaux observés par nos équipes de chercheurs.



	Novembre	Avril
Argentine	2 %	7 %
Allemagne	2 %	6 %
Chine	11 %	5 %
Iran	1 %	4 %
Japon	2 %	7 %
Espagne	3 %	7 %
Royaume-Uni	2 %	4 %

Les tendances

Nos experts en sécurité font part de leur analyse des menaces et des tendances observées au cours du premier semestre 2014, et de leurs projections sur ce à quoi nous devons nous attendre dans les mois à venir.

Une sécurité compromise
Des connexions cryptées

Les récentes attaques de grande envergure ayant exploité des certificats de chiffrement et de sécurité, comme Heartbleed et la faille « goto fail » d'Apple[20], ont révélé que de nombreuses implémentations courantes du protocole TLS sont le maillon le plus faible pour tous les utilisateurs. Que des mesures de sécurité telles que le chiffrement et la cryptographie constituent désormais des points faibles est assez ironique. Pendant des années, les utilisateurs ont été encouragés à rechercher l'icône de cadenas sur les sites, un symbole leur confirmant qu'ils étaient sur le point d'effectuer une transaction sûre. De nombreux utilisateurs pensent que leurs informations sont en sécurité sur les terminaux de paiement hors ligne. Ils sont certains que des procédures de chiffrement de bout en bout sont en place (quand ils savent que de telles procédures existent).

Les événements des six derniers mois ont prouvé que malgré la vigilance et les précautions dont font preuve les utilisateurs et quel que soit le nombre de mesures de sécurité mises en place, les maillons faibles hors de leur contrôle continuent de représenter un risque majeur.

Tout commerce acceptant des paiements par carte doit impérativement remédier au problème des failles de sécurité dans les connexions cryptées. Il faut pour cela s'intéresser de très près à la façon dont les solutions de chiffrement et autres produits de sécurité arrivent sur le marché.

Le succès de programmes malveillants tels que Heartbleed prouve que de nombreuses entreprises ayant recours à des connexions cryptées sécurisées et les technologies connexes partent du principe que :

- Les protocoles cryptographiques qui reposent sur des normes et du code open source populaire assurent une protection robuste.
- L'ensemble du code source intégré dans les services et les produits de sécurité, y compris le code fourni par des tiers, a été entièrement vérifié par des experts en sécurité.

Aucune de ces suppositions n'est vraie. Mais elles constituent toutes deux des facteurs qui contribuent à la réussite d'attaques comme Heartbleed qui exploitent les vulnérabilités et autres failles, et qui abusent de la confiance des utilisateurs.

L'amélioration des processus ne sera pas chose aisée. D'après nos experts en sécurité, en l'état actuel, OpenSSL est trop complexe pour être mis en œuvre et testé correctement. Le processus actuel de vérification du code open source et propriétaire requiert une approche plus solide. Mais à qui cette tâche incombe-t-elle ? Parallèlement, la communauté tente de déterminer si le système d'autorité de certification défaillant peut vraiment être réparé.

En matière de sécurité, la simplicité est primordiale. Réduire la quantité de code à approuver constitue une étape importante pour parvenir à des implémentations sécurisées. Selon nos experts, pour améliorer les bibliothèques de sécurité SSL/TLS open source, il faudra au minimum :

- Simplifier les protocoles et leur mise en œuvre
- Vérifier que le code a été correctement implémenté, et qu'il est exempt de vulnérabilités et de failles dissimulées
- S'assurer que les personnes qui testent et valident le code sont compétentes

Une retombée positive d'attaques récentes telles que Heartbleed : nombre de développeurs de la communauté vérifient désormais leur code pour le corriger de manière proactive. La Fondation Linux a également récemment annoncé le lancement de la Core Infrastructure Initiative grâce à laquelle « les entreprises du secteur technologique peuvent participer au financement de projets open source dans le besoin, tout en permettant aux développeurs de continuer à travailler dans le respect de l'esprit de l'open source qui en a fait le succès ».[21] OpenSSL a été l'un des premiers projets sélectionnés pour recevoir du financement de la Core Infrastructure Initiative. Cisco est l'un des premiers contributeurs de ce projet.

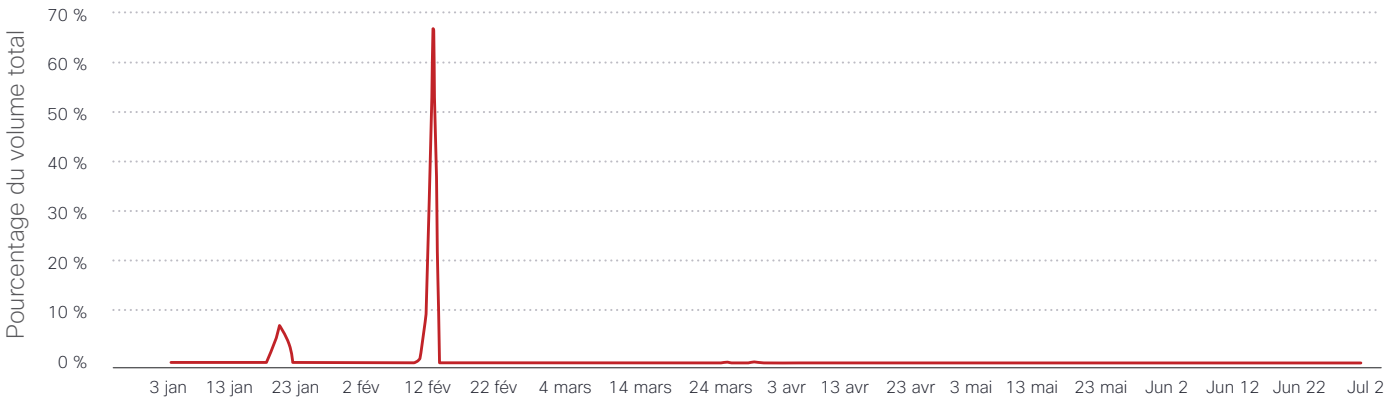
Attaques par amplification : les cybercriminels se mettent à l'heure du NTP

Dans notre *rapport annuel 2014 sur la sécurité*, nos experts attirent l'attention sur le fait que les attaques DDoS, à savoir les attaques lancées par amplification DNS, demeurent un risque majeur dans les entreprises en 2014.[22] Même avant cela, nos chercheurs affirmaient que le NTP, un protocole conçu pour synchroniser les horloges d'ordinateurs via un réseau, était un maillon faible amené à devenir un vecteur d'attaques DDoS amplifiées. Ils sont parvenus à cette conclusion après avoir constaté que les outils d'attaque conçus pour utiliser le nombre croissant de serveurs NTP vulnérables commençaient à se répandre dans la communauté des pirates.[23]

