Rapport Cisco du 1er semestre 2017 sur la cybersécurité

Table des matières

Synthèse

Cisco publie des rapports complets sur la cybersécurité depuis près de dix ans. L'objectif de ces rapports est d'informer les équipes de sécurité et les entreprises des nouvelles cybermenaces et vulnérabilités, ainsi que des mesures à prendre pour améliorer la sécurité et la cyber-résilience. Nous essayons d'alerter les acteurs de la protection de la sophistication croissante des menaces et des techniques utilisées par les hackers pour usurper l'identité des utilisateurs, voler des informations et créer des perturbations.

Dans ce nouveau rapport, nous relevons encore le niveau d'alerte. Nos experts s'inquiètent de plus en plus de l'accélération des changements et de la sophistication des cybermenaces mondiales. Les acteurs de la protection ont amélioré leurs méthodes de détection et de défense contre les menaces, et aident les utilisateurs et les entreprises à se protéger et à remédier rapidement aux problèmes. Mais deux dynamiques atténuent ces résultats obtenus si difficilement, ralentissant les progrès et amplifiant les effets d'une nouvelle ère de cybercriminalité :

L'impact croissant des failles de sécurité

La génération de revenus reste le principal objectif de la majorité des cybercriminels. Cependant, certains hackers ont maintenant la capacité, et de plus en plus la volonté, de bloquer les systèmes et de détruire des données par leurs attaques. Comme nous l'avons expliqué à la page 7 de l'introduction du *Rapport Cisco sur la cybersécurité du 1er semestre 2017*, nos chercheurs estiment que cette activité malveillante préfigure un nouveau type d'attaque dans un avenir proche : la destruction de service (ou DeOS).

Au cours de l'année écoulée, nous avons également constaté que certains hackers utilisaient des objets IoT dans leurs attaques par déni de service (DDOS). L'activité des botnets dans les environnements IoT suggère que certains acteurs préparent le terrain pour une attaque de grande ampleur aux retombées majeures pouvant même compromettre Internet.

Le rythme et l'ampleur des technologies

Nos chercheurs spécialistes des menaces étudient depuis des années la manière dont la mobilité, le cloud computing et les autres évolutions et tendances technologiques modifient l'ampleur du périmètre de sécurité devant être défendu par les entreprises. Or, il apparaît clairement aujourd'hui que les cybercriminels tirent parti de cette surface d'exposition aux attaques toujours plus grande. L'ampleur des dernières attaques par ransomware témoigne à elle seule de l'inclination des hackers à exploiter les vulnérabilités et les failles des appareils et des réseaux pour avoir un maximum d'impact.

Le manque de visibilité des environnements informatiques dynamiques, les risques présentés par le « Shadow IT », le déferlement constant des alertes de sécurité et la complexité de l'environnement de sécurité informatique ne sont que quelques-unes des raisons pour lesquelles les équipes de sécurité à court de ressources peinent à garder une longueur d'avance sur les cybermenaces actuelles, toujours plus furtives et puissantes.

Contenu de ce rapport

Le *rapport Cisco du 1er semestre 2017 sur la cybersécurité* explore les dynamiques précédemment évoquées en abordant les points suivants :

Tactiques des hackers

Nous examinons certaines des méthodes employées par les hackers pour compromettre les données des utilisateurs et infiltrer leurs systèmes. Il est essentiel que les acteurs de la protection comprennent les changements de tactique des hackers pour pouvoir adapter leurs pratiques de sécurité et former les utilisateurs. Ce rapport couvre : les nouveautés en matière de malwares, les tendances en matière d'attaques web et de spams, les risques liés aux applications potentiellement indésirables (PUA) comme les spywares, les attaques de messageries d'entreprise (BEC), l'évolution des modèles économiques des hackers et les menaces visant

les systèmes médicaux. Nos chercheurs spécialistes des menaces présentent également leur analyse de l'évolution rapide des outils et des techniques de certains hackers, et fournissent des informations actuelles sur les efforts déployés par Cisco pour réduire le temps de détection des menaces.

Vulnérabilités

Dans ce rapport, nous donnons également un aperçu des vulnérabilités et autres expositions qui augmentent le risque de compromission ou d'attaque des utilisateurs et des entreprises. Nous évoquons aussi les pratiques de sécurité insuffisantes, comme l'application trop tardive des correctifs de vulnérabilités connues, la non-limitation des accès privilégiés aux systèmes cloud et l'absence de gestion de l'infrastructure et des terminaux. Autre aspect important : les raisons pour lesquelles le développement de l'IoT et la convergence des départements IT et OT (technologies opérationnelles) augmentent les risques encourus par les entreprises, leurs utilisateurs et leurs clients, et les mesures à prendre dès maintenant pour limiter ces risques avant qu'il soit trop tard.

Opportunités pour les acteurs de la protection

Le *rapport Cisco du 1er semestre 2017 sur la cybersécurité* présente d'autres conclusions de l'enquête Cisco sur l'efficacité des mesures de sécurité. Nous proposons une analyse approfondie des principaux problèmes de sécurité dans huit secteurs : celui des opérateurs télécoms, du secteur public, du commerce, de la production industrielle, de la distribution d'énergie, de la santé, des transports et des services financiers. Les experts de Cisco fournissent des recommandations pour aider ces entreprises à améliorer leur solution de sécurité, notamment en utilisant des services qui pallient la pénurie de personnel compétent et de connaissances, en réduisant la complexité de leur environnement informatique et en adoptant l'automatisation.

La conclusion du rapport invite les responsables de la sécurité à discuter dès que possible des risques et des budgets concernant la cybersécurité avec leurs dirigeants et leurs conseils d'administration, et fournit des recommandations pour commencer cette conversation.

Remerciements

Nous tenons à remercier notre équipe de spécialistes de la cybersécurité, tous les autres experts Cisco et nos partenaires technologiques pour leur contribution à la rédaction du *Rapport Cisco sur la cybersécurité du 1er semestre 2017*. Leurs recherches et leurs points de vue sont déterminants. Grâce à eux, Cisco peut fournir à la communauté des spécialistes de la sécurité, aux entreprises et aux utilisateurs des informations pertinentes sur la complexité et l'étendue des cybermenaces mondiales modernes, et leur présenter les bonnes pratiques et les connaissances nécessaires à l'amélioration de leur protection.

Nos partenaires technologiques jouent également un rôle vital en nous aidant à développer des solutions de sécurité simples, ouvertes et automatisées qui permettent aux entreprises d'intégrer les solutions dont elles ont besoin pour sécuriser leurs environnements.

La liste complète des auteurs ayant participé à la rédaction du *Rapport Cisco sur la cybersécurité du 1er semestre 2017*, partenaires technologiques compris, est disponible à la page 87.

Principales conclusions

- Les attaques de messagerie d'entreprise (BEC) sont devenues un vecteur de menace très lucratif pour les hackers. Selon l'Internet Crime Complaint Center (IC3), les fraudes BEC ont permis le vol de 5,3 milliards de dollars entre octobre 2013 et décembre 2016. En comparaison, les exploits de type ransomware ont permis le vol d'un milliard de dollars en 2016.
- Le risque d'infection par spywares de type PUA (applications potentiellement indésirables) est sous-estimé, voire complètement ignoré, par de nombreuses entreprises. Pourtant, un spyware peut voler les données des utilisateurs et de l'entreprise, affaiblir le dispositif de sécurité des appareils et accroître les infections par malware. Par ailleurs, les infections par spyware se propagent. Les chercheurs Cisco spécialistes des menaces ont étudié trois familles de spywares et découvert qu'ils étaient présents dans 20 % des 300 entreprises de l'échantillon.
- L'Internet des objets (IoT) est porteur de promesses pour la collaboration et l'innovation dans l'entreprise. Mais à mesure qu'il se développe, le risque pour la sécurité augmente. Le manque de visibilité est un problème : les acteurs de la protection n'ont tout simplement pas connaissance des appareils IoT connectés à leur réseau. Ils doivent agir vite pour surmonter ce problème, ainsi que les autres freins à la sécurité IoT. Les cybercriminels exploitent déjà les failles de sécurité des appareils IoT. Les appareils connectés servent de bastions aux hackers. Ils leur permettent de s'infiltrer discrètement et relativement facilement dans les réseaux.
- Cisco traque son temps de détection moyen depuis novembre 2015. Depuis cette date, la tendance globale est à la baisse. Nous sommes passés d'un peu plus de 39 heures au début de notre étude à environ 3,5 heures pour la période de novembre 2016 à mai 2017.
- Cisco a observé une croissance globale du volume de spams depuis le 2e semestre 2016, ce qui semble coïncider avec une baisse sensible de l'activité des kits d'exploit pendant la même période. Les hackers qui utilisaient principalement des kits d'exploit pour diffuser des ransomwares optent désormais pour des spams, qui contiennent notamment des documents malveillants exécutant des macros capables de contourner la plupart des solutions de sandboxing car l'interaction de l'utilisateur est requise pour infecter les systèmes et propager les charges utiles.
- Les attaques de chaîne d'approvisionnement sont un moyen pour les hackers de propager un malware vers de nombreuses entreprises par le biais d'un seul site compromis. Dans le cas d'une attaque étudiée par RSA, un partenaire de Cisco, la page web de téléchargement d'un éditeur de logiciels a été compromise, permettant à l'infection de se propager vers toutes les entreprises ayant téléchargé le logiciel de cet éditeur.
- Selon Radware, un partenaire de Cisco, l'augmentation spectaculaire de la fréquence, de la complexité et de l'ampleur des cyberattaques au cours de l'année écoulée suggère que le modèle économique du piratage a passé un cap. Radware observe que les hackers ont aujourd'hui rapidement et facilement accès à une gamme étendue de ressources aussi peu coûteuses qu'efficaces.
- En matière de sécurité d'entreprise, le cloud n'est pas suffisamment pris en compte. Pourtant, le risque lié à OAuth (Open authorization) et la gestion insuffisante des comptes d'utilisateur privilégiés créent des failles facilement exploitables par les hackers. D'après nos recherches, le cloud intéresse désormais les hackers qui cherchent par tous les moyens à exploiter ses nouveaux environnements.
- L'activité des kits d'exploit a considérablement diminué, et l'innovation dans ce domaine a stagné, depuis qu'Angler et d'autres kits d'exploit ont disparu ou changé de modèle économique. Mais les tendances passées sur ce marché indiquent que cette situation est probablement temporaire. Toutefois, d'autres facteurs comme la difficulté à exploiter les vulnérabilités des fichiers créés avec la technologie Adobe Flash pourraient ralentir cette résurgence.
- Selon une étude menée par Rapid7, un partenaire de Cisco, les services DevOps déployés de façon incorrecte ou intentionnellement laissés ouverts pour faciliter l'accès des utilisateurs légitimes représentent un risque non négligeable pour les entreprises. En fait, beaucoup de ces instances ont déjà été rançonnées.
- L'analyse par ThreatConnect des domaines co-localisés utilisés par les hackers du groupe de cyber-espionnage Fancy Bear a démontré l'intérêt d'étudier l'infrastructure IP de ces cybercriminels. En étudiant cette infrastructure, on peut établir une liste plus complète des domaines, adresses IP et adresses e-mail qui doivent être bloqués de façon proactive.
- À la fin de l'année 2016, les chercheurs Cisco spécialistes des menaces ont découvert et signalé trois vulnérabilités de type exécution de code à distance sur des serveurs Memcached. Quelques mois plus tard, une analyse a révélé que 79 % des 110 000 serveurs Memcached exposés et précédemment identifiés étaient toujours sensibles aux trois vulnérabilités, car ils n'avaient pas été corrigés.

Introduction

Introduction

Les menaces changent constamment. Mais leur évolution rapide et l'amplitude des attaques observées par les spécialistes de la cybersécurité Cisco et leurs partenaires technologiques ont lieu d'inquiéter. Selon les experts, certains acteurs de l'économie parallèle pourraient actuellement préparer une infrastructure permettant de déployer des attaques à l'impact aussi durable que dévastateur.

Une nouvelle stratégie malveillante : la destruction de service (DeOS)

Les hackers cherchent maintenant à éliminer le « filet de sécurité » mis en place par les entreprises pour restaurer leurs systèmes et leurs données en cas de contamination par un programme malveillant, une campagne de ransomware ou tout autre cyberincident perturbant gravement leurs opérations. Le déroulement d'une attaque DeOS et ses manifestations dépendent des motivations des hackers, de leur créativité et de leurs compétences.

Ce dont nous sommes certains, c'est que l'émergence de l'Internet des objets et la myriade d'appareils et de systèmes IoT comportant des failles prêtes à être exploitées joueront un rôle central dans la prolifération de ces campagnes aux retombées dévastatrices. L'IoT est le nouveau terrain sur lequel les hackers et les acteurs de la protection s'affrontent.

En attendant, dans l'environnement actuel, les hackers disposent d'espaces et de périodes limités pour mener leur action. Ils doivent constamment changer de stratégie pour ne pas être détectés. Ils sont obligés d'innover rapidement pour optimiser l'impact de leurs menaces, comme ils ont su le faire en adoptant les technologies Bitcoin et Tor de façon à rendre leurs ransomwares plus efficaces. Il leur arrive parfois de devoir utiliser ou réutiliser des méthodes telles que les e-mails malveillants et l'ingénierie sociale, notamment lorsque leurs outils habituels (kits d'exploit ou autres) perdent en efficacité grâce au travail des acteurs de la sécurité ou ne sont plus assez innovants.

La clé : réduire la fragmentation des outils de sécurité

Les acteurs de la protection peuvent revendiquer de nombreux succès, mais ils doivent compter sur le fait que les hackers parviennent à déjouer les systèmes de défense. Ils disposent déjà de la plupart des solutions nécessaires pour ralentir les attaques et limiter le champ d'action des hackers. Malheureusement, ils n'utilisent pas toujours ces outils à bon escient. Dans tous les secteurs, les professionnels de la sécurité déclarent déployer un assortiment d'outils de plusieurs fournisseurs. Cette complexité se situe à l'opposé de l'approche globale et simplifiée que nous recommandons.

Les solutions multiproduits fragmentées entravent la capacité d'une entreprise à répondre correctement aux attaques. Elles multiplient aussi les alertes à traiter, alors que les équipes de sécurité manquent souvent de ressources. Quand ces équipes parviennent à réduire le nombre de fournisseurs et à adopter une approche de la sécurité ouverte, intégrée et simplifiée, elles peuvent réduire la surface d'exposition aux menaces. Elles peuvent également mieux se préparer à faire face aux enjeux sécuritaires d'un monde de l'IoT de plus en plus présent, et à se conformer au nouveau Règlement général sur la protection des données (RGPD), qui entrera en vigueur dans l'Union européenne dès mai 2018.

Comportement des hackers

COMPORTEMENT DES HACKERS

Cette section propose une présentation générale des tendances et des innovations constatées en matière d'attaques web et e-mail. Les spécialistes de la cybersécurité de Cisco et nos partenaires technologiques présentent leurs recherches, leurs observations et leurs conseils pour aider les dirigeants d'entreprises et leurs équipes de sécurité à comprendre les tactiques auxquelles les hackers peuvent recourir pour cibler leurs réseaux dans les mois à venir, alors que l'IoT se développe. Nous exposons également quelques recommandations en matière de sécurité qui contribueront à réduire l'exposition de votre entreprise et de vos utilisateurs.

Kits d'exploit : en déclin, mais encore bien présents

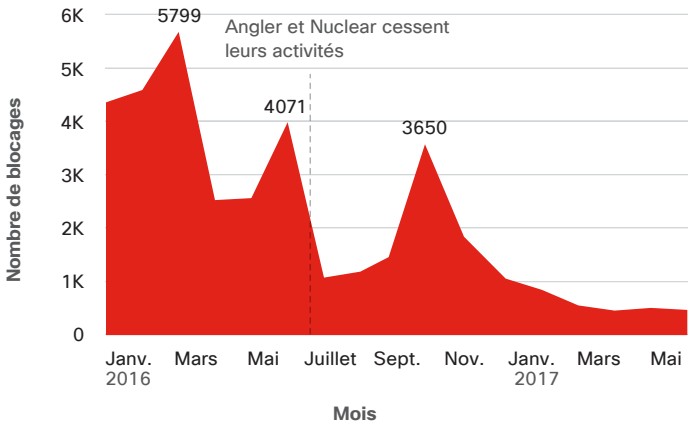
En 2016, trois des plus importants kits d'exploit existants, Angler, Nuclear et Neutrino, ont soudainement disparu.[1] Angler et Nuclear n'ont pas réapparu. La disparition de Neutrino n'était que temporaire : le kit d'exploit est toujours actif, même s'il ne réapparaît que pendant de courtes périodes. Ses créateurs le louent à certains opérateurs dans le cadre d'accords exclusifs. Cette approche permet de contenir l'activité de Neutrino de manière à ce qu'il ne devienne pas trop prévalent et facile à détecter.

Dans le *Rapport annuel Cisco 2017 sur la cybersécurité*, nous avons évoqué comment de tels bouleversements sur la scène des kits d'exploit permettent aux hackers marginaux ou débutants de s'illustrer à peu de frais. Cependant, en cette fin du premier semestre 2017, aucun nouvel acteur ne semble se présenter. Il ne reste qu'une poignée de kits d'exploit en activité. Le Kit RIG, longtemps compté parmi les favoris des hackers, reste le plus visible. On connaît sa capacité à cibler les vulnérabilités des technologies Adobe Flash, Microsoft Silverlight et Microsoft Internet Explorer.

Dans l'ensemble, l'activité des kits d'exploit a connu un déclin spectaculaire depuis janvier 2016, comme le montre la Figure 1.

Cette tendance confirme ce que nous avons constaté après l'arrestation, en Russie, de l'auteur et distributeur d'un autre kit d'exploit très répandu, Blackhole.[2] La fin de Blackhole a eu un fort impact sur le marché des kits d'exploit. Il a fallu du temps aux nouveaux acteurs pour faire leur apparition. Le grand gagnant de cette course fut Angler, qui a fait atteindre de nouveaux records de sophistications aux kits d'exploit et aux téléchargements de type « drive-by ».[3]

Figure 1 Activité des kits d'exploit



Source : Cisco Security Research

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

1 *Rapport Cisco sur la cybersécurité – 1er semestre 2016 :* cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html
2 « Meet Paunch: The Accused Author of the Blackhole Exploit Kit » de Brian Krebs, KrebsonSecurity blog, 6 décembre 2013 : krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/.
3 « Connecting the Dots Reveals Crimeware Shake-Up », de Nick Biasini, Talos, 7 juillet 2016 : blog.talosintelligence.com/2016/07/lurk-crimeware-connections.html.

Angler ciblait une multitude de vecteurs d'attaque. Plus rapides que leurs concurrents, ses auteurs innovaient sans cesse et ajoutaient instantanément toute nouvelle vulnérabilité à leur kit d'exploit. à bien des égards, ils ont redéfini les critères d'excellence en matière de kits d'exploit, ce qui a entraîné une augmentation du vol de données et de techniques entre les hackers qui voulaient rester compétitifs. Suite à sa disparition, les kits d'exploit semblent avoir ralenti dans leurs innovations.

Mais la fin d'Angler n'est qu'une cause possible de cette stagnation. L'autre cause est que la technologie Flash est devenue plus difficile à exploiter. Les vulnérabilités de Flash ont contribué au développement et à la vitalité du marché des kits d'exploit pendant des années. Mais une attention accrue à ces vulnérabilités et la publication plus rapide de correctifs ont rendu la technologie Flash plus sûre. Aujourd'hui, les hackers sont souvent contraints de cibler plusieurs vulnérabilités pour exploiter un système.

Les mises à jour de sécurité automatiques des navigateurs et systèmes d'exploitation modernes contribuent aussi à protéger les utilisateurs de nouvelles attaques par kit d'exploit. Une autre tendance s'est ainsi développée : face à la baisse du marché des kits d'exploit, les cybercriminels se tournent (ou se replient) vers les e-mails pour envoyer leurs ransomwares et autres malwares de façon rapide et peu onéreuse. Ils font également preuve de plus d'imagination dans leurs méthodes pour échapper aux détections. Par exemple, les chercheurs de Cisco ont remarqué une augmentation du volume de spams contenant des documents porteurs de macros malveillantes, comme des fichiers Word, Excel ou PDF, qui peuvent déjouer de nombreuses solutions de sandboxing en forçant l'utilisateur à interagir avec ces fichiers afin d'installer des logiciels malveillants et d'infecter leurs systèmes.[4]

Une mutation souterraine en cours ?

Une résurgence prochaine du marché des kits d'exploit ne fait aucun doute : la cybercriminalité est un secteur qui pèse des milliards. Il suffira de l'apparition d'un nouveau vecteur d'attaque associant facilité d'exploitation et potentiel d'impact à grande échelle pour que les kits d'exploit retrouvent toute leur popularité, à grand renfort de concurrence et d'innovation.

Il est donc essentiel de rester vigilant. De nombreux kits d'exploit restent utilisés et parviennent à compromettre les données des utilisateurs et à installer des programmes malveillants dans leurs systèmes. Ces attaques peuvent survenir en tout lieu et à tout moment. Il suffit qu'un seul système présente une vulnérabilité pour qu'elle soit exploitée. Les entreprises peuvent limiter ces risques en prenant soin d'appliquer les correctifs dès leur publication (en particulier s'ils portent sur des vulnérabilités de navigateur web, ou de plug-ins associés à ces navigateurs) et en protégeant leurs systèmes en profondeur. Il est important de s'assurer que les utilisateurs travaillent avec des navigateurs sécurisés, en désactivant et en supprimant tous les plug-ins inutiles pour réduire de façon significative les risques liés aux kits d'exploit.

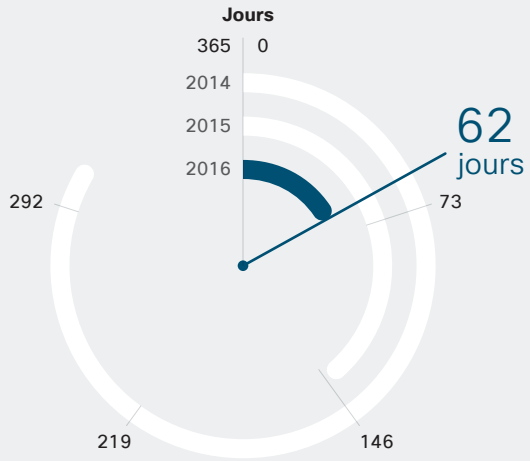
4 « Threat Spotlight: Mighty Morphin Malware Purveyors: Locky Returns via Necurs » de Nick Biasini, blog Talos, 21 avril 2017 : blogs.cisco.com/security/talos/locky-returns-necurs.

Les acteurs de la protection forcent les hackers à s'adapter

La réduction du délai de correction des vulnérabilités connues des logiciels Flash par les acteurs de la protection est un facteur qui a contribué à ralentir la croissance et l'innovation sur le marché des kits d'exploit. Comme évoqué dans les précédents rapports de Cisco sur la cybersécurité, le logiciel Flash a été l'un des vecteurs d'attaque web de prédilection des hackers qui souhaitaient exploiter et compromettre les systèmes. Toutefois, il devient de plus en plus difficile à exploiter, notamment en raison d'une amélioration des pratiques de correction.

Une étude de Qualys, partenaire de Cisco spécialisé dans la gestion des vulnérabilités et de la sécurité du réseau, montre que les acteurs de la protection ont réduit le temps moyen requis pour corriger 80 % des vulnérabilités Flash de leurs entreprises, de 308 jours en 2014 à 144 jours en 2015, puis 62 jours en 2016 (voir la Figure 2). L'étude s'appuie sur des données obtenues sur plus de trois milliards d'analyses des vulnérabilités effectuées chaque année par Qualys sur sa base internationale de clients.

Figure 2 Nombre de jours requis pour appliquer un correctif à 80 % des vulnérabilités Flash.



Source : Qualys

Face à des entreprises plus réactives dans l'application de correctifs lorsque des vulnérabilités sont détectées dans Flash, certains auteurs de kits d'exploit sont susceptibles de porter leur attention sur d'autres vulnérabilités négligées jusqu'alors. Les équipes de sécurité doivent donc prendre le temps de vérifier si toutes les vulnérabilités Flash ont bien été corrigées, puis de traiter en priorité les vulnérabilités présentant le plus de risques pour leur entreprise.

En outre, certains hackers qui avaient l'habitude de recourir à des kits d'exploit ciblant Flash pour installer leurs ransomwares et autres programmes malveillants vont certainement utiliser d'autres techniques, au moins à court terme, afin de continuer à atteindre leurs objectifs en matière de revenus.

Les spécialistes de la cybersécurité de Cisco ont ainsi constaté, par exemple, une augmentation du volume d'e-mails indésirables aux pièces jointes d'apparence anodine, mais contenant des macros malveillantes (voir « Les nouveaux malwares : analyse de six mois d'évolutions », page 23). Cette tendance semble coïncider avec le récent déclin constaté dans l'utilisation de kits d'exploit (pour en savoir plus, voir le chapitre « Kits d'exploit : en déclin, mais encore bien présents », page 9).

Les méthodes d'attaque sur le web démontrent qu'Internet est arrivé à maturité

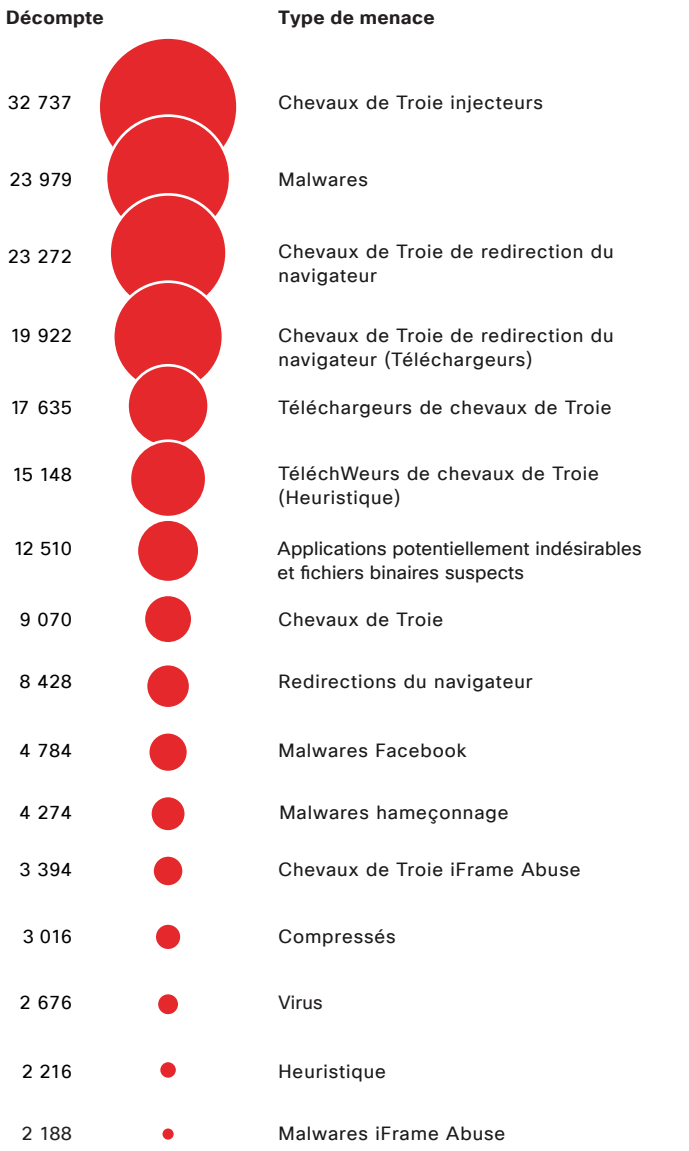
Les proxys existent depuis les toutes premières années du web, et leurs fonctionnalités ont mûri au rythme des évolutions d'Internet. Aujourd'hui, les acteurs de la protection utilisent des proxys pour analyser les contenus et détecter les menaces potentielles, les infrastructures Internet vulnérables ou les vulnérabilités réseau grâce auxquelles les hackers peuvent accéder aux ordinateurs des utilisateurs, infiltrer les entreprises et mener à bien leurs campagnes d'attaques. Ces menaces comprennent :

- Les applications potentiellement indésirables (PUA), telles que des extensions de navigateur malveillantes
- Les chevaux de Troie (injecteurs et téléchargeurs)
- Les liens vers des sites de spam et de publicités malveillantes
- Les vulnérabilités propres aux navigateurs, telles que JavaScript ou les moteurs d'affichage graphique
- Les redirections de navigateurs, les détournements de clics (« clickjacking ») et autres méthodes servant à diriger les utilisateurs vers des contenus web malveillants

La Figure 3 représente les catégories de programmes malveillants favorisées par les hackers entre novembre 2016 et mai 2017. Les experts de la cybersécurité CISCO ont créé ce graphique à partir des évènements de sécurité web de notre société. La liste de la Figure 3 recense une sélection de méthodes parmi les plus fiables et les moins coûteuses pour compromettre les données d'un grand nombre d'utilisateurs en infectant leurs ordinateurs et leurs systèmes. Ces méthodes incluent :

- Les « kits d'approche initiale », tels que les chevaux de Troie et les utilitaires servant à faciliter l'infection initiale d'un ordinateur. (Une macro de virus dans un document Word malveillant, par exemple.)
- Les applications potentiellement indésirables (PUA), comme les extensions de navigateur malveillantes.
- Les fichiers binaires Windows suspects, qui délivrent des programmes comme des logiciels publicitaires et des spywares.[5]
- Les escroqueries sur Facebook, qui comprennent des offres factices, certains contenus multimédias et de fausses enquêtes.
- Les malwares (de type ransomware ou des logiciels d'enregistrement des frappes) conçus pour installer du code actif sur les hôtes compromis.

Figure 3 Logiciels malveillants les plus fréquemment bloqués entre novembre 2016 et mai 2017

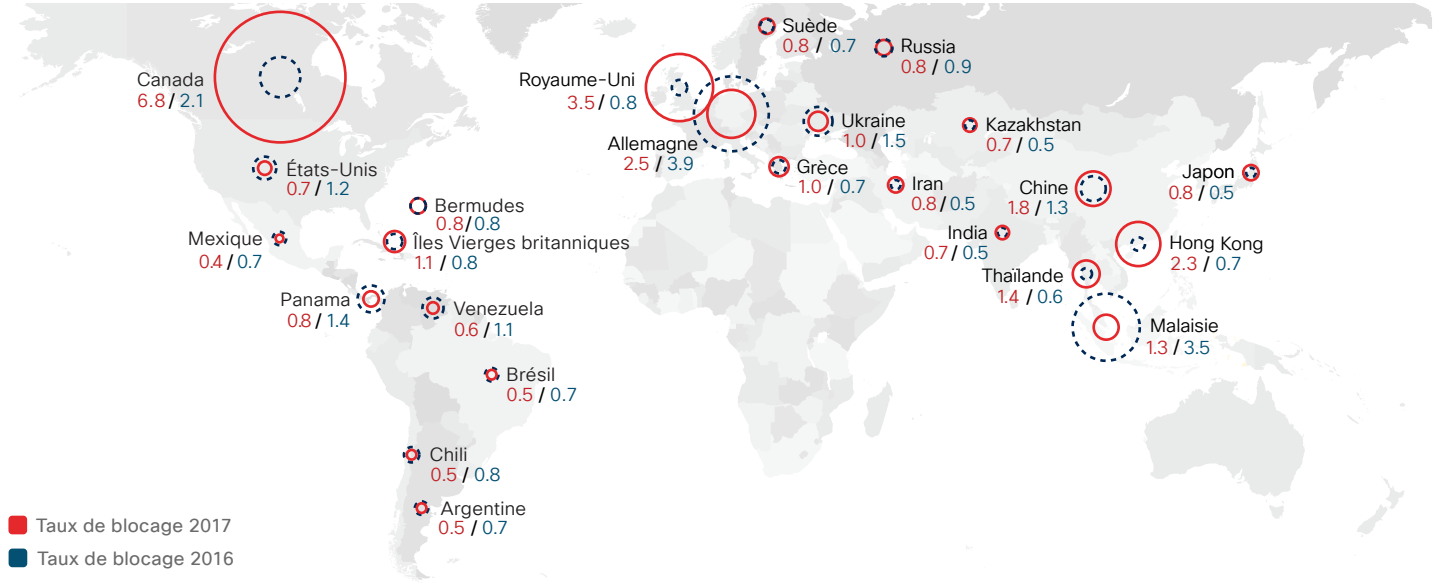


Source : Cisco Security Research

5 Remarque : dans le *Rapport annuel Cisco 2017 sur la cybersécurité* (disponible à la page -us-annual-cybersecurity-report-2), les chercheurs de Cisco signalent que les logiciels publicitaires malveillants, y compris les injecteurs de publicités, les mécanismes de piratage des paramètres du navigateur, les utilitaires et les téléchargeurs malveillants, présentent un problème de plus en plus présent. En page 14 de ce rapport, nous examinons les risques encourus par les utilisateurs et les entreprises face aux applications potentiellement indésirables (PUA) telles que les spywares.

Tous les logiciels ci-dessus apparaissent dans notre liste de logiciels malveillants les plus fréquemment rencontrés. Au vu de la stabilité de cette liste, on peut penser qu'Internet est arrivé à un point de maturité tel que les hackers savent désormais pertinemment quelles méthodes d'attaque utiliser pour compromettre les données d'utilisateurs à grande échelle et sans grande difficulté. L'utilisation de navigateurs sécurisés et la désactivation de tous les plug-ins inutiles restent deux des principaux moyens de limiter l'exposition aux menaces les plus fréquentes sur le web.

Figure 4 Blocages de sites web dans le monde, de novembre 2016 à mai 2017



Source : Cisco Security Research

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

Blocages de site web à travers le monde

Cisco suit les blocages de malwares par pays et par région. Les hackers changent sans arrêt de zone d'opération, à la recherche d'infrastructures défaillantes à partir desquelles ils peuvent lancer leurs attaques. En examinant le volume global du trafic Internet et l'activité de blocage, les chercheurs Cisco en sécurité peuvent fournir des informations sur la provenance des programmes malveillants.

Nous avons sélectionné les pays de l'étude en fonction de leur volume de trafic Internet. Un taux de blocage de 1 indique que le nombre de blocages observés est proportionnel à la taille du réseau. Les pays et régions présentant une activité de blocage supérieure au taux normal ont probablement de nombreux hôtes et serveurs web présentant des failles sur leurs réseaux. Le graphique ci-dessus représente les blocages de sites web à travers le monde.

Les spywares méritent leur mauvaise réputation

Une grande partie des logiciels publicitaires appelés applications potentiellement indésirables (PUA) sont des spywares. Les éditeurs de spywares présentent leurs logiciels comme des outils légitimes qui fournissent des services utiles et sont soumis à des contrats de licence de l'utilisateur final (CLUF). Mais quelle que soit la manière dont ils présentent les choses, les spywares sont tout simplement des malwares.

Les spywares se faisant passer pour des applications potentiellement indésirables (PUA) sont des logiciels qui collectent et transmettent subrepticement des informations sur les activités de l'utilisateur. Ils s'installent généralement sur l'ordinateur à l'insu de l'utilisateur. Dans le cadre de cette présentation, nous pouvons classer les spywares dans trois grandes catégories : les logiciels publicitaires (« adwares »), les logiciels d'analyse des systèmes et les chevaux de Troie).

Dans l'environnement professionnel, le spyware présente plusieurs risques. Par exemple, il peut :

- Voler les informations d'un utilisateur et de son entreprise, en particulier des informations nominatives, sensibles ou confidentielles.
- Affaiblir la sécurité de certains appareils en modifiant leurs configurations, en installant des logiciels supplémentaires et en autorisant l'accès à des tiers. Un logiciel peut aussi potentiellement activer l'exécution du code à distance sur l'appareil, permettant aux hackers de le contrôler entièrement.
- Accroître les infections par malware. Une fois les utilisateurs infectés par des PUA, comme un spyware ou un logiciel publicitaire, ils sont vulnérables à d'autres infections par malware.

Pour mieux comprendre les infections par spyware, les chercheurs Cisco ont étudié le trafic réseau d'environ 300 entreprises entre novembre 2016 et mars 2017 afin de déterminer quels types de spywares étaient présents dans ces entreprises et dans quelle mesure.

Notre étude nous a permis de découvrir que trois familles de spywares avaient affecté plus de 20 % des entreprises de notre échantillon pendant la période observée : Hola, RelevantKnowledge et DNSChanger/DNS Unlocker. Chaque mois, des infections ont été identifiées dans plus de 25 % des entreprises de notre échantillon (voir la Figure 5).

Il existe des centaines de familles de spywares. Cependant, nous en avons traité en priorité trois, car elles sont parmi les types les plus fréquemment rencontrés dans les environnements d'entreprise analysés. Voici quelques informations supplémentaires concernant ces trois familles de spyware.

Figure 5 Pourcentage d'entreprises affectées par les familles de spywares sélectionnées (novembre 2016 – mars 2017).

25 % des entreprises interrogées tous les mois étaient contaminées par Hola, RelevantKnowledge ou DNSChanger/DNS Unlocker

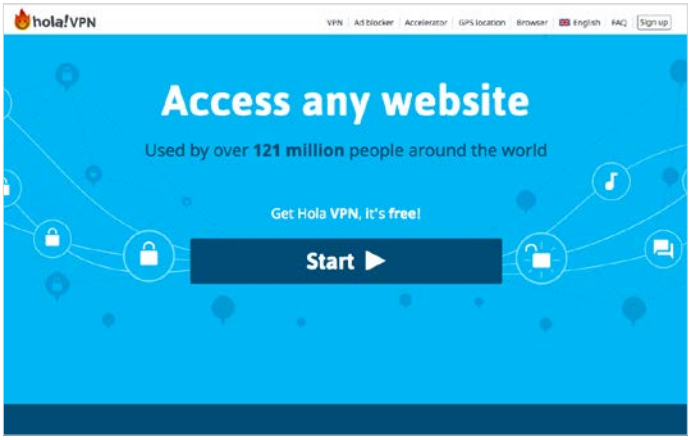
Source : Cisco Security Research

VPN Hola

Hola (spyware et logiciel publicitaire) est une application web et mobile en freemium qui fournit un type de VPN à ses utilisateurs via un réseau peer to peer. Cette application pratique également la mise en cache peer to peer, qui suppose que les utilisateurs doivent « stocker » des contenus téléchargés par d'autres utilisateurs. Hola est distribué comme une application côté client accessible par navigateur. L'application est disponible sous forme d'extension ou de logiciel autonome.

La capture d'écran du site web de Hola, sur la Figure 6, montre la façon dont ce spyware est présenté par ses créateurs : un service gratuit et utile permettant à ses utilisateurs « d'accéder à n'importe quel site ». Ils prétendent également que Hola est « utilisé par plus de 121 millions de personnes à travers le monde ».

Figure 6 Capture d'écran de la page d'accueil du VPN Hola



Pourquoi estimons-nous qu'il s'agit d'un spyware ?
Les fonctionnalités de Hola incluent, entre autres choses, la vente de bande passante d'autres utilisateurs via un service appelé Luminati, l'installation de son propre certificat de signature de code sur les systèmes des utilisateurs, le téléchargement de n'importe quel fichier avec l'option de contourner l'antivirus et l'exécution de code à distance.

RelevantKnowledge

RelevantKnowledge (spyware et logiciel d'analyse de système) collecte des quantités massives d'informations sur les comportements de navigation Internet, les systèmes et les configurations des utilisateurs. RelevantKnowledge peut être installé directement ou via des regroupements de logiciels, parfois sans le consentement direct de l'utilisateur.

Figure 7 Capture d'écran de la page d'accueil de RelevantKnowledge

Comme pour Hola, cette page d'accueil (Figure 7) est conçue pour associer l'abonnement au produit à un service rendu à l'utilisateur. Par exemple, les créateurs de ce spyware promettent des dons d'arbres à l'association « Trees for Knowledge » au nom de chaque membre.

Pourquoi estimons-nous qu'il s'agit d'un spyware ?
Comme nous l'avons indiqué plus tôt, RelevantKnowledge permet l'installation de logiciels sans le consentement de l'utilisateur. L'application collecte également des informations pour créer des profils destinés à être vendus à des tiers, de façon anonyme, soit individuellement, soit au sein d'un ensemble de données, dans une optique de « recherche ».

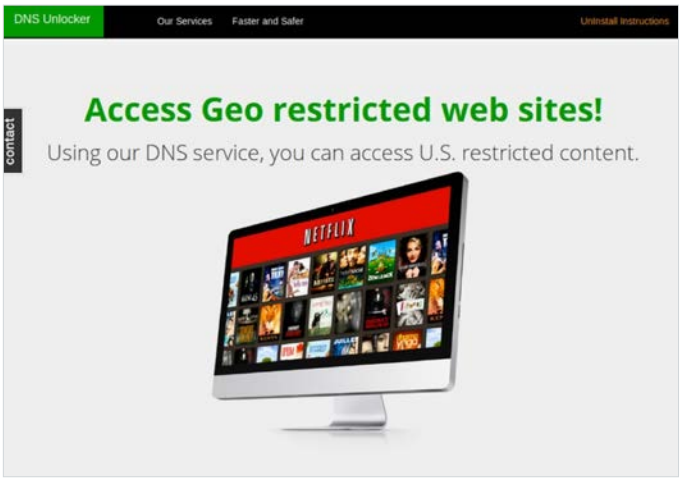
DNS Changer et DNS Unlocker

DNS Changer et DNS Unlocker sont deux versions d'un même logiciel malveillant. Le premier est un cheval de Troie qui modifie ou détourne les réglages DNS de l'hôte infecté.[6] DNS Unlocker est un service de logiciel publicitaire proposant une option de désinstallation.

Ce spyware remplace les serveurs de noms par les siens pour envoyer les requêtes HTTP et autres depuis l'hôte vers un ensemble de serveurs contrôlés par les hackers et capables d'intercepter, d'inspecter et de modifier le trafic de l'hôte. Il n'infecte pas les navigateurs, mais les terminaux. Il utilise PowerShell, un langage de programmation orienté objet et un interpréteur interactif des lignes de commandes de Microsoft Windows pour exécuter des commandes sur l'hôte infecté. Cela permet aux hackers d'accéder à distance au système.

À en croire les créateurs de DNS Unlocker, ce spyware serait un service conçu pour permettre aux utilisateurs d'accéder aux contenus sujets à des restrictions géographiques, tels que certains flux vidéo.

Figure 8 Capture d'écran de la page d'accueil de DNS Unlocker

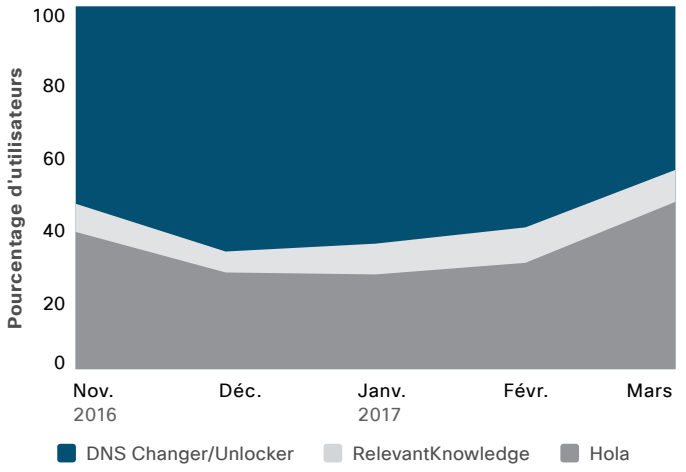


Pourquoi estimons-nous qu'il s'agit d'un spyware ? Outre la fonctionnalité citée ci-dessus et d'autres capacités, DNS Unlocker peut voler des informations nominatives, rediriger le trafic utilisateur en temps réel en injectant des contenus dans des services spécifiques, comme la publicité en ligne.

Notre étude montre que DNS Unlocker est le plus répandu

DNS Unlocker est le plus répandu des trois familles de spywares évoquées dans notre étude. Il est à l'origine de plus de 40 % des infections de spywares dans les entreprises de notre sélection.

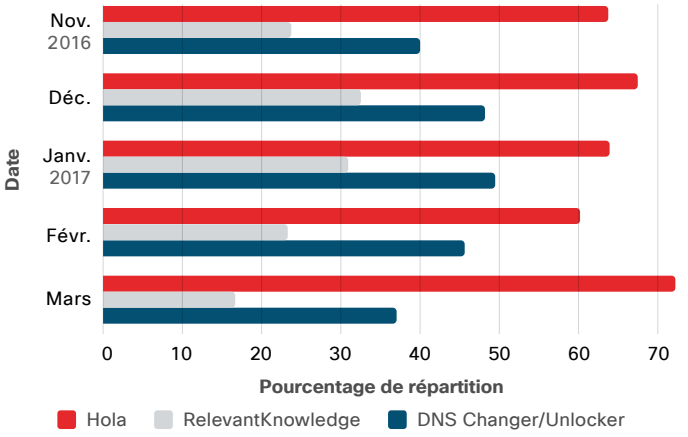
Figure 9 Comparatif des utilisateurs affectés, par famille de spyware



Source : Cisco Security Research

6 « DNSChanger Outbreak Linked to Adware Install Base », de Veronica Valeros, Ross Gibb, Eric Hulse et Martin Rehak, blog Cisco Security, 10 février 2016 : blogs.cisco.com/security/dnschanger-outbreak-linked-to-adware-install-base.

Figure 10 Distribution des spywares



Source : Cisco Security Research

Parmi ces trois familles, nous avons constaté que Hola était le plus distribué, puisqu'il a affecté plus de 60 % des entreprises de notre échantillon tous les mois pendant la période considérée (voir la Figure 10). Cette famille de spywares devient aussi progressivement la plus distribuée, même si sa progression est lente.

DNS Unlocker, de son côté, affecte un plus grand nombre d'utilisateurs, dans un nombre moins élevé d'entreprises (Figure 10). En janvier, le nombre d'infections liées à cette famille de spywares a augmenté de façon significative par rapport au taux observé en novembre, mais il semble avoir décliné depuis selon nos chercheurs.

Les infections de spywares doivent être prises au sérieux

Les infections de spywares se généralisent dans de nombreuses entreprises, mais on ne les considère généralement pas comme un risque significatif pour la sécurité. Toutefois, à l'instar des infections liées aux logiciels publicitaires, présentes dans les trois quarts des entreprises analysées lors d'une autre enquête récente,[7] les infections de spywares augmentent le risque d'activité malveillante pour les utilisateurs et les entreprises.

Même si les opérateurs présentent les spywares comme des services conçus pour protéger ou aider les utilisateurs, le véritable objectif du malware est de localiser et recueillir des informations sur les utilisateurs et leurs entreprises, souvent à leur insu ou sans leur consentement direct. Les entreprises fournissant ces spywares sont réputées pour vendre et fournir un accès aux données collectées, permettant à des tiers de récolter des informations dans un anonymat relatif. Ces informations peuvent être utilisées pour identifier des ressources critiques, cartographier les infrastructures internes des entreprises et orchestrer des attaques ciblées.

Les infections par spyware des navigateurs et des terminaux doivent être traitées rapidement. Les équipes de sécurité doivent constamment s'informer des capacités des spywares et déterminer le type d'informations menacé. Elles doivent également prendre le temps de créer un guide des mesures à prendre pour remédier aux infections causées par les spywares, logiciels publicitaires et autres applications à risque[8], tout en informant les utilisateurs finaux sur les risques liés aux applications potentiellement indésirables (PUA). Avant d'accepter un contrat de licence d'utilisateur final pour une PUA, les utilisateurs doivent, au minimum, prendre le temps de lire les sections relatives à la collecte, au stockage et au partage de leurs informations.

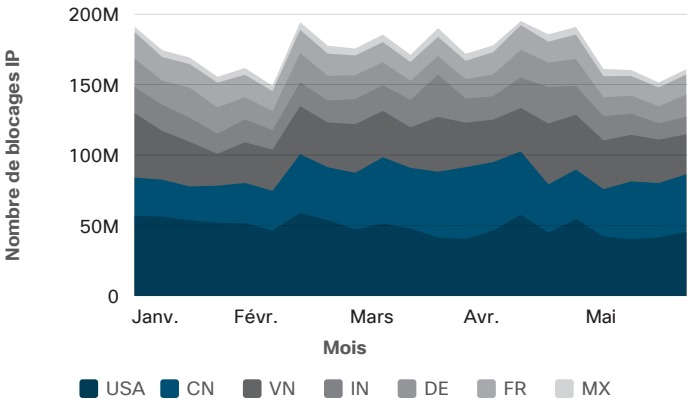
Lorsque l'on refuse de considérer les spywares se faisant passer pour des applications potentiellement indésirables (PUA) comme une forme de malware, on s'expose à des risques d'infections et de sécurité supplémentaires. Le problème des spywares est appelé à prendre de l'ampleur, car les opérateurs intègrent des fonctionnalités toujours plus malveillantes dans leurs logiciels et continuent à tirer parti de l'incapacité des entreprises à y remédier.

7 Pour en savoir plus, téléchargez le *rapport annuel Cisco 2017 sur la cybersécurité*, disponible à la page : cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.
8 Riskware est un logiciel légitime qui pouvait être modifié par les cybercriminels et utilisé à des fins malveillantes.

La recrudescence mondiale du nombre de spams est sans doute liée au déclin des kits d'exploit

Les chercheurs Cisco dédiés à la sécurité ont constaté une augmentation des blocages de connexions des adresses IP chinoises entre janvier et mai 2017. Les volumes globaux de spams, en ce premier semestre, ont diminué et se stabilisent si on les compare aux sommets atteints vers la fin de 2016.

Figure 11 Blocages d'adresses IP par pays



Source : Cisco Security Research

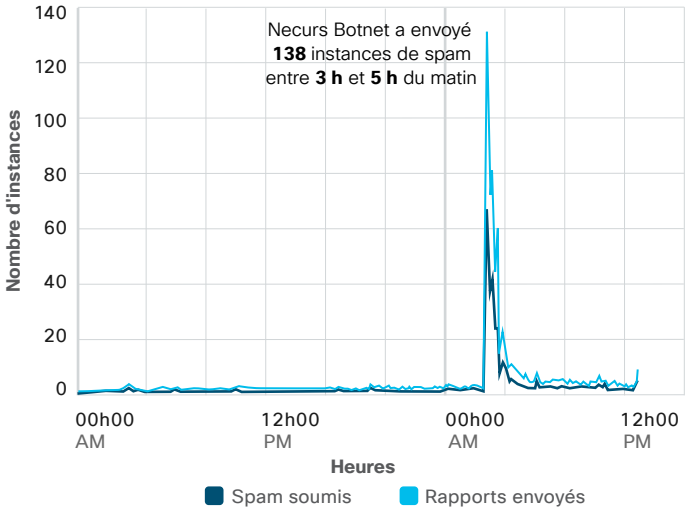
L'augmentation globale du volume de spams constatée par nos chercheurs depuis août 2016[9] semble liée au déclin significatif de l'activité liée aux kits d'exploit qui s'est amorcé à la même période. Les hackers se sont repliés sur d'autres méthodes qui ont fait leurs preuves, comme les e-mails, pour distribuer leurs ransomwares et malwares et générer des revenus (voir « Kits d'exploit : en déclin, mais encore bien présents », page 9).

Les experts de Cisco estiment que le volume de spams accompagnés de pièces jointes malveillantes continuera d'augmenter tant que les kits d'exploit poursuivront leur évolution. Les e-mails permettent d'accéder directement au terminal. Les hackers peuvent aussi compter sur les utilisateurs imprudents qui les aident à franchir le seuil des boîtes de réception. Grâce à une pratique avisée de l'ingénierie sociale (avec le phishing ou, de façon plus ciblée, le « spear phishing »), ils peuvent facilement tromper les utilisateurs et parvenir à compromettre les données d'entreprises entières.

Certains hackers utilisent également des spams contenant des documents malveillants porteurs de macros pour installer leurs ransomwares. Ces attaques peuvent déjouer bien des solutions de sandboxing, car elles requièrent une participation active de l'utilisateur, comme un clic sur le bouton « OK » d'une boîte de dialogue, pour infecter des systèmes et installer du code actif (voir « Les nouveaux malwares : analyse de six mois d'évolutions », page 23).

Les botnets spécialisés dans l'envoi de spams (en particulier l'énorme botnet Necurs) sont aussi très utilisés et contribuent à l'augmentation du volume global de spams. En début d'année, Necurs a rencontré un grand succès avec la méthode « pump and dump » (centrée sur la diffusion de fausses informations sur des actions à bas prix appelées « penny stocks ») et a envoyé moins de spams contenant des attaques sophistiquées de type ransomware.[10] La Figure 12 est un graphique interne créé par le service SpamCop de Cisco et représente un exemple de ce type d'activité de Necurs. Le fait que les propriétaires de botnets privilégient les campagnes de spams de faible qualité laisse entendre que ces initiatives, réclamant moins de ressources de leur part, rapportent suffisamment de revenus.

Figure 12 Activité des spams « pump and dump » de Necurs (sur 24 heures)



Source : SpamCop

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

Plus récemment, le botnet Necurs a envoyé Jaff, une nouvelle version de ransomware, via plusieurs campagnes de spams à grande échelle. Ces e-mails étaient accompagnés d'un fichier PDF en pièce jointe avec un document Word intégré, lequel déclenchait le téléchargement du ransomware Jaff.[11]

9 Pour en savoir plus, téléchargez le *rapport annuel Cisco 2017 sur la cybersécurité*, disponible à la page : cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

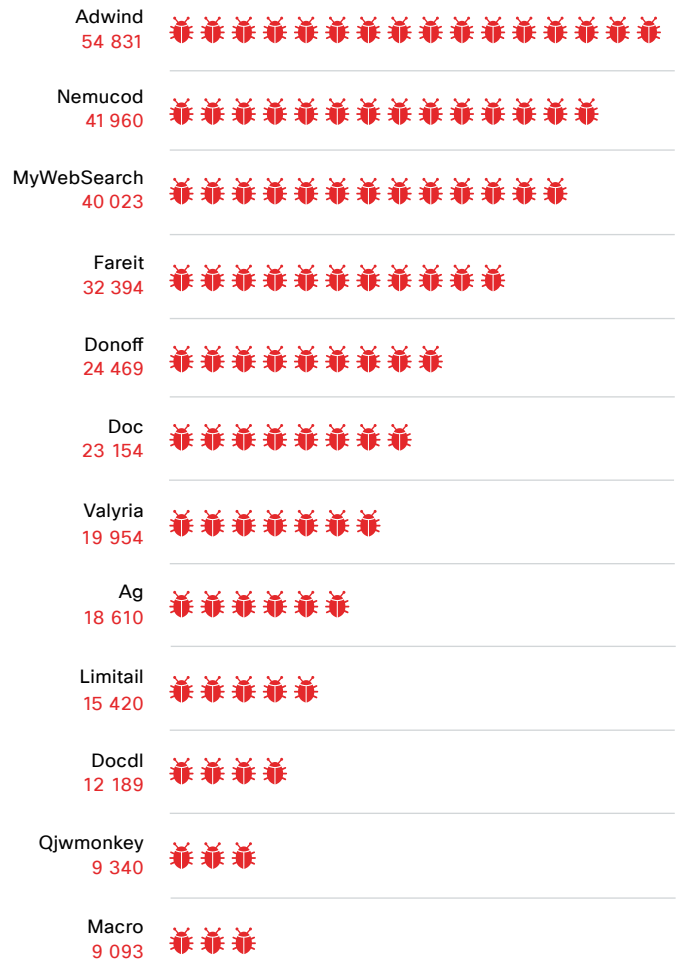
10 « Necurs Diversifies Its Portfolio », de Sean Baird, Edmund Brumaghin et Earl Carter, avec la participation de Jaeson Schultz, blog Talos, 20 mars 2017 : blog.talosintelligence.com/2017/03/necurs-diversifies.html.

11 « Jaff Ransomware : Player 2 Has Entered the Game », de Nick Biasini, Edmund Brumaghin et Warren Mercer, avec la participation de Colin Grady, blog Talos, 12 mai 2017 : blog.talosintelligence.com/2017/05/jaff-ransomware.html.

E-mails malveillants : les types de fichiers utilisés par les hackers

Les cybercriminels utilisent ou réutilisent de plus en plus les e-mails comme vecteur principal de propagation des ransomwares et autres malwares. Les chercheurs Cisco spécialistes des menaces ont donc identifié les types de fichiers employés par les principales familles de malwares. Cette information nous permet de réduire nos délais moyens de détection pour les attaques connues, et d'analyser les différentes modifications apportées aux attaques par leurs instigateurs, en particulier le changement des extensions de fichiers (voir page 26 pour en savoir plus sur les délais de détection, voir également « Tendances en matière de délais d'évolution : Nemucod, Ramnit, Kryptik et Fareit », page 28).

Figure 13 Familles de malwares les plus fréquemment détectées



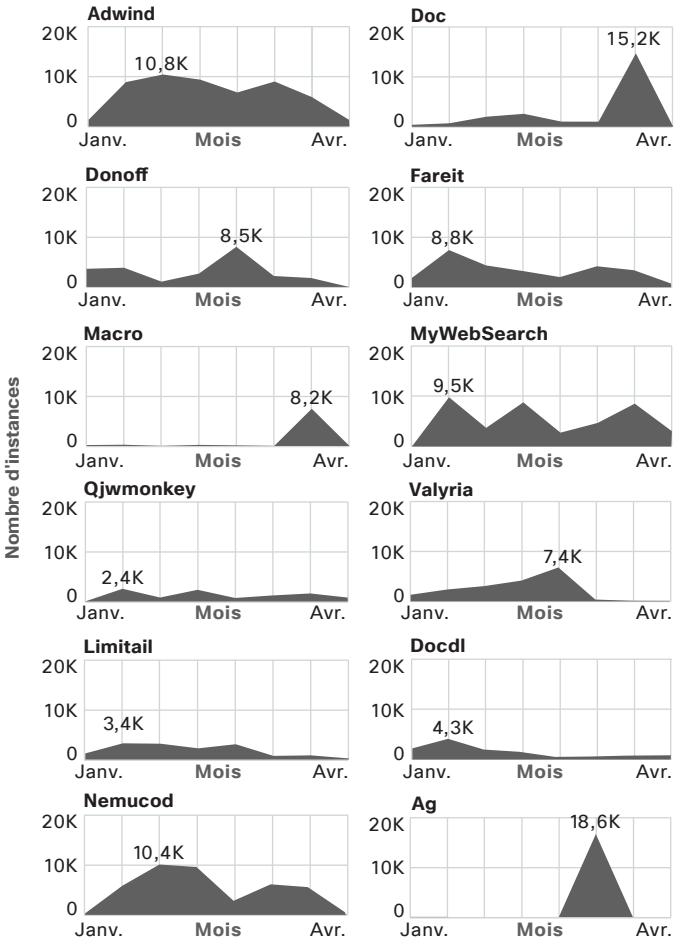
Source : Cisco Security Research

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

Nous avons analysé les détections de malwares effectuées entre janvier et avril 2017 pour recenser les 20 familles de malwares les plus souvent rencontrées dans des codes actifs distribués par des e-mails malveillants au cours de cette période (voir la Figure 13).

La Figure 14 représente le nombre de détections par famille, dans les cas incluant un fichier dont l'extension signalait un code actif, telle que .zip ou .exe. On observe un pic de malwares utilisant des macros au mois d'avril, qui correspond à la période de déclaration des impôts dans plusieurs pays, dont les États-Unis et le Canada (pour en savoir plus sur les spams accompagnés de documents malveillants porteurs de macros, voir « Les nouveaux malwares : analyse de six mois d'évolutions » à la page 23).

Figure 14 Profils des principales familles de malwares en 2017

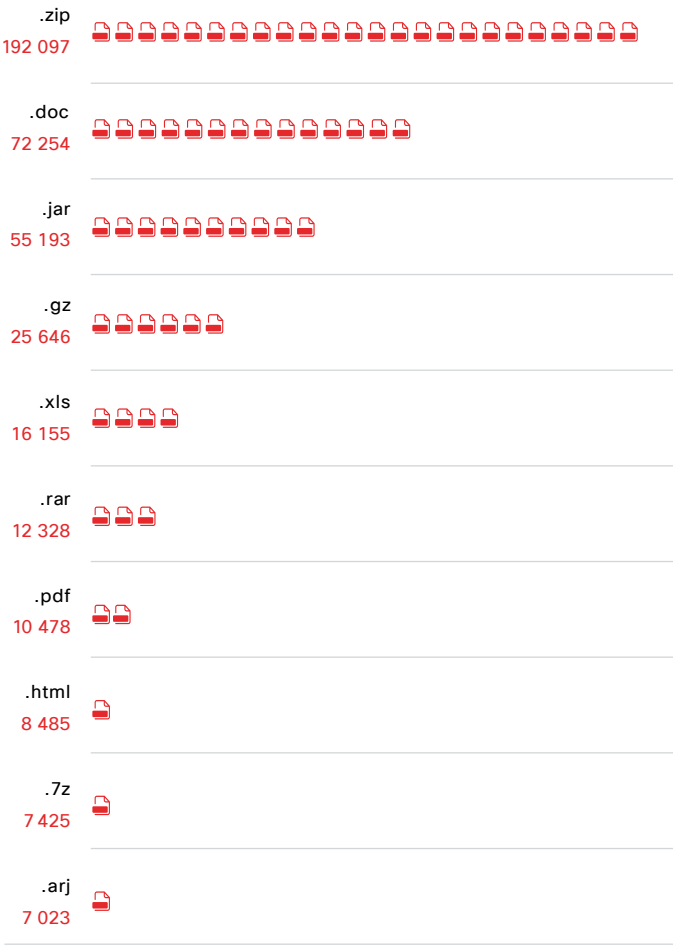


Source : Cisco Security Research

Nous avons également compté les pièces jointes malveillantes pour créer une liste des extensions de fichier suspectes les plus fréquemment rencontrées dans des documents envoyés par e-mail (voir la Figure 15). Les fichiers .zip malveillants sont les plus répandus, suivis des extensions .doc de Microsoft Word.

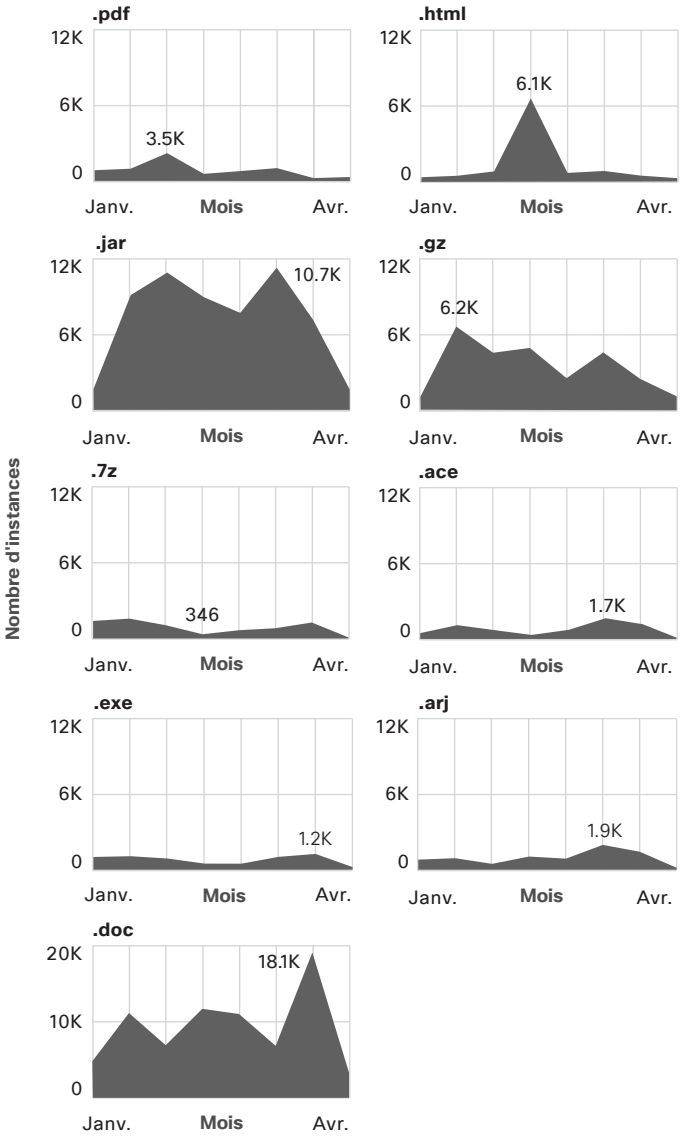
Nous nous sommes ensuite penchés sur l'évolution de l'utilisation de ces différentes extensions sur le long cours (voir la Figure 16).

Figure 15 Extensions de fichiers malveillants les plus souvent détectés



Source : Cisco Security Research

Figure 16 Profils des principales extensions de fichiers malveillants en 2017



Source : Cisco Security Research

Types de fichiers « favoris » associés aux principales familles de malwares

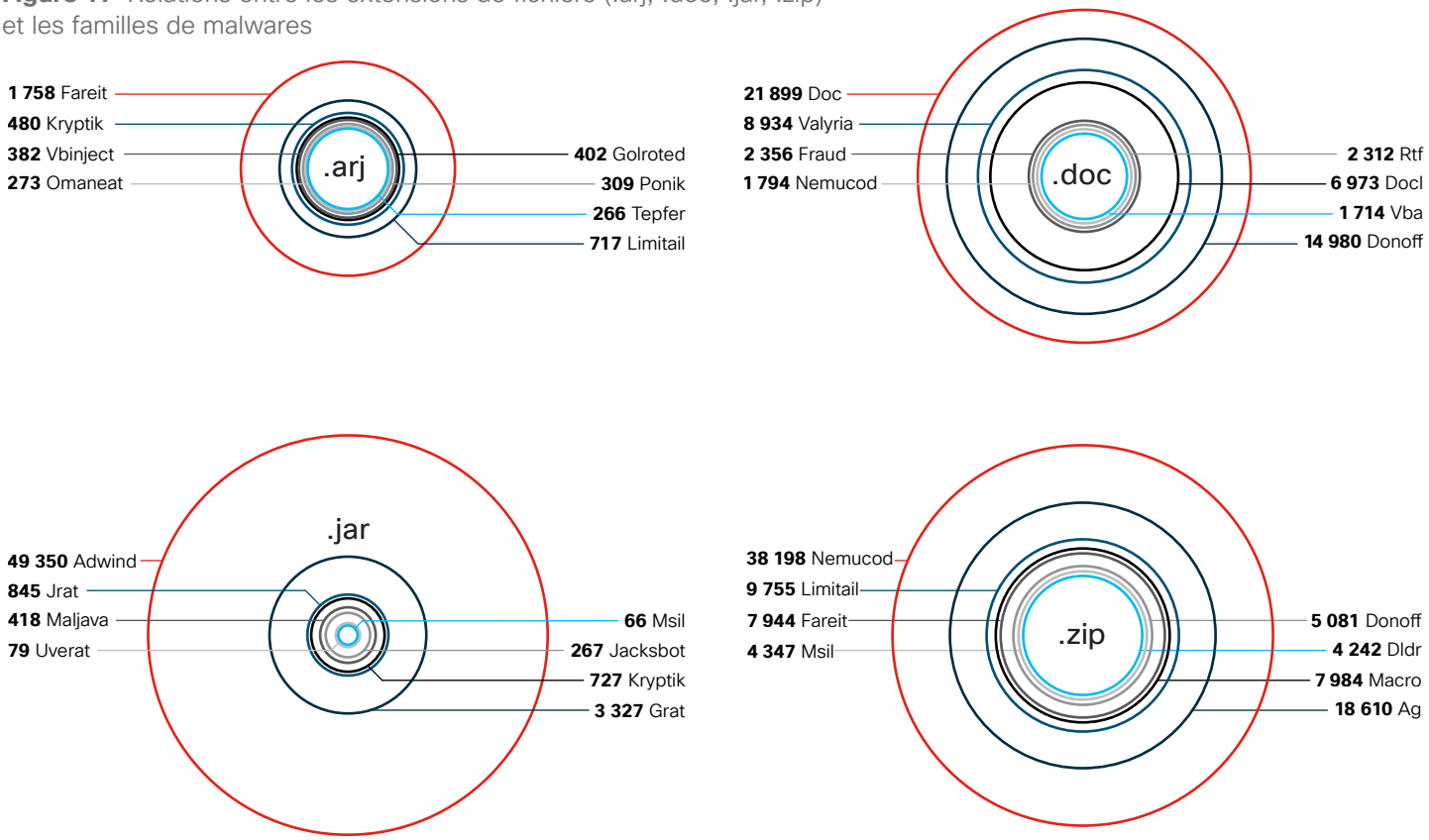
L'observation des cinq principales familles de malwares de notre échantillon de recherche permet de constater que chacune utilise des stratégies de type de fichier différentes, ainsi que des extensions récurrentes. Par exemple :

- Le cheval de Troie en accès à distance (RAT) Adwind utilise fréquemment des fichiers .jar (extension de fichier archive Java).
- Le téléchargeur de chevaux de Troie Nemucod, connu pour distribuer des ransomwares, utilise couramment l'extension de fichier .zip.
- Le logiciel publicitaire malveillant MyWebSearch est très sélectif : il emploie uniquement des extensions de fichier .exe, en n'utilisant parfois qu'un type par mois.
- Fareit, un autre RAT, utilise une grande variété de types de fichiers, mais semble privilégier les extensions de fichier .zip et .gz (ce dernier étant une extension de fichier archive).
- Le malware Donoff, un ransomware malveillant qui installe des macros, utilise principalement des types de fichiers document Microsoft Office, en particulier .doc et . xls.

La Figure 17 offre une autre représentation des tendances associées aux e-mails malveillants : les relations existant entre certaines extensions de fichiers et différentes familles de malwares. Notre analyse montre que les types de fichiers couramment utilisés dans les environnements d'entreprise, comme .zip et .doc, sont régulièrement employés par plusieurs des principales familles de malwares, notamment Nemucod et Fareit.

Cependant, de nombreuses familles de malwares utilisent aussi des types d'extension de fichier moins connus ou plus anciens, comme .jar et .arj (ce dernier est un type de fichier compressé).

Figure 17 Relations entre les extensions de fichiers (.arj, .doc, .jar, .zip) et les familles de malwares



Source: Cisco Security Research

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

Les ransomwares vous inquiètent ? Les attaques de type BEC représentent sans doute une menace encore plus grave

Ces derniers temps, les ransomwares ont mobilisé l'attention des experts de la sécurité. Toutefois, il existe une menace bien moins connue qui rapporte bien plus à ses créateurs que les ransomwares : les attaques de type BEC (Business E-mail Compromise). Flashpoint, spécialiste des informations sur les risques et partenaire de Cisco, a étudié le problème des BEC et déterminé qu'il s'agit actuellement de la méthode la plus lucrative et la plus rentable pour dérober de grandes quantités d'argent à une entreprise. Ce vecteur d'attaque relativement complexe utilise des techniques d'ingénierie sociale pour perpétrer un vol.