FIGURE 13

Attaque DDoS NTP de CloudFlare, 2014

SOURCE : Cisco Threat Intelligence Platform

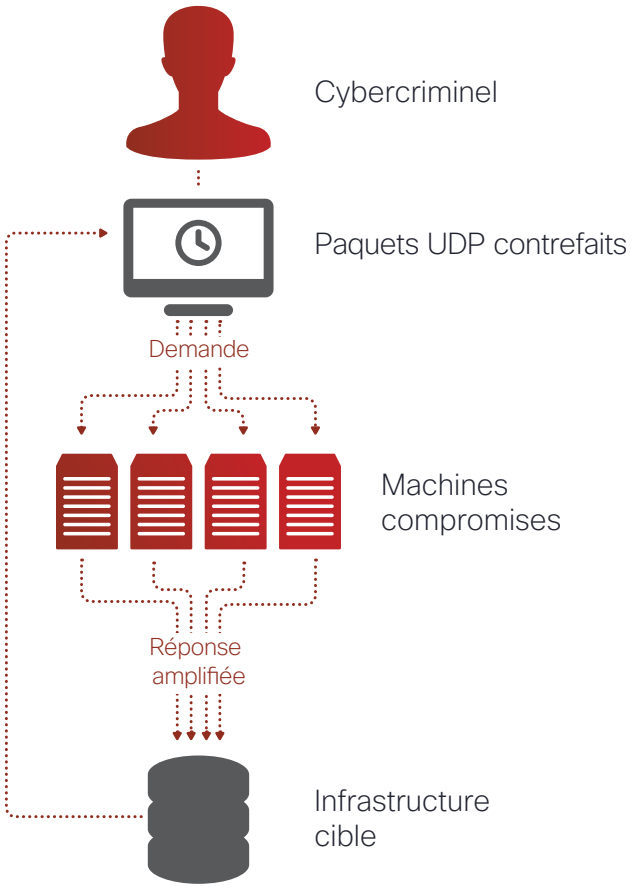


L'une des attaques avec amplification NTP les plus importantes a été observée au cours du premier semestre 2014. Elle visait un client du fournisseur mondial de services DNS CloudFlare (voir la Figure 13). À son paroxysme, l'attaque de février a atteint près de 400 Gbit/s en trafic UDP, dépassant l'attaque DDoS de Spamhaus de mars 2013 de 300 Gbit/s, impliquant 30 000 résolveurs DNS ouverts.[24]

Il est facile de comprendre pourquoi certains pirates expérimentent le NTP comme outil pour fomenter leurs attaques DDoS : OpenNTPProject.org, un projet d'analyse du NTP destiné à sensibiliser les utilisateurs aux problèmes liés à ce protocole, a identifié plus d'un million de serveurs NTP vulnérables.[25] La bande passante cumulée de ces serveurs est très certainement plus importante que toute attaque DDoS observée jusqu'à maintenant.

FIGURE 14

Le déroulement d'une attaque NTP



Pour mener une attaque avec amplifications NTP, le cybercriminel envoie de petites demandes à des serveurs NTP, en falsifiant l'adresse du paquet UDP afin que les demandes semblent provenir du système ciblé par le pirate. Le paquet UDP est sans état. La possibilité d'usurper l'adresse UDP est une composante indispensable des attaques par amplification DNS et NTP. Les serveurs NTP impliqués dans l'attaque renvoient une réponse conséquente aux petites demandes, renvoyant toutes les informations à la cible. Le serveur se retrouve alors submergé et mis hors ligne. (Des efforts sont actuellement consentis pour empêcher l'usurpation d'adresses UDP. Ils doivent être poursuivis.)

Pour empêcher les attaques par amplification NTP, les serveurs NTP publics doivent être mis à jour pour exécuter la dernière version du protocole (qui est la version 4.2.7 au moment de la rédaction de ce document). Avec cette mise à jour, la commande à distance MON_GETLIST ou « monlist », qui renvoie les adresses des 600 dernières machines avec lesquelles un serveur NTP a interagi, n'est plus prise en charge. Si la mise à niveau est impossible, l'option *noquery* de la configuration du NTP permet également d'empêcher l'exécution des requêtes monlist.

Les attaques par amplification NTP constituent peut-être un nouveau type d'attaque DDoS, mais les amplifications DNS restent une technique privilégiée pour de nombreux pirates. D'après The Open Resolver Project, depuis octobre 2013, 28 millions de résolveurs ouverts représentent une menace significative.[26]

Kits d'exploits : l'ouverture à la concurrence

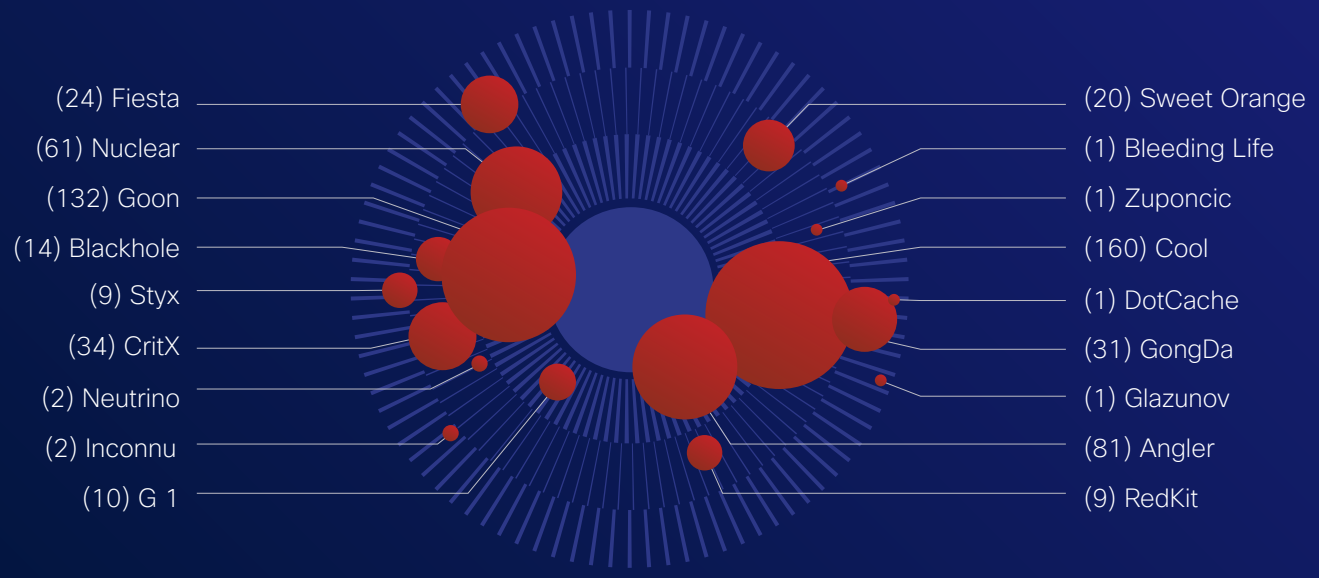
Lorsque Paunch, le cerveau présumé du kit d'exploits Blackhole, a été arrêté en Russie en octobre 2013[27], il n'a pas fallu longtemps avant que de nouveaux créateurs de kits d'exploits ne prennent la relève.

Blackhole était de loin le kit d'exploits le plus utilisé et le mieux géré. Lorsque Paunch et Blackhole ont été mis hors d'état de nuire, les pirates se sont intéressés à de nouveaux kits d'exploits. D'après nos chercheurs, bien que le podium ait été âprement disputé au cours du premier semestre 2014, aucun kit ne s'est encore clairement démarqué.