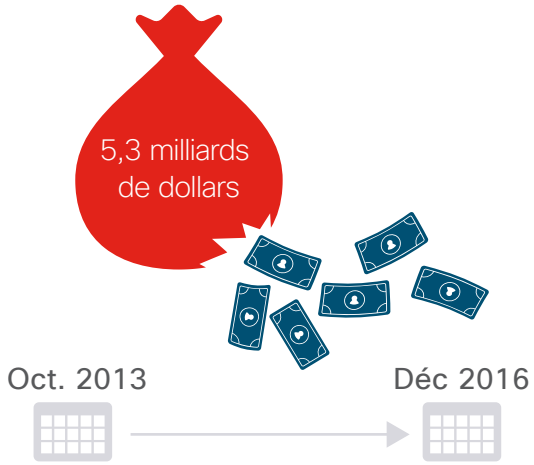
Dans sa forme la plus basique, une campagne BEC consiste à envoyer un e-mail aux employés d'un service financier (parfois en usurpant l'identité d'un collègue) pour qu'ils transfèrent des fonds par virement. Les hackers ont généralement fait des recherches préalables sur la hiérarchie et les employés de l'entreprise en utilisant par exemple les profils disponibles sur les réseaux sociaux pour reconstituer la chaîne des responsabilités. L'e-mail semble parfois provenir du PDG ou d'un autre dirigeant. Il demande au destinataire d'envoyer un paiement par virement à un prétendu associé ou fournisseur. Le message insiste sur le caractère urgent pour forcer le destinataire à envoyer l'argent, généralement sur des comptes bancaires étrangers ou domestiques appartenant à des cybercriminels.

Les arnaques BEC ciblent les grandes entreprises, qui tombent dans le piège en dépit des protections et des mesures évoluées contre les fraudes qu'elles ont mises en place. Facebook et Google ont tous deux été victimes d'attaques de type BEC et de fraude électronique.[12] Étant donné que les messages de type BEC ne contiennent ni malwares ni liens suspects, ils parviennent généralement à déjouer la grande majorité des mesures de protection.

Quelle est la gravité des attaques de type BEC ? L'Internet Crime Complaint Center (ou IC3, fruit d'un partenariat entre le FBI, le département américain de la Justice et le National White Collar Crime Center) indique que 5,3 milliards de dollars ont été volés lors d'attaques de type BEC conduites entre octobre 2013 et décembre 2016, soit une moyenne de 1,7 milliard par an[13] (voir la Figure 18). à titre de comparaison, le cumul des butins obtenus par ransomware s'élevait environ à 1 milliard de dollars en 2016.[14]

On recense au total 22 300 victimes américaines des attaques de type BEC subies entre octobre 2013 et décembre 2016.

Figure 18 Montant des pertes dues à des attaques de type BEC



Source : Internet Crime Complaint Center

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

12 « Exclusive : Facebook and Google Were Victims of $100M Payment Scam »," de Jeff John Roberts, Fortune.com, 27 avril 2017 : fortune.com/2017/04/27/facebook-google-rimasauskas/.
13 « Business E-mail Compromise, E-Mail Account Compromise: The 5 Billion Dollar Scam », Internet Crime Complaint Center (IC3) et (FBI), 4 mai 2017 : ic3.gov/media/2017/170504.aspx.
14 « Ransomware Took In $1 Billion in 2016–Improved Defenses May Not Be Enough to Stem the Tide », de Maria Korolov, CSOonline.com, 5 janvier 2017 : csoonline.com/article/3154714/security/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html.

Généralement, pour lutter contre les attaques de type BEC, il ne s'agit pas de se doter de nouveaux outils de protection, mais plutôt d'améliorer les processus opérationnels de l'entreprise. Flashpoint recommande d'informer les utilisateurs, par exemple en leur apprenant à identifier des requêtes atypiques liées à des transferts financiers, comme un virement à l'étranger pour une entreprise aux opérations généralement limitées à son propre pays. Il est également possible de demander aux employés de confirmer les transferts électroniques auprès d'un collègue, par exemple au téléphone, afin de les protéger contre les e-mails à l'origine usurpée.

Comme c'est le cas pour les outils de protection, les normes de vérification de domaines Sender Policy Framework (SPF) peuvent contribuer au blocage des e-mails aux adresses IP usurpées. Toutefois, certaines entreprises peuvent hésiter à activer cette fonctionnalité, étant donné que la norme SPF bloque également certains e-mails authentiques (comme les messages marketing ou les newsletters) lorsqu'elle n'est pas gérée correctement par les équipes informatiques.

L'essentiel est de savoir que toute entreprise ayant une présence en ligne peut être ciblée par une attaque de type BEC, depuis les géants comme Facebook et Google aux entreprises ne comptant que quelques douzaines d'employés. Comme c'est une méthode à bas coût et à rentabilité élevée, nous pouvons nous attendre à la voir prendre de l'importance.

Les nouveaux malwares : analyse de six mois d'évolutions

Les chercheurs Cisco spécialistes de la sécurité ont observé l'évolution des malwares au cours du 1er semestre 2017 et identifié plusieurs tendances. Ils ont ainsi pu apporter un éclairage sur les principales intentions des créateurs des malwares lorsqu'ils développent leurs stratégies, à savoir la diffusion, l'obfuscation et le contournement.

Tendance 1 : les hackers utilisent des systèmes de distribution pour lesquels les malwares sont activés suite à une action de l'utilisateur

Nous avons remarqué une hausse des pièces jointes d'e-mail malveillantes capables de contourner les systèmes de détection automatique des malwares. Lorsqu'elles sont placées dans un environnement de sandbox, ces pièces jointes n'apparaissent pas comme malveillantes et sont donc transmises à l'utilisateur qui peut alors être confronté aux éléments suivants :

- Un document malveillant protégé par mot de passe (auquel cas le mot de passe est fourni à l'utilisateur dans le texte de l'e-mail)
- Un document malveillant affichant une boîte de dialogue qui demande l'autorisation à l'utilisateur (par exemple, « Cliquez sur OK »)
- Objets OLE malveillants dans un document Word
- Documents Word malveillant intégrés dans des fichiers PDF[15]

Tendance 2 : les hackers exploitent les bases de code des ransomwares

Certains hackers créent des malwares rapidement, facilement et à bas coût en exploitant des bases de code Open Source, comme Hidden Tear ou EDA2, publiées en ligne dans un but « pédagogique ». Les hackers modifient le code pour qu'il semble différent de l'original, puis déploient le malware. Bon nombre des « nouvelles » familles de ransomwares observées par les chercheurs Cisco spécialistes des menaces ces derniers mois sont basées sur un code open source issu des bases de code pédagogiques.

Tendance 3 : les plates-formes RaaS (Ransomware-as-a-service) se développent rapidement

Les plates-formes RaaS, comme Satan, sont parfaites pour les hackers qui veulent entrer facilement sur le marché des ransomwares et lancer une campagne réussie sans avoir à coder, programmer ou consacrer des ressources au développement de tactiques innovantes. Les opérateurs de ces plates-formes, dont le nombre ne cesse de croître, récupèrent une part des profits de ces hackers. Certains déploient même le ransomware et fournissent des services supplémentaires, comme le suivi des progrès des campagnes de leurs clients.

15 « Threat Spotlight: Mighty Morphin Malware Purveyors: Locky Returns via Necurs » de Nick Biasini, Talos, 21 avril 2017 : blogs.cisco.com/security/talos/locky-returns-necurs.

Tendance 4 : les malwares sans fichiers, ou résidant en mémoire, se répandent

Nous avons observé ce type de malware infectant les systèmes partout dans le monde. Il utilise PowerShell ou WMI pour exécuter le malware entièrement en mémoire sans écrire d'objets dans le système de fichiers ou le registre, sauf si le hacker souhaite mettre des mécanismes persistants en place.[16] Les malwares sont ainsi plus difficiles à détecter. Il complique également les analyses et la réponse aux incidents.

Tendance 5 : les hackers ont de plus en plus souvent recours à des infrastructures anonymes et décentralisées pour dissimuler leurs activités de commande-contrôle

Les spécialistes de la cybersécurité Cisco ont remarqué une utilisation accrue de services intermédiaires servant à faciliter l'accès aux malwares et aux services de commande-contrôle hébergés dans le réseau Tor. Tor2web est un exemple de ce type de service intermédiaire créant un proxy qui permet aux systèmes sur Internet d'accéder à des éléments hébergés dans Tor, sans nécessiter l'installation d'une application cliente Tor locale.[17]

Essentiellement, Tor2web permet aux hackers d'utiliser plus facilement Tor sans avoir à changer leur code de malware ni à inclure un client Tor dans la charge utile du malware. Étant donné qu'un hacker peut configurer un serveur proxy Tor2web sur le domaine de son choix, il est plus difficile de bloquer ces serveurs une fois qu'ils sont déployés.

Threat Intelligence de Talos : sur la piste des attaques et des vulnérabilités

Le site Talos de Cisco (blog.talosintelligence.com) se veut une ressource pour l'identification des vulnérabilités et des tendances observées en matière d'attaques. L'identification des vulnérabilités est un aspect particulièrement important, car elle permet de mieux comprendre la lutte opposant les hackers aux acteurs de la protection dans la durée.

On estime généralement que les hackers ont un avantage, étant donné que le temps joue en leur faveur, ce qui n'est pas le cas des professionnels de la sécurité. Ces derniers doivent agir vite pour remédier aux dégâts causés par les attaques. La recherche de vulnérabilités permet aux spécialistes de la sécurité d'y remédier avant qu'elles soient exploitées par les hackers. Le décalage peut être comblé en identifiant les vulnérabilités de type « zero-day » et en collaborant avec les fournisseurs de logiciels afin de s'assurer que les correctifs soient développés et distribués.

Les spécialistes de la sécurité ont appris à mieux maîtriser le problème des ransomwares. Les kits d'exploit sont en déclin, ce qui donne aux chercheurs de Talos davantage de temps pour se pencher sur d'autres menaces. En bref, les professionnels de la sécurité en ligne ont acquis une meilleure compréhension du fonctionnement des ransomwares et savent désormais mieux identifier les nouvelles versions de ce type de logiciel.

Autre tendance clé abordée dans le blog de Talos : la transition observée chez les hackers, qui délaissent désormais les kits d'exploit pour privilégier les attaques par e-mail. Depuis la disparition, en 2016, d'Angler, le kit d'exploit le plus utilisé, les chercheurs sont à l'affût du prochain leader en matière d'attaques ou des grandes tendances appelées à survenir (voir la section « Kits d'exploit : en déclin, mais encore bien présents », page 9). Les chercheurs constatent un déclin des menaces utilisant les applications Flash et Java, tandis que les développeurs de navigateurs, de leur côté, bloquent les plug-ins associés à ces attaques, qui présentent dès lors moins d'intérêt pour les hackers.

16 Pour en savoir plus sur ce sujet, lisez l'article « Covert Channels and Poor Decisions: The Tale of DNSMessenger », de Edmund Brumaghin et Colin Grady, blog Talos, 2 mars 2017 : blogs.cisco.com/security/talos/covert-channels-and-poor-decisions-the-tale-of-dnsmessenger.

17 Pour en savoir plus, consultez l'article « Go RAT, Go! AthenaGo Points 'TorWords' Portugal », de Edmund Brumaghin, avec la participation d'Angel Villegas, blog Talos, 8 février 2017 : blog.talosintelligence.com/2017/02/athena-go.html.

Les articles qui suivent sont parus sur le blog de Talos et décrivent l'actualité de la recherche portant sur des menaces spécifiques. Ils fournissent également des informations utiles sur la façon dont les hackers sont obligés d'innover pour garder une longueur d'avance sur les professionnels de la sécurité :

Player 3 Has Entered the Game: Say Hello to 'WannaCry' : cet article permet de découvrir le célèbre ransomware WannaCry et offre des recommandations pour protéger les réseaux de cette menace.

MBRFilter: Can't Touch This! : à l'occasion de cet article, les chercheurs de Talos ont publié MPRFilter, un filtre de disque permettant d'éviter toute écriture du secteur 0 sur l'ensemble des disques connectés à un système. Cette tactique est utilisée par certains types de ransomwares, comme Petya. Ce malware tente d'écraser le disque principal d'initialisation d'un système infecté, puis remplace le programme d'amorçage par une version malveillante.

Sundown EK: You Better Take Care : cet article décrit le kit d'exploit Sundown. La campagne associée était conduite depuis une poignée d'adresses IP, mais les chercheurs de Talos ont découvert plus de 80 000 sous-domaines malveillants liés à plus de 500 domaines utilisant divers comptes d'utilisateurs. Cette approche permet au kit d'exploit de déjouer les solutions classiques, reposant sur des listes noires.

Without Necurs, Locky Struggles : les chercheurs de Talos décrivent dans cet article le déclin de l'activité du ransomware Locky suite à la mise hors ligne temporaire du botnet Necurs. Nos chercheurs ont suivi de près l'activité du botnet Necurs. Lorsqu'il fonctionne, il peut distribuer des volumes immenses de spams porteurs de Locky et du malware bancaire Dridex.

Go RAT, Go! AthenaGo Points “TorWords” Portugal : cet article identifie AthenaGo, une campagne de malwares diffusés à l'aide de documents Word malveillants et ciblant des victimes situées au Portugal. Selon les chercheurs, la stratégie unique d'AthenaGo consistait à utiliser un cheval de Troie à accès distant ayant la capacité de télécharger et d'exécuter des fichiers binaires sur les systèmes infectés. Ce malware a été conçu avec le langage de programmation Go, ce qui est rare. Quant aux communications de commande-contrôle utilisées par le malware, elles s'appuient sur des proxys Tor2web qui permettent aux auteurs du programme d'échapper aux détections.

Covert Channels and Poor Decisions: The Tale of DNSMessenger : les chercheurs de Talos détaillent ici leur analyse d'un échantillon de malwares utilisant les requêtes et réponses TXT DNS pour créer un canal bidirectionnel de commande-contrôle, une tactique furtive rarement utilisée qui permet aux hackers d'éviter toute détection dans les environnements ciblés.

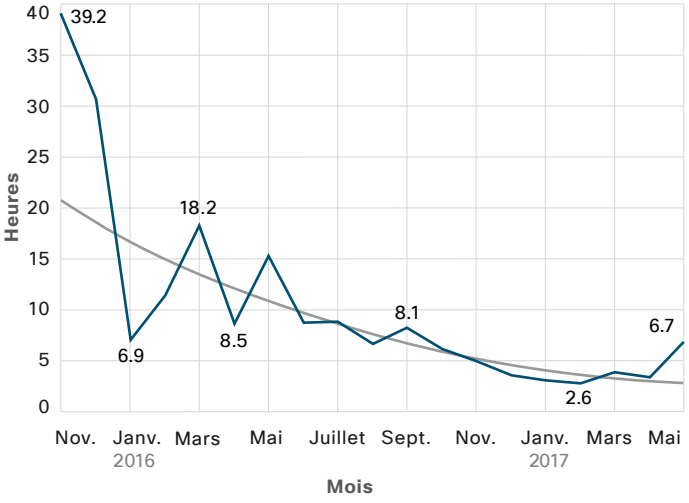
Necurs Diversifies Its Portfolio : dans cet article, les chercheurs évoquent les nouvelles opérations liées au botnet géant Necurs, qui a ouvert sa diffusion de spams aux stratégies d'escroquerie « pump and dump » portant sur des actions à très bas prix.

Threat Spotlight: Mighty Morphin Malware Purveyors : avec la remise en service du botnet Necurs, qui avait temporairement suspendu son activité, les chercheurs ont identifié une nouvelle effervescence du côté de Locky, une campagne de spams à grande échelle.

Délais de détection : un bras de fer de plus en plus musclé entre les hackers et les entreprises

Cisco analyse son temps de détection moyen depuis novembre 2015. Depuis cette époque, la tendance générale a été à la réduction de ce délai, d'un peu plus de 39 heures au début de notre recherche, à environ 3,5 heures pour la période allant de novembre 2016 à mai 2017 (voir la Figure 19).

Figure 19 Délai de détection médian par mois



Source : Cisco Security Research

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

Toute augmentation de ce délai indique une période où les hackers ont créé de nouvelles attaques. Les diminutions correspondent aux périodes où les professionnels parviennent à identifier les menaces plus rapidement. Depuis l'été 2016, le rapport de force permanent entre les cybercriminels et les acteurs de la protection est moins prononcé, ces derniers reprenant rapidement pied après chaque tentative des hackers de prendre le dessus et de le conserver.

Pour Cisco, le terme « délai de détection » désigne le laps de temps entre une compromission et la détection d'une menace. Nous déterminons cette fenêtre à l'aide des données télémétriques de sécurité collectées sur une base volontaire à partir des produits de sécurité Cisco déployés dans le monde entier. Grâce à une visibilité globale et à un modèle d'analyse continue, nous pouvons mesurer le délai entre l'exécution du code malveillant sur un terminal et le moment où cette menace est détectée. Cette mesure concerne les codes malveillants non classés au moment de la détection.

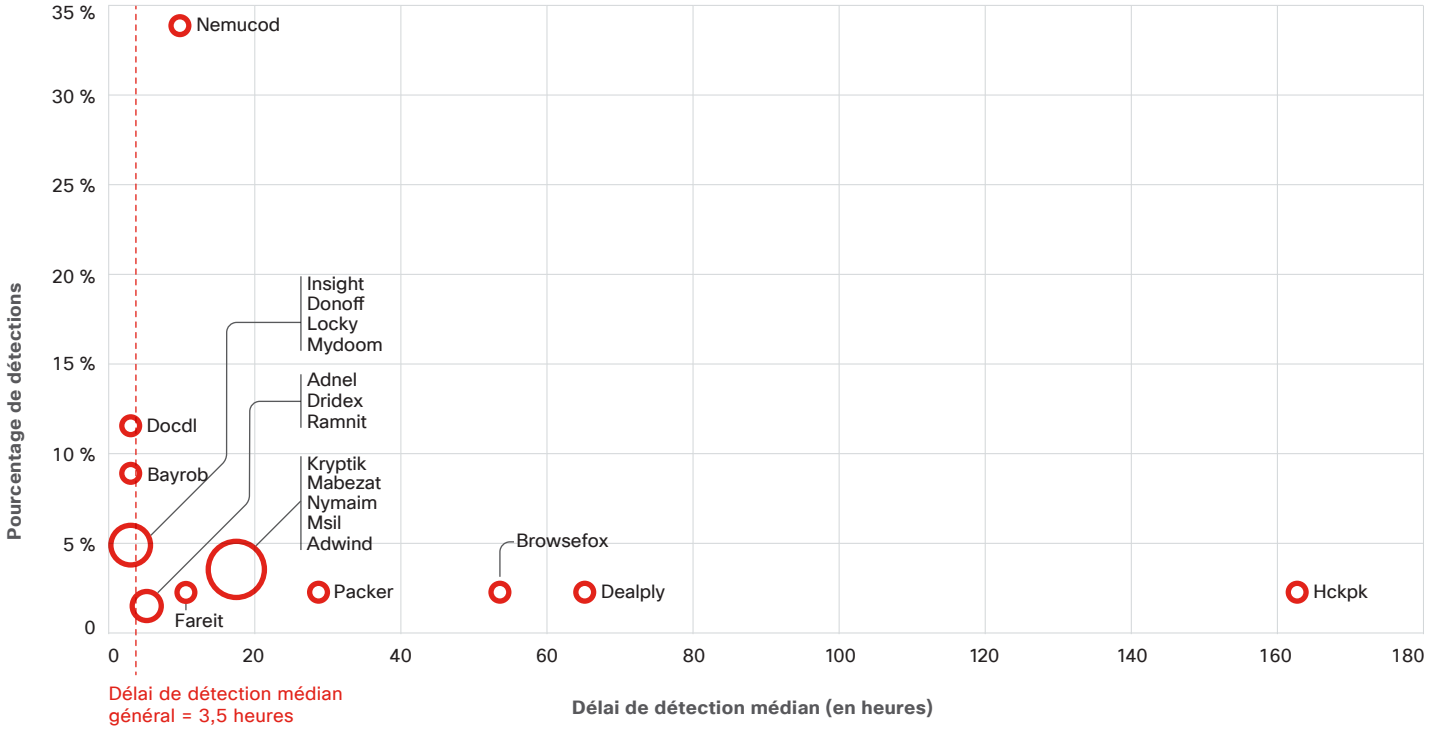
Les évolutions constatées au niveau des menaces, en particulier au cours des six derniers mois, montrent que les cybercriminels sont de plus en plus souvent contraints de faire évoluer leurs attaques et de mettre au point de nouvelles techniques afin d'échapper aux outils de détection.

La Figure 20 représente le délai de détection médian pour les 20 plus grandes familles de malwares (par pourcentage de détections) observées par nos chercheurs de novembre 2016 à avril 2017. Un grand nombre de familles d'attaques détectées par les produits Cisco dans notre délai de détection médian de 3,5 heures sont menées de façon industrielle, se déplacent rapidement et sont très répandues. Les menaces anciennes et répandues sont aussi généralement détectées avant le temps de détection moyen.

Bon nombre de familles de malwares restent longues à identifier par les acteurs de la protection bien qu'elles soient connues de la communauté des spécialistes de la sécurité. C'est parce que les auteurs de ces menaces utilisent diverses techniques d'obfuscation pour que leur malware reste actif et rentable. Dans la partie suivante, nous examinons la façon dont quatre familles de malwares utilisent des stratégies spécifiques pour garder une longueur d'avance sur les professionnels de la sécurité. Ces familles sont : Fareit (un cheval de Troie à accès distant, ou « RAT »), Kryptik (autre RAT), Nemucod (un cheval de Troie téléchargeur) et Ramnit (un cheval de Troie spécialisé dans le secteur bancaire).

Leurs méthodes sont efficaces : comme le montre la Figure 20, ces malwares se situent tous en dehors de notre délai médian de détection de 3,5 heures, en particulier Kryptik. Même Nemucod, qui fait partie des principales familles connues et est très souvent détecté, est plus long à identifier car il évolue très rapidement.

Figure 20 Délais de détection médians des 20 principales familles de malwares



Source : Cisco Security Research

Tendances en matière de délais d'évolution : Nemucod, Ramnit, Kryptik et Fareit

Cisco suit attentivement les modifications que les auteurs de malwares apportent aux types de diffusion de leur code actif et le rythme auquel ils génèrent de nouveaux fichiers (pour déjouer les méthodes de détection exclusivement basées sur les hashs). Nous vérifions également s'ils emploient des algorithmes de génération de domaines (DGA) pour que leurs malwares restent à jour et compromettent de façon efficace les données des utilisateurs et leurs systèmes. Certaines familles de malwares génèrent d'importants volumes de domaines de type DGA, qui sont tous de proches variantes d'un même nom de domaine de départ, afin de dissimuler leur trafic et d'échapper aux détections (pour en savoir plus sur les domaines créés à l'aide d'algorithmes DGA, reportez-vous à la section « L'allongement des durées de vie des domaines DGA et la fréquence croissante de leurs utilisations croisées », page 33).

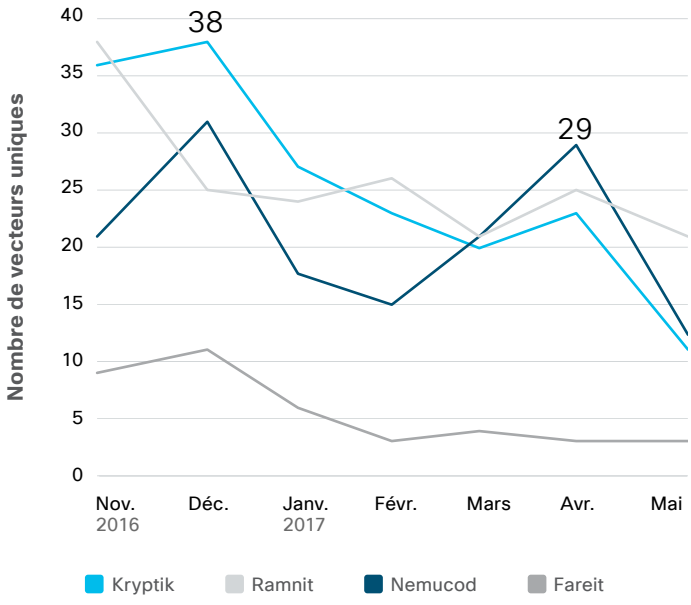
Nous avons analysé les données liées aux attaques web de différentes sources Cisco, plus précisément les données des proxys web, des détecteurs de malwares avancés pour le cloud ou les terminaux, et de plusieurs moteurs antimalwares. Les données obtenues nous permettent de mesurer le délai d'évolution, c'est-à-dire la durée nécessaire aux hackers pour modifier la manière dont des malwares spécifiques sont diffusés, ainsi que la durée entre chaque changement de tactique.

Des informations précises sur les profils d'évolution propres à chaque famille de malwares (et la façon dont leurs auteurs associent des outils et tactiques anciens et nouveaux pour garder une longueur d'avance sur les acteurs de la protection) nous aident à perfectionner nos pratiques et nos technologies de sécurité afin de continuer à réduire nos délais de détection (pour plus d'information sur ces délais, reportez-vous à « Délais de détection : un bras de fer de plus en plus musclé entre les hackers et les entreprises », en page 26.)

De novembre 2016 à mai 2017, nous avons centré notre analyse sur quatre familles de malwares bien connues : Nemucod, Ramnit, Kryptik et Fareit. Nous avons observé les modifications des extensions de fichiers lors de la diffusion des malwares et le type de contenu des fichiers (ou MIME) défini par le système des utilisateurs. Pour chaque famille, nous avons examiné les modèles propres aux méthodes de diffusion sur le web et par e-mail.

La Figure 21 représente le nombre de vecteurs distincts utilisés par chacune des quatre familles de malwares pour exécuter leurs attaques sur le web pendant la période concernée.

Figure 21 Nombre de vecteurs d'attaque distincts observés par mois lors d'attaques web



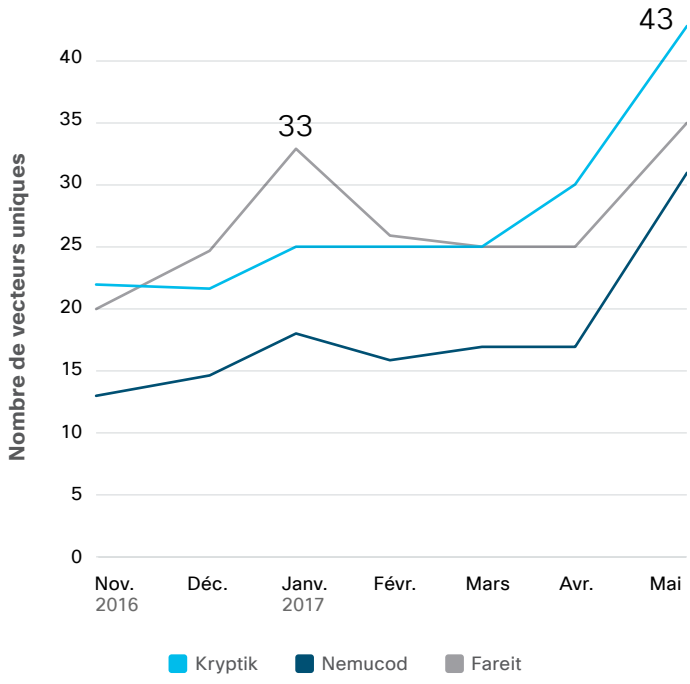
Source : Cisco Security Research

La Figure 22 représente le nombre de vecteurs d'attaque distincts utilisés par chaque famille dans le cadre d'attaques par e-mail pendant la période concernée. Comme vous pouvez le constater, la famille de malwares Ramnit n'est pas prise en compte dans notre analyse, car nos chercheurs n'ont recensé qu'un très faible nombre d'événements (blocages) concernant des fichiers liés à Ramnit.

Notre analyse du délai d'évolution comprend un examen de l'âge des hashs qu'une famille de malwares utilise (par mois) au moment du blocage. Cela nous permet de déterminer la fréquence et la rapidité d'évolution nécessaires à un malware pour échapper à une détection basée sur les hashs.

Voici une présentation des principales conclusions de nos recherches pour les quatre familles de malwares étudiées.

Figure 22 Nombre de vecteurs d'attaque distincts observés par mois lors d'attaques par e-mail



Source : Cisco Security Research

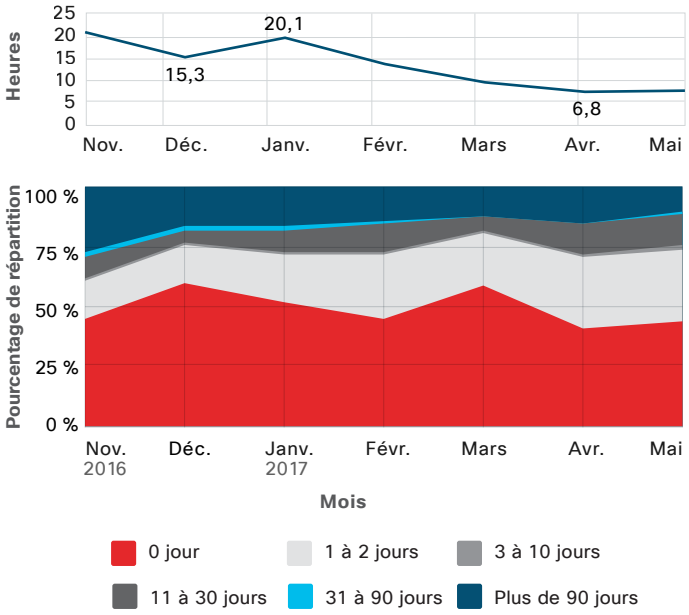
Analyse des délais d'évolution : Kryptik

Le malware Kryptik (également appelé GozNym) a été conçu en fusionnant un téléchargeur et un cheval de Troie spécialisé dans les systèmes bancaires dont le code a été divulgué publiquement.[18] Environ un tiers (35 %) des événements web constatés pour la famille de malwares Kryptik lors de notre dernière étude des délais d'évolution utilisait JavaScript, alors que 26 % employaient un fichier avec l'extension .php. Les types de contenus de fichiers identifiés comprennent Microsoft Word, le type octet-stream et HTML. La plupart des événements touchant aux e-mails pour le RAT Kryptik employaient des fichiers .zip, .js ou des exécutables.

Nous avons également découvert que la famille de malwares Kryptik utilisait des hashs d'âges variés pendant la période concernée (voir la Figure 23).

Les courbes représentant les délais de détection sur la Figure 23 montrent qu'il reste difficile de détecter ce malware, même si les produits Cisco sont parvenus à l'identifier plus rapidement au cours des derniers mois. Fin avril 2017, notre délai médian de détection pour le RAT Kryptik était d'environ le double de notre délai médian de détection global de 3,5 heures (pour en savoir plus sur le calcul des délais de détection, voir la page 26). Toutefois, ce chiffre reste largement inférieur au délai de 21,5 heures mesuré pour Kryptik en novembre 2016.

Figure 23 Délais de détection et âge des hashs pour la famille de malwares Kryptik par mois



Source : Cisco Security Research

18 « Visualizing 2016's Top Threats », d'Austin McBride et Brad Antoniewicz, bloc Cisco Umbrella, 8 février 2017 : umbrella.cisco.com/blog/blog/2017/02/08/visualizing-2016s-top-threats/.

Analyse des délais d'évolution : Nemucod

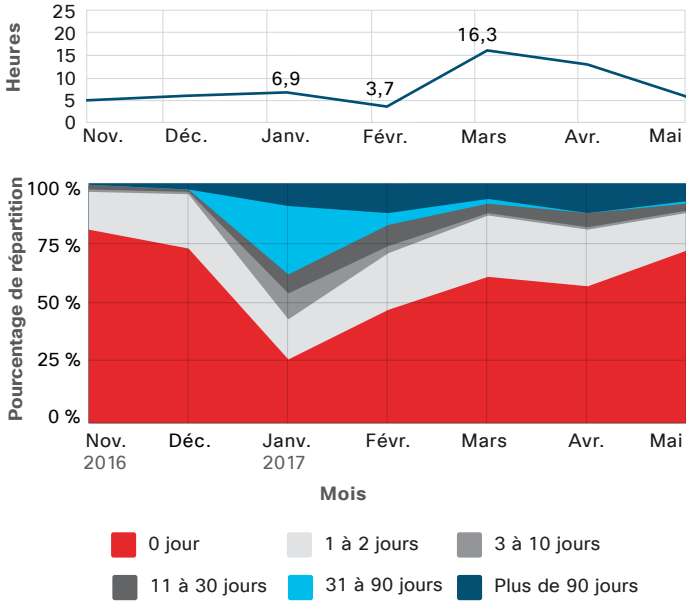
Nemucod reste l'une des familles de malware les plus fréquentes en 2017. Ce malware téléchargeur est utilisé pour diffuser des ransomwares et d'autres menaces, telles que des chevaux de Troie de type portes dérobées qui facilitent le vol d'identité ou la fraude au clic. Des variantes servent également de mécanismes pour diffuser la charge utile du malware Nemucod.

Il va sans dire que l'évolution de Nemucod est fortement liée à son succès continu. La Figure 24 montre que Nemucod recourt régulièrement à un minimum de 15 combinaisons d'extensions et de types de contenus de fichiers. Par exemple, 70 % des événements web Nemucod observés impliquaient JavaScript et se partageaient principalement entre des extensions de fichier .php (16 %) ou .zip (9 %). En outre, les événements Nemucod ayant donné lieu à des blocages d'e-mails étaient généralement associés à des fichiers .zip, .wsf (fichiers de script Windows) ou .js.

Dans la Figure 24, nous pouvons voir que Nemucod utilise principalement des hashs créés moins d'un jour plus tôt afin de garder une longueur d'avance sur les professionnels de la sécurité.

Ces derniers mois, le malware a utilisé davantage de hashs plus anciens. Cela peut indiquer que la communauté des spécialistes de la sécurité détecte plus efficacement de nouvelles instances de Nemucod, obligeant les cybercriminels à revenir à des hashs plus anciens ayant démontré leur efficacité. Quoi qu'il en soit, la Figure 24 montre que le délai de détection pour Nemucod a augmenté en mars et en avril, ce qui illustre les fluctuations constantes du rapport de forces entre hackers et professionnels de la sécurité. Les créateurs de Nemucod ont apparemment développé des mécanismes de diffusion plus difficiles à détecter, qu'il s'agisse des hashs utilisés, des méthodes de diffusion ou d'autres méthodes d'obfuscation.

Figure 24 Délais de détection et âge des hashs pour la famille de malwares Nemucod par mois



Source : Cisco Security Research

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

Analyse des délais d'évolution : Ramnit

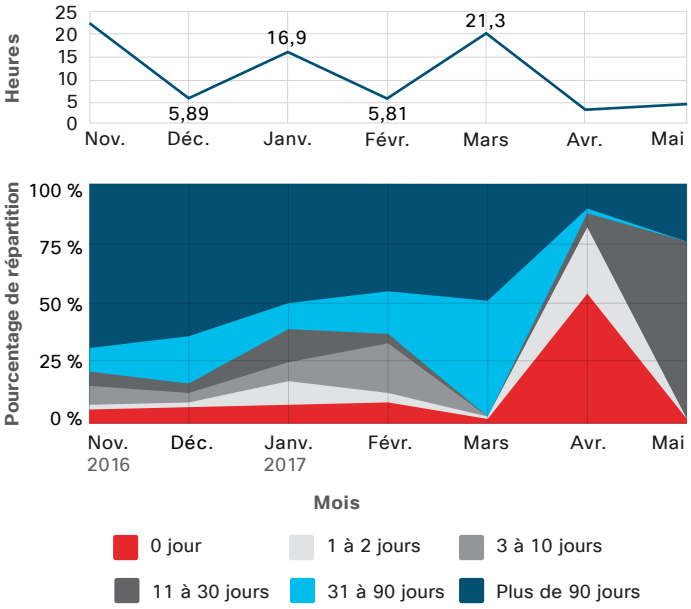
La première apparition de Ramnit, sous forme de ver autoreproducteur, date de 2010. Par la suite, ses développeurs l'ont enrichi de fonctionnalités diverses, dont le vol de données à l'aide du code source dévoilé du célèbre cheval de Troie Zeus. Aujourd'hui, Ramnit fait partie des chevaux de Troie bancaires les plus persistants.

Dans notre dernière étude des délais d'évolution, nous avons constaté que la quasi totalité des événements web (99 %) impliquant le malware Ramnit avait un type MIME texte ou HTML. Les extensions de fichiers diffèrent, mais comportent une majorité de HTML (41 %).

Selon nos recherches, Ramnit a également réussi à échapper aux mesures de protection pendant plusieurs mois en utilisant principalement des hashs vieux de 90 jours ou plus (Figure 25).

Toutefois, le graphique montre également que, dès avril, les hackers pilotant Ramnit sont passés à une utilisation majoritaire de nouveaux hashs, dont plus de la moitié avaient moins d'un jour. Ceci est certainement dû au fait que les entreprises sont devenues plus efficaces dans la détection d'instances de Ramnit utilisant de vieux hashs. En fait, notre délai médian de détection pour Ramnit est passé d'un peu plus de 21 heures en mars à environ 5 heures dès le début du mois de mai.

Figure 25 Délais de détection et âge des hashs pour la famille de malwares Ramnit par mois



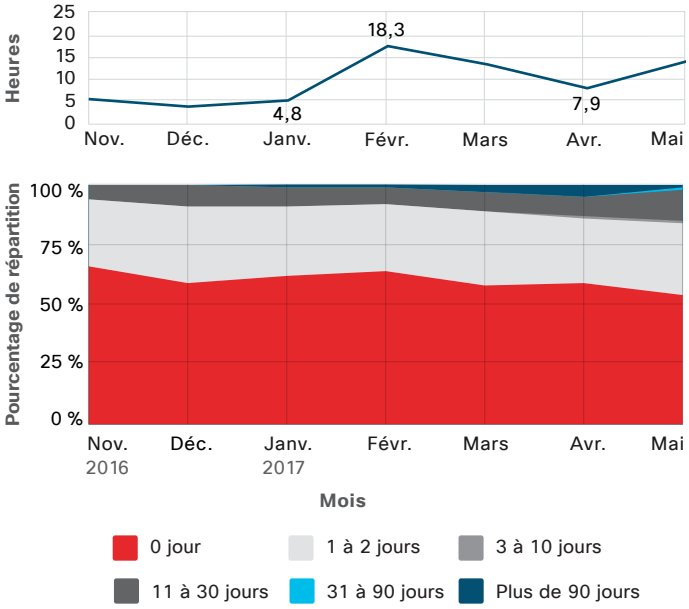
Source : Cisco Security Research

Analyse des délais de détection : Fareit

Fareit fait aussi partie des familles de malwares aussi notoires qu'omniprésentes. Le RAT Fareit vole des informations d'identification et distribue divers types de programmes malveillants. D'après nos recherches, la quasi totalité (95 %) des variantes de Fareit utilisées dans des attaques web présentait des extensions de fichier .dll. 84 % d'entre elles avaient un type de contenu de fichier msdos ou msdownload. Les extensions de fichier Fareit dans les e-mails étaient majoritairement associées à des documents Word, des fichiers ACE (archive compressée), des exécutables ou des fichiers .zip.

Comme les malwares Kryptik, Fareit change fréquemment de hashs pour ne pas être détecté (Figure 26). Le délai médian de détection pour Fareit a connu un pic significatif en février et en mars. Pendant cette période, ce malware avait légèrement augmenté son utilisation de nouveaux hashs, tout en enrichissant ses attaques de hashs nettement plus vieux (90 jours ou plus).

Figure 26 Délais de détection et âge des hashs pour la famille de malwares Fareit par mois



Source: Cisco Security Research

Activité liée aux domaines : Nemucod et Ramnit

Les chercheurs de Cisco ont analysé les domaines liés à deux des familles de malwares apparaissant dans notre dernière étude consacrée aux délais d'évolution : Nemucod et Ramnit. Le but de cet exercice était d'en apprendre davantage sur la façon dont ces familles de malwares utilisent les domaines pour distribuer leurs programmes malveillants.

Au cours de la période observée (de novembre 2016 à mars 2017), nous avons constaté que Nemucod exploitait un grand nombre de sites web compromis (plus que Ramnit).

De son côté, Ramnit semblait utiliser des centaines d'algorithmes de génération de noms de domaines, ou DGA (pour en savoir plus sur les domaines créés à l'aide d'algorithmes DGA, voir « L'allongement des durées de vie des domaines DGA et la fréquence croissante de leurs utilisations croisées », page 33).

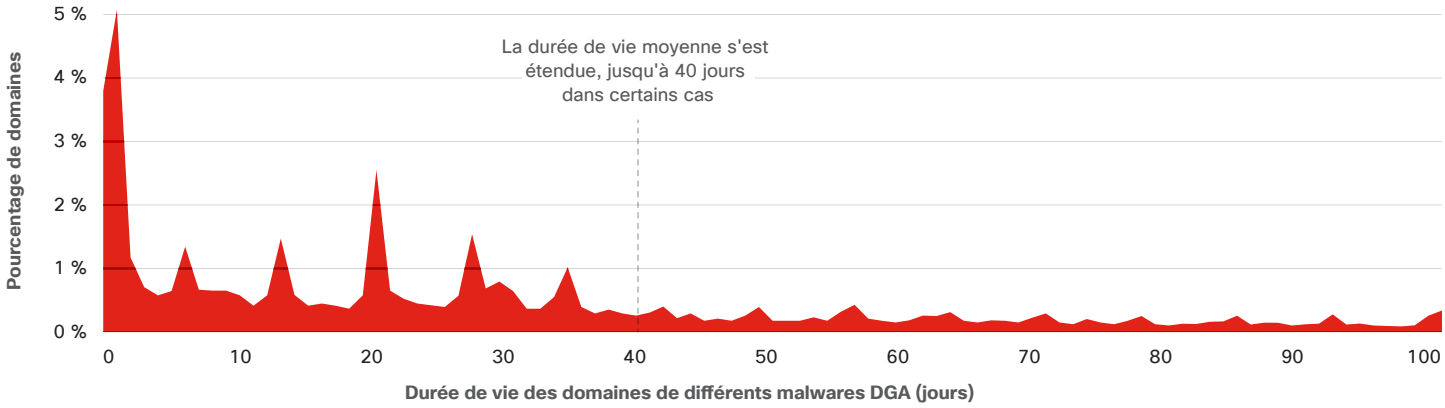
L'allongement des durées de vie des domaines DGA et la fréquence croissante de leurs utilisations croisées

De nombreuses familles de malwares utilisent des algorithmes de génération de noms de domaines, ou DGA, pour créer rapidement des noms de domaines pseudo-aléatoires leur permettant d'échapper aux détections. Les domaines DGA ont généralement une durée de vie courte mais peuvent parfois durer plusieurs mois, ce qui rend les blocages heuristiques encore plus difficiles à empêcher pour les acteurs de la protection.

Anomali, un partenaire de Cisco spécialisé dans la Threat Intelligence suit les durées de vie des domaines soupçonnés d'être générés par des algorithmes DGA qui sont associés à un grand nombre de familles de malwares. Selon les chercheurs d'Anomali spécialistes des menaces, la plupart des domaines DGA observés il y a 5 ans avaient une durée de vie de 3 jours maximum. Depuis lors, la durée de vie moyenne des domaines DGA s'est rallongée de façon significative pour atteindre environ 40 jours dans certains cas (voir la Figure 27). Certains durent plus longtemps que cela.

Remarque : l'échantillon contient environ 45 familles de malwares différentes.

Figure 27 Durée de vie des domaines DGA



Source : Anomali

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

Cette tendance est probablement due au fait que les hackers doivent faire évoluer leurs attaques plus rapidement afin de contourner les blocages ou rester plus longtemps dans des entreprises déjà compromises sans être détectés (pour en savoir plus, voir « Tendances en matière de délais d'évolution : Nemucod, Ramnit, Kryptik et Fareit » à la page 28). Les auteurs de malwares doivent réagir assez rapidement pour éviter d'être ajoutés aux listes de blocage, mais s'ils vont trop vite, les équipes en charge de la sécurité peuvent prendre le dessus en bloquant tous les nouveaux domaines.

Dans la majorité des cas, les algorithmes utilisés par les malwares générant des domaines DGA ne diffèrent les uns des autres qu'à deux niveaux en matière de création de domaines : la longueur du nom de domaine et les noms utilisés pour les domaines de premier niveau. (Remarque : presque tous les algorithmes utilisent différentes approches pour sélectionner de façon aléatoire les lettres du domaine de second niveau.)

Ces limites, combinées à la nécessité de générer constamment de nouveaux domaines, se traduisent souvent par un chevauchement des efforts des familles de malwares pour générer et enregistrer des domaines DGA. Cela peut conduire à la collision de combinaisons ultra saturées de domaines .com de 8 à 10 caractères, par exemple. Dans ces environnements saturés, il arrive qu'un domaine DGA soit bloqué parce qu'un concurrent utilise un domaine DGA similaire identifié par les acteurs de la protection.

L'analyse des infrastructures permet de mieux connaître les outils des hackers

Comme nous l'avions indiqué dans la partie consacrée aux différents secteurs de notre enquête sur l'efficacité des mesures de sécurité (voir page 78), nombreuses sont les équipes de sécurité qui peinent à interpréter les milliers d'alertes reçues au quotidien. L'exploitation des tactiques d'enregistrement et d'hébergement des hackers, en particulier de l'infrastructure qu'ils utilisent, aide les professionnels de la sécurité à identifier les sources de menaces et à les bloquer.

Dans une analyse de l'infrastructure utilisée par le groupe de cyberespionnage Fancy Bear, l'équipe de recherche de ThreatConnect (un partenaire Cisco qui est également le fournisseur de la seule plate-forme de sécurité extensible reposant sur la collecte d'informations dans le secteur) a identifié des domaines, des adresses IP et des alias potentiellement malveillants, ce qui a permis aux entreprises de réagir avant que les hackers ne parviennent à accéder aux réseaux.[19] En plus d'être proactive, cette approche est aussi prédictive, puisqu'elle permet aux fournisseurs de collecter des informations sur les hackers de façon préventive.

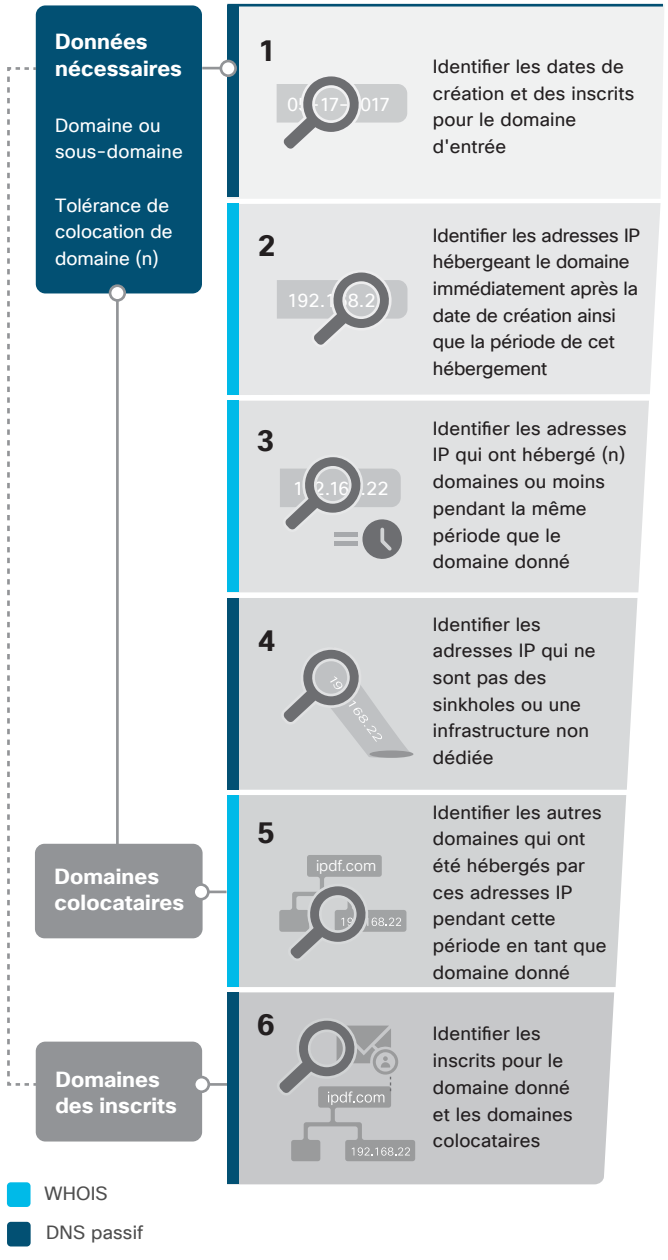
Les domaines et les adresses IP analysés étaient associés aux attaques par phishing dirigées contre Bellingcat, un site de journalisme citoyen ciblé par les menaces persistantes avancées de Fancy Bear. La théorie de ThreatConnect est que certains cybercriminels ont accès à une infrastructure IP limitée et hébergent donc plus d'un de leurs domaines sur l'infrastructure qu'ils contrôlent. En analysant ces domaines hébergés sur la même infrastructure, les experts de la sécurité peuvent identifier des infrastructures supplémentaires (comme des domaines et des adresses IP) que les hackers sont susceptibles de contrôler, et procéder à leur blocage préventif ou à leur incorporation dans leurs stratégies de défense.

19 Pour en savoir plus, consultez « Comment l'équipe de recherche de ThreatConnect a utilisé sa plate-forme pour rechercher l'origine des incidents liés à Fancy Bear, identifier des informations et procéder à une analyse probante » threatconnect.com/blog/how-to-investigate-incidents-in-threatconnect/

Comme le démontre l'analyse de ThreatConnect, le processus suivait les étapes suivantes :

- Bellingcat a fourni les en-têtes d'e-mails de campagnes de spear-phishing, ou phishing ciblé, soupçonnées de provenir de hackers financés par l'État russe. En se basant sur les informations connues concernant les opérations précédentes de Fancy Bear, ThreatConnect a déterminé que ce groupe était probablement à l'origine des opérations qui avaient ciblé Bellingcat.
- ThreatConnect a utilisé les informations d'enregistrement WHOIS pour identifier la date à laquelle le domaine dont provenaient les messages de spear-phishing avait été enregistré et l'adresse e-mail utilisée pour enregistrer le domaine en question, ce qui lui a permis de délimiter une période sur laquelle focaliser ses recherches.
- Un DNS passif a permis d'identifier les adresses IP ayant hébergé le domaine après son enregistrement initial. Cela a permis de recenser les adresses IP susceptibles d'être associées aux hackers.
- Les chercheurs ont ensuite de nouveau utilisé un DNS passif pour identifier les adresses IP ayant hébergé moins d'un nombre donné de domaines afin d'éliminer les IP hébergeant des domaines multiples pour plusieurs clients.
- Grâce à WHOIS et au DNS passif, ThreatConnect a pu identifier le sous-groupe d'adresses IP probablement associées aux hackers, déterminant la liste d'adresses IP vraisemblablement connectées à la menace persistante avancée.
- Une fois ce sous-groupe d'adresses IP identifié, ThreatConnect a utilisé un DNS passif pour identifier d'autres domaines hébergés par la même adresse IP et au même moment que le domaine d'origine. (Si les domaines sont hébergés par la même adresse IP que le domaine initial, on peut identifier ceux qui sont susceptibles d'être contrôlés par la même menace persistante avancée.)
- ThreatConnect a également identifié d'autres domaines enregistrés à l'aide de la même adresse e-mail que celle qui avait été utilisée pour l'enregistrement du domaine d'origine. Lorsqu'une adresse e-mail est utilisée pour enregistrer un domaine associé à des menaces persistantes avancées, d'autres domaines enregistrés avec cette même adresse sont susceptibles de participer à ce type de menaces.
- ThreatConnect a utilisé des domaines nouvellement identifiés (hébergés avec le domaine d'origine ou enregistrés avec la même adresse e-mail que ce dernier) pour conduire chaque nouvelle répétition de l'analyse.
- ThreatConnect a ensuite utilisé un DNS passif pour identifier tous les sous-domaines connus correspondant aux domaines identifiés. Ces informations peuvent aider à identifier les serveurs de messagerie ou les autres sous-domaines qui n'étaient pas hébergés sur les mêmes IP que le domaine identifié, ce qui a donné de nouvelles pistes de recherche.

Figure 28 Méthodologie de colocation



Source : ThreatConnect

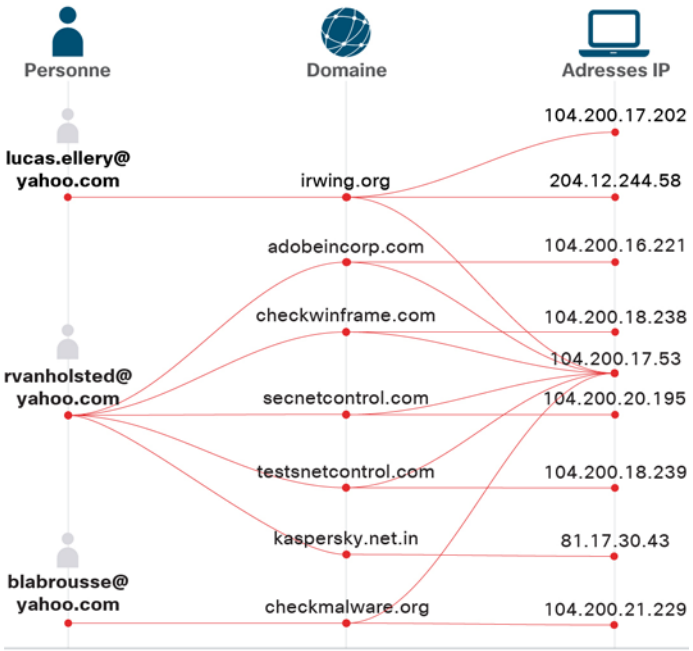
Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

Des méthodologies d'analyses comme celle qui est représentée sur la Figure 28 peuvent contribuer à identifier un groupe d'adresses e-mail, d'adresses IP et de domaines largement plus important susceptible d'être associé avec l'activité décelée et le suspect envisagé. L'examen décrit ci-dessus a porté sur six domaines, cinq adresses IP et trois inscrits aux e-mails identifiés dans les en-têtes d'e-mails fournis par Bellingcat.

Le processus décrit ci-dessus a permis d'identifier 32 adresses e-mail et alias, plus de 180 domaines et plus de 50 adresses IP vraisemblablement associés aux menaces persistantes avancées de Fancy Bear. La Figure 29 montre un sous-groupe des liens existant entre les domaines, adresses e-mail et adresses IP, et leurs connexions aux incidents de spear-phishing subis bar Bellingcat.

Les entreprises effectuant une analyse du même type peuvent bloquer de façon préventive les domaines, les adresses IP et les adresses e-mail pouvant être à l'origine d'attaques. Rechercher et identifier des infrastructures permet aux entreprises d'obtenir des informations tactiques à utiliser dans le cadre de la réponse à un incident, mais aussi d'identifier l'infrastructure utilisée par les hackers avant que celle-ci soit utilisée contre l'entreprise et de bénéficier d'un contexte reflétant les liens historiques entre les infrastructures et les hackers.

Figure 29 Relations dans l'infrastructure utilisée par un groupe responsable de menaces persistantes avancées



Source : ThreatConnect

Attaques de la chaîne d'approvisionnement : un maillon faible peut affecter de nombreuses entreprises

À l'instar de toute entreprise qui cherche à gagner en efficacité et à faire des économies, les hackers cherchent à être plus performants. Comme l'a découvert RSA, partenaire de Cisco, les attaques de chaîne d'approvisionnement exigent un minimum d'effort de la part des cybercriminels pour un maximum d'impact. Dans le cas examiné par RSA, les hackers avaient inséré un cheval de Troie dans un logiciel légitime généralement utilisé par les administrateurs système des entreprises pour l'analyse des journaux des événements système.[20]

Le logiciel compromis pouvait être téléchargé sur le site du fournisseur, de même que les mises à jour. Ainsi, un seul vecteur compromis (le site du fournisseur) pouvait ensuite diffuser la menace vers beaucoup d'autres réseaux d'entreprise, en proposant simplement le logiciel et les mises à jour automatiques.

Dans le cadre de cette recherche visant un groupe de hackers surnommé « Kingslayer », RSA a localisé le logiciel compromis après avoir remarqué un balisage non identifié visant une URL qui correspondait à une adresse IP associée à un domaine malveillant connu. En localisant l'origine du malware (une variante de PGV_PVID) trouvé sur le domaine, l'équipe de RSA a découvert une entreprise qui semblait avoir été infectée par ce malware, puis a déterminé que le malware venait du logiciel d'administration du système.

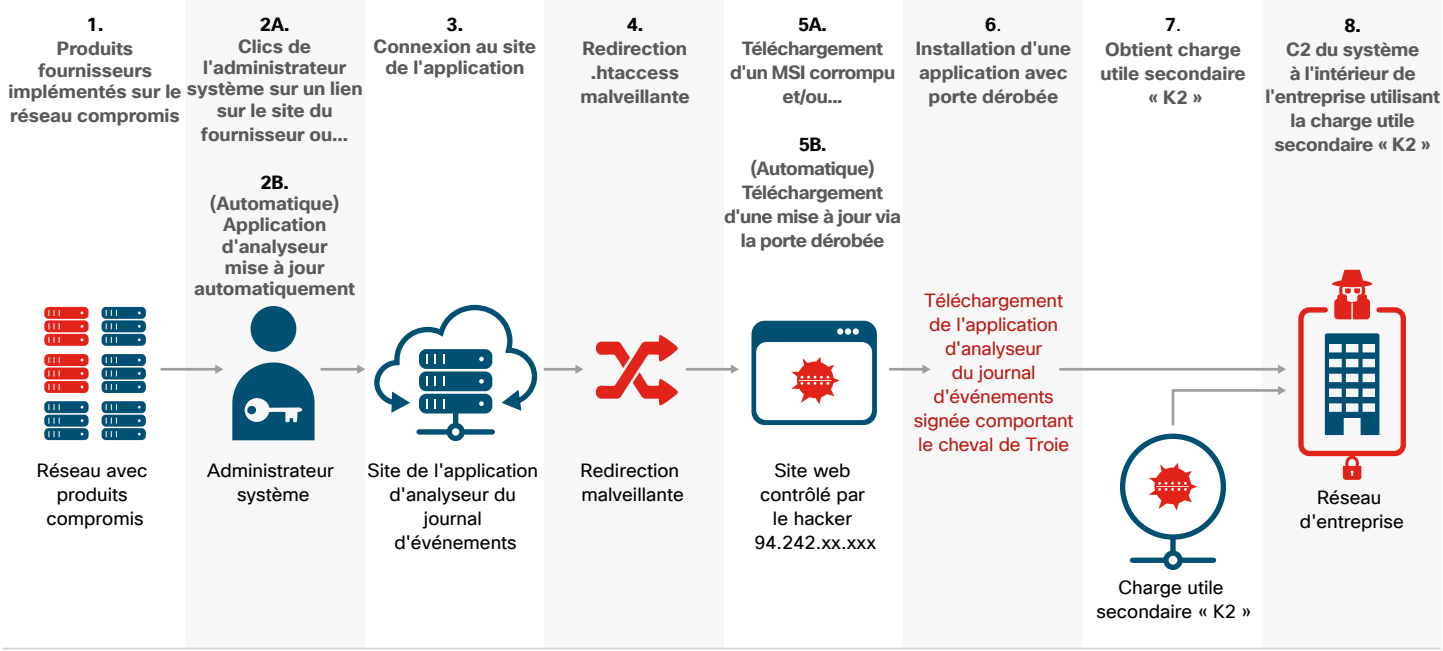
RSA a établi que la page de téléchargement du logiciel avait été compromise, au même titre que la page de mise à jour du fournisseur de logiciels (voir la Figure 30 à la page suivante). Les entreprises qui avaient précédemment téléchargé la version non compromise du logiciel étaient donc tout de même menacées si elles avaient accepté les mises à jour automatiques, car la mise à jour diffusait également le malware.

20 Pour en savoir plus sur ces recherches, voir le rapport RSA « Kingslayer–A Supply Chain Attack » : rsa.com/en-us/resources/kingslayer-a-supply-chain-attack.

La période de compromission n'a duré que deux semaines. Toutefois, comme le fournisseur n'a informé les utilisateurs du logiciel compromis que plusieurs mois plus tard, le malware a pu rester en place jusqu'à ce que les entreprises le détectent ou jusqu'à ce que la notification du fournisseur déclenche des efforts de correction.

Pour bloquer les menaces ciblant les chaînes d'approvisionnement, les entreprises doivent tout miser sur la détection. La sécurité des terminaux est la meilleure protection, car elle permet d'alerter les équipes de sécurité qu'un logiciel communique avec un autre. La surveillance en temps réel facilite également la détection d'activités suspectes.

Figure 30 Chaîne d'infection des éléments compromis par Kingslayer



Source : RSA

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

Bien que les analystes de RSA ne connaissent pas le nombre d'entreprises ayant installé l'application compromise avant qu'ils aient informé le fournisseur du problème, les clients de ce dernier sont indiqués sur son site web et sont enregistrés dans le journal des événements, disponible sur son portail d'information. La liste des clients, et donc des entreprises potentiellement compromises, incluait au moins :

- 4 importants opérateurs télécoms
- Plus de 10 agences militaires
- Plus de 24 entreprises du Fortune 500
- 5 importants prestataires de l'armée
- Plus de 24 banques et institutions financières
- Plus de 45 établissements d'enseignement supérieur

Sans avoir de certitude quant aux objectifs finaux des hackers du groupe Kingslayer, les analystes de RSA ont tout de même constaté que l'importance et la sophistication des clients de ce fournisseur en faisaient des cibles extrêmement lucratives. Les hackers cherchaient peut-être à obtenir des identifiants de connexion des clients d'entreprises financières, à moins qu'ils n'aient agi comme agents perturbateurs pour le compte d'un autre État.

La stratégie consistant à attaquer la chaîne d'approvisionnement doit être prise au sérieux pour plusieurs raisons. Il suffit aux hackers de compromettre un maillon de la chaîne pour infecter de nombreuses cibles. En outre, ces attaques sont discrètes par nature, ce qui donne aux hackers un temps précieux pour agir sans être détectés. Enfin, si le logiciel compromis est utilisé en priorité par des administrateurs système ou réseau ou par des responsables de la sécurité, il fournit aux hackers une base idéale pour lancer des attaques contre de grandes entreprises.

Les réseaux universitaires ciblés par les stratégies d'exploitation de l'infrastructure

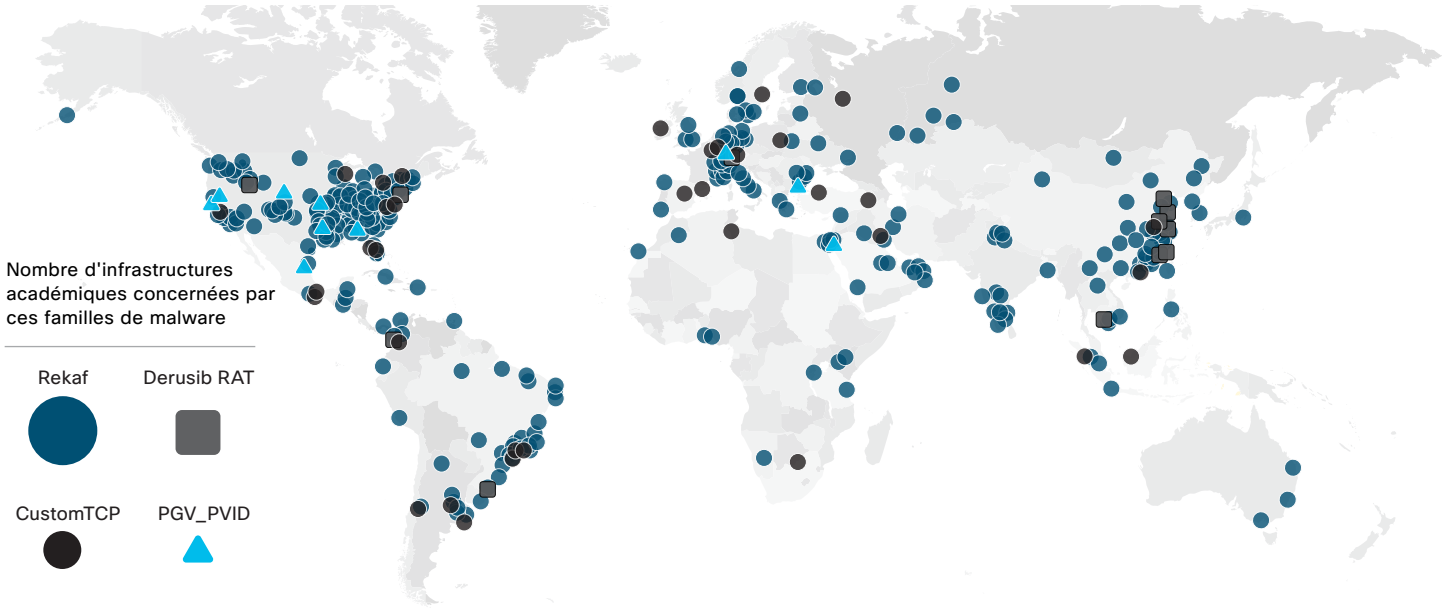
Dans le cas de Kingslayer, l'approche des hackers consistant à exploiter l'infrastructure exige de dissimuler l'attaque dans un matériel légitime, ce qui donne aux utilisateurs l'impression qu'ils obtiennent un produit sain alors qu'ils s'apprêtent à l'ajouter à leur réseau. Dans le cas du botnet Schoolbell,[21] les hackers utilisent l'infrastructure comme une rampe de lancement, étant donné que les ressources réseau n'inspirent aucune méfiance et se trouvent dans un emplacement d'apparence anodin. Dans les deux cas, les hackers exploitent la bonne réputation du fournisseur et de l'emplacement.

De la même façon que la sécurité des terminaux et le suivi en temps réel peuvent aider les entreprises à éviter les attaques de la chaîne logistique telle que celle que nous avons décrite plus haut, les mêmes principes peuvent contribuer à détecter ce que RSA appelle « l'exploitation d'infrastructure ». Dans ce type d'attaque, les hackers tentent de prendre le contrôle de l'infrastructure d'une entreprise dans l'espoir de l'utiliser pour des attaques à grande échelle.

Le botnet Schoolbell (qui doit son nom au fait qu'il ciblait des infrastructures universitaires) est un exemple de cette stratégie ; à l'époque de son pic d'activité, RSA a identifié presque 2 000 infections spécifiques dans l'infrastructure du botnet Schoolbell (voir la Figure 31).

Le botnet Schoolbell et l'approche consistant à exploiter les infrastructures doivent alerter les entreprises ou les institutions convaincues de ne pas pouvoir être ciblées par des attaques de cybercriminels car elles ne possèdent pas de données lucratives. Les institutions universitaires peuvent mettre moins l'accent sur la sécurité du réseau que d'autres structures de taille égale dans d'autres secteurs, comme les services financiers. Pour cette raison, les réseaux universitaires peuvent constituer des cibles attrayantes pour les hackers à la recherche d'un accès facile et de beaucoup de temps pour agir sans être détectés. Les institutions universitaires peuvent être une cible idéale pour les hackers en quête de ressources d'infrastructures.

Figure 31 Infections du malware Schoolbell dans le monde



Source : RSA

21 Pour en savoir plus sur le botnet Schoolbell et l'exploitation d'infrastructures, voir « Schoolbell: Class Is in Session », de Kent Backman et Kevin Stear, RSA, 13 février 2017 : blogs.rsa.com/schoolbell-class-is-in-session/

L'IoT en est à ses débuts, mais les botnets IoT existent déjà

Une menace DDoS crainte depuis longtemps s'est concrétisée en 2016 : des cyberattaques ont été lancées à partir de plusieurs appareils connectés transformés en botnets. En septembre, le blogueur spécialiste de la sécurité Brian Krebs a été ciblé par une attaque à 665 Gbit/s.[22] Peu de temps après, une attaque de 1 To/s a été lancée contre l'hébergeur français OVH.[23] Et en octobre, DynDNS a subi une attaque qui a mis hors service des centaines de sites web parmi les plus populaires : c'était la plus importante de ces trois attaques DDoS exploitant l'IoT.[24]

Avec ces attaques, nous sommes entrés dans l'ère des attaques DDoS à 1 To/s. Ces attaques ont bouleversé les paradigmes habituels de sécurité en montrant que la menace d'attaques DDoS via l'IoT par des botnets doit être prise au sérieux, en particulier par les entreprises.

Radware, un partenaire Cisco, s'est penché récemment sur l'activité de trois grands botnets IoT : Mirai, BrickerBot et Hajime. Voici son analyse.

Caractéristiques communes aux botnets IoT

- Leur installation est rapide et facile. Une heure suffit pour l'effectuer.
- La distribution est rapide. Le mécanisme d'infection récurrente entraîne une croissance exponentielle de la taille du botnet. D'ailleurs, les hackers peuvent disposer d'un botnet de plus de 100 000 appareils infectés en 24 heures.
- Le malware a un taux de détection faible. Il est très difficile de récupérer des échantillons car le code malveillant réside dans la mémoire de l'appareil et est nettoyé une fois ce dernier redémarré.

Mirai

Le botnet Mirai, responsable de l'attaque DynDNS, a infecté des centaines de milliers d'appareils IoT, les transformant en « armée de zombies » capable de lancer de puissantes attaques par DDoS de grande ampleur. Les chercheurs estiment que des millions d'objets IoT vulnérables participent activement à ces attaques coordonnées. Le code source du malware Mirai a été divulgué publiquement à la fin 2016.[25]

Fonctionnement

1. Mirai se connecte aux machines exploitées en exécutant une attaque par force brute contre les serveurs Telnet et en utilisant plus de 60 identifiants correspondant aux valeurs d'usine par défaut des logiciels BusyBox.
2. Chaque appareil infecté se verrouille automatiquement pour se protéger d'autres bots.
3. Mirai envoie l'IP de la victime et ses informations d'identification à un service centralisé ScanListen.[26]
4. La nouvelle victime aide alors à créer de nouveaux bots, par un mécanisme d'autoréplication.

Plus d'informations sur Mirai

Outre le fait que ce malware génère des volumes de trafic supérieurs à 1 To/s, Mirai dispose d'une sélection de 10 vecteurs d'attaque prédéfinis (voir la Figure 32). Certains vecteurs ont été en mesure de démolir l'infrastructure des opérateurs télécoms et des nettoyeurs de cloud en attaquant leurs protections.

Figure 32 Liste des vecteurs d'attaque de Mirai

```
#define ATK_VEC_UDP          0  /* Straight up UDP flood */
#define ATK_VEC_VSE          1  /* Valve Source Engine query flood */
#define ATK_VEC_DNS          2  /* DNS water torture */
#define ATK_VEC_SYN          3  /* SYN flood with options */
#define ATK_VEC_ACK          4  /* ACK flood */
#define ATK_VEC_STOMP        5  /* ACK flood to bypass mitigation devices */
#define ATK_VEC_GREIP        6  /* GRE IP flood */
#define ATK_VEC_GREETH       7  /* GRE Ethernet flood */
//#define ATK_VEC_PROXY      8  /* Proxy knockback connection */
#define ATK_VEC_UDP_PLAIN    9  /* Plain UDP flood optimized for speed */
#define ATK_VEC_HTTP        10  /* HTTP layer 7 flood */
```

Source : Radware

Parmi ces 10 vecteurs se trouvent des vecteurs d'attaque hautement sophistiqués comme les inondations GRE ainsi que les attaques TCP STOMP et Water Torture. Les attaques DDoS de Mirai illustrent les difficultés auxquelles sont confrontées les entreprises cherchant à identifier la légitimité d'un trafic GRE ou de requêtes DNS récursives.

22 « KrebsOnSecurity Hit with Record DDoS » de Brian Krebs, blog KrebsOnSecurity, 21 septembre 2016 : krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.
23 « 150,000 IoT Devices Abused for Massive DDoS Attacks on OVH », d'Eduard Kovacs, *SecurityWeek*, 27 septembre 2016 : securityweek.com/150000-iot-devices-abused-massive-ddos-attacks-ovh.
24 « DDoS Attack on Dyn Came from 100,000 Infected Devices », de Michael Kan, IDG News Service pour *ComputerWorld*, 26 octobre 2016 : computerworld.com/article/3135434/security/ddos-attack-on-dyn-came-from-100000-infected-devices.html.
25 « Source Code for IoT Botnet 'Mirai' Released », de Brian Krebs, blog KrebsOnSecurity, 1er octobre 2016 : krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/.
26 « BusyBox Botnet Mirai–the Warning We've All Been Waiting For? », de Pascal Geenens, Radware, 11 octobre 2016 : blog.radware.com/security/2016/10/busybox-botnet-mirai/.