FIGURE 15

Kits d'exploits observés depuis janvier 2014

SOURCE : Cisco Threat Intelligence Platform



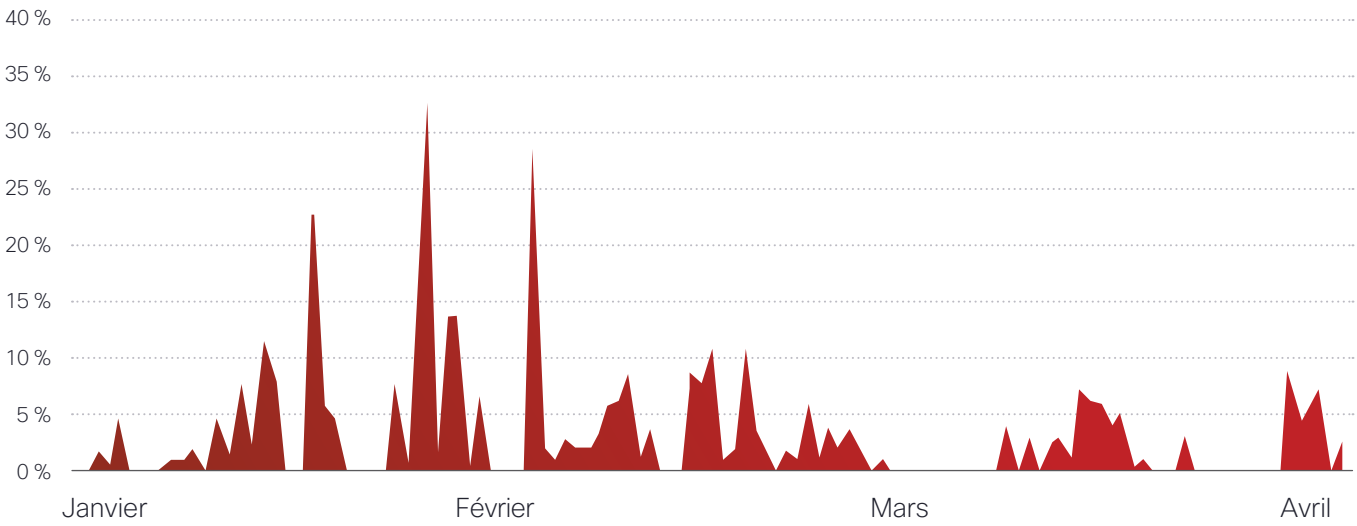
(Nombre d'attaques) Nom du kit d'exploits

Malgré la concurrence féroce, nos chercheurs ont constaté que le nombre de kits d'exploits a baissé de 87 % depuis l'arrestation de Paunch l'année dernière (voir figure 16).

FIGURE 16

Baisse du nombre de kits d'exploits (janvier-avril 2014)

SOURCE : Cisco Threat Intelligence Platform



Les cybercriminels utilisent également des kits d'exploits dans le cadre de campagnes plus ciblées et plus sophistiquées, au cours desquelles ils visent des utilisateurs spécifiques pour découvrir des vulnérabilités dans des applications, des programmes et des systèmes qui leurs donneront accès directement à l'infrastructure. Par exemple, les kits d'exploits « LightsOut » et « Hello » visent tout particulièrement le secteur de l'énergie.

Publicités frauduleuses : un grain de sable dans les rouages de la cyberéconomie

Les budgets de la cyberpublicité dépassent à présent ceux de toutes les autres formes de support de promotion commerciale. 28 Lorsqu'on pense aux débuts de la publicité en ligne, une simple bannière publicitaire de Hotwired en 1994, l'augmentation des deux dernières décennies est d'autant plus impressionnante. La publicité sur Internet, aussi agaçante qu'elle puisse être pour les internautes, est importante, car elle permet la gratuité de la majorité des contenus. Si ce modèle venait à changer ou si les internautes ne faisaient plus confiance à ce mode de publicité, les répercussions seraient graves pour Internet.

Les publicités frauduleuses, ou malvertising, utilisées pour diffuser des programmes malveillants, menacent ce modèle et érodent la confiance des internautes. Elles touchent tous les internautes et perturbent l'économie sur Internet. D'après nos experts en sécurité, les publicités frauduleuses témoignent de la sophistication de la cybercriminalité moderne, en termes de répartition du travail, de coopération et de spécialisation sur toute la chaîne d'attaque.

Les publicités frauduleuses sont de plus en plus courantes et les pirates sont en mesure de lancer des campagnes très ciblées. Un pirate qui souhaite cibler un public spécifique à un moment donné, par exemple les fans de foot en Allemagne pendant un match de la Coupe du Monde, peut le faire via une plate-forme publicitaire légitime. Tout comme un véritable annonceur, il contacte des régies publicitaires qui gèrent ce type de plate-forme. Il paie à l'avance, peut-être 2000 $ ou plus par campagne de diffusion et demande à ce que les plates-formes mettent en ligne les publicités le plus vite possible, afin d'empêcher toute inspection du contenu.

Les victimes de publicités frauduleuses sont infectées par le programme malveillant au cours de leurs activités normales sur Internet et n'ont ainsi aucune idée de la manière dont elles ont été infectées, ni de l'endroit où cela s'est produit. Il est pratiquement impossible d'en retrouver la source, car la publicité qui a transmis le programme malveillant a disparu depuis longtemps.

PARTAGER LE RAPPORT SEMESTRIEL 2014 CISCO SUR LA CYBERSÉCURITÉ

Des publicités très nuisibles : le malvertising au service des logiciels rançonneurs

Comme notre ***rapport annuel 2014 sur la sécurité*** l'indique, les publicités frauduleuses ont joué un rôle clé dans la diffusion du logiciel rançonneur CryptoLocker. Les logiciels rançonneurs sont aussi nuisibles que leur nom l'indique : il s'agit de programmes malveillants qui cryptent les fichiers sur les ordinateurs des victimes jusqu'à ce qu'elles paient une rançon.[29]

CryptoLocker a été neutralisé il y a peu de temps : le Ministère de la Justice des États-Unis a annoncé en juin qu'ils travaillaient avec les services de police d'autres pays et des entreprises technologiques pour mettre fin à « Gameover Zeus », un botnet actif depuis deux ans et l'un des principaux vecteurs de CryptoLocker.[30] Mais il n'a pas fallu longtemps pour qu'un autre type de rançonneur, « CryptoWall », prenne sa place.

Au cours du premier semestre 2014, nos chercheurs ont disséqué des campagnes de cyberattaques, en particulier celles qui utilisent les publicités frauduleuses pour rediriger les internautes vers des sites qui hébergent des kits d'exploits (loués ou achetés par les pirates) et qui poussent un « injecteur » (ou dropper) sur les systèmes des utilisateurs pour infecter les systèmes vulnérables. Au cours de leurs recherches, nos experts ont remarqué des niveaux de trafic élevés cohérents avec un nouveau kit d'exploits nommé « RIG », observé pour la première fois en avril 2014 sur des forums fréquentés par les cybercriminels.[31] RIG utilise les publicités frauduleuses pour s'attaquer à des internautes qui se rendent sur des sites légitimes très connus. Ce toolkit est utilisé par les pirates pour diffuser le rançonneur CryptoWall.

Dès juin, Cisco a bloqué des requêtes vers de nombreux sites WordPress compromis vers lesquels des internautes étaient redirigés par des publicités frauduleuses.

(Voir Vulnérabilités WordPress : qui est aux commandes ?, à la page 37.)

Les pages d'accueil de ces sites hébergent des kits d'exploits pour Java, Flash et le protocole multimédia Microsoft Silverlight. D'après nos chercheurs, l'utilisation du plug-in Silverlight pour lancer des exploits semble se développer dans la communauté cybercriminelle. Fiesta a été le premier kit d'exploits connu à incorporer une exploitation de Silverlight en 2013. RIG et un autre kit d'exploits, Angler, ont rapidement suivi, le marché des kits d'exploits étant très concurrentiel. (Voir Kits d'exploits : l'ouverture à la concurrence, page 33.)