BrickerBot

Les attaques par déni de service permanent (PDoS) sont des attaques rapides menées par des bots conçues pour mettre hors service les composants matériels. Cette forme d'attaque se répand de plus en plus.[27]

Parfois appelées « phlashing », les attaques PDoS peuvent endommager les systèmes avec une telle sévérité qu'il peut être nécessaire de réinstaller ou de remplacer leurs composants matériels. En exploitant les failles de sécurité ou les erreurs de configuration, les attaques PDoS peuvent détruire les micrologiciels et les fonctions de base des systèmes.

BrickerBot peut :

- **Compromettre des appareils** : les attaques PDoS de BrickerBot utilisent une méthode de force brute avec Telnet (le même vecteur d'attaque que Mirai) pour accéder aux appareils des utilisateurs.
- **Corrompre des appareils** : une fois qu'il a accédé à un appareil, BrickerBot exécute une série de commandes Linux qui finissent par corrompre le stockage. Il envoie ensuite une commande pour perturber la connectivité Internet et les performances de l'appareil, dont il supprime tous les fichiers.

La Figure 33 illustre la séquence des commandes effectuées par BrickerBot.

Hajime

Le fonctionnement de Hajime est encore mystérieux, et les chercheurs en Threat Intelligence le suivent de très près. En effet, Hajime n'est toujours pas passé à l'action, alors qu'il a déjà infecté des centaines de milliers d'appareils à ce jour. Son ampleur le rend particulièrement inquiétant. Le responsable de Hajime déclare être un hacker bienveillant, ou « white hat » (Figure 34).

Figure 33 Séquence des commandes de BrickerBot.1

```
fdisk -l
busybox cat /dev/urandom >/dev/mtdblock0 &
busybox cat /dev/urandom >/dev/sda &
busybox cat /dev/urandom >/dev/mtdblock10 &
busybox cat /dev/urandom >/dev/mmc0 &
busybox cat /dev/urandom >/dev/sdb &
busybox cat /dev/urandom >/dev/ram0 &
fdisk -C 1 -H 1 -S 1 /dev/mtd0
w
fdisk -C 1 -H 1 -S 1 /dev/mtd1
w
fdisk -C 1 -H 1 -S 1 /dev/sda
w
fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
w
route del default;iproute del default;ip route del default;rm -rf /* 2>/dev/null &
sysctl -w net.ipv4.tcp_timestamps=0;sysctl -w kernel.threads-max=1
halt -n -f
reboot
```

Source : Radware

Figure 34 Message du créateur de Hajime

```
Just a white hat, securing some systems.
Important messages will be signed like this!
Hajime Author.
Contact CLOSED
Stay sharp!
```

Source : Radware

Fonctionnement

Hajime est un botnet IoT sophistiqué, flexible, évolutif et conçu avec soin. Il peut se mettre à jour automatiquement et communiquer ses fonctionnalités enrichies aux bots de son réseau avec vitesse et efficacité. Comme bien d'autres botnets IoT, Hajime parcourt Internet pour détecter et infecter de nouvelles cibles, recherchant de nouveaux ports TCP 23 (Telnet) et TCP 5358 (WSDAPI) ouverts. Il utilise se connecte aux appareils par force brute pour en prendre le contrôle.

Il est à noter qu'Hajime peut éliminer les malwares se trouvant dans les appareils qu'il s'apprête à infecter. Il peut ensuite le protéger de toute contamination future en contrôlant ses communications Telnet. Ainsi, l'appareil redevient neutre, même si le créateur de Hajime y a toujours accès.

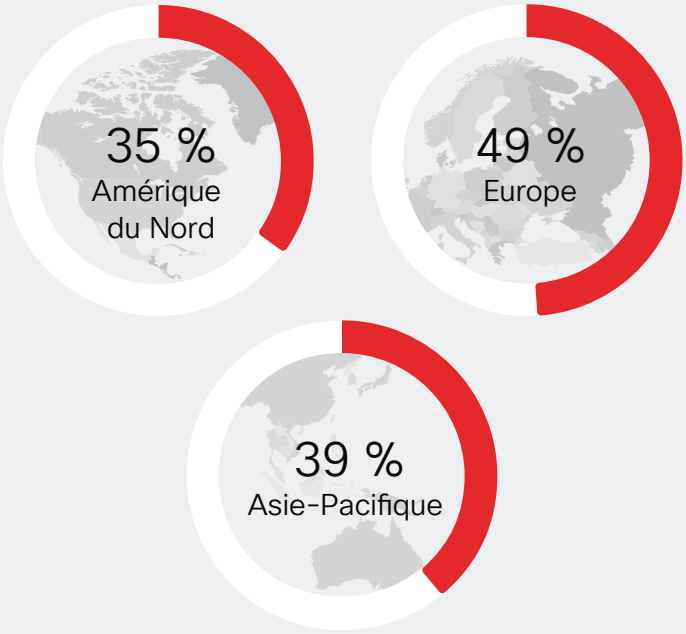
Des chercheurs ont observé des cas où Hajime avait nettoyé des appareils infectés avec Mirai.[28] (Alors que BrickerBot détruit les appareils infectés avec Mirai ou Hajime.)

27 Pour en savoir plus, consultez « BrickerBot PDoS Attack : Back With a Vengeance », Radware, 21 avril 2017 : security.radware.com/ddos-threats-attacks/brickerbot-pdos-back-with-vengeance/.
28 Pour en savoir plus, consultez « Hajime – Sophisticated, Flexible, Thoughtfully Designed and Future-Proof », de Pascal Geenens, Radware, 26 avril 2017 : blog.radware.com/security/2017/04/hajime-futureproof-botnet/

L'extorsion de fonds dans le cyberespace : l'attaque par RDoS

En 2016, presque une entreprise sur deux (49 %) a subi au moins un incident de demande de rançon en ligne, soit par ransomware (39 %), soit par attaque par déni de service avec demande de rançon, ou RDoS (17 %).[29] La Figure 35 montre le pourcentage d'entreprises de régions spécifiques du monde ayant subi un incident de demande de rançon en ligne en 2016.[30]

Figure 35 Répartition des attaques sur Internet avec demande de rançons par pays en 2016



Source : Radware

Selon Radware, le groupe de cybercriminels Armada Collective serait responsable de la plupart des attaques RDoS perpétrées à ce jour. La somme demandée tourne généralement autour de 10 à 200 bitcoins (entre 3 000 € et 60 000 € au moment de l'étude). Une « démonstration » ou un « avant-goût » de l'attaque accompagne généralement la demande de rançon. Lorsque le délai de paiement expire, les cybercriminels paralysent les data centers ciblés avec des volumes de trafic dépassant généralement 100 Gbit/s.

D'autres groupes se font également passer pour Armada Collective. On recense notamment une tentative d'extorsion visant trois banques grecques pour un montant total d'environ 7,2 millions de dollars.[31] Ces hackers envoient de fausses lettres de demande de rançon dans l'espoir de générer des revenus rapidement et à peu de frais. Voici quelques conseils utiles pour reconnaître une fausse demande de rançon :

1. **Évaluez la demande.** Le groupe Armada Collective demande généralement 20 bitcoins. D'autres campagnes ont pu demander des montants supérieurs ou inférieurs. En réalité, des demandes de rançons peu élevées proviennent probablement de faux groupes qui espèrent avoir fixé un montant assez bas pour obtenir un paiement.
2. **Vérifiez votre réseau.** Les véritables hackers exécutent d'abord une attaque de faible ampleur lorsqu'ils envoient une demande de rançon. Si vous constatez un changement dans l'activité du réseau, la lettre et la menace sont probablement authentiques.
3. **Recherchez une structure.** Les véritables hackers sont bien organisés. Quant aux faux, ils n'indiquent pas de lien vers un site web et n'ont pas de comptes officiels.
4. **Pensez aux autres cibles.** Les véritables groupes de hackers ciblent parfois plusieurs entreprises dans un même secteur. Contactez d'autres entreprises pour savoir si elles ont également reçu des menaces.

29 Cette enquête internationale, réalisée pour Radware par un institut spécialisé tiers, a interrogé environ 600 personnes.
30 Ibid.
31 « Greek Banks Face DDoS Shakedown », de Mathew J. Schwartz, BankInfoSecurity.com, 2 décembre 2015 : bankinfosecurity.com/greek-banks-face-ddos-shakedown-a-8714.

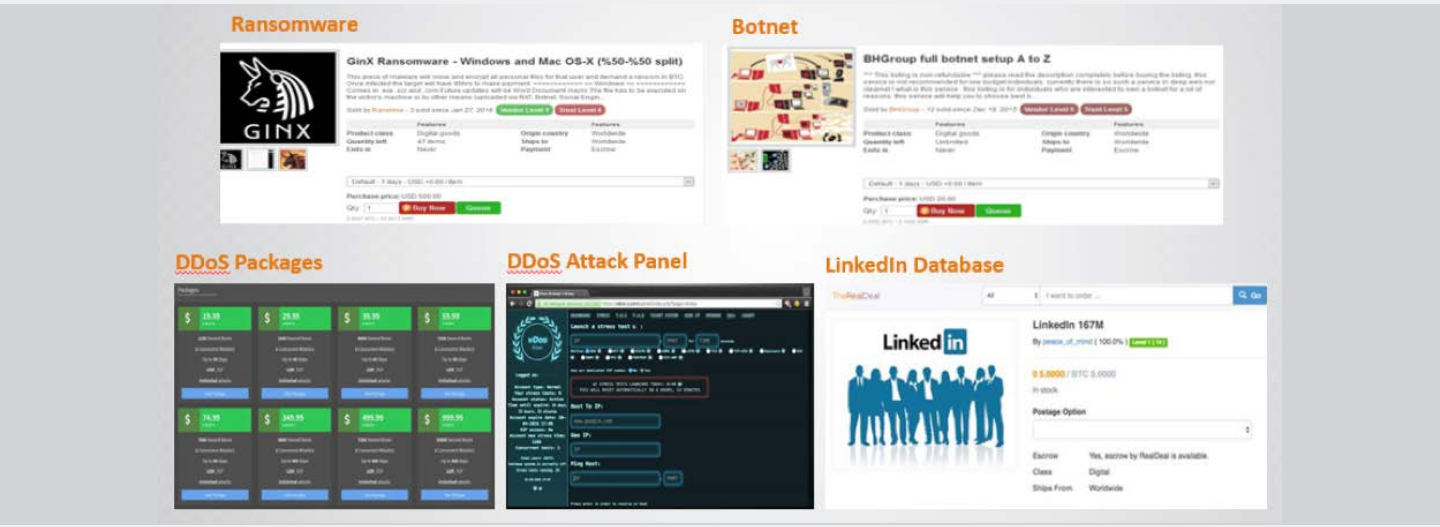
La nouvelle logique économique des hackers

L'augmentation spectaculaire de la fréquence, de la complexité et du volume des attaques en ligne au cours de l'année écoulée laisse à penser que la logique de rentabilité du hacking est entrée dans une nouvelle phase. Radware remarque que la nouvelle communauté de hackers bénéficie de plusieurs facteurs :

- Un accès rapide et facile à de nombreuses ressources pratiques et peu coûteuses (voir Figure 36)
- Une augmentation spectaculaire du nombre de cibles de grande valeur, de plus en plus vulnérables, et qui mettent en ligne un volume croissant d'informations de plus en plus précieuses.
- Le niveau de maturité de l'économie parallèle et d'Internet permet aux hackers d'agir avec efficacité, en toute sécurité et de façon anonyme.

Remarque : certaines des ressources représentées dans la Figure 36 ne sont plus actives.

Figure 36 Exemples d'outils et de consoles d'attaques en ligne



Source : Radware

Rançonner les équipements médicaux : une pratique qui se développe

Bon nombre de secteurs d'activité, y compris le secteur de la santé, doivent intégrer leurs technologies de l'information (IT) et leurs technologies opérationnelles (OT) pour continuer à fonctionner efficacement dans un monde toujours plus interconnecté. Cependant, en raison de l'interconnexion croissante des opérations, les failles de sécurité connues des appareils et des systèmes auparavant séparés les uns des autres représentent aujourd'hui un risque encore plus grand pour les entreprises. Par exemple, en utilisant des tactiques éprouvées comme les e-mails d'hameçonnage pour compromettre les utilisateurs, les hackers peuvent entrer dans un réseau, établir un point d'ancrage dans un appareil pourvu d'un système d'exploitation obsolète et, de là, s'infiltrer sur le réseau pour voler des informations, préparer le terrain pour une campagne de ransomware, et bien plus encore.

La récente attaque de ransomware WannaCry a démontré que l'interconnexion croissante des systèmes de santé et des pratiques de sécurité insuffisantes représentaient un risque pour les établissements et les patients. Même s'il ne s'agissait pas de la première attaque par ransomware ciblant le secteur de la santé, la campagne a été la première à affecter des appareils de radiologie utilisant Windows dans deux hôpitaux américains.[32]

Les chercheurs spécialistes des menaces de TrapX Security, un partenaire de Cisco qui développe des solutions de cybersécurité basées sur la tromperie, nous mettent en garde contre la croissance de certaine des attaques par ransomwares et autres malwares ciblant les dispositifs médicaux. Trapx appelle ce vecteur d'attaque MEDJACK (abréviation de Medical Device Hijack).

L'impact potentiel est évident dans la mesure où un hôpital de taille moyenne équipé de cinq ou six salles d'opération possède environ 12 000 à 15 000 appareils. Parmi ces équipements, environ 10 % à 12 % sont connectés à des adresses IP, d'après TrapX.

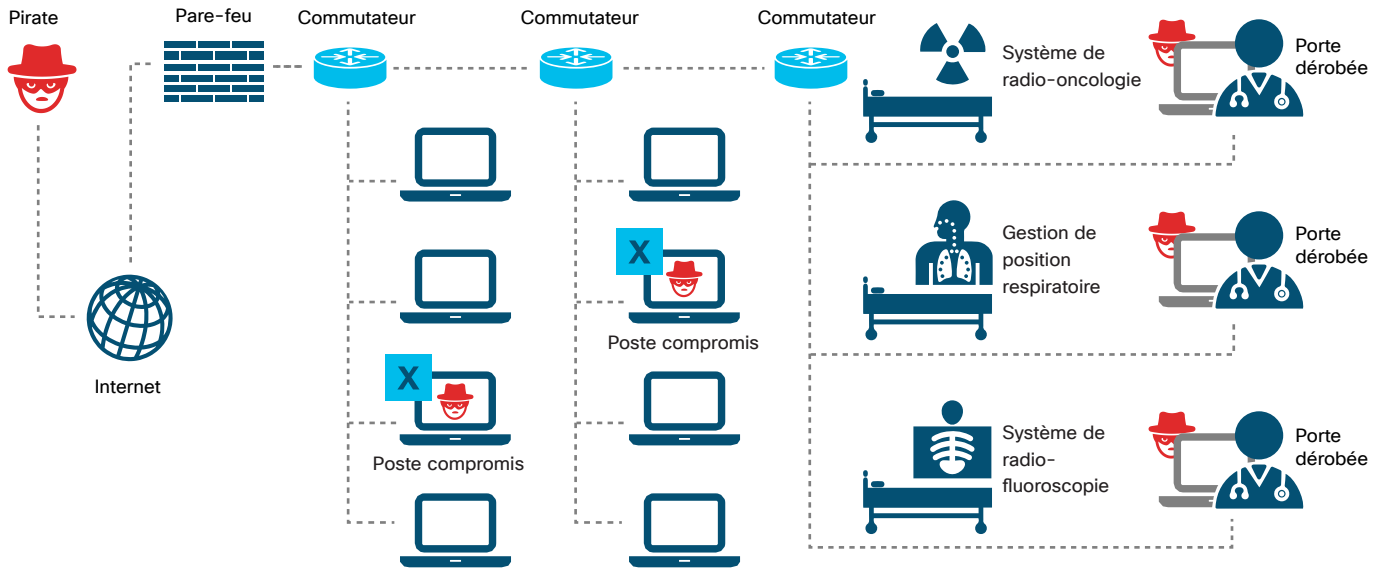
32 « #WannaCry Hits Medical Devices in US », de Tara Seals, *InfoSecurity Magazine*, 18 mai 2017 : infosecurity-magazine.com/news/wannacry-hits-medical-devices-in-us/.

Comme beaucoup d'autres appareils IoT actuels, les dispositifs médicaux n'ont pas été et ne sont toujours pas conçus en tenant compte de la sécurité. Ils exécutent souvent des systèmes anciens non corrigés et sont rarement surveillés par le personnel informatique de l'hôpital. Même lorsque les équipes de sécurité sont conscientes des vulnérabilités, elles ne peuvent pas toujours agir car seul le fournisseur a accès à ces produits. Dans d'autres cas, les équipes de sécurité doivent reporter à plus tard l'application des correctifs car l'établissement ne peut pas se permettre d'arrêter les équipements critiques, même pendant une courte période, ni risquer de compromettre l'efficacité d'un appareil. Enfin, parfois le fournisseur et d'autres parties, y compris l'administration publique, doivent approuver toute modification apportée à ces appareils, ce qui peut prendre plusieurs années. Le coût de l'assistance pour les dispositifs médicaux peut aussi être très élevé.

Beaucoup de cybercriminels cherchent à compromettre des dispositifs médicaux qui, selon les chercheurs de TrapX, sont devenus pour eux de véritables passerelles pour infiltrer les réseaux des hôpitaux. Les hackers savent également que les campagnes de ransomware qui paralysent les dispositifs médicaux contre une rançon peuvent être très rentables. Des cybercriminels encore plus malveillants pourraient également prendre le contrôle de ces dispositifs, y compris des dispositifs implantables, et blesser des patients.

Les chercheurs de TrapX ont récemment examiné l'exploitation d'un système d'oncologie avec des vulnérabilités Windows XP connues. Les hackers ont infecté trois machines (dont une qui contrôlait un puissant équipement laser) et en ont transformé une en botnet maître, qui a ensuite diffusé un programme malveillant (une version de Conficker) dans l'ensemble du réseau de l'hôpital (voir Figure 37).

Figure 37 Attaque d'un service d'oncologie

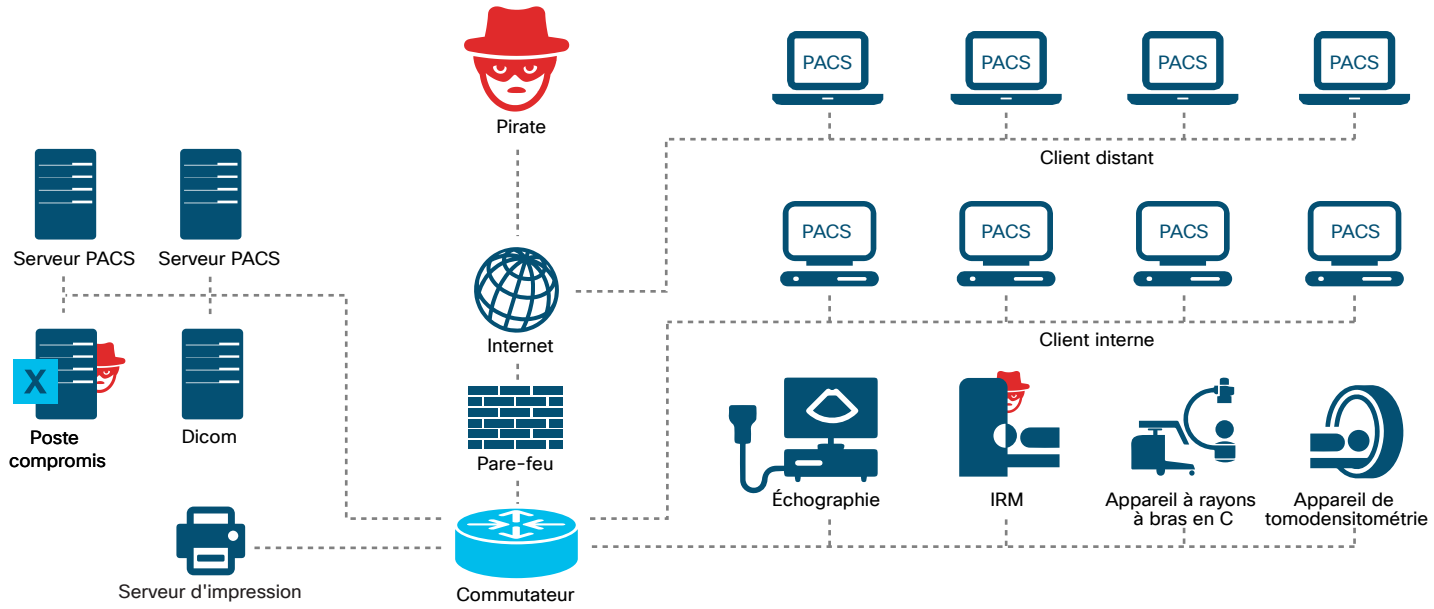


Source : TrapX

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

Un autre incident MEDJACK étudié récemment par TrapX présentait un système IRM compromis. Ici encore, c'est une vulnérabilité de Windows XP qui a été exploitée. Après avoir accédé aux données des patients, les hackers se sont rapidement rendu compte qu'ils pouvaient profiter de l'occasion pour déplacer leur attaque latéralement et prendre le contrôle des systèmes d'archivage et d'échange des informations sur les patients. (Ces systèmes appelés PACS sont utilisés pour centraliser et archiver les dossiers des patients et d'autres informations sensibles.) L'analyse des enquêteurs a montré que les hackers avaient été libres d'agir à leur guise dans le réseau de l'hôpital pendant plus de 10 mois.

Figure 38 Attaque d'un système IRM



Source : TrapX

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

Windows XP est l'un des systèmes d'exploitation les plus fréquemment utilisés avec les technologies opérationnelles dans les domaines de la santé, de l'énergie, de la fabrication ou d'autres secteurs. Les hackers savent que ce système d'exploitation est un talon d'Achille, car il n'est plus mis à jour par Microsoft et qu'il est extrêmement difficile et coûteux pour des entreprises de remplacer des appareils essentiels utilisant XP. C'est pour cette raison que ces appareils sont des cibles particulièrement attractives pour les hackers qui utilisent des ransomwares. Ils savent que les entreprises préfèreront payer la rançon demandée plutôt que risquer une interruption du fonctionnement de l'équipement, voire une mise hors service définitive.

Prendre les devants face à la menace

Les chercheurs de TrapX conseillent aux entreprises de prendre les mesures suivantes pour réduire la probabilité et l'impact d'une attaque par ransomware ciblant des équipements médicaux ou d'autres technologies opérationnelles :

- Identifiez les équipements médicaux dotés de connexions à des adresses IP et informez-vous sur le fonctionnement de ces connexions.
- Actualisez les contrats souscrits auprès de vos fournisseurs et assurez-vous que les engagements de ces contrats sont respectés en matière de mise à jour ou de remplacement des logiciels, appareils et systèmes.
- Abordez ce problème avec vos dirigeants et votre conseil d'administration pour les sensibiliser et les impliquer dans le processus.
- Déployez des outils technologiques améliorant la visibilité sur le réseau et automatisant la détection des menaces et leur correction.

Vulnérabilités

Vulnérabilités

Cette section présente les vulnérabilités et autres facteurs qui peuvent augmenter le risque d'attaque pour les entreprises ou les utilisateurs. Nous évoquons notamment les pratiques autorisant des délais trop importants dans la correction de vulnérabilités connues, l'absence de restriction des privilèges d'accès aux systèmes cloud ou encore la non-gestion de l'infrastructure et des terminaux. Nous expliquons également comment la conjecture géopolitique est source de challenges, mais aussi d'opportunités pour les fournisseurs de technologies et les entreprises.

Actualité géopolitique : l'attaque WannaCry souligne le risque associé à la rétention d'informations relatives aux vulnérabilités exploitables

Les débats mondiaux sur la cybersécurité avaient commencé à prendre de l'ampleur et un ton plus sérieux bien avant l'attaque massive du ransomware WannaCry survenue à la mi-mai. WannaCry ne fait que souligner que la communauté mondiale a encore beaucoup de travail à accomplir pour réduire la menace et l'impact des futures attaques des cybercriminels et des États-nations.

Selon Cisco, cette attaque mondiale récente nous fournit trois enseignements :

1. **Les organismes publics doivent signaler rapidement les failles des logiciels aux éditeurs et, dans la mesure où ces failles sont exploitées, codifier ces décisions pour mettre en œuvre une surveillance et une évaluation indépendantes.**

Il n'y a qu'en créant une plus grande transparence autour des vulnérabilités exploitables que nous pouvons espérer réduire leur occurrence et leur impact global. Les organismes publics doivent aussi mettre en place un processus continu correctement structuré qui leur permet de prendre des décisions relatives à la gestion des risques, notamment la gestion et la diffusion d'informations concernant les vulnérabilités exploitables aux développeurs de technologies et au public.

2. **Les développeurs de technologies doivent mettre en œuvre des mécanismes de gestion des risques connus du public pour recevoir, traiter et révéler des informations concernant la présence ou non de vulnérabilités, de correctifs, d'atténuations et de contournements connus.**

En plus d'assurer la sécurité tout au long du cycle de vie naturel des produits, les développeurs de technologies doivent communiquer publiquement sur tous les aspects de la gestion des vulnérabilités (comment, quoi, pourquoi et quand). Ils doivent aussi s'efforcer d'accroître la transparence concernant les processus de co-développement. Enfin, ils doivent s'assurer que les utilisateurs savent précisément qui contacter pour signaler des vulnérabilités afin qu'elles soient annoncées et corrigées.

3. **Les dirigeants d'entreprise doivent faire de la cybersécurité une priorité absolue.**

Cisco encourage depuis longtemps les responsables IT à saisir toute opportunité de former leur direction et leur conseil d'administration aux risques présentés par les attaques qui frappent l'entreprise, ses employés et ses clients, et entachent la réputation de l'entreprise. Il est temps de faire passer le message et d'agir : les dirigeants doivent faire de la cybersécurité un sujet prioritaire et souligner son importance pour toute l'entreprise. Les responsables doivent également s'assurer que l'infrastructure informatique de leur entreprise est à jour et régulièrement contrôlée, notamment en allouant un budget suffisant (pour en savoir plus, voir « Il est temps pour les responsables de la sécurité de s'inviter à la table des dirigeants de l'entreprise », à la page 83).

Il existe un débat légitime concernant la manière dont les pays partagent mondialement des informations sur les vulnérabilités et le moment où ils le font. Pourtant, comme nous l'avons vu avec WannaCry, Shadow Brokers, WikiLeaks Vault 7 et Year Zero, les organismes publics qui ne communiquent pas sur les vulnérabilités exploitables créent les conditions des fuites, offrant une occasion en or aux États-nations et aux cybercriminels.

Les hackers tentent déjà d'exploiter les nouveaux systèmes IoT, qui abondent en vulnérabilités connues et inconnues. Les organismes publics ont les moyens d'aider les développeurs de technologies à sécuriser les environnements IoT, mais ils doivent commencer à changer leurs pratiques et à favoriser davantage de transparence.

Les développeurs de technologies doivent quant à eux encourager la création de mécanismes de reporting allant dans le sens des incitations gouvernementales visant à collecter les exploits ainsi qu'à accélérer le reporting et le partage d'informations.

Les utilisateurs aussi ont une responsabilité importante : ils doivent être proactifs en appliquant les derniers correctifs et mises à jour et en mettant à niveau les produits qui ne sont plus pris en charge.

Actualité des vulnérabilités : des attaques en hausse suite à des divulgations majeures

Les divulgations de vulnérabilités à haute visibilité évoquées dans nos rapports précédents sur la cybersécurité, telles que les vulnérabilités OpenSSL, [33] se sont stabilisées au cours des derniers mois (voir la Figure 39). Toutefois, nos recherches ont identifié une importante activité en lien avec les vulnérabilités associées à des divulgations majeures, comme la publication par le groupe Shadow Brokers des vulnérabilités de Microsoft Windows,[34] la campagne d'Operation Cloud Hopper concernant les attaques de phishing contre les fournisseurs de services managés,[35] et la diffusion par WikiLeaks d'une série de documents du renseignement américain baptisée « Vault 7 » et expliquant comment les solutions logicielles et les systèmes d'exploitation les plus répandus pouvaient être compromis.[36]

Il est important de noter qu'une vulnérabilité peut exister et être exploitée sans que le public en soit conscient. Par exemple, les vulnérabilités exposées par Shadow Brokers ont été activement utilisées pendant des années. Les fuites de vulnérabilités ont permis à un plus grand nombre de personnes de les exploiter, mais aussi aux acteurs de la protection de se protéger contre elles.

Figure 39 Alertes critiques (novembre 2016 – mai 2017)

Date	Activité	Date	Activité
24/05/2017	Chargement de CVE-2017-7494 par la bibliothèque non sécurisée Samba	**06/03/17**	Vulnérabilité CVE-2017-5638 avec exécution de code distant sur Apache Struts2
11/04/17	CVE-2017-0199 sur Microsoft Office (attaque Dridex)	**06/02/17**	Vulnérabilités CVE-2017-3733 sur OpenSSL
08/04/17	Divulgation par le Shadow Brokers Group des exploits de l'Equation Group	**26/01/17**	Vulnérabilités sur Open SSL
06/04/17	Campagnes internationales continues Operation Cloud Hopper	**18/01/17**	Vulnérabilités sur Oracle CPU et Oracle OIT (Talos)
29/03/17	CVE-2017-7269 dans les services IIS WebDav de Microsoft	**03/01/17**	Injection de commande arbitraire CVE-2016-10033 CVE-2016-10045 sur PHPMailer
21/03/17	Protocole Network Time (NTP)	**22/11/16**	Protocole Network Time (NTP)
14/03/17	CVE-2017-0108 dans Microsoft Windows Graphics	**10/11/16**	Attaque DOS ICMP BlackNurse
07/03/17	Publication de Vault 7 par WikiLeaks	**04/11/16**	Problèmes de mise en œuvre de OAuth 2.0 mobile

Source : Cisco Security Research

33 *Rapport annuel Cisco 2015 sur la sécurité :* cisco.com/web/offer/gist_ty2_asset/Cisco_2015_ASR.pdf
34 « Cisco Coverage for Shadow Brokers 2017-04-14 Information Release », blog Talos, 15 avril 2017 : blog.talosintelligence.com/2017/04/shadow-brokers.html.
35 « Operation Cloud Hopper: China-Based Hackers Target Managed Service Providers », de Kevin Townsend, SecurityWeek.com, 6 avril 2017 : securityweek.com/operation-cloud-hopper-china-based-hackers-target-managed-service-providers.
36 « The WikiLeaks Vault 7 Leak – What We Know So Far », d'Omar Santos, blog Cisco Security, 7 mars 2017 : blogs.cisco.com/security/the-wikileaks-vault-7-leak-what-we-know-so-far.

L'examen des vulnérabilités divulguées par WikiLeaks a fait naître un sujet de préoccupation chez les acteurs de la protection : ils n'avaient pas connaissance des exploits développés par les administrations publiques et donc des vulnérabilités associées. Les acteurs de la protection peuvent à juste titre s'inquiéter des autres vulnérabilités qui existent et n'ont pas été divulguées.

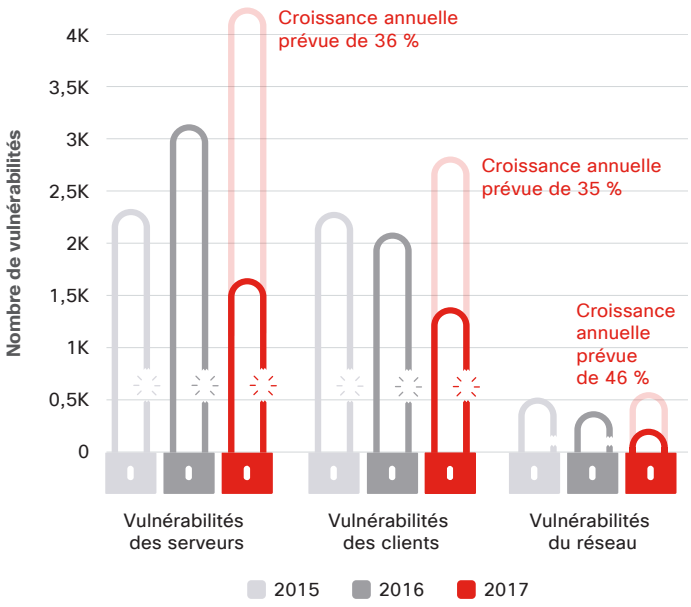
À retenir également sur la liste de la Figure 39 : les vulnérabilités divulguées de Microsoft Office, qui ont été rapidement exploitées par le botnet Dridex.[37] Comme l'a signalé Cisco, des exemples d'exploitation de la vulnérabilité Microsoft ont été constatés lors d'attaques e-mail porteuses de pièces jointes malveillantes. En outre, la vulnérabilité Apache Struts2 a aussi été rapidement exploitée.[38]

Une augmentation des vulnérabilités client-serveur

Comme nous avons pu l'évoquer dans notre *rapport sur la cybersécurité du 1er semestre 2016*, les vulnérabilités côté serveur ont augmenté : les hackers ont compris qu'en attaquant les vulnérabilités des logiciels de serveurs, ils pouvaient accéder à l'ensemble des réseaux de certaines entreprises.[39] Selon la tendance des premiers mois de 2017, les vulnérabilités côté serveur devraient afficher une augmentation de 36 % par rapport au nombre de vulnérabilités de 2016, tandis que les vulnérabilités côté client devraient augmenter de 35 % (voir la Figure 40).

Le fait que les vulnérabilités des logiciels tiers exigent une correction manuelle est une des raisons de leur croissance. Si les correctifs ne sont pas appliqués manuellement avec rapidité, le champ d'action des hackers ciblant les vulnérabilités côté serveur s'agrandit. Même si les vulnérabilités côté client augmentent également, elles peuvent être corrigées à l'aide de mises à jour automatiques, ce qui permet de réduire très rapidement les opportunités d'attaque.

Figure 40 Vulnérabilités client-serveur



Source : Cisco Security Research

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

37 « Cisco Coverage for CVE-2017-0199 » blog Talos, 14 avril 2017 : blog.talosintelligence.com/2017/04/cve-2017-0199.html.
38 « Content-Type: Malicious - New Apache Struts2 0-Day Under Attack », de Nick Biasini, blog Talos, 8 mars 2017 : blog.talosintelligence.com/2017/03/apache-0-day-exploited.html.
39 « L'essor des campagnes d'attaques axées sur les serveurs », *Rapport Cisco sur la cybersécurité - 1er semestre 2016* : cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html.

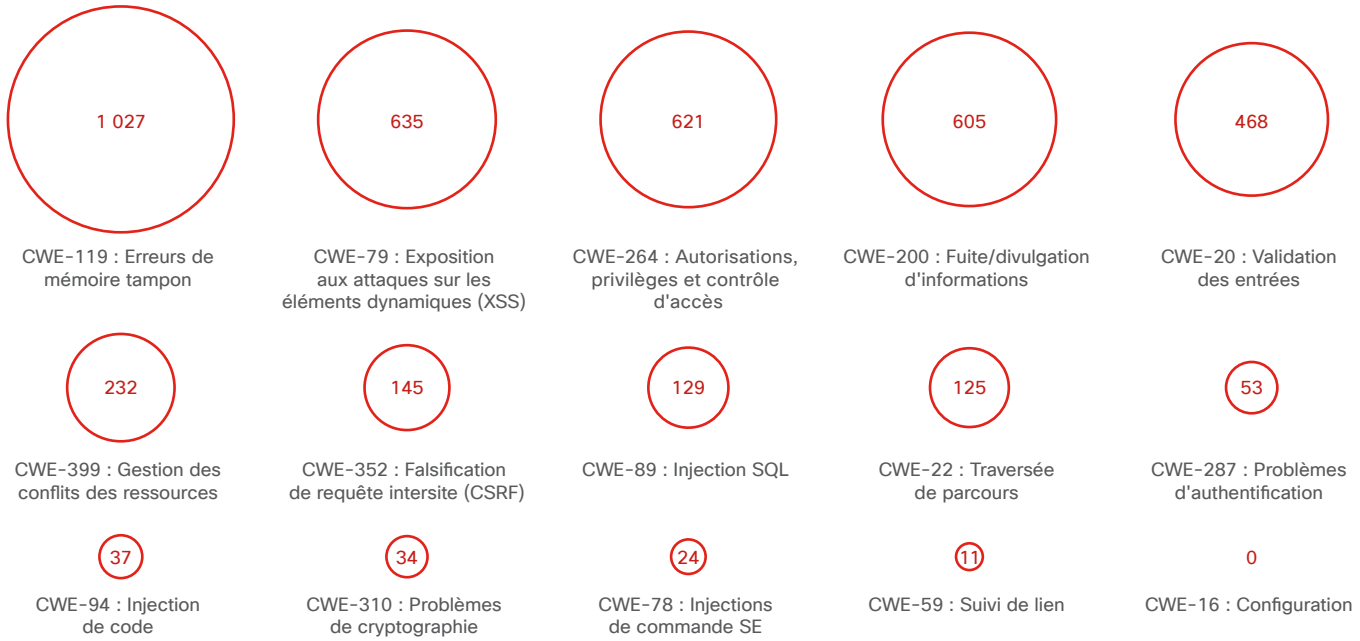
Diminution considérable des kits d'exploit

L'activité des kits d'exploit connaît une baisse sensible qui reflète le déclin global de leur utilisation par les hackers (voir page 9). Depuis que les fournisseurs de logiciels, en particulier de navigateurs web, ont bloqué l'utilisation des vecteurs d'attaque les plus fréquents, comme les contenus créés avec Adobe Flash et Java, les hackers se tournent de plus en plus vers des approches plus accessibles, comme celles utilisant des ransomwares, des attaques DDoS et des attaques de type BEC (voir page 22).

Catégories de vulnérabilité : le débordement de tampon reste en tête

L'examen de la CWE, la liste des vulnérabilités des logiciels de sécurité, nous apprend que le débordement de tampon est la plus fréquente erreur de codage exploitée par les criminels (voir Figure 41). Les développeurs de logiciels ne cessent de répéter cette erreur. Pour l'éviter, les développeurs doivent s'assurer que l'accès à la mémoire tampon est réglementé.

Figure 41 Principales catégories de menaces (novembre 2016 – mai 2017)



Source : Cisco Security Research

Ne laissez pas les technologies de DevOps mettre en danger votre entreprise

En janvier 2017, des hackers se sont lancés dans une opération de chiffrement des instances MongoDB publiques, suivie de demandes de paiement de rançons en échange des clés et logiciels de déchiffrement. Depuis, les hackers ont étendu leur liste de cibles en s'attaquant à d'autres bases de données telles que CouchDB et Elasticsearch.[40] Ces services de DevOps sont souvent exposés parce qu'ils n'ont pas été correctement déployés ou parce qu'ils ont été intentionnellement laissés ouverts pour pouvoir être facilement accessibles par les utilisateurs légitimes.

Rapid7, partenaire de Cisco et fournisseur de solutions d'analyse et de données de sécurité, qualifie les attaques sur MongoDB, CouchDB et Elasticsearch « d'attaques de ransomware DevOps ». L'entreprise inclut des technologies comme Docker, MySQL et MariaDB, ainsi que d'autres composants DevOps courants dans sa définition.

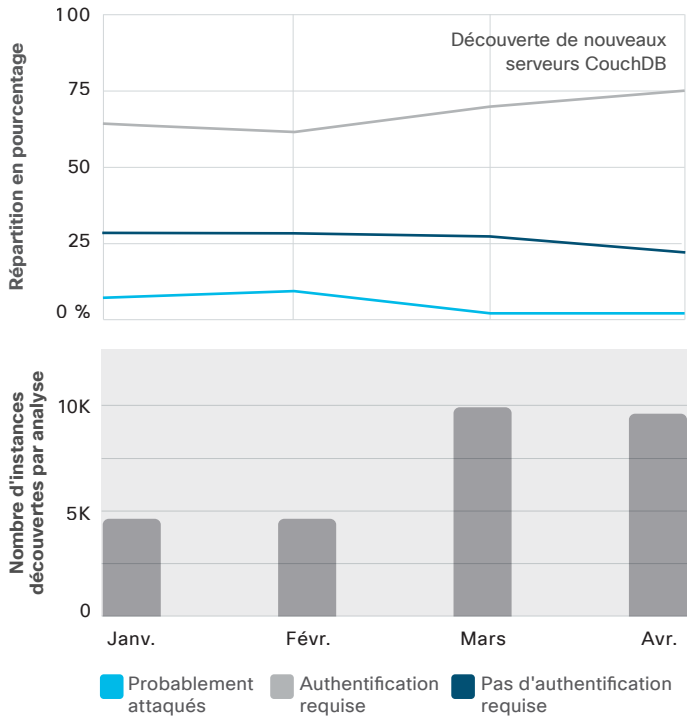
Depuis janvier 2017, Rapid7 a régulièrement analysé Internet à la recherche de ces technologies et a catalogué les instances ouvertes et les instances rançonnées. à en juger par les noms des tables exposées sur Internet, certains de ces services DevOps contiennent des informations personnelles identifiables (PII).

Ce qui suit est une présentation d'un échantillon de conclusions tirées des analyses réalisées par Rapid7.

CouchDB

Environ 75 % des serveurs CouchDB peuvent être catégorisés comme largement ouverts (exposés sur Internet et sans dispositif d'authentification). Un peu moins d'un quart requiert une authentification (au minimum des informations d'identification). Environ 2 à 3 % sont susceptibles d'avoir été rançonnés. Cela peut sembler très peu, sauf qu'environ 2 % des serveurs CouchDB découverts par Rapid7 contenaient des informations personnelles identifiables. Ces PII incluaient des informations sur des essais cliniques de médicaments, des numéros de carte bancaire et des coordonnées personnelles.

Figure 42 Statuts CouchDB



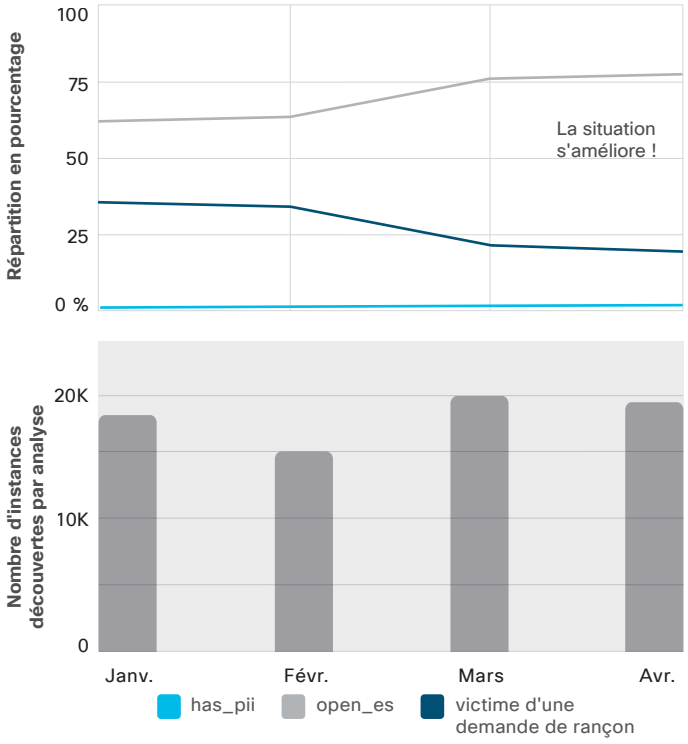
Source : Rapid7

Elasticsearch

À l'instar de CouchDB, plus de 75 % des serveurs Elasticsearch peuvent être catégorisés comme largement ouverts. Environ 20 % sont susceptibles d'avoir été rançonnés. Selon l'analyse de Rapid7, la bonne nouvelle est qu'un très faible pourcentage de ces serveurs contiennent des PII.

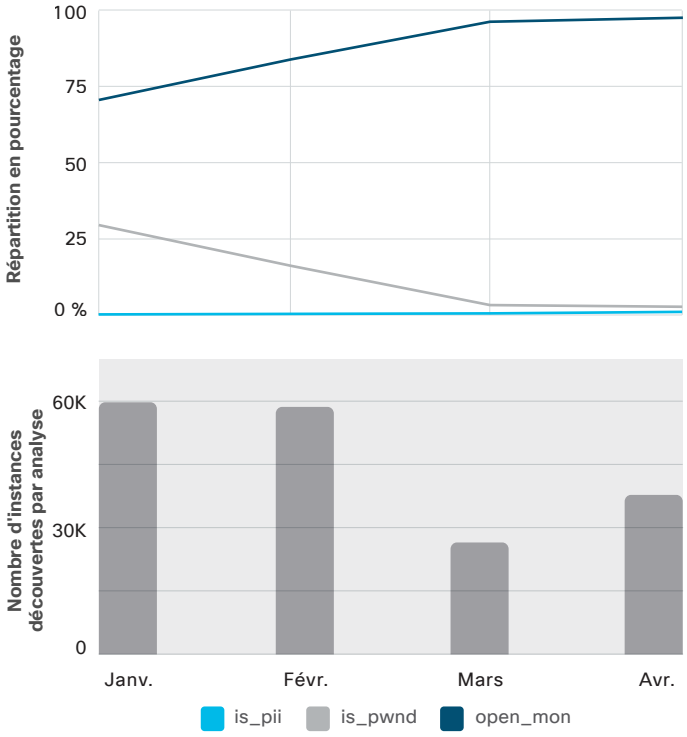
40 « After MongoDB, Ransomware Groups Hit Exposed Elasticsearch Clusters » par Lucian Constantin, IDG News Service, 13 janvier 2017 : pcworld.com/article/3157417/security/after-mongodb-ransomware-groups-hit-exposed-elasticsearch-clusters.html.

Figure 43 Statuts Elasticsearch



Source : Rapid7

Figure 44 Statuts MongoDB



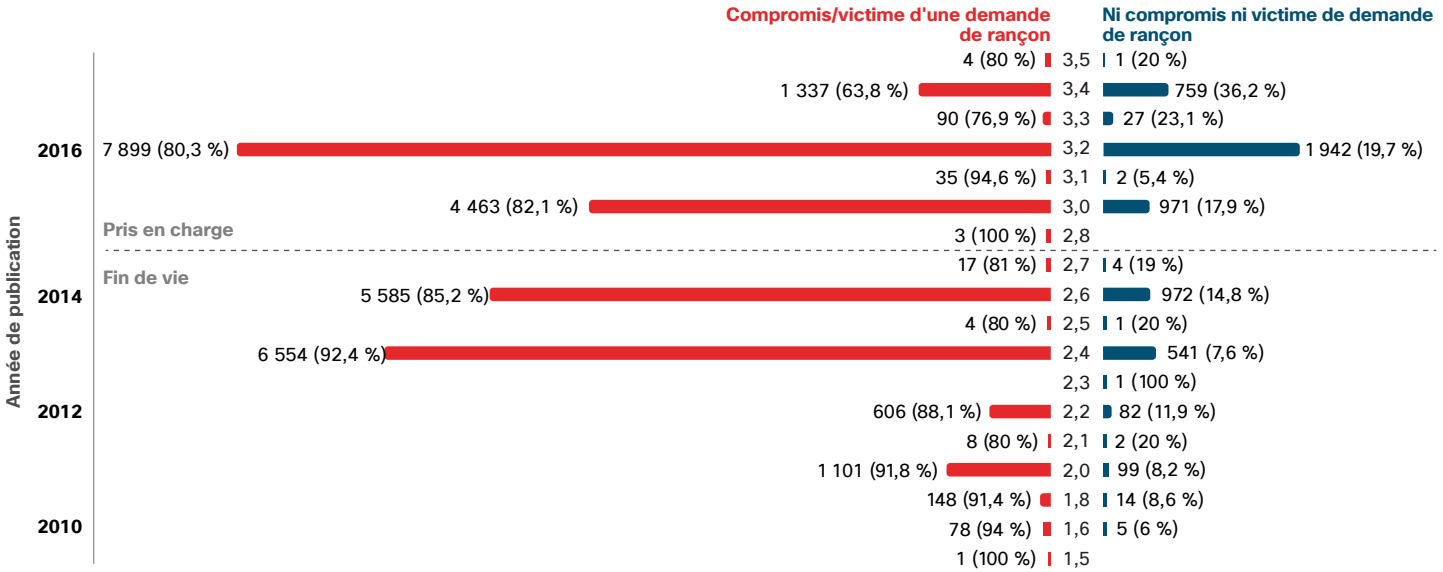
Source : Rapid7

MongoDB

En dépit de l'attaque de ransomware du mois de janvier ayant touché des milliers de serveurs MongoDB, les utilisateurs et les entreprises utilisant ces serveurs doivent encore améliorer leurs pratiques de sécurité. Près de 100 % des serveurs repérés par Rapid7 pendant ses analyses peuvent être catégorisés comme largement ouverts. Heureusement, très peu de ces serveurs semblent contenir des données sensibles.

Rapid7 a également établi que nombre des serveurs MongoDB susceptibles d'avoir été ciblés par une attaque par ransomware étaient en fin de vie. Cependant, une part importante étaient plus récents et prenaient toujours en charge des versions qui n'avaient probablement pas été récemment mises à jour ou corrigées, et peut-être jamais (voir Figure 45).

Figure 45 Versions MongoDB

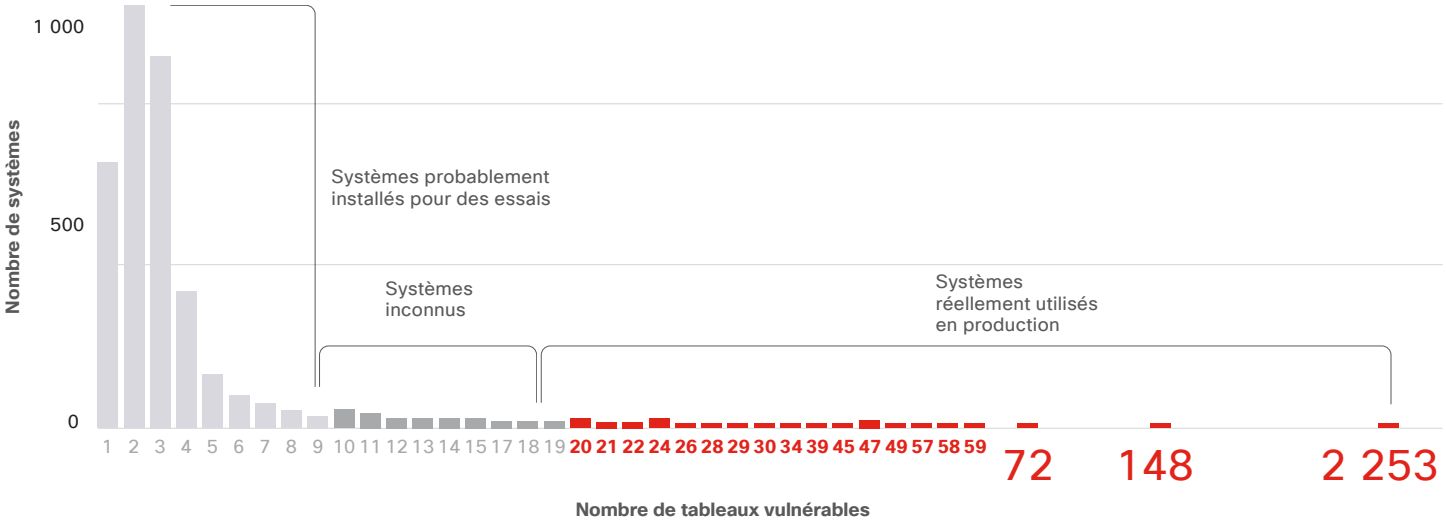


Source : Rapid7

La Figure 46 illustre le nombre de tables exposées parmi les serveurs MongoDB identifiés par Rapid7 dans son étude. La plupart a moins de 10 tables et il s'agit de serveurs probablement mis en place pour des tests.

Cependant, certains serveurs ont 20 tables ou plus. Ceci indique que ce sont de véritables systèmes de production. Un serveur exposé à Internet avait plus de 2 200 tables.

Figure 46 Taille des bases de données MongoDB et nombre de tables exposées (janvier – avril 2017)



Source : Rapid7

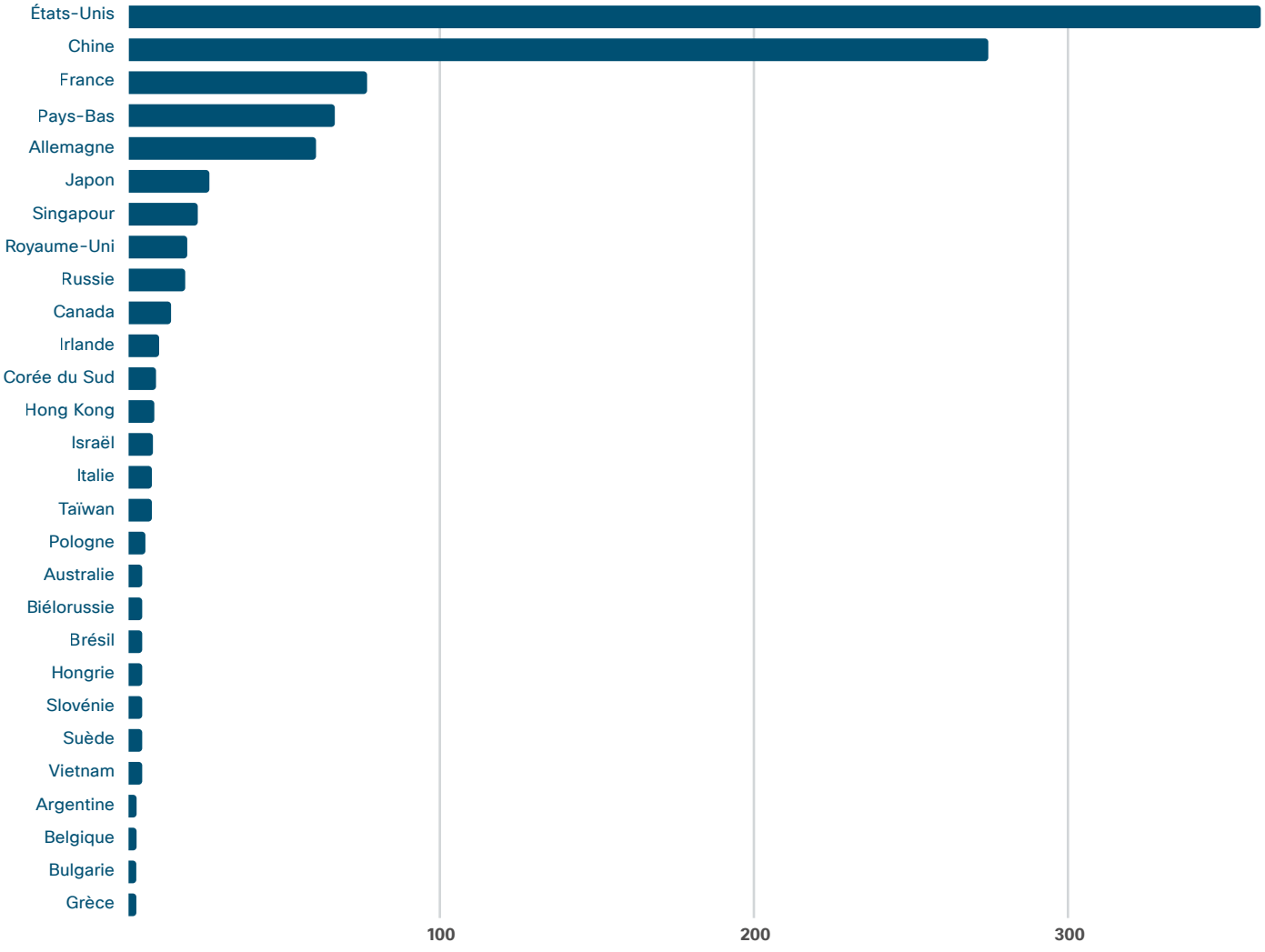
Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

Docker

Rapid7 a également étudié Docker, un système d'orchestration dont les opérateurs ont dès le départ été très portés sur les questions de sécurité. Cependant, d'après l'analyse de Rapid7, plus de 1 000 instances Docker sont largement ouvertes en dépit de leurs efforts. La plupart des instances Docker identifiées sont aux États-Unis ou en Chine (voir la Figure 47).

Bon nombre des instances Docker ouvertes sont des systèmes test abandonnés ou oubliés. Mais 245 de ces 1 000 instances ouvertes ont au moins 4 Go de mémoire et sont susceptibles d'être des systèmes de production actifs (voir la Figure 48).

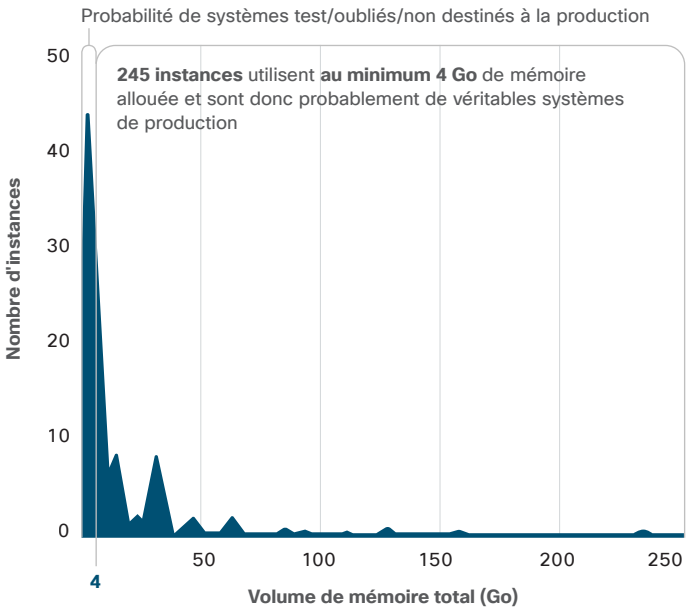
Figure 47 Instances Docker par pays (janvier - avril 2017)



Source : Rapid7

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

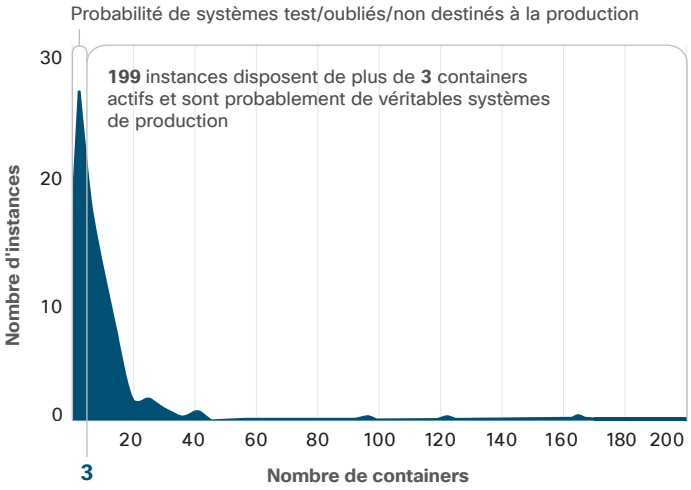
Figure 48 Mémoire totale allouée pour l'utilisation des instances Docker (janvier – avril 2017)



Source : Rapid7

Par ailleurs, Rapid7 a établi que 199 des instances Docker complètement ouvertes présentent au moins trois containers actifs et en fonctionnement. Certaines en comptent jusqu'à 160 (Figure 49). Les entreprises qui utilisent ces systèmes de production non sécurisés courent d'immenses risques. Un hacker pourrait créer une connexion shell depuis Internet vers chacun de ces systèmes et en prendre le contrôle.

Figure 49 Distribution des containers en fonctionnement par instance (janvier – avril 2017)



Source : Rapid7

Les entreprises qui utilisent des instances Internet publiques de ces systèmes et d'autres technologies DevOps doivent prendre des mesures pour se protéger contre les menaces. Les équipes chargées de la sécurité doivent :

- Développer de solides standards pour le déploiement sécurisé des technologies de DevOps
- Conserver une visibilité active de l'infrastructure publique détenue par l'entreprise
- Appliquer tous les correctifs et mises à jour des technologies DevOps
- Réaliser des analyses de vulnérabilité

Les entreprises ne corrigent pas assez rapidement les vulnérabilités Memcached de leurs serveurs

Les hackers s'emploient activement à trouver des bases de données non sécurisées et exposées à Internet qu'ils attaqueront, dépouilleront de leurs données ou rançonneront. Cette dernière approche a pris de l'ampleur rapidement depuis le lancement de l'attaque par ransomware de janvier, qui a ciblé des milliers de bases de données MongoDB.[41]

Il n'a jamais été envisagé que les services tels que MongoDB soient exposés à des environnements non fiables et ces services ne présentent pas de puissantes procédures d'authentification (parfois il n'y en a pas du tout). Les chercheurs en menaces de Cisco étudient les vulnérabilités dans les services similaires. à la fin de l'année 2016, nous avons conduit un audit du code pour évaluer la sécurité des serveurs de mémoire cache Memcached. Les entreprises utilisent Memcached pour augmenter la vitesse et la performance des services et applications web.

Cet examen nous a permis de découvrir l'existence de trois vulnérabilités liées à l'exécution de code à distance.[42] L'une des vulnérabilités résidait dans le mécanisme d'authentification du serveur. Ceci veut dire que même les serveurs disposant d'un mécanisme d'authentification activé peuvent être exploités. Les chercheurs en menaces de Cisco ont fait connaître les vulnérabilités au fournisseur, lequel a rapidement créé un correctif.

41 « MongoDB Databases Actively Hijacked for Extortion, » par Ionut Arghire, *SecurityWeek*, 4 janvier 2017 : securityweek.com/mongodb-databases-actively-hijacked-extortion.

42 Pour en savoir plus, reportez-vous aux rapports de Talos sur les vulnérabilités pour 2016 : « Memcached Server Append/Prepend Remote Code Execution Vulnerability » talosintelligence.com/vulnerability_reports/TALOS-2016-0219 ; Memcached Server Update Remote Code Execution Vulnerability »talosintelligence.com/vulnerability_reports/TALOS-2016-0220 ; et « Memcached Server SASL Authentication Remote Code Execution Vulnerability »talosintelligence.com/vulnerability_reports/TALOS-2016-0221.

Quelques mois après, nous avons réalisé des analyses partout sur Internet pour connaître la situation suite au déploiement du correctif. Bien que le fournisseur ait rapidement créé le correctif, et que les distributions Linux aient vite publié les mises à jour, nous avons pu déterminer que 79 % des presque 110 000 serveurs Memcached exposés étaient encore soumis aux vulnérabilités liées à l'exécution de code à distance que nous avions fait connaître (voir Figure 50).

En outre, seulement 22 % des serveurs disposent d'un mécanisme d'authentification actif. Et presque tous les serveurs nécessitant un mécanisme d'authentification étaient toujours vulnérables – 23 707 sur 23 907 (voir Figure 50). Les serveurs couverts par notre étude sont répartis partout dans le monde, mais la plupart sont concentrés aux États-Unis et en Chine. La plupart des ces serveurs vulnérables se trouve dans ces deux pays, comme le montre la dernière analyse que nous avons effectuée en mars (voir Figure 51).

En bref, il faut comprendre que, même si les chercheurs en menaces de Cisco n'ont pas pu établir que l'un de ces serveurs a été l'objet d'une attaque parce qu'il est soumis à ces vulnérabilités, c'est une question de temps avant que cela se produise. Les informations concernant ces vulnérabilités et les correctifs permettant de régler le problème sont connus du public depuis plusieurs mois.

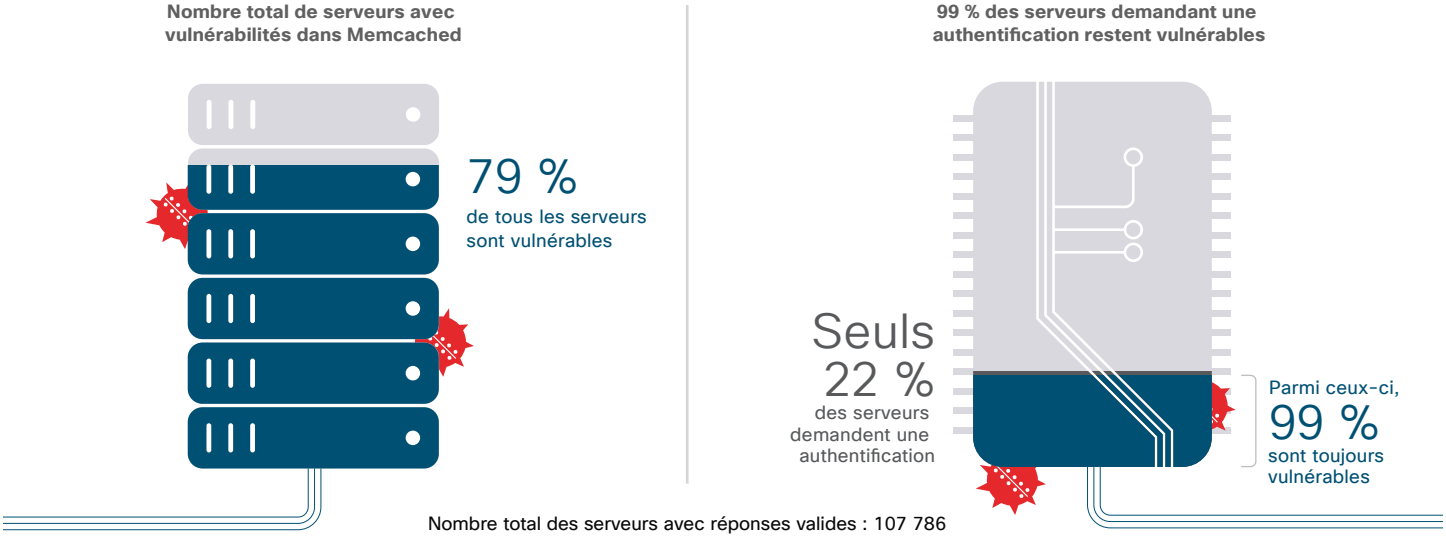
Face à la tendance qui se dessine, qui consiste à attaquer des bases de données et d'autres infrastructures exposées à Internet, la nécessité de corriger ce type de vulnérabilités est encore plus urgente. Même avec des mécanismes d'authentification, les services de DevOps présentent un risque. C'est la raison pour laquelle ils doivent être tenus à l'écart des environnements sécurisés (pour en savoir plus sur ce risque, reportez-vous à « Ne laissez pas les technologies de DevOps mettre en danger votre entreprise », page 50).

Figure 51 Serveurs Memcached par pays (février – mars 2017)

Pays	Serveurs vulnérables	Total du nbre de serveurs
États-Unis	29 660	36 937
Chine	16 917	18 878
Royaume-Uni	4 713	5 452
Allemagne	3 047	3 698
France	3 209	5 314
Japon	3 003	3 607
Pays-Bas	2 556	3 287
Inde	2 460	3 464
Russie	2 266	3 901
Hong Kong	1 820	1 939

Source : Cisco Security Research

Figure 50 Vulnérabilités : Memcached



Source : Cisco Security Research

Les hackers utilisent le cloud pour atteindre plus rapidement les cibles les plus intéressantes

Pour les hackers, le cloud ouvre de nouveaux horizons. Ils exploitent pleinement son potentiel comme vecteur d'attaque. Ils savent que les systèmes cloud sont aujourd'hui critiques pour de nombreuses entreprises. Ils ont également compris qu'ils pouvaient infiltrer les systèmes connectés plus rapidement en entrant dans les systèmes cloud.

Cisco a constaté, depuis la fin de l'année 2016, une augmentation du nombre d'attaques visant les systèmes cloud, des attaques présentant des degrés de sophistication divers.

En janvier 2017, nos chercheurs ont repéré des hackers qui cherchaient des identités d'entreprise valides à exploiter. Par le biais d'attaques frontales, les hackers créaient une bibliothèque d'identifiants vérifiés (noms d'utilisateur et mots de passe), des identifiants permettant l'accès aux systèmes d'une entreprise,utilisant potentiellement des listes connues de comptes compromis issues d'Internet. Ils essayaient de se connecter à plusieurs solutions cloud d'entreprise au moyen de serveurs utilisant 20 IP très suspectes.

À l'aide d'analyses des comportements et d'autres outils, nos chercheurs ont analysé des milliers d'environnements cloud d'entreprise de clients entre décembre 2016 et mi-février 2017. Nous avons identifié des modèles similaires d'activités suspectes de tentative de connexion ciblant plus de 17 % des entreprises de notre étude. Les hackers alternaient de façon aléatoire entre les 20 IP pour éviter d'être détectés.

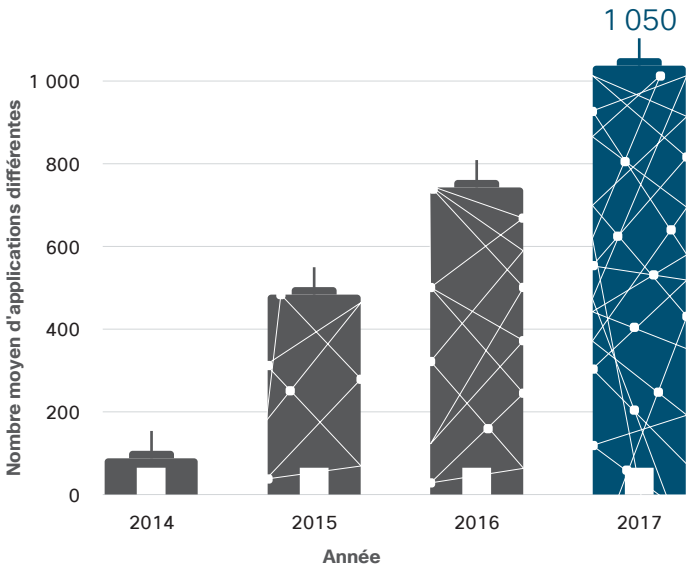
Nous avons alerté les clients et inscrit les IP suspectes sur une liste noire. Nous ne savons pas comment les hackers voulaient utiliser la bibliothèque d'identifiants. Il s'agissait peut-être d'une des étapes dans la préparation d'une campagne d'attaques par hameçonnage ciblé ou par ingénierie sociale. Les hackers souhaitaient peut-être aussi vendre les combinaisons valides de noms d'utilisateur et de mots de passe, ou utiliser eux-mêmes ces identifiants pour aller sur les comptes des utilisateurs et en extraire des données sensibles ou infecter d'autres collaborateurs. Ce que nous savons, c'est que la plupart des identifiants que les hackers essayaient d'utiliser pour accéder aux systèmes cloud d'entreprise étaient liés à des comptes professionnels qui avaient déjà fait l'objet d'une attaque.

OAuth renforce le cloud, mais crée aussi un risque

Dans le *rapport annuel 2017 de Cisco sur la cybersécurité*, nous avons examiné le risque lié à l'introduction dans l'entreprise d'applications cloud tierces par les employés. Ces applications ont un certain niveau d'accès à l'infrastructure et peuvent communiquer librement avec les plates-formes cloud et SaaS professionnelles une fois que l'utilisateur les y autorise via OAuth (Open Authorization).

Comme le montre la Figure 52, le nombre d'applications cloud connectées uniques par entreprise a augmenté de manière spectaculaire depuis 2014, d'après notre étude. Aujourd'hui, une entreprise moyenne possède plus de 1 000 applications uniques dans son environnement et plus de 20 000 installations différentes de ces applications.