Vulnérabilités WordPress : qui est aux commandes ?

Des entreprises de toutes tailles font confiance à WordPress, un logiciel web composé d'un ensemble de scripts et de modules complémentaires qui permet aux utilisateurs de faire ce qu'ils veulent de leur site : blog, hébergement de forums, e-commerce, etc.

WordPress a été conçu pour sa fonctionnalité, pas pour la sécurité.

La plupart des utilisateurs de WordPress ne disposent pas des connaissances ou des compétences adéquates pour sécuriser leur site correctement. Et bien souvent, les sites web créés avec le système de gestion de contenu WordPress ou un système similaire finissent par être abandonnés.

Les sites de ce genre sont légion sur le web et ils constituent un maillon faible de la chaîne de sécurité. Les pirates qui s'introduisent sur ces sites oubliés depuis longtemps peuvent alors charger des codes malveillants et les utiliser comme des sites de diffusion de kits d'exploits. Les utilisateurs arrivent sur ces sites en navigant sur d'autres sites actifs et légitimes qui ont également été piégés. Un iFrame prend le contenu du site abandonné et le propose aux utilisateurs sur le site légitime.

WordPress n'est pas le seul système de gestion de contenu qui présente ce problème, mais il se distingue des autres, comme Joomla et e107, en raison de sa popularité. Les sites web abandonnés présentent un grand risque pour la sécurité globale sur Internet, et comme personne n'est aux commandes, il n'est pas simple de faire nettoyer ces sites ou de les mettre hors ligne. Même si les propriétaires de site pensent à prendre des mesures, la plupart se contentent d'appliquer un correctif sur le point d'entrée et ne regardent pas si leur site a déjà été compromis. Ils ne trouvent pas la faille et ne la corrigent pas.

Dans le cadre de leurs offres, de nombreux hébergeurs proposent à présent des services d'installation WordPress gérés à bas coût pour les sites commerciaux. Ils s'assurent que tous les patchs et les paramètres de sécurité appropriés sont appliqués. À l'avenir, alors que de plus en plus d'utilisateurs se tourneront vers ce type de service, le nombre de sites WordPress vulnérables devrait diminuer.

Terminaux de paiement : une cible de choix pour les voleurs de données de cartes de paiement

Plusieurs tendances convergentes ont fait des terminaux de paiement électronique (TPE) une cible idéale pour les criminels qui cherchent à voler de grandes quantités de données de cartes de paiement et à les monétiser rapidement. Les récents incidents largement relayés par la presse qu'ont subis de grandes enseignes démontrent que ce type d'attaque peut être mené rapidement et avec succès. Il est recommandé d'examiner les capacités de détection avant une attaque ciblant les données de cartes de paiement tout en réduisant les délais de résolution pendant et après l'attaque.

Ces attaques consistent à voler les données enregistrées dans les bandes magnétiques des cartes de paiement. Une fois volées, les données peuvent être utilisées pour créer de fausses cartes qui serviront ensuite à effectuer des achats frauduleux en magasin. Les programmes malveillants qui s'attaquent aux terminaux de paiement permettent d'extraire les données de la mémoire, en évitant les données cryptées sur les disques et le réseau. Ce vol organisé peut fonctionner à grande échelle pour plusieurs raisons :

Connexion à Internet du point de vente

La probabilité de plus en plus forte que les terminaux de paiement soient reliés à Internet fait que les criminels disposent d'un point d'accès aux réseaux d'entreprise.

Absence de prise de conscience

De nombreuses entreprises n'ont pas pris conscience que les données de cartes de paiement sont sensibles et ne les protègent pas suffisamment.

Fournisseurs tiers

Le recours de plus en plus fréquent à des fournisseurs par les entreprises pour la totalité ou une partie de leurs solutions de point de vente offre d'autres points d'entrée aux criminels.

Les données de cartes de paiement sont une marchandise très demandée et elles sont très rentables. Pour les criminels, il est plus efficace de voler les données sur les systèmes de point de vente que de s'attaquer directement à une boutique en ligne, car les banques détectent plus facilement ce genre de vol et peuvent y remédier.

De plus, les États-Unis étant une des rares économies majeures où les cartes à bande magnétique sont plus répandues que les cartes à puce et à code PIN plus sécurisées, il est facile de monétiser les données des bandes magnétiques. (Notez que si les données des cartes ne sont pas cryptées à chaque étape, il est possible de voler les numéros de carte et leur date d'expiration pour les utiliser lors de transactions en ligne, sans passer par le système de puce et code PIN.)

Renforcer le contrôle des données de carte de paiement

Pour empêcher les vols de données de carte de paiement ou de toute autre information au point de vente, les enseignes doivent investir massivement dans des barrières technologiques pour bloquer les criminels. Elles doivent également prendre conscience que les données de carte de paiement doivent faire l'objet d'une grande attention de la part de tous leurs employés.

Certaines enseignes choisissent d'équiper leurs terminaux de paiement de dispositifs de cryptage qui peuvent empêcher l'interception des données de carte de paiement qui transitent sur leurs réseaux. Si cet investissement est trop lourd pour elles, elles devraient au moins considérer ces données comme « sensibles » et les surveiller afin de détecter toute intrusion ou mouvement anormal. Les moyens de compromettre un réseau étant extrêmement nombreux, les entreprises devraient partir du principe que les pirates se sont déjà introduits sur le leur.

L'IOC le plus logique qui indiquerait un vol de données de carte de paiement est l'importation d'un ensemble d'outils, un nouveau processus exécuté sur un terminal de paiement et l'exfiltration de fichiers compressés avec un volume et à une fréquence uniformes. Les enseignes devraient envisager l'utilisation de systèmes capables d'analyser ce type de comportement sur l'ensemble du réseau.

Une autre bonne pratique consiste à détecter les changements dans les applications et les processus sur tous les systèmes de traitement des cartes de paiement. Tout changement sur un terminal devrait déclencher une analyse immédiate. De plus, même si la plupart des protocoles utilisent la compression pour gagner en efficacité et en rapidité, les outils de compression devraient faire partie d'une « liste blanche d'applications » de l'entreprise.

Enfin, les réseaux devraient être segmentés afin de ne pas faciliter la tâche aux pirates qui cherchent à accéder à de grandes quantités de données. Les terminaux de paiement devraient être connectés à un segment distinct du réseau de l'entreprise afin de limiter l'accès et les attaques pivotantes sur les terminaux de paiement.

Avec l'explosion du nombre de terminaux mobiles et leur prolifération sur les réseaux d'entreprise, la segmentation doit inclure des mécanismes d'identification performants permettant de savoir qui se connecte, avec quel terminal et avec quelle méthode. Par exemple, l'accès depuis un ordinateur portable appartenant à l'entreprise via le réseau Wi-Fi de l'entreprise peut être autorisé alors que l'accès depuis une tablette via un VPN d'accès à distance refusé, en raison du caractère confidentiel des données traitées par les terminaux de paiement.

D'après Cisco, les pirates à la recherche de données de carte bancaire vont continuer à concentrer leurs efforts sur les terminaux de paiement. Cependant, l'utilisation de systèmes de détection et d'alerte performants ainsi que l'installation de dispositifs de cryptage peuvent empêcher de telles opérations.

L'ingénierie sociale : rencontrer le maillon faible en personne

Les entreprises paient parfois des centaines de milliers de dollars pour s'équiper du tout dernier logiciel de sécurité et s'imaginent alors protégées des attaques ciblant le réseau. Mais si la menace vient d'une personne réelle qui peut s'introduire dans un bureau ou dans un centre de serveurs, une protection logicielle ne sera pas d'une grande utilité.

Pour des criminels pleins de ressources, il est plus lucratif de se présenter dans les locaux ou de se connecter physiquement à un réseau que de concevoir des e-mails d'hameçonnage avec des liens qui mènent à des sites piégés. (Le spam et les campagnes d'ingénierie sociale en ligne sont loin d'avoir disparu pour autant, voir page 26 pour plus d'informations.) La possibilité de simplement se connecter à une prise Ethernet ou de débrancher un téléphone IP et d'en utiliser le câble pour accéder aux informations sur le réseau peut avoir de graves conséquences. L'ingénierie sociale fait référence à l'exploitation de failles humaines, où les personnes (vos employés) deviennent le maillon faible de votre chaîne de sécurité numérique et physique.

Les criminels utilisent les mêmes techniques d'ingénierie sociale lorsqu'ils se rendent en personne dans votre entreprise que celles qu'ils utilisent pour les e-mails et les sites compromis. Le but est de développer une relation de confiance (même si cette confiance est mal placée) avec une personne qui peut leur donner accès aux sites de l'entreprise.

En effectuant des recherches sur la personne ciblée sur LinkedIn, par exemple, les criminels peuvent tout découvrir à son sujet, depuis la nature de son travail jusqu'à l'université où elle a obtenu son diplôme et son équipe de foot préférée. Ils peuvent ensuite se présenter à la personne ciblée comme une connaissance ou quelqu'un en qui elle peut avoir confiance.

Grâce à la popularité des réseaux sociaux, en particulier auprès des professionnels, un criminel qui cherche un point d'entrée peut aisément trouver des informations et des photos.

Avec les informations récoltées en ligne, un criminel peut se faire passer pour un journaliste qui souhaite faire une interview ou pour un partenaire ou un prospect qui souhaiterait être reçu personnellement. Ce criminel peut également porter un faux badge lui donnant un semblant de légitimité.

Les criminels ont aussi découvert qu'il n'est pas nécessaire d'organiser de telles escroqueries à l'entrée de l'entreprise ciblée. Il leur suffit de trouver le maillon faible, c'est-à-dire un partenaire commercial ou un fournisseur moins sécurisé, qui a accès ou qui peut se connecter à la vraie cible : le réseau. Cette technique s'avère particulièrement efficace lorsque la cible est très sécurisée, mais pas le partenaire commercial de confiance. Les pirates sont toujours à la recherche du point d'accès le plus facile.

Un moyen de limiter les tentatives d'accès physique au réseau est de s'assurer que les ports d'accès authentifient et autorisent les connexions avant d'autoriser l'accès au réseau. De plus, les entreprises peuvent créer des « domaines de sécurité dynamiques » par utilisateur et/ou par appareil, ou toute autre configuration requise. Ces domaines de sécurité dynamiques peuvent utiliser des technologies comme le 802.1x, les listes de contrôle d'accès aux ports (ACL), le VPN et l'évaluation de la configuration de l'hôte.

La solution

Quelle que soit la méthode d'accès utilisée par le pirate (filaire, sans fil ou VPN), les informaticiens peuvent créer dynamiquement un domaine de sécurité, ou une « bulle » juste pour lui. Si un criminel connecte un ordinateur portable à un port dans les locaux, le réseau arrête la personne, l'authentifie, lui crée un profil, évalue sa configuration, surveille son comportement, puis donne des autorisations très spécifiques et dynamiques qui restreignent l'accès au réseau en fonction d'une politique contextuelle.

Perspectives

Nos experts expliquent pourquoi en traitant la sécurité comme un processus métier, en améliorant le dialogue entre les responsables de la technologie et les responsables commerciaux, et en utilisant des nouvelles solutions qui permettent de mieux détecter des menaces de plus en plus difficiles à voir, les entreprises peuvent mieux se prémunir contre les attaques.

Les conditions d'une cybersécurité intelligente et concrète

Renforcer les maillons faibles de la chaîne de sécurité repose essentiellement sur la capacité des entreprises et du secteur à amener les dirigeants à prendre conscience des risques liés à la cybercriminalité et de l'importance de la cybersécurité. Définir une stratégie commerciale, une stratégie de sécurité et des mécanismes de contrôle cohérents qui favorisent la cyberrésilience est également essentiel, tout comme la capacité à obtenir une meilleure visibilité sur un réseau « bruyant » à l'aide de nouvelles techniques intelligentes telles que l'analytique prédictive.

Pour se protéger à tous les stades d'une attaque, avant, pendant et après, les entreprises doivent lutter contre un grand nombre de vecteurs avec des solutions qui fonctionnent partout où une menace peut apparaître : réseau, terminaux mobiles, environnements virtuels, cloud, data centers...

La sécurité de tous ne pourra être renforcée qu'au prix d'une réduction des failles, qu'il s'agisse des vulnérabilités connues et exploitées de Java, de Flash ou d'Adobe PDF, des sites web WordPress laissés à l'abandon, des failles trop longtemps ignorées de OpenSSL, des réseaux non protégés contre les intrusions physiques ou de serveurs NTP vulnérables, d'une part et de la réduction de la complexité causée par des systèmes et des solutions disparates, d'autre part. Pour garantir la résilience d'un réseau au service des activités de l'entreprise, il est essentiel d'évaluer l'état du cycle de vie des équipements réseau détectés, les éventuelles vulnérabilités et la gestion de la version des systèmes d'exploitation.[32]

La stratégie de Cisco, qui consiste à aider les entreprises à faire face aux problématiques de sécurité d'aujourd'hui et de demain, repose sur trois impératifs :

Orientée sur la visibilité

Plus notre visibilité est grande, meilleure est notre capacité à corréler et à exploiter les informations pour comprendre le contexte, prendre de meilleures décisions et agir en conséquence, manuellement ou automatiquement.

Axée sur les menaces

Nous devons nous concentrer sur la détection, la compréhension et l'interception des menaces en effectuant des analyses continues et en exploitant en temps réel les informations issues du cloud et partagées avec toutes les solutions de sécurité, pour une efficacité accrue.

Basée sur une plate-forme

La sécurité ne se limite pas au réseau. Elle nécessite un système de plates-formes flexibles et ouvertes qui intègrent tous les équipements réseau et le cloud.

Une cybersécurité intelligente et concrète permettra de sécuriser l'Internet des objets. Elle formera la base de l'Internet of Everything où la sécurité, comme le traitement informatique, sera puissante, omniprésente et facile à appréhender pour les utilisateurs.

L'opérationnalisation de la sécurité : la sécurité doit devenir un processus métier

Les évaluations révèlent que les dysfonctionnements opérationnels ou les pannes techniques sont souvent à l'origine d'un problème de sécurité. Les contrôles de sécurité sont faibles, voire non existants, en raison d'un manque de maturité opérationnel ou de capacités, ou de la combinaison des deux.

Alors que la cybersécurité est un enjeu stratégique de plus en plus important pour les entreprises, la « maturité des opérations de sécurité » devient l'objectif. Il s'agit pour l'entreprise d'avoir une vue globale des risques et d'améliorer constamment ses pratiques en matière de cybersécurité.