Figure 52 Nombre d'applications cloud connectées uniques par entreprise



Source : Cisco Security Research

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

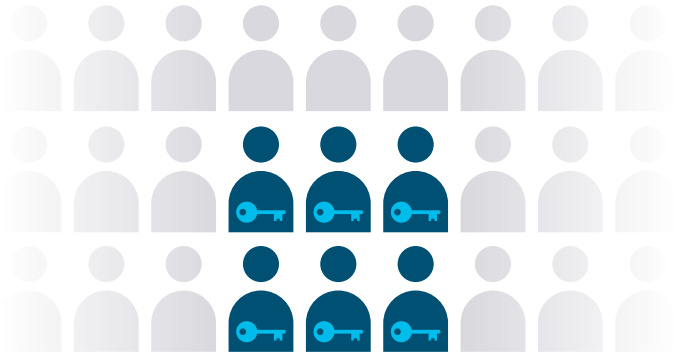
La dernière campagne d'attaques par hameçonnage qui a visé les utilisateurs de Gmail et tenté de tromper l'infrastructure OAuth souligne le risque que représente l'autorisation ouverte pour la sécurité.[43] Les hackers ont cherché à prendre le contrôle des comptes de messagerie des utilisateurs et à propager un ver informatique dans le compte de leurs contacts. Google a fait savoir qu'environ 0,1 % de son milliard d'utilisateurs avait été touché par cette attaque.[44] Les chercheurs en menaces de Cisco estiment qu'au moins 300 000 entreprises ont été infectées par le ver.[45]

Le cloud n'est pas assez surveillé : l'utilisateur doté de privilèges présente un risque fort

Certaines des failles les plus graves ont commencé par la compromission et l'utilisation frauduleuse d'un compte d'utilisateur doté de privilèges. En obtenant l'accès à un compte privilégié, les hackers disposent des « clés virtuelles de la maison » et peuvent procéder à des vols généralisés ou provoquer des dommages considérables. Pourtant, la plupart des entreprises ne sont pas suffisamment attentives à cette menace.

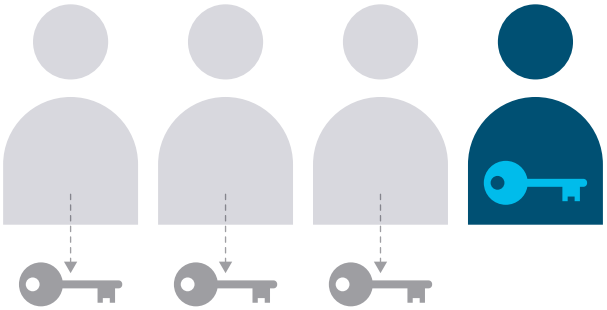
Afin de mieux évaluer l'ampleur de ce problème de sécurité, les chercheurs en menaces de Cisco ont examiné 4 410 comptes d'utilisateurs dotés de privilèges dans 495 entreprises. Ils ont établi que 6 % des utilisateurs de plate-forme cloud disposaient d'un compte doté de privilèges. Cependant, dans la plupart des entreprises, seuls deux utilisateurs dotés de privilèges en moyenne réalisent la plupart des tâches administratives (88 %). Nous avons déterminé également que les entreprises pouvaient retirer les privilèges de « super administrateur » de 75 % des comptes d'administration avec un impact faible ou nul sur l'entreprise.

Figure 53 L'augmentation des comptes d'utilisateurs dotés de privilèges

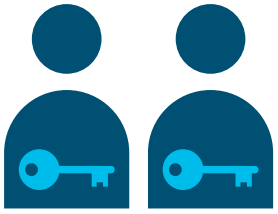


6 utilisateurs finaux sur 100

par plate-forme cloud disposent de comptes d'utilisateurs privilégiés



75 % des privilèges peuvent être retirés aux comptes d'administrateurs **sans impact significatif sur l'activité**



88 % des tâches d'administration sont effectuées par les deux utilisateurs privilégiés principaux

Source : Cisco Security Research

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

43 « Google Docs Phishing Attack Underscores OAuth Security Risks » par Michael Kan, IDG News Service, 5 mai 2017 : pcworld.com/article/3194816/security/google-docs-phishing-attack-underscores-oauth-security-risks.html.

44 « A Massive Google Docs Phish Hits 1 Million Gmail Accounts–UPDATED » par Thomas Fox-Brewster, *Forbes*, 3 mai 2017 : forbes.com/sites/thomasbrewster/2017/05/03/massive-google-gmail-phish-many-victims/#219602e142a1.

45 L'estimation de Cisco repose sur le nombre d'entreprises qui paient pour les outils cloud de productivité de Google (voir « More than 3M businesses now pay for Google's G Suite » par Frederic Lardinois, TechCrunch, 26 janvier 2017 : techcrunch.com/2017/01/26/more-than-3m-businesses-now-pay-for-googles-g-suite/) et sur le nombre de clients qui utilisent les solutions CASB (cloud access security broker) de Cisco et qui ont été touchés par l'attaque par hameçonnage ciblant les utilisateurs de Gmail (environ 10 %).

D'après notre étude, environ 82 % des utilisateurs dotés de privilèges ne se connectent que depuis une ou deux adresses IP par mois (Figure 54). Toute activité éloignée de ce schéma doit faire l'objet d'une enquête.

Nous avons établi également que 60 % des utilisateurs dotés de privilèges ne se déconnectent jamais. Pour les utilisateurs non autorisés, il est donc plus facile d'accéder au système sans se faire repérer (Figure 55). Les utilisateurs doivent se connecter quotidiennement pour accomplir les tâches administratives et se déconnecter quand leur travail est terminé.

Figure 54 Activité des utilisateurs dotés de privilèges (connexions mensuelles depuis les adresses IP)

Source : Cisco Security Research

Accepter de partager les responsabilités pour la sécurité du cloud

Les entreprises qui cherchent à étendre leur utilisation du cloud doivent comprendre qu'elles ont un rôle à jouer dans sa sécurité. Les fournisseurs de services cloud sont responsables de la sécurité physique, juridique, opérationnelle et infrastructurelle des technologies qu'ils vendent. Mais les entreprises ont pour charge de sécuriser l'utilisation des services cloud sous-jacents. Pour éviter l'accès non autorisé aux systèmes cloud, les entreprises peuvent appliquer les bonnes pratiques qu'elles utilisent déjà pour assurer la sécurité de leurs environnements sur site.

Figure 55 60 % des utilisateurs dotés de privilèges ne se déconnectent jamais

Source : Cisco Security Research

Les infrastructures et les terminaux non gérés sont un risque pour l'entreprise

Les réseaux dynamiques actuels étendent la surface d'exposition aux attaques en introduisant de nouvelles failles et de nouveaux risques pour la sécurité, et en diminuant la visibilité. Le cloud est en grande partie responsable de ce problème, tout comme les appareils et applications non autorisés (Shadow IT). Les réseaux et les terminaux qui ne sont plus pris en compte par les solutions de gestion peuvent également créer des failles inconnues et non gérées.

Nombreuses sont les entreprises qui sous-estiment les risques liés aux angles morts (souvent nombreux) de leur infrastructure réseau, de terminaux et cloud d'entreprise. Selon une étude de Lumeta, un partenaire de Cisco spécialiste des technologies de visibilité du réseau, 20 à 40 % de l'infrastructure de réseau et des terminaux de l'entreprise peuvent être inconnus ou non gérés. Ce problème touche des entreprises de nombreux secteurs – secteur public, santé, services financiers et technologies notamment.

L'infrastructure réseau et les terminaux non gérés peuvent facilement être compromis par des hackers cherchant un point d'ancrage pour infiltrer une entreprise et attaquer des cibles spécifiques. Ils peuvent également être utilisés pour extraire des données ou envoyer du trafic Tor non autorisé, ou peuvent servir à un botnet. Il suffit d'une mauvaise configuration de routeur, de pare-feu réseau ou de segmentation pour fournir aux hackers une occasion d'entrer dans l'infrastructure et d'accéder à des données sensibles.

Pour gagner en visibilité, les entreprises doivent pouvoir accéder en temps réel à des informations sur la sécurité reposant sur le contexte. En l'absence de solutions qui permettent la surveillance en temps réel et la détection des fuites, les hackers peuvent facilement infiltrer un réseau sans être détectés et contrôlés. Par ailleurs, les entreprises doivent revoir leurs politiques de segmentation et utiliser des outils robustes qui testent leur efficacité.

Elles doivent aussi tenir un inventaire des appareils et des systèmes qui se connectent au réseau. Si les équipes de sécurité disposent seulement de vues instantanées ou de listes anciennes des appareils gérés pour référence, elles risquent d'ignorer la présence d'au moins 20 % des éléments effectivement connectés au réseau. Ces inventaires doivent être réguliers et automatiques, car l'infrastructure réseau, de terminaux et cloud d'entreprise change constamment et ne peut pas être surveillée efficacement par le personnel de sécurité à lui seul.

Challenges et opportunités pour les professionnels de la sécurité

Challenges et opportunités pour les professionnels de la sécurité

Dans cette section et au travers de courtes études de cas, nous explorons les conclusions de la dernière enquête de Cisco sur l'efficacité des mesures de sécurité. Nous présentons également les données qui suggèrent que les entreprises peuvent améliorer leur sécurité en réduisant le nombre de prestataires avec lesquels elles travaillent, et traitons de l'impact de la taille de l'entreprise sur sa sécurité. Pour finir, nous étudions l'opportunité pour les responsables de la sécurité d'inviter leurs dirigeants à parler de cybersécurité et de « prendre les commandes ».

Enquête sur l'efficacité des mesures de sécurité : les secteurs d'activité à la loupe

En utilisant les données de l'étude 2017, nous avons examiné plusieurs secteurs d'activité.[46] Les conclusions sont associées à des informations sur des problématiques telles que la protection des données des consommateurs, la prise en compte des contraintes réglementaires et l'intégration de systèmes nouvellement connectés avec des logiciels anciens.

Bien que chaque secteur soit confronté à des problèmes de sécurité spécifiques, et bien que la maturité des systèmes de sécurité varie selon les secteurs, certaines préoccupations sont récurrentes. Les professionnels de la sécurité de tous les secteurs sont conscients de la sophistication croissante des menaces et de la nécessité de garder un temps d'avance sur les hackers. Beaucoup d'entreprises ont été victimes d'une faille de sécurité rendue publiques. Leur priorité est donc de limiter les dommages (comme la perte de clients) et d'éviter les failles similaires.

Dans de nombreux secteurs, il est essentiel d'intégrer les technologies de l'information (IT) et les technologies opérationnelles (OT), et surtout de s'assurer que les systèmes intégrés sont protégés. WannaCry, la récente attaque par ransomware, a causé des arrêts dans les usines de production automobile Renault-Nissan. C'est un aperçu de ce que peut être l'impact d'une attaque sur des systèmes connectés. Si la connectivité n'est pas mise en place de manière sécurisée et coordonnée, même un ransomware non ciblé peut parvenir à affecter les systèmes OT.[47]

Dans le passé, ces technologies et les équipes responsables étaient séparées : l'équipe OT s'occupait des machines et des usines, tandis que l'équipe IT s'employait à la gestion des applications professionnelles. Aujourd'hui, la plupart des capteurs et des systèmes OT sont accessibles côté entreprise. Par exemple, les systèmes d'exécution de la fabrication (MES) récupèrent maintenant les flux de télémétrie de ces capteurs pour améliorer l'optimisation et la prévision des opérations.

Les systèmes connectés s'invitant dans l'environnement OT, les technologies de l'information et les technologies opérationnelles ne peuvent plus être séparées. Les équipes OT et IT peuvent tirer parti du partage des données en effectuant des analyses qui permettent d'améliorer la sécurité et la qualité des produits. Elles peuvent aussi collaborer pour gérer la cybersécurité. Mais pour ce faire, elles doivent développer leurs capacités de protection en profondeur, car les systèmes déconnectés et en silos ne fournissent pas une vue complète des technologies IT et OT.

Pour en savoir plus sur la convergence de l'IT et des technologies opérationnelles, consultez le livre blanc de Cisco, IT/OT Convergence: Moving Digital Manufacturing Forward (Convergence de l'IT et de l'OT dans le secteur industriel : progresser sur la voie de la transformation numérique)

46 *Rapport annuel Cisco 2017 sur la cybersécurité*, p. 49 : b2me.cisco.com/en-us-annual-cybersecurity-report-2017?keycode1=001464153.
47 « Renault-Nissan Is Resuming Production After a Global Cyberattack Caused Stoppages at 5 Plants » par Laurence Frost et Naomi Tajitsu, BusinessInsider.com, 15 mai 2017 : businessinsider.com/renault-nissan-production-halt-wannacry-ransomeware-attack-2017-5.

La taille de l'entreprise influence son approche de la sécurité

Quand des hackers pénètrent dans des réseaux et volent des informations, les petites et moyennes entreprises (PME) gèrent moins facilement les conséquences que les entreprises plus grandes. Lorsque la divulgation d'une faille endommage l'image de l'entreprise et pousse les clients à se diriger vers la concurrence, une plus grande entreprise peut mieux résister qu'une petite. Étant donné le fort risque de perturbation, les PME peuvent renforcer leur position en s'assurant qu'elles disposent des procédures et des outils de sécurité nécessaires pour réduire l'impact des menaces et des failles.

L'examen de notre enquête sur l'efficacité des mesures de sécurité de 2017 indique que les PME (comptant entre 250 et 499 employés) présentent des carences dans leurs systèmes de défense comparés aux entreprises plus grandes. Naturellement, les PME disposent de moyens moindres et d'une expertise limitée pour sécuriser leurs services, et certaines menaces ou fonctions présentent des risques forts. à la question relative aux domaines présentant de gros risques pour leurs services, 29 % des PME parlent de ransomwares, contre 21 % pour les entreprises comptant plus de 10 000 employés ; 30 % des PME considèrent que les contraintes réglementaires représentent un risque élevé, contre 20 % pour les entreprises de plus grande taille (voir Figure 56).

Figure 56 Perception des risques selon la taille de l'entreprise

Risque : parmi les éléments suivants, quels sont ceux que vous considérez comme des facteurs de risque ÉLEVÉS pour votre entreprise ?	**Pourcentages** Taille de l'entreprise 250-499	500-999	1 000-9 999	Plus de 10 000
Essor du BYOD et multiplication des appareils intelligents	29	28	29	25
Viabilité des plans de reprise après incident et de continuité de l'activité	28	25	26	21
Contraintes liées au respect des réglementations	30	25	24	20
Menaces persistantes avancées	34	33	34	30
Ransomwares	29	25	25	21

Source : Enquête Cisco 2017 sur l'efficacité des mesures de sécurité

Parce que leurs budgets et leur expertise sont plus faibles, les PME sont moins enclines à mettre en place les systèmes de sécurité les plus essentiels. Par exemple, seulement 34 % des PME déclarent avoir sécurisé leur messagerie électronique, contre 45 % pour les grandes entreprises (voir Figure 57) ; 40 % des PME ont recours à un système de prévention des pertes de données, contre 52 % pour les grandes entreprises.

Figure 57 Probabilité de mettre en place les principaux systèmes de défense selon la taille de l'entreprise

Complexité : parmi les mesures suivantes, quelles sont celles que votre entreprise utilise actuellement ?	**Pourcentages** Taille de l'entreprise 250-499	500-999	1 000-9 999	Plus de 10 000
Prévention des pertes de données	40	43	47	52
Protection contre les attaques par déni de service (DDoS)	33	35	42	39
Sécurisation de la messagerie	34	41	45	45
Cryptage/confidentialité/protection des données	39	38	49	52
Protection des terminaux/Antivirus, antimalware	36	37	45	45
Application de correctifs et configuration	26	28	32	35
Sécurité du web	37	39	44	45
Réseau sans fil sécurisé	32	35	40	42

Source : Enquête Cisco 2017 sur l'efficacité des mesures de sécurité

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

Les entreprises plus grandes sont également plus susceptibles d'avoir instauré des stratégies formelles et écrites que les PME (66 % contre 59 %), et plus susceptibles d'exiger de leurs fournisseurs qu'ils aient la certification ISO 27018 (36 % contre 30 %).

Les PME cherchant à améliorer leur situation sur le plan de la sécurité pourraient se concentrer sur l'amélioration des politiques et des procédures, et sur l'adoption plus large de systèmes de défense contre les menaces communes pour réduire le risque d'avoir à gérer une attaque. Travailler avec des services de sécurité externes peut permettre de bénéficier de l'expertise nécessaire pour mettre en œuvre une stratégie de sécurité formelle et efficace afin de développer de bonnes pratiques ; parallèlement, le personnel acquiert une meilleure expertise pour ce qui est de la surveillance et de la gestion des incidents.

Pour pouvoir adopter une infrastructure de sécurité compatible avec les besoins de l'entreprise et ses budgets, les équipes de sécurité doivent travailler avec des fournisseurs qui leur offrent des solutions intégrées pour simplifier l'environnement de sécurité et l'amener à un niveau gérable mais efficace. De la même façon, les entreprises qui se développent peuvent suivre des standards, tels que ceux contenus dans le « Cybersecurity Framework » de la NIST, pour construire leur infrastructure de sécurité. Pour toutes les entreprises, une approche de la sécurité plus globale offre une protection plus efficace contre des menaces qui évoluent.

Utiliser des services pour compenser le manque de personnel qualifié

Au sein des équipes de sécurité, se poursuit le débat sur la meilleure approche à adopter : appliquer des solutions ciblées ou déployer une architecture intégrée. Mais les équipes de sécurité sont confrontées à une autre problématique qui affecte toutes les décisions à prendre : le manque d'expertise en interne. Les menaces continuant d'évoluer et les options technologiques de proliférer, les entreprises sont contraintes de se fier aux services de sécurité pour pallier le manque de compétences.

Les équipes de sécurité continuent d'avoir du mal à trouver et à garder les personnels qualifiés : notre enquête sur l'efficacité des mesures de sécurité établit que, dans de nombreux secteurs, la pénurie de personnel compétent constitue un obstacle majeur à l'adoption des processus et technologies de sécurité avancée. De fait, le manque de personnel compétent est un problème global. Ici encore, les services externes peuvent aider.

Selon les spécialistes de Cisco, la connaissance de la sécurité fait souvent défaut dans les stratégies de protection mises en œuvre. L'expertise des professionnels de la sécurité les plus aguerris permet de bénéficier d'une analyse que les produits ne sont pas toujours en mesure de fournir, y compris les meilleures solutions automatisées.

La désensibilisation aux alertes est un problème récurrent des équipes de sécurité. Comme évoqué dans les articles sectorisés de notre enquête 2017 sur l'efficacité des mesures de sécurité, les professionnels de la sécurité reçoivent quotidiennement bien plus d'alertes qu'ils n'en peuvent examiner, et d'importantes menaces peuvent passer à travers les mailles du filet. Les alertes de faible priorité peuvent être automatisées quand elles sont très nombreuses. Pourtant, peu d'entreprises utilisent cette fonctionnalité, sans doute en raison d'un manque de ressources ou d'une absence de compétences. En automatisant le traitement des alertes de faible priorité, les entreprises peuvent se concentrer sur les alertes de priorité supérieure susceptibles d'avoir des répercussions importantes sur le reste de leur environnement.

Les causes d'indifférence aux alertes sont multiples. Les systèmes en silos créent parfois des doublons d'alertes, ou bien les équipes n'ont pas les connaissances nécessaires pour distinguer les alertes de priorité faible des alertes de priorité élevée, ou des faux positifs. Elles ne disposent pas toujours des outils d'audit, par exemple, pour identifier la source de menaces potentielles. Dans ce cas, l'appel à des équipes de services externes permet de pallier cette « désensibilisation » et de bénéficier de conseils sur les menaces à gérer.

Le manque de connaissance du produit peut aussi empêcher les équipes de sécurité de tirer le meilleur parti de leurs achats de solutions. Les produits sont souvent installés par des spécialistes du produit, pas par des spécialistes de la sécurité. Les équipes de sécurité ne savent pas toujours comment intégrer les produits pour avoir une vue globale des menaces, pourtant nécessaire pour véritablement connaître l'efficacité des systèmes de sécurité. Des équipes expérimentées en gestion de la sécurité peuvent aussi aider les professionnels de la sécurité à gérer des solutions cloud et à comprendre comment leurs données sont protégées (ou non). Les fournisseurs de cloud n'utilisent peut-être pas des systèmes de protection tels que l'authentification à deux facteurs ; les experts peuvent aider les entreprises à étudier les attentes en matière de service (ou SLA) et les contrats pour déterminer les systèmes de défense que les fournisseurs de cloud utilisent.

Services externalisés et données relatives aux alertes par pays

L'étude du recours à l'externalisation des services par pays nous montre que les PME de certains pays sont plus susceptibles d'utiliser des services externalisés que les grandes entreprises. En Australie par exemple, 65 % des PME ont externalisé les services de gestion des incidents, contre 41 % des grandes entreprises. Au japon, 54 % des PME ont externalisé les services de surveillance, contre 41 % des grandes entreprises (voir Figure 58).

L'examen, par région et par taille d'entreprise, des alertes ayant fait l'objet d'une investigation et d'une procédure de remédiation, montre les pourcentages les plus élevés pour les PME en Inde, au Brésil et aux États-Unis. En ce qui concerne les alertes ayant occasionné une procédure de remédiation, les PME de Chine, de Russie et de Grande-Bretagne enregistrent les plus forts pourcentages (voir Figure 59).

Figure 58 Pourcentage de PME et de grandes entreprises externalisant les services de sécurité, par pays

En termes de sécurité, quels sont les services sous-traités entièrement ou partiellement à des tiers ?	US		BR		DE		IT		GB		AU		CN	
Conseil	49	47	40	44	41	47	45	44	43	51	63	52	50	57
Audit	51	48	48	56	45	49	40	44	49	48	39	30	28	44
Gestion des incidents	43	46	43	32	45	41	61	42	45	40	65	41	32	42
Surveillance	54	44	44	38	38	41	50	39	46	41	47	36	33	35
Remédiation	34	34	26	21	45	42	32	23	30	34	38	28	46	47
Threat intelligence	43	40	33	37	38	40	44	36	29	42	54	34	28	42
Aucun de ces services n'est sous-traité	14	15	7	13	6	15	2	10	11	20	5	14	20	12
	IN		JP		MX		RU		FR		CA			
Conseil	56	62	60	59	58	63	46	50	52	51	48	50		
Audit	43	50	35	25	57	64	37	43	44	56	44	50		
Gestion des incidents	53	55	69	55	39	41	37	35	54	42	49	45		
Surveillance	42	51	54	41	44	46	34	44	51	57	49	50		
Remédiation	44	43	40	28	12	24	31	50	34	35	36	45		
Threat intelligence	50	60	41	31	36	38	39	39	43	45	45	42		
Aucun de ces services n'est sous-traité	6	5	1	6	5	5	6	7	2	5	10	11		

Taille de l'entreprise PME (299 à 500 employés) Grandes entreprises (1,000 employés ou plus)

Figure 59 Moyennes d'alertes par pays

	US		BR		DE		IT		GB		AU		CN	
En moyenne, quel pourcentage du nombre total d'alertes fait l'objet d'un examen ?	59,7	62,8	61	65,5	44,4	52	45,8	61,3	47,4	44,2	55,6	60,8	44,8	42,5
Quel pourcentage de ces alertes examinées correspond à des incidents légitimes ?	30,6	25,7	27,1	26,2	20,2	28,2	22,8	15,2	26,3	23	27,2	28,6	30,6	44,5
Quel pourcentage de ces incidents légitimes est corrigé ?	40,9	45,3	35,4	46,3	43,7	50,4	34,8	40,9	47,3	45,6	40,6	46,2	53,5	67,9
	IN		JP		MX		RU		FR		CA			
En moyenne, quel pourcentage du nombre total d'alertes fait l'objet d'un examen ?	60,5	65,1	50,6	58,1	59,1	60,6	59,3	65,9	49,1	51,3	49,3	48,8		
Quel pourcentage de ces alertes examinées correspond à des incidents légitimes ?	37,1	39,7	25,4	33,8	27,8	20,5	23,4	33,2	21,8	25,5	22,2	23,8		
Quel pourcentage de ces incidents légitimes est corrigé ?	45,8	48,3	44,3	38,4	43,8	48,6	47,3	60,5	41,6	52,4	35,8	37,6		

Taille de l'entreprise PME (299 à 500 employés) Grandes entreprises (1 000 employés ou plus)

Source : Enquête Cisco 2017 sur l'efficacité des mesures de sécurité

Risques associés à l'IoT : se préparer pour l'avenir – et pour le présent

L'Internet des objets (IoT), comme Cisco le désigne, est l'interconnexion des appareils, des véhicules, des bâtiments et autres éléments (appelés également « appareils connectés » et « appareils intelligents ») dans lesquels ont été implantés des circuits électroniques, des logiciels, des capteurs, des actionneurs et des solutions de connectivité permettant à ces objets de recueillir et d'échanger des données. Pour Cisco, trois dimensions coexistent dans l'IoT : les technologies de l'information (IT), les technologies opérationnelles (OT) et les technologies client (CT).

L'Internet des objets industriel (IIoT), quant à lui, fait spécifiquement référence aux appareils connectés dans un réseau de contrôle industriel, par opposition à un réseau informatique ou à un data center d'entreprise.

L'IoT est porteur de promesses pour la collaboration et l'innovation dans l'entreprise. Mais à mesure qu'il se développe, les risques pour la sécurité des entreprises et des utilisateurs augmentent.

Le manque de visibilité est un problème. La plupart des entreprises ne savent pas quels objets IoT sont connectés à leur réseau. Les objets IoT, qui incluent des appareils aussi divers que des caméras, des thermostats ou des compteurs intelligents, ne sont généralement pas conçus en tenant compte de la sécurité. Nombre de ces appareils ne disposent même pas de fonctions de sécurité et présentent des vulnérabilités dont l'élimination nécessite des mois ou des années. Par ailleurs, généralement :

- Ils ont peu ou pas de fonctions CVE de communication ou de mise à jour
- Ils s'exécutent sur des architectures spécialisées
- Ils intègrent des applications non corrigées ou obsolètes vulnérables, comme Windows XP
- Ils sont rarement corrigés

Il arrive également que les propriétaires d'appareils connectés à l'IoT ne peuvent pas y accéder facilement, voire pas du tout, ce qui ne permet pas de traiter, ou alors rarement, les systèmes compromis. En bref, ces appareils peuvent servir de bases pour les hackers (voir la section traitant des attaques par ransomware d'appareils médicaux à la page 42 pour découvrir des exemples concrets).

En plus des problèmes de sécurité que posent les appareils connectés à l'IoT, les équipes de sécurité ont parfois du mal à comprendre la nature des alertes générées par ces appareils. En outre, il n'est pas toujours facile de savoir qui dans l'entreprise est chargé de traiter les attaques ciblant les appareils connectés à l'IoT. Les équipes responsables de la mise en œuvre de ces technologies quittent l'entreprise ou sont invitées à le faire une fois le projet terminé.

Les entreprises doivent se concentrer sur les faiblesses potentielles de leurs systèmes IoT, car les hackers cherchent à les cibler pour lancer des campagnes de ransomwares, voler des informations sensibles et s'infiltrer sur les réseaux. Les objets IoT sont des cibles vulnérables que les hackers peuvent exploiter rapidement.

Il faut savoir qu'une compromission massive de ces appareils peut potentiellement entraîner de graves perturbations pour les entreprises et les organismes publics, et même pour Internet. Des attaques DDoS ciblant des objets IoT se sont déjà produites, et le risque de botnets IoT (voir page 39) laisse penser que les hackers sont en train de préparer des campagnes destructrices d'ampleur inédite.

Pour faire face aux problèmes de sécurité liés à l'IoT (une surface d'exposition aux attaques qui se développe rapidement et devient de plus en plus difficile à surveiller et à gérer), les acteurs de la protection vont devoir :

- Maintenir les anciennes signatures actives
- Installer des systèmes de protection contre les intrusions (IPS) tout autour des objets IoT
- Surveiller de près le trafic sur le réseau (ceci est particulièrement important pour les environnements IIoT où les types de trafic réseau sont très prévisibles)
- Suivre les contacts des objets IoT avec le réseau et leurs interactions avec les autres appareils (par exemple, un appareil connecté à l'IoT qui en analyse un autre peut être le signe d'une activité malveillante)
- Mettre en œuvre les correctifs rapidement
- Travailler avec des fournisseurs dont la sécurité des produits est standardisée et qui publient des avis de sécurité

Dans le monde de l'IoT, une approche proactive et dynamique de la sécurité, et une stratégie de défense multidimensionnelle, sont essentielles pour protéger les objets IoT des infections et des attaques – ou pour au moins en atténuer l'impact lorsque certains sont inévitablement compromis par les hackers.

Enquête sur l'efficacité des mesures de sécurité : les secteurs d'activité à la loupe

Les opérateurs télécoms

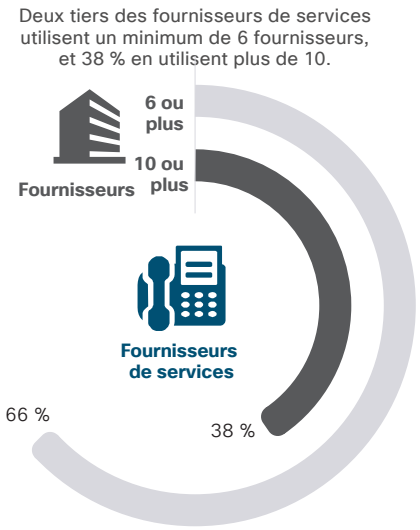
Principales problématiques

Comme le montre notre enquête, le marché des opérateurs télécoms est très varié : il inclut les télécommunications, l'infrastructure et l'hébergement cloud et web, les services multimédias et les applications fournies dans le cadre du modèle SaaS (Software-as-a-Service). En outre, les opérateurs télécoms vendent souvent des services de sécurité managés : 71 % des opérateurs interrogés déclarent offrir à leurs clients des services de sécurité managés.

Les opérateurs télécoms sont confrontés à de nombreux défis, comme la protection de leur infrastructure de production, de leur environnement IT et des données de leurs clients. 59 % des professionnels de la sécurité chez les opérateurs télécoms déclarent que leur priorité principale est de sécuriser leurs data centers et réseaux de production centraux.

Plus les activités des opérateurs télécoms sont étendues, plus ces défis sont complexes. Les professionnels de la sécurité craignent que la taille de leur entreprise, et le fait que la surface d'exposition augmente, accroissent les chances que les hackers parviennent à arrêter leur activité principale : les services aux clients. Dans un secteur où la perte de clientèle est importante, les failles de sécurité portées à la connaissance du grand public peuvent nuire aux résultats financiers de l'entreprise : 34 % des opérateurs télécoms déclarent avoir subi, au cours de l'année passée, une perte de chiffre d'affaires suite à des attaques.

Figure 60 Pourcentage d'opérateurs télécoms qui utilisent les solutions de 6 fournisseurs ou plus



La principale difficulté pour nombre d'opérateurs télécoms est de parvenir à comprendre comment intégrer les outils et procédures de sécurité pour une efficacité maximale, et de réduire la quantité de services et d'outils à leur disposition.

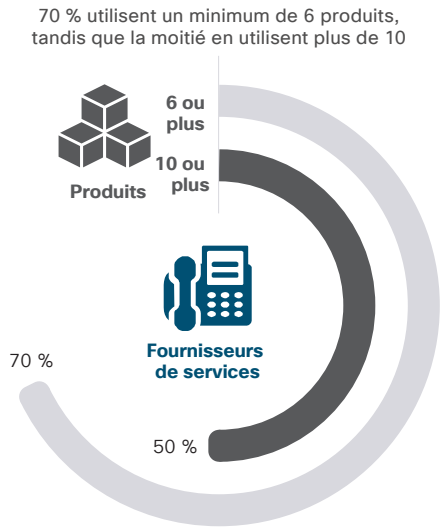
Pour les opérateurs télécoms, la réalité économique est celle-ci : à moins d'être fournie sous la forme d'un service managé, la sécurité est un centre de coût plutôt qu'un centre de profit et ne doit donc pas être source de gaspillage. Mais sous la pression de la concurrence et des menaces, ils doivent pourtant concentrer leurs efforts sur la sécurité.

La taille de l'opérateur télécom présente un véritable challenge

Comme dans tous les secteurs d'activité, la prolifération des fournisseurs et des outils de sécurité est un problème, car les solutions ne sont généralement pas intégrées et ne fournissent pas une vue exploitable des menaces auxquelles ils sont confrontés. Dans le secteur des opérateurs télécoms, l'échelle du marché amplifie le problème. Deux tiers des professionnels de la sécurité chez les opérateurs télécoms déclarent travailler avec 6 fournisseurs ou plus ; 38 % déclarent travailler avec 10 fournisseurs ou plus (Figure 60).

À propos des produits utilisés, 70 % disent utiliser au moins 6 produits de sécurité, et la moitié d'entre eux plus de 10 produits. Selon les experts Cisco de ce marché, l'intégration des produits est très réduite, ce qui expose les fournisseurs à une croissance exponentielle de la complexité chaque fois qu'ils renforcent la sécurité.

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**



Source : Enquête Cisco 2017 sur l'efficacité des mesures de sécurité

Les failles peuvent induire une perte de clientèle

Plus de la moitié (57 %) des opérateurs télécoms disent avoir eu à faire face à la méfiance du public après une violation de données. Parmi ceux ayant subi une faille rendue publique, presque la moitié disent que l'incident a conduit à améliorer les systèmes de sécurité dans une large mesure ; pour 90 %, les incidents ont conduit à des améliorations d'ampleur au moins modeste. Les professionnels de la sécurité chez les opérateurs télécoms semblent donc rapidement tirer les enseignements de leurs expériences.

34 % des opérateurs télécoms ont perdu du chiffre d'affaires suite à des attaques survenues dans les douze derniers moins ; environ 30 % ont perdu des clients ou des opportunités commerciales à cause d'attaques (voir Figure 61). Les opérateurs télécoms déclarent que leurs opérations, leur réputation et la préservation de leur clientèle ont été les éléments les plus impactés par la divulgation de failles de sécurité.

Dans un marché vaste et compétitif, les opérateurs télécoms ont beaucoup à perdre en cas de faille de sécurité. Les clients ont un grand choix d'opérateurs et en changeront rapidement s'ils pensent que leurs données ou leurs clients ne peuvent pas être protégés.

Forte adoption des standards

Les opérateurs télécoms semblent clairement devant les acteurs dans d'autres secteurs pour ce qui est de l'adoption de standards – ce qui est peut-être le résultat de leur capacité à gérer la portée et la taille de leur entreprise. Environ deux tiers ont des politiques de sécurité formellement définies et suivent des pratiques standardisées pour les politiques de sécurité de l'information. En outre, presque tous les opérateurs télécoms interrogés sont d'accord pour dire que, dans leur entreprise, les processus et les procédures de sécurité sont clairs et bien compris.

Figure 61 Pertes de chiffre d'affaires suite à des attaques

34 %

des fournisseurs de services ont déploré des pertes de revenus dues à des attaques subies au cours de l'année précédente

Environ 30 %

d'entre eux ont déclaré avoir perdu des clients ou des opportunités commerciales suite à de telles attaques

Source : Enquête Cisco 2017 sur l'efficacité des mesures de sécurité

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

Secteur public

Principales problématiques

En raison de diverses contraintes, les organismes du secteur public sont généralement plus réactifs que proactifs face aux attaques. Les budgets limités, la difficulté à attirer des talents et le manque de visibilité sur les menaces sont autant de facteurs qui affectent la capacité du secteur public à protéger les réseaux contre les hackers.

Cependant, le secteur public est également tenu de respecter des réglementations strictes en matière de cybersécurité, souvent plus exigeantes que dans le secteur privé. Par exemple, aux États-Unis, les agences fédérales doivent se conformer à la loi FISMA (Federal Information Security Management Act), qui protège la confidentialité et l'intégrité des systèmes d'information critiques. Sur le plan national et local, les exigences sont les mêmes : l'administration publique est régie par une vaste quantité de réglementations plus ou moins récentes en fonction des services fournis.