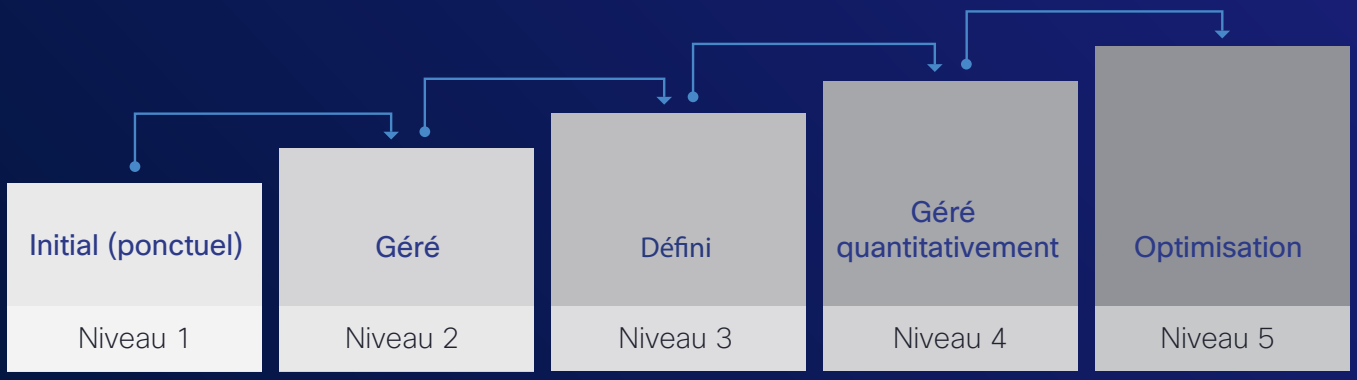
Avec l'aide des prestataires de services spécialisés, de nombreuses entreprises travaillent à la création d'un processus métier hautement standardisé et mesuré, ou d'un ensemble de processus, évalué régulièrement pour vérifier que les objectifs stratégiques sont atteints. La décision de considérer la sécurité comme un processus métier vient généralement d'initiatives plus vastes, conçues pour améliorer la gouvernance, la gestion des risques et la conformité au sein de l'entreprise. De nombreuses entreprises découvrent, souvent trop tard, qu'en termes de sécurité IT, il ne suffit pas d'être aux normes.

Les entreprises qui font de la sécurité un processus métier en savent plus sur :

1. Ce qu'elles doivent protéger
2. Le degré d'efficacité de leurs mesures de sécurité
3. Les actions à mener en matière de cybersécurité

FIGURE 17

Le modèle CMMI



L'opérationnalisation de la sécurité offre une meilleure visibilité sur le fonctionnement global des mesures de sécurité dans toute l'entreprise. Elle permet de voir qui en est responsable, si ces personnes sont les mieux placées et si elles font leur travail correctement. Les entreprises qui opérationnalisent la sécurité peuvent également déterminer si les ressources IT sont déployées et utilisées de manière efficace.

Un élément important de l'opérationnalisation de la sécurité est l'instauration d'un dialogue constructif entre les responsables de la sécurité, comme les directeurs des systèmes d'information (DSI) et les responsables de la sécurité des systèmes d'information (RSSI), et les responsables commerciaux. Pour faire de la cybersécurité un processus métier formel, ces deux groupes de responsables doivent collaborer plus étroitement et plus fréquemment pour définir des niveaux acceptables de risques et des objectifs stratégiques en matière de sécurité. Pour favoriser ce dialogue, les RSSI doivent trouver des moyens de présenter les informations sur la cybersécurité dans des termes compréhensibles par les responsables commerciaux. Par exemple, des statistiques permettent de représenter l'importance de mesures de sécurité à adopter pour éviter un risque donné.

L'opérationnalisation de la sécurité implique également de suivre un « modèle de maturité ». Le modèle CMMI (Capability Maturity Model Integration) de Carnegie Mellon en est un exemple. Très répandu, le CMMI a été créé dans le cadre d'un projet du Software Engineering Institute dans les années 80. Comme le montre la Figure 17, le point de départ du modèle de maturité est la phase « ponctuelle », qui est essentiellement un mode « pompier ». Lorsqu'une entreprise atteint la dernière phase, elle utilise des processus standardisés qui peuvent être répétés et mesurés.

Comprendre les risques liés à la cybersécurité en termes commerciaux

De nombreuses entreprises jouent l'avenir de leurs modèles commerciaux sur les promesses d'hyperconnectivité de l'Internet des objets. Mais pour se préparer, et réussir, dans cet environnement qui émerge rapidement, les dirigeants doivent comprendre, en termes commerciaux, ce que la dépendance croissante au réseau signifie en matière de cyberrisques.

Il a longtemps été d'usage de ne pas parler de cybersécurité en public, mais l'attitude des entreprises évolue. De plus en plus de dirigeants commencent à prendre conscience que les problématiques de cybersécurité concernent toutes les entreprises, tout particulièrement en raison du passage au tout numérique et de la valeur stratégique que prennent les informations.

Ces dirigeants commencent également à réaliser que, dans le monde de l'Internet des objets, il est important qu'un dialogue franc sur les menaces et les meilleures pratiques pour limiter les risques s'établisse dans l'entreprise, entre les entreprises (y compris les concurrents) et entre les secteurs publics et privés. La pression accrue qu'exerce les conseils d'administration, qui cherchent à s'informer sur les risques liés à la cybersécurité, aide à faire évoluer le point de vue des dirigeants.

Des actions récentes de la Securities and Exchange Commission (SEC), un organisme fédéral américain, ont contribué à faire de la cybersécurité un sujet prioritaire au sein des conseils d'administration. En 2011, la SEC a rendu obligatoire la déclaration d'incidents de cybersécurité pour les sociétés par actions.[33] Ces entreprises doivent à présent informer leurs actionnaires de toute « occurrence importante de vol ou de cyberattaque ou de situation constituant un risque matériel ».[34] La SEC a organisé plus tôt cette année une table ronde « pour discuter de la cybersécurité et des problèmes et défis qu'elle pose pour les acteurs du marché et les entreprises par actions et sur les moyens qu'ils utilisent pour y remédier ».[35]

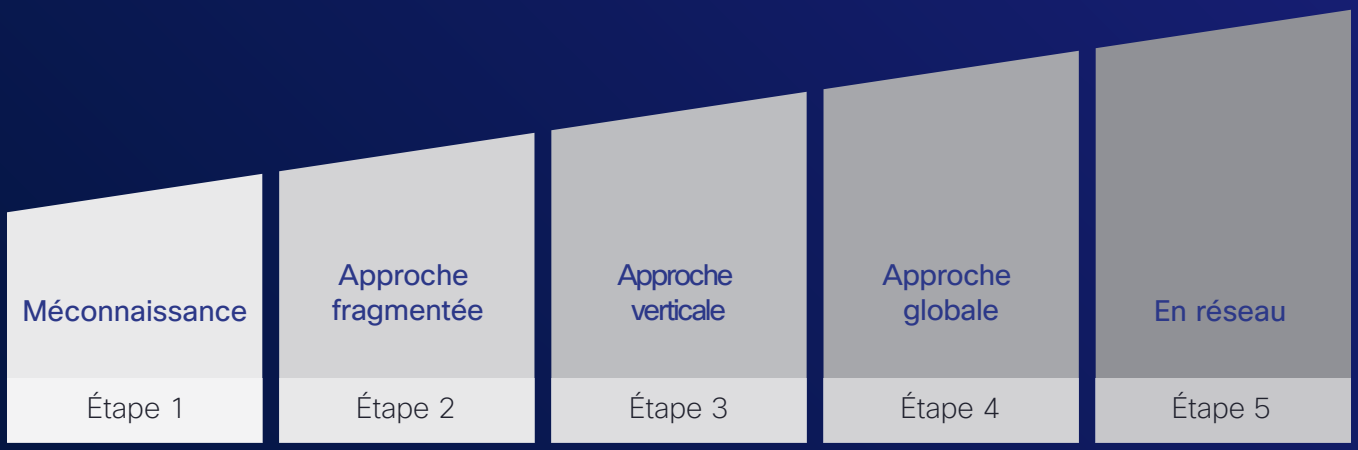
La même année, le Forum économique mondial (WEF), une institution internationale qui s'est donné pour mission d'améliorer l'état du monde via la coopération entre les secteurs publics et privés, a introduit le concept de « cyberrésilience ». Son but est de souligner l'importance de la cybersécurité et d'autres problématiques liés à Internet auprès des conseils d'administration. Le WEF présente la cyberrésilience comme un écosystème interdépendant où la force de chaque entreprise est équivalente à celle du maillon le plus faible de la chaîne de sécurité. Il s'agit de l'un des quatre principes fondamentaux du projet « Partenariat pour la cyberrésilience »[36] du WEF :

Notre force est équivalente à celle du maillon le plus faible de la chaîne dont nous dépendons tous. Nous contribuons tous à la sécurité de notre monde hyperconnecté. Un espace en ligne ouvert, sécurisé et résilient est un bien public. Tous ses acteurs partagent la responsabilité de la création et de la gestion de cette ressource.

Le « Partenariat pour la cyberrésilience » du WEF est destiné à aider les hauts dirigeants, y compris les DSI et les RSSI, à entamer des débats sur la cybersécurité dans leur entreprise et à parler en termes commerciaux des risques et des opportunités liés à Internet. Par exemple : « Quel serait le coût pour l'entreprise, si nous décidons de renoncer à une technologie pour des questions de risque cybersécuritaire ? ».

FIGURE 18

Modèle de maturité de la cyberrésilience organisationnelle



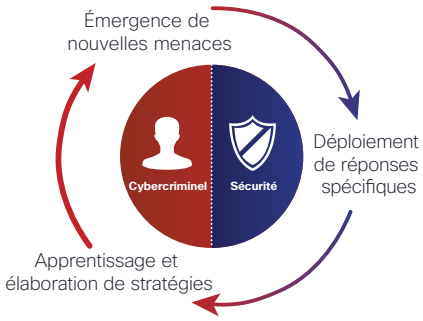
D'après le WEF, pour atteindre la cyberrésilience, les entreprises doivent aborder la cybersécurité sous l'angle des risques. Cette approche s'applique à toute entreprise qui souhaite améliorer sa cybersécurité. Le WEF propose ce modèle de maturité, qui ouvre une voie vers la cyberrésilience.

Le WEF insiste sur le fait que la cybersécurité ne peut pas se cantonner à un seul département dans l'entreprise, en l'occurrence le département IT. En effet, les capacités liées à Internet ne sont pas seulement techniques, elles sont aussi institutionnelles. De plus, le WEF souligne qu'il incombe en grande partie aux dirigeants de sensibiliser les employés à la cybersécurité tout comme il leur incombe d'aider leurs entreprises à devenir cyberrésilientes.

PARTAGER LE RAPPORT SEMESTRIEL 2014 CISCO SUR LA CYBERSÉCURITÉ

L'analytique prédictive : un détective au service de la sécurité

C'est un cercle vicieux : le secteur de la sécurité crée une réponse spécifique pour contrer une menace et les pirates trouvent un nouveau moyen de passer inaperçus. Les pirates cherchent par tous les moyens à savoir quel type de solutions de sécurité sont mises en œuvres. Ils adoptent des techniques plus difficilement décelables afin de mieux dissimuler leurs attaques. Il y a aujourd'hui moins de menaces faciles à détecter par les solutions de sécurité et les professionnels du secteur. En revanche, on constate davantage de trafic crypté, de brouillage et de codage aléatoire de la part d'acteurs malveillants afin de rendre les attaques « commande-and-control» encore plus difficiles à distinguer du trafic légitime.



Les réseaux « bruyants » sont particulièrement difficiles à surveiller et recèlent de nombreuses cachettes. Pour pouvoir passer outre ce bruit et comprendre si une activité anormale est en cours, il faut d'abord savoir reconnaître ce qu'est une activité « normale ». L'analytique prédictive repose sur un mécanisme de détection en plein essor qui fournit ce type d'informations et qui aide les entreprises à améliorer la résilience de leurs solutions de sécurité. Elle permet de détecter tout comportement inhabituel sur un réseau, les symptômes d'une infection, via des analyses de comportement et la détection des anomalies.

En utilisant l'analytique prédictive, les entreprises peuvent évaluer le comportement des entités (serveurs hôtes et utilisateurs) sur leur réseau. Un modèle, conçu à partir de plusieurs petits modèles et d'une représentation concise du comportement passé, est conçu et utilisé pour prédire le comportement normal des entités. Dans l'idéal, les données sont corrélées dans le cloud pour améliorer la vitesse, l'agilité et la profondeur de la détection des menaces. Si une activité présente un écart important ou prolongé par rapport au comportement attendu, elle est devra être inspectée.

L'analytique prédictive permet de rendre les techniques de sécurité existantes plus précises et plus à même de détecter des comportements inconnus ou inhabituels sur le réseau. Elle fait appel à des algorithmes pour la prise de décision avancés qui analysent de nombreux paramètres et captent en direct les données du trafic. Des capacités d'apprentissage automatique permettent au système d'apprendre et de s'adapter à ce qu'il voit.

Les systèmes à apprentissage automatique sont comme des détectives. Ils recherchent ce qui peut constituer un danger et des preuves qu'un incident s'est produit, est en cours ou est sur le point de se produire. Et bien qu'ils ne gèrent pas forcément la sécurité ou la mise en application des politiques, ils permettent à d'autres systèmes de rechercher des menaces non anticipées et de mettre en œuvre des mesures de protection. Pour apporter de la valeur et permettre aux entreprises d'améliorer l'efficacité de la sécurité, les solutions d'analytique prédictive doivent être déployées avec des solutions de sécurité basées sur le contenu, de gestion du périmètre et de gestion des politiques.

À propos de Cisco

Cisco crée des solutions de cybersécurité intelligentes et concrètes. Sa vision repose sur une approche de la sécurité axée sur les menaces qui vise à réduire la complexité, tout en assurant une meilleure visibilité, un contrôle continu et une protection avancée contre les menaces à tous les stades de l'attaque. Ce nouveau modèle de sécurité permet aux entreprises d'agir plus intelligemment et plus rapidement avant, pendant et après l'attaque.

Grâce à leurs vastes connaissances et à leur maîtrise des systèmes Big Data, les chercheurs spécialisés de notre écosystème de sécurité adaptative collective contribuent à découvrir et à analyser les menaces connues et émergentes et à nous en prémunir. Nos experts réputés s'appuient sur une infrastructure et des systèmes sophistiqués qui offrent une visibilité inédite obtenue grâce l'agrégation et l'analyse d'un volume de données télémétriques auquel seul Cisco a accès : des milliards de requêtes web et d'e-mails, des millions d'échantillons de programmes malveillants, des datasets open source et des milliers d'intrusions réseau.