Les entreprises du secteur public ont du mal à gérer la transition vers le cloud, un processus également affecté par les réglementations. Aux États-Unis, au niveau fédéral, le programme FedRAMP (Federal Risk and Authorization Management Program) fournit des normes pour l'utilisation des produits et services cloud. Les administrations nationales et locales des États-Unis exigent également une certification pour les fournisseurs cloud hébergeant les données des organismes publics.

Gérer les données dans le cloud

La transition vers le cloud présente de nombreux avantages, mais aussi un certain nombre de difficultés pour les entreprises du secteur public qui doivent assurer une protection homogène contre les menaces. Pour un tiers des organismes du secteur public, le risque d'attaques ciblées, de menaces persistantes avancées et d'exfiltrations d'utilisateurs malveillants est élevé. En outre, les professionnels de la sécurité du secteur public déclarent que le stockage cloud public et l'infrastructure cloud sont les éléments les plus difficiles à protéger contre les attaques.

Menaces persistantes avancées

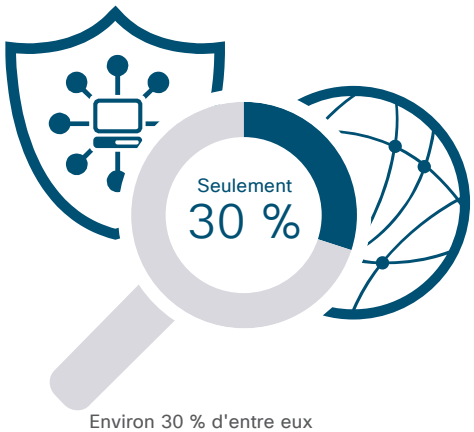
Les menaces persistantes avancées sont des attaques qui élargissent la fenêtre d'action du hacker. La menace est conçue de telle sorte que le hacker n'est pas détecté sur le réseau pendant une longue période, généralement dans le but de voler des données.

Selon les experts en sécurité du secteur public de Cisco, le problème du stockage cloud est qu'il offre différents jeux d'outils pour protéger les données, obligeant les équipes de sécurité à repenser la configuration de leurs outils et processus pour assurer la protection. Par exemple, les fonctionnalités de l'outil d'analyse NetFlow ne correspondent pas précisément aux outils d'analyse des services cloud, si bien que les processus et les résultats diffèrent.

Le manque de budget et de personnels qualifiés impacte l'analyse des menaces

Dans le secteur public, les contraintes de budget, de talent et de réglementation peuvent également mettre un frein aux objectifs de sécurité. Par exemple, les organismes mettent parfois du temps à adopter certains outils en raison d'un manque de personnel compétent pour les mettre en œuvre et analyser les résultats. Seulement 30 % des professionnels de la sécurité dans le secteur public déclarent que leur entreprise utilise des outils pour effectuer des tests d'intrusion, ou analyser les terminaux ou le réseau (voir Figure 62). Or, ces outils sont considérés comme essentiels pour une stratégie de protection en profondeur. Ne pas les adopter constitue donc un risque. Les entreprises qui ne disposent pas de ces services intégrés dans leurs systèmes de sécurité doivent s'attendre à des failles répétées sur le réseau.

Figure 62 Pourcentage des organismes du secteur public utilisant plusieurs systèmes de défense



Environ 30 % d'entre eux seulement ont recours à des tests de pénétration et à des analyses de terminaux ou de réseaux

Source : Enquête Cisco 2017 sur l'efficacité des mesures de sécurité

Les organismes du secteur public manquent d'experts en sécurité, ce qui diminue leur capacité d'examen des menaces. Près de 40 % des organismes du secteur public indiquent que 65 % seulement des milliers d'alertes quotidiennes font l'objet d'un examen. Parmi les menaces examinées, 32 % sont jugées légitimes, mais seulement 47 % sont traitées.

Le nombre de menaces non examinées prouve qu'il est nécessaire d'utiliser des outils de partage d'informations sur les alertes et d'analyse. De tels outils permettent de contextualiser et de comprendre les alertes (ce qui les rend plus utiles), et de déterminer lesquelles exigent une attention immédiate. En outre, l'automatisation facilite la résolution de certaines menaces, réduisant la charge de travail des équipes de sécurité.

Selon les experts en sécurité de Cisco, pour véritablement examiner un grand nombre d'alertes quotidiennes, un organisme du secteur public a besoin d'un effectif d'une dizaine de personnes, ce qui est rarement le cas. 35 % des entreprises du secteur public déclarent avoir moins de 30 personnes dédiées à la sécurité. En outre, 27 % d'entre eux considèrent le manque de personnel qualifié comme un obstacle majeur à l'adoption de technologies et de processus de sécurité avancés. C'est un autre argument en faveur de la nécessité d'utiliser des outils d'automatisation pour construire un système de défense capable de traiter la quantité d'alertes générées quotidiennement.

Les attaques conduisent à des améliorations sur le plan de la sécurité

Le manque de personnel et d'outils de sécurité testés dans le secteur public a un impact sur les attaques. 53 % des entreprises du secteur public ont été confrontés à la méfiance du public suite à des violations de données. Il faut pourtant s'attendre à ce que les attaques surviennent. Les organismes ne peuvent pas compter sur le fait qu'ils auront de la chance et seront épargnés. Le problème, c'est que la stratégie de sécurité repose sur la réponse aux attaques et non pas sur une approche globale prenant en compte les risques. Réagir aux attaques demande tant d'efforts qu'il ne reste plus de ressources pour la planification à long terme.

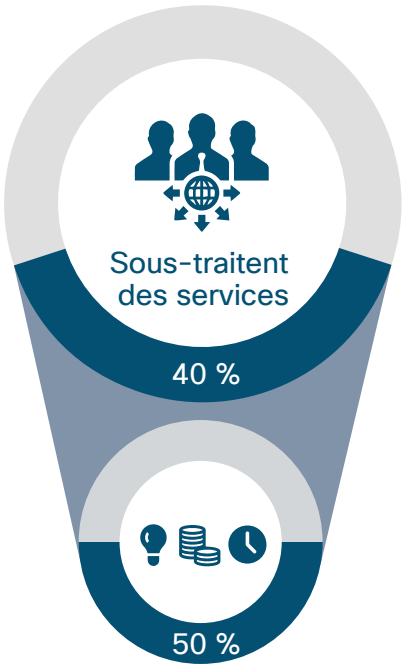
Les entreprises du secteur public indiquent clairement que les équipes de sécurité tirent les leçons des failles : 46 % déclarent que les failles de sécurité ont conduit à des améliorations dans une large mesure. Cependant, les entreprises doivent investir dans une technologie qui leur évitera d'être dépassées par ces failles, pour mieux réduire les risques et gérer plus efficacement les systèmes de défense.

L'externalisation est un plus, mais elle n'augmente pas l'expertise en interne

Pour les organismes du secteur public qui veulent accroître leurs ressources, l'externalisation est une stratégie clé. Plus de 40 % déclarent externaliser complètement ou partiellement les services tels que la surveillance ou l'audit. Parmi les entreprises qui externalisent leurs services de sécurité, à peu près la moitié d'entre elles citent comme raisons principales l'objectivité des données, la réduction des coûts et les réponses rapides aux incidents (voir Figure 62).

S'il est préférable que l'analyse des infiltrations et les autres services d'audit soient effectués par un organisme extérieur, se reposer complètement sur des services externalisés présente un inconvénient : les organismes du service public n'acquièrent pas d'expertise en interne sur le long cours. Ces connaissances internes sont essentielles pour protéger les réseaux contre des attaques sophistiquées. Les solutions automatisées peuvent être économiques et efficaces, mais il faut maintenir un équilibre entre l'externalisation et l'expertise immédiatement disponible pour pouvoir exploiter les informations et les analyses les plus importantes.

Figure 63 L'externalisation permet de bénéficier de services utiles



Source : Enquête Cisco 2017 sur l'efficacité des mesures de sécurité

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

Commerce

Principales problématiques

Lorsqu'une faille de sécurité frappe le secteur du commerce, la nouvelle se propage rapidement. Ce type d'attaques implique que les informations financières ou personnelles des clients sont exposées, c'est pourquoi elles reçoivent beaucoup d'attention de la part des médias et obligent l'entreprise à s'adresser à ses clients. Dans le secteur du commerce, les attaques et les violations de données entachent davantage la réputation des marques que dans d'autres secteurs, comme la santé ou la distribution d'énergie. Le consommateur dispose d'un vaste choix, et s'il perçoit qu'une entreprise néglige la sécurité, il peut facilement se tourner vers une autre entreprise.

Les attaques très médiatisées, comme celles impliquant l'utilisation de malwares pour voler les numéros de carte bancaire des clients, inquiètent les professionnels de la sécurité. Cependant, relativement peu d'enseignes semblent prendre les choses au sérieux. Les grandes enseignes pensent peut-être que si elles protègent les numéros de carte bancaire derrière leurs pare-feu, les données sont en sécurité. Pourtant, la protection de leur réseau n'a que peu d'importance si elles transmettent ces données sans les chiffrer aux banques et à d'autres partenaires.

L'impression de sécurité est peut-être le signe d'un excès de confiance

Les enseignes ont une perception enjolivée de leurs systèmes de protection, une vision qui ne colle pas avec le nombre de failles dont rendent compte les médias presque tous les jours. Par exemple, 61 % des professionnels de la sécurité dans le secteur du commerce affirment que la règlementation PCI est parfaitement respectée, et 63 % affirment que les données confidentielles de leurs clients sont protégées pendant tout le temps qu'elles passent dans le système de l'entreprise.

Pour vraiment protéger les données, les enseignes doivent adopter l'utilisation de cartes de paiement à puce et à code – particulièrement aux États-Unis où l'adoption y est très lente. Les banques et organismes de cartes de paiement ne remboursent d'ailleurs les dépenses que lorsque l'achat a été effectué à partir d'un système pour cartes à puce et à code, les enseignes doivent donc adopter cette solution de paiement sous peine de se voir demander de rembourser elles-mêmes.[48]

Les attaques ciblées et l'exfiltration par des agents internes à l'entreprise sont des préoccupations majeures

Toujours concernant les inquiétudes liées à la perte de chiffre d'affaires et l'atteinte à la réputation de l'entreprise, les professionnels de la sécurité du secteur du commerce déclarent que les attaques ciblées (38 %) et l'exfiltration par des agents internes (32 %) constituent les plus gros risques pour leur entreprise (Figure 64). Ils sont en droit d'être inquiets : souvent, les attaques sont lancées de l'intérieur. Ceci veut dire qu'un système de sécurité reposant sur l'examen des indicateurs de compromission (IOC) ne suffit pas. Les entreprises ont également besoin d'outils pour étudier les indicateurs d'attaque.

Pour détecter les attaques ciblées sophistiquées, telles que les menaces persistantes avancées ou les attaques par hameçonnage, les enseignes doivent distinguer le trafic anormal du trafic normal, qui peut varier d'un jour, d'une semaine, d'une saison à l'autre.

Figure 64 Les attaques ciblées et l'exfiltration par des agents internes à l'entreprise sont des préoccupations majeures

Source : Enquête Cisco 2017 sur l'efficacité des mesures de sécurité

48 « New Credit Card Chips Shift Liability to Retailers »" par Andrew Cohn, *Insurance Journal*, 7 décembre 2015 : insurancejournal.com/news/national/2015/12/07/391102.htm.

Pallier le manque de personnel

Les enseignes ont du mal à construire leur système de sécurité, à la fois en matière de personnel et d'outils. Pour 24 % des professionnels de la sécurité dans le secteur du commerce, le manque de personnel est un obstacle majeur à l'adoption de procédures et de technologies de sécurité avancée. De plus, les enseignes font constamment face à des volumes d'alertes qu'elles ne peuvent pas traiter complètement : 45 % reçoivent plusieurs milliers d'alertes chaque jour, mais seulement 53 % de ces alertes sont examinées. 27 % des alertes sont jugées légitimes et seulement 45 % d'entre elles sont traitées.

Quand le manque de personnel est un problème, il devient important de déployer des solutions de sécurité automatisées. L'automatisation peut pallier le manque de personnel – par exemple, certaines solutions permettent la segmentation automatique d'un appareil infecté dans un espace de mise en quarantaine. De cette façon, l'infection ne se propage pas et l'appareil n'a plus accès aux informations confidentielles.

L'automatisation peut également éliminer le problème induit par les environnements distribués, une difficulté propre au secteur du commerce – en réduisant le nombre d'alertes que le personnel doit traiter, par exemple. Les sites physiques (et donc les données) étant géographiquement disséminés, les responsables de la sécurité doivent supposer (ou espérer) que chaque site applique les bonnes pratiques utilisées au siège de l'entreprise. Sans une communication constante avec les sites distants, les magasins peuvent utiliser des solutions de sécurité qui n'ont pas été corrigées ou qui sont dépassées depuis des années.

Les enseignes externalisent peut-être pour pallier le manque de personnel, au moins en partie. Presque la moitié des professionnels de la sécurité dans le secteur du commerce déclarent externaliser au moins partiellement les services de conseil : 45 % externalisent les audits dans une certaine mesure. Parmi les enseignes ayant recours à l'externalisation, environ la moitié donnent comme motifs principaux, l'optimisation des coûts, l'utilisation d'informations objectives et le traitement rapide des incidents.

Le chiffre d'affaires et la réputation de l'entreprise pâtissent de la divulgation des failles de sécurité

Les enseignes savent que les failles de sécurité ont un impact concret sur leur activité. Les professionnels de la sécurité dans ce secteur déclarent que c'est sur le plan des opérations, des finances et de la réputation de leur entreprise que les failles de sécurité ont eu l'impact le plus négatif au cours de l'année passée. 54 % ont été confrontés à la méfiance du public suite à des violations de données. En outre, 32 % ont perdu du chiffre d'affaires suite à des attaques au cours de l'année passée (voir Figure 65). Près d'un quart a perdu des clients ou des opportunités commerciales suite à des attaques.

Les failles de sécurité pousseront peut-être les enseignes à changer leur stratégie de sécurité. Alors que seulement 29 % déclarent que les failles rendues publiques sont « en grande partie » à l'origine d'améliorations, près de 90 % pensent qu'elles ont donné lieu à des améliorations au moins « modestes ».

Figure 65 Pourcentage d'entreprises qui ont dû gérer les conséquences d'une violation de données

54 %
ont dû gérer la méfiance du public suite à des failles de données

32 %
ont subi des pertes de revenus suite à des attaques subies au cours de l'année dernière

25 %
ont déclaré avoir perdu des clients ou des opportunités commerciales suite à de telles attaques

Source : Enquête Cisco 2017 sur l'efficacité des mesures de sécurité

Industrie

Principales problématiques

80 % des usines aux États-Unis ont plus de 20 ans et ne disposent peut-être pas de systèmes de défense à jour.[49] Contrairement aux systèmes de bureau, les machines sont souvent déployées progressivement, de sorte que les vulnérabilités connues restent parfois inactives pendant plusieurs années avant de se réveiller. Alors que les industriels connectent des appareils à des machines obsolètes, les professionnels de la sécurité sont inquiets de l'exploitation que peuvent en faire les hackers.

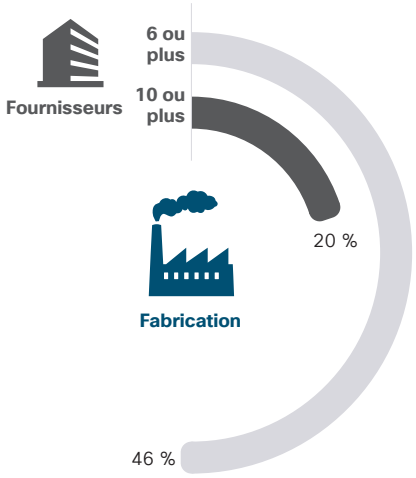
Les systèmes vulnérables peuvent occasionner l'arrêt de la production, ce qui inquiète fortement les équipes en charge de l'automatisation. Les industriels veulent à tout prix éviter les arrêts de production non programmés ainsi que les problèmes de qualité des produits, qui peuvent être occasionnés par des machines compromises ne fonctionnant pas correctement.

Pour les professionnels de la sécurité dans l'industrie, l'objectif est de mettre à niveau les systèmes vieillissants, pour empêcher les hackers d'y accéder facilement, et d'intégrer des solutions comme les systèmes IIoT. La bonne nouvelle pour les industriels, c'est que de simples mesures permettent d'améliorer la sécurité : le processus doit être vu comme une démarche progressive, plutôt que comme une initiative visant à traiter en un coup toutes les menaces. Par exemple, une politique de sécurité formellement définie peut être un cadre favorisant les améliorations. Cependant, d'après l'enquête de Cisco, 40 % des professionnels de la sécurité dans l'industrie ne disposent pas de politiques de sécurité formellement définies ni de pratiques standardisées en matière de sécurité de l'information, telles que ISO 27001 ou IST 800-53. Respecter ce type de bonnes pratiques permet de renforcer facilement la sécurité.

La nécessité d'avoir des systèmes plus simples

Pour mettre en œuvre des systèmes de fabrication mis à jour et intégrés, les fabricants doivent résoudre le problème de complexité des solutions de sécurité. 46 % des professionnels de la sécurité dans l'industrie déclarent travailler avec 6 fournisseurs de solutions de sécurité ou plus ; 20 % déclarent travailler avec plus de 10 fournisseurs (voir Figure 66). Interrogés spécifiquement sur les produits, 63 % des professionnels de la sécurité disent utiliser 6 produits au minimum, tandis que 30 % utilisent plus de 10 produits.

Figure 66 Pourcentage d'industriels qui utilisent les solutions de 6 fournisseurs ou plus



Source : Enquête Cisco 2017 sur l'efficacité des mesures de sécurité

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

La multitude de produits et de fournisseurs suscite la confusion chez les experts en sécurité. Une telle complexité traduit le fait que les équipes IT et OT se concentrent sur les menaces – en utilisant des produits permettant de régler les problèmes du moment. Les industriels peuvent envisager de mettre en œuvre des politiques favorisant la défense en profondeur, avec notamment de simples protections pour les ressources physiques, telles que le blocage de l'accès aux ports dans les commutateurs non managés ou le recours à des commutateurs managés dans l'infrastructure réseau de l'usine.

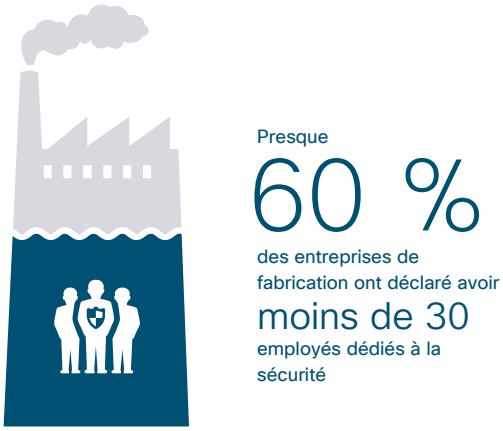
49 « America Is Aging in More Ways Than One » par Sho Chandra et Joran Yadoo, Bloomberg, 6 octobre 2016 : bloomberg.com/news/articles/2016-10-06/america-is-aging-in-more-ways-than-one.

Combiner l'expertise des équipes IT et OT

La composition des équipes de sécurité est parfois un obstacle à la protection efficace des ressources sur le site de fabrication. Lorsque le personnel spécialiste des systèmes de production propriétaires prend sa retraite et n'est pas remplacé, un manque d'expertise peut se faire sentir. Presque 60 % des entreprises industrielles déclarent avoir moins de 30 personnes dédiées à la sécurité (voir Figure 67) ; en outre, 25 % déclarent que le manque de personnel formé est un obstacle majeur sur la voie de l'adoption des procédures et des technologies de sécurité avancée.

En plus de renforcer leur pool de professionnels de la sécurité, les industriels doivent également organiser le partage de connaissance entre les services IT et OT. Traditionnellement, l'implication des équipes IT s'arrêtait au seuil de l'usine et les équipes OT prenaient le relais. Les conflits sont fréquents. Par exemple, les correctifs engagés par les équipes IT peuvent par inadvertance occasionner l'arrêt d'équipements fonctionnant dans d'anciens réseaux propriétaires et compliquer la tâche des équipes OT. Les industriels les mieux organisés s'emploient à combiner les équipes IT et OT pour favoriser la compréhension des menaces ainsi que des bonnes pratiques qui permettent de gérer les nouvelles technologies, celles liées à l'IoT et aux appareils connectés notamment.

Figure 67 Nombre de professionnels de la sécurité formés dans les entreprises industrielles



Source : Enquête Cisco 2017 sur l'efficacité des mesures de sécurité

Éviter les failles de sécurité peut améliorer la position de l'entreprise sur le marché

Étant donné la présence de systèmes vieillissants utilisés dans le secteur, les industriels sont conscients de la nécessité de les améliorer et de les mettre à niveau, non seulement pour des questions de sécurité, mais également pour stimuler leur avantage concurrentiel. Selon une étude réalisée par le Global Center for Digital Business Transformation,[50] 4 industriels sur 10 perdront des parts de marché dans les 5 prochaines années, en partie parce qu'ils ne modernisent pas leurs systèmes pour pouvoir se mesurer aux offres de concurrents plus avancés. La sécurité est essentielle pour l'avantage concurrentiel d'une entreprise, parce qu'elle contribue au maintien d'une bonne réputation, et permet d'éviter la perte de chiffre d'affaires et de clientèle.

Les résultats de l'enquête de Cisco indiquent que les failles de sécurité médiatisées peuvent impacter négativement la réputation des industriels. 40 % des entreprises industrielles ont fait face à la méfiance du public après une violation de données ; 28 % ont subi une perte de chiffre d'affaires suite à des attaques au cours de l'année passée. Cependant, ces incidents peuvent constituer une motivation à améliorer la sécurité : 95 % des professionnels de la sécurité dans l'industrie déclarent que la médiatisation de failles a conduit à des améliorations d'ampleur au moins « modeste ».

50 « Life in the Digital Vortex: The State of Digital Disruption in 2017 », Global Center for Digital Business Transformation : imd.org/dbt/digital-business-transformation.

Distribution d'eau/énergie

Principales problématiques

L'attaque des réseaux électriques ukrainiens en 2016 par des hackers russes souligne les difficultés rencontrées par les entreprises évoluant dans le domaine de la distribution d'énergie pour la protection des infrastructures stratégiques.[51] Les entreprises de distribution d'énergie n'utilisent plus de réseaux d'acquisition et de surveillance des données SCADA fermés. Les mêmes stations de travail à partir desquelles sont surveillés et contrôlés à distance la génération d'électricité, sa transmission et les équipements de distribution sont connectés simultanément aux réseaux d'entreprise et aux systèmes IT. Ces systèmes OT, qui surveillent et contrôlent les processus physiques, sont ciblés car leur vulnérabilité est connue et les dégâts matériels potentiels sont importants.

En juin 2017, les chercheurs ont découvert que l'attaque avait été réalisée avec des outils dotés d'un nouveau degré de sophistication. Les hackers ont utilisé des modules spécialisés qui ciblent directement les protocoles de contrôle. Au cours des attaques précédentes, l'utilisation à distance des outils de contrôle étaient manuelle. Avec ces nouvelles fonctions, les attaques peuvent être programmées et réalisées de manière autonome.

La connectivité étendue et la complexité généralisée des systèmes IT et OT modernes, combinées aux faiblesses sur le plan de la sécurité des logiciels et micrologiciels OT déployés, induisent l'élargissement de la surface d'attaque à protéger. Parce que les distributeurs d'énergie cherchent à numériser leurs entreprises, ils adoptent de plus en plus de nouveaux logiciels qui permettent de surveiller et d'actionner des processus physiques sans intervention humaine. Cette convergence cyberphysique – l'intégration de logiciels et de systèmes embarqués dans des appareils physiques – augmente les problématiques auxquelles sont confrontés les professionnels de la sécurité.

Ces problématiques s'étendent à la chaîne d'approvisionnement. La Federal Energy Regulatory Commission (FERC) a récemment demandé à la North American Energy Reliability Corporation (NERC) de développer de nouveaux standards pour la protection des infrastructures essentielles, et particulièrement la chaîne d'approvisionnement des distributeurs d'énergie. Les standards doivent s'articuler autour de la gestion du risque dans la chaîne d'approvisionnement pour le matériel des systèmes de contrôle industriels, les logiciels, et les services informatiques et de réseau associés aux opérations du distributeur.[52]

Les attaques ciblées et les menaces persistantes avancées sont source d'inquiétude

Les attaques arrivent en tête des inquiétudes des professionnels de la sécurité du secteur de la distribution d'eau et d'énergie. Ces derniers déclarent que les attaques ciblées (42 %) et les menaces persistantes avancées (40 %) représentent le danger le plus élevé pour leur entreprise (Figure 68). En outre, ils indiquent que les problématiques liées aux appareils mobiles, au comportement des utilisateurs, au stockage dans les clouds publics et aux données des clients occupent une place importante dans leurs stratégies de défense.

Les menaces persistantes avancées inquiètent parce qu'elles peuvent rester indétectables pendant de longues périodes dans les réseaux stratégiques de l'entreprise, augmentant ainsi l'impact des attaques. Parce que les réseaux de données convergent et que le nombre d'appareils connectés augmente, le potentiel de nuisance – comme l'arrêt du système de distribution – est plus fort qu'avant.

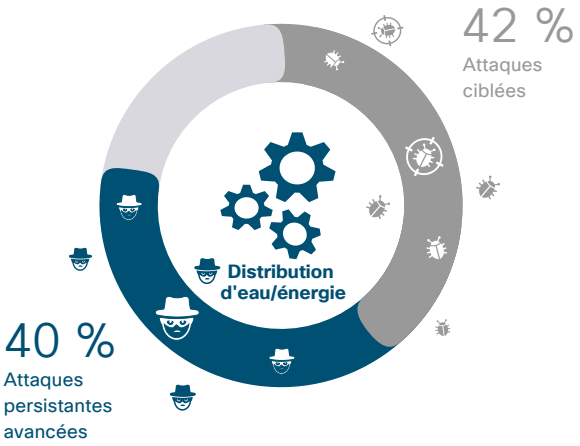
51 « Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks » par Jamie Condliffe, MIT Technology Review, 2 décembre 2016 : technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/.

52 « Revised Critical Infrastructure Protection Reliability Standards », U.S. Federal Energy Regulatory Commission : ferc.gov/whats-new/comm-meet/2016/072116/E-8.pdf.

De par leur exposition publique, les entreprises de distribution d'eau et d'énergie sont au fait des toutes dernières technologies de sécurité, mais elles ont besoin qu'on les conseille pour pouvoir correctement intégrer ces technologies de façon à se protéger efficacement contre les menaces persistantes avancées et les attaques ciblées. Elles comprennent le besoin de renforcer la sécurité. Ce qu'elles attendent des fournisseurs de solutions de sécurité, c'est de savoir « comment » : comment mettre en œuvre une approche multidimensionnelle de la sécurité de la chaîne de création de valeur, en incluant la sécurité physique et les standards de cybersécurité.

Parce que leurs réseaux sont complexes, les distributeurs d'énergie et d'eau doivent également évaluer l'impact des alertes et décider quelles alertes méritent d'être traitées. Presque la moitié des professionnels de la sécurité de ce secteur déclarent que, sur les milliers d'alertes quotidiennes qu'ils reçoivent, seulement 63 % d'entre elles sont examinées. Parmi les alertes examinées, 41 % sont jugées légitimes, dont 63 % sont traitées.

Figure 68 Les attaques ciblées et les menaces persistantes avancées suscitent le plus d'inquiétude



Source : Enquête Cisco 2017 sur l'efficacité des mesures de sécurité

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

Bien qu'une fraction des alertes légitimes soient examinées, les distributeurs d'eau et d'énergie enregistrent le taux de traitement d'alertes le plus élevé des secteurs étudiés. En outre, une alerte n'implique pas l'existence d'une menace. Les professionnels de la sécurité peuvent orienter les ressources vers les menaces qui pourraient avoir un impact grave sur la sécurité du réseau.

Le contrôle strict des budgets peut impacter le recours à l'externalisation

Parce qu'elles sont soumises à une réglementation stricte, les entreprises de la distribution d'eau et d'énergie ne disposent pas de budgets supplémentaires pour la sécurité. Une extension de budget peut nécessiter un processus d'approbation approfondi et chronophage. Selon notre étude, cela peut expliquer le recours à l'externalisation des services de sécurité. Plus de 60 % des professionnels de la sécurité de ce secteur déclarent externaliser au moins une partie des services de conseil. En outre, près de la moitié déclarent externaliser les services de surveillance et de Threat Intelligence. Plus de la moitié des professionnels de la sécurité des entreprises du secteur de l'énergie qui utilisent des prestataires de sécurité externes ont indiqué que ce qui motivait ce choix était principalement la rentabilité et l'objectivité des informations.

Parce que leur fonctionnement est soumis à un contrôle réglementaire strict, les distributeurs d'eau et d'énergie sont susceptibles de respecter des politiques de sécurité formellement définies et des procédures standardisées. Presque deux tiers des professionnels de la sécurité du secteur déclarent disposer de politiques de sécurité formellement définies et respecter des pratiques standardisées en matière de sécurité de l'information telles que ISO 27001 ou IST 800-53.

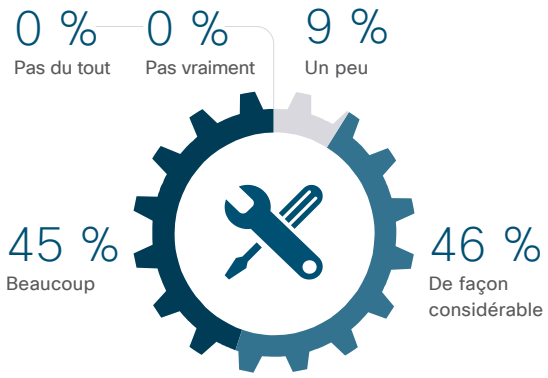
Les failles conduisent à des améliorations

Quand les entreprises de distribution d'eau/énergie subissent une faille rendue publique, cela marque fortement les esprits. Pour le public, les entreprises de distribution d'eau/énergie font partie de l'infrastructure essentielle du pays. Les populations savent que les failles mettent en péril des services clés. 61 % des distributeurs disent avoir eu à faire face à la méfiance du public après une violation de données.

La bonne nouvelle, c'est que ces failles ont peut-être provoqué des changements : 91 % des professionnels de la sécurité disent que les incidents ont conduit à des améliorations d'ampleur au moins modeste (Figure 69). Ceci peut illustrer le processus d'amélioration. Une faille peut offrir d'intéressantes informations sur le mode d'action des hackers pour pénétrer dans les réseaux et montrer aux professionnels de la sécurité la chaîne des points d'entrée au réseau – et donc où placer les contrôles de sécurité.

Les attaques peuvent avoir un impact également sur le chiffre d'affaires et la fidélité de la clientèle. 29 % des professionnels de la sécurité du secteur déclarent que leur entreprise a perdu du chiffre d'affaires suite à des attaques au cours de l'année passée ; 21 % disent avoir perdu des clients. Dans de nombreux cas, les consommateurs ne peuvent pas choisir leur distributeur d'eau/énergie parce que la région dans laquelle ils se trouvent ne compte qu'un distributeur. C'est pourquoi la perte de clientèle (et donc de chiffre d'affaires) dans ce secteur n'est pas aussi significative que dans ceux où l'environnement concurrentiel motive les décisions commerciales.

Figure 69 Pourcentage de professionnels de la sécurité qui pensent que les failles favorisent les améliorations



Source : Enquête Cisco 2017 sur l'efficacité des mesures de sécurité

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

Les simulations d'attaques sont monnaie courante

Les professionnels de la sécurité du secteur réalisent fréquemment des simulations afin de détecter les faiblesses de leur infrastructure de protection. 92 % d'entre eux affirment organiser des exercices une ou deux fois par an pour tester les plans de gestion des incidents. Lors de ces exercices, 84 % des entreprises impliquent leurs partenaires de sécurité.

De plus, 78 % exécutent des simulations d'attaques dans leur entreprise au moins une fois par trimestre. Dans un peu moins de la moitié des entreprises (45 %), les professionnels de la sécurité estiment que les simulations d'attaques ont largement contribué aux améliorations qui ont été apportées (par exemple, les modifications de politiques, de procédures et de technologies de sécurité). Le nombre élevé d'entreprises qui simulent des attaques peut révéler que les professionnels de la sécurité utilisent davantage d'outils automatisés, qui leur permettent d'accomplir des simulations plus rapidement, sans monopoliser trop de collaborateurs.

Bien que le secteur de l'eau et de l'énergie soit confronté aux problèmes de sécurité les plus complexes, il est aussi le plus avancé en termes de méthodologies et de pratiques de cybersécurité, et d'adoption de systèmes de contrôle des technologies. Les menaces ne cessent d'évoluer et les fournisseurs d'infrastructures de distribution d'eau et d'énergie doivent en faire de même afin d'identifier, de prévenir et de détecter les incidents, puis d'y répondre et de restaurer leurs systèmes.

Santé

Principales problématiques

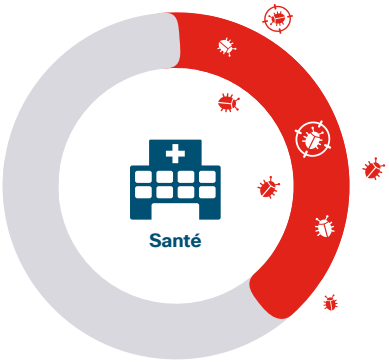
Dans le domaine de la santé, la plupart des décisions en matière de sécurité sont dictées par la protection des patients, les exigences réglementaires et la protection des ressources de l'entreprise. Les directeurs des établissements de santé craignent que, en cas d'attaque, les équipements essentiels à leur activité tombent en panne, ce qui mettrait en danger la vie des patients. Or, ils craignent également que les mesures de sécurité conçues pour surveiller le trafic en ligne et détecter les menaces ralentissent le flux de données dans les systèmes critiques et empêchent ainsi le personnel médical de poser un diagnostic approprié et de soigner les patients. En plus d'assurer des soins fondamentaux, les établissements de santé reconnaissent que leurs systèmes de sécurité ne doivent pas négliger la protection des données personnelles des patients, comme cela est imposé par exemple aux États-Unis par la loi HIPAA (Health Insurance Portability and Accountability Act).

Dans la mesure où les établissements de santé intègrent de plus en plus de connectivité dans leurs locaux et leurs dispositifs, les responsables de la sécurité s'interrogent sur la sécurité des réseaux convergés. Par le passé, les appareils médicaux complexes, comme les systèmes PACS (Picture Archiving Collection System), les pompes à perfusion et les dispositifs de surveillance des patients, étaient généralement dotés de réseaux de données gérés par les fournisseurs. Ils étaient donc physiquement isolés des autres réseaux. De nos jours, au vu de l'importante bande passante disponible, les établissements de santé estiment qu'il est plus pratique de transmettre des données sur un seul réseau. Ils font donc appel à la segmentation logique pour séparer les divers types de trafic réseau, comme les appareils cliniques et les réseaux sans fil administrateur et invité. Toutefois, si cette segmentation n'est pas réalisée convenablement, les cybercriminels ont beaucoup plus de chances d'accéder aux données essentielles ou aux appareils.

Des attaques ciblées qui inquiètent les équipes chargées de la sécurité

Les attaques par ransomware ont déjà causé de sérieux dommages dans les établissements de santé. Ces derniers représentent des cibles privilégiées pour les cybercriminels qui savent que la protection des patients passe avant tout, quel que soit le prix à payer. Une étude Cisco révèle que 37 % des établissements de santé courent des risques très élevés face aux attaques ciblées (voir Figure 70). De plus, les cyberattaques ciblées sont beaucoup plus préoccupantes que les failles qui impliquent la perte ou le vol de matériel. Elles nécessitent une approche plus précise en matière de détection et d'élimination des menaces.

Figure 70 Les attaques ciblées présentent des risques plus importants pour la sécurité