Ces Big Data sont immédiatement traduites en mesures de protection capables d'assurer la protection des réseaux étendus à l'échelle de la planète.

Pour en savoir plus sur notre approche axée sur les menaces, rendez-vous sur www.cisco.com/go/security.

Notes

1 *Estimating the Cost of Cyber Crime and Cyber Espionage*, Center for Strategic and International Studies (CSIS), Juillet 2013 : https://csis.org/event/estimating-cost-cyber-crime-and-cyber-espionage.

2 « Internet of Things », Cisco.com : http://www.cisco.com/web/solutions/trends/iot/overview.html.

3 Infographie « Internet of Things », Cisco Internet Business Solutions Group : http://share.cisco.com/internet-of-things.html.

4 « Hackers Reveal Nasty New Car Attacks–With Me Behind The Wheel », par Andy Greenberg, *Forbes*, 12 août 2013 : http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/.

5 « Hackers Reportedly Targeted Three Large Medical Device Makers » iHealthBeat.com, 11 février 2014 : www.ihealthbeat.org/articles/2014/2/11/hackers-reportedly-targeted-three-large-medical-device-makers.

6 « How secure is your baby monitor? What can happen when the 'Internet of Things' gets hacked », par Matt Hartley, *Financial Post,* 3 mai 14 : http://business.financialpost.com/2014/05/03/how-secure-is-your-baby-monitor-what-can-happen-when-the-internet-of-things-gets-hacked/?__lsa=bc1b-f93e.

7 « The Internet of Everything, Including Malware », par Craig Williams, blog Cisco Security, 4 décembre 2014 : http://blogs.cisco.com/security/the-internet-of-everything-including-malware/.

8 L'objet de ce rapport est de présenter le nombre de requêtes pour des FDQN, des domaines, des sites potentiellement malveillants émanant du client.

9 *Rapport annuel Cisco 2014 sur la sécurité :* https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

10 Les clients qui souhaitent partager des informations de veille dans le cadre du projet AEGIS mené par l'équipe de recherche de vulnérabilités peuvent écrire à l'adresse threatintel@cisco.com.

11 Ibid.

12 Pour plus d'informations sur Heartbleed, visitez www.cisco.com/web/about/security/intelligence/ERP-Heartbleed.html.

13 « OpenSSL Heartbleed vulnerability CVE-2014-0160 – Cisco products and mitigations », par Pano Kampanakis, blog Cisco Security, 9 avril 2014 : http://blogs.cisco.com/security/openssl-heartbleed-vulnerability-cve-2014-0160-cisco-products-and-mitigations.

14 Pour plus d'informations sur les moyens de réduire les risques liés à Heartbleed, la vulnérabilité de OpenSSL, reportez-vous à « Cisco Event Response: OpenSSL Heartbleed Vulnerability CVE-2014-0160 », 22 avril 2014, sur Cisco.com : www.cisco.com/web/about/security/intelligence/ERP-Heartbleed.html.

15 « New OpenSSL Defects – Another Heartbleed? Tor Stripped? », par James Lyne, *Forbes*, 5 juin 2013 : www.forbes.com/sites/jameslyne/2014/06/05/new-openssl-defects-another-heartbleed.

16 « Severe OpenSSL Security Bug Uncovered by Japanese Researcher Months After Heartbleed », par Luke Villapaz, *International Business Times*, 5 juin 2014 : www.ibtimes.com/severe-openssl-security-bug-uncovered-japanese-researcher-months-after-heartbleed-1594989.

17 *Rapport annuel Cisco 2014 sur la sécurité :* https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

18 Ibid.

19 « Spam Hits Three Year High-Water Mark », blog Cisco Security, 2 mai 2014 : http://blogs.cisco.com/security/spam-hits-three-year-high-water-mark.

20 « Major Apple security flaw: Patch issued, users open to MITM attacks », par Violet Blue, blog « Zero Day », *ZDNet*, 22 février 2014 : http://www.zdnet.com/major-apple-security-flaw-patch-issued-users-open-to-mitm-attacks-7000026624/.

21 « Amazon Web Services, Cisco, Dell, Facebook, Fujitsu, Google, IBM, Intel, Microsoft, NetApp, Rackspace, VMware and The Linux Foundation Form New Initiative to Support Critical Open Source Projects », édition presse, Linux Foundation, 24 avril 2014. Pour plus d'informations sur le projet, rendez-vous sur http://www.linuxfoundation.org/news-media/announcements/2014/04/amazon-web-services-cisco-dell-facebook-fujitsu-google-ibm-intel

22 *Rapport annuel Cisco 2014 sur la sécurité :* https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

23 « When Network Clocks Attack », par Jaeson Schultz, blog Cisco Security, 10 janvier 2014 : http://blogs.cisco.com/security/when-network-clocks-attack/.

24 « Chronology of a DDoS: Spamhaus », par Seth Hanford, blog Cisco Security, 28 mars 2013 : http://blogs.cisco.com/security/chronology-of-a-ddos-spamhaus/.

25 Pour savoir si votre serveur NTP est vulnérable, rendez-vous sur le site openntpproject.org. Pour en savoir plus sur les bonnes pratiques concernant le DNS, reportez-vous à « DNS Best Practices, Network Protections, and Attack Identification » : http://www.cisco.com/web/about/security/intelligence/dns-bcp.html.

26 Projet Open Resolver : www.openresolverproject.org.

27 « Meet Paunch: The Accused Author of the Blackhole Exploit Kit », par Brian Krebs, blog KrebsOnSecurity, 6 décembre 2013 : http://krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/.

28 « Global Internet Ad Spend Sees Double-Digit Growth, Outpaces Other Media », *Nielsen,* 10 juillet 2012 : http://www.nielsen.com/us/en/newswire/2012/global-internet-ad-spend-sees-double-digit-growth-outpaces-other-media.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+NielsenWire+(Nielsen+Wire).

29 *Rapport annuel Cisco 2014 sur la sécurité :* https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

30 « Malicious Advertisements on Major Websites Lead to Ransomware », par Jeremy Kirk, IDG News Service, 6 juin 2014 : http://www.pcworld.com/article/2360820/malicious-advertisements-on-major-websites-lead-to-ransomware.html.

31 « RIG Exploit Kit Strikes Oil », par Andrew Tsonchev, blog Cisco Security, 5 juin 2014 : http://blogs.cisco.com/security/rig-exploit-kit-strikes-oil/.

32 « Network Barometer Report: A gauge of global networks' readiness to support business », *Dimension Data,* 2013 : http://www.dimensiondata.com/Global/Documents/Network%20Barometer%20Report%202013.pdf.

33 « CF Disclosure Guidance: Topic No. 2: Cybersecurity », Division of Corporation Finance, SEC, 13 octobre 2011 : http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

34 « Cybersecurity: SEC outlines requirement that companies report data breaches », par Ellen Nakashima et David S. Hilzenrath, *The Washington Post,* 14 octobre 2011 : http://www.washingtonpost.com/world/national-security/cybersecurity-sec-outlines-requirement-that-companies-report-data-breaches/2011/10/14/gIQArGjskL_story.html.

35 « Cybersecurity Roundtable », SEC : http://www.sec.gov/spotlight/cybersecurity-roundtable.shtml.

36 Pour en savoir plus sur le partenariat du WEF pour l'initiative de cyberrésilience, rendez-vous sur http://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience.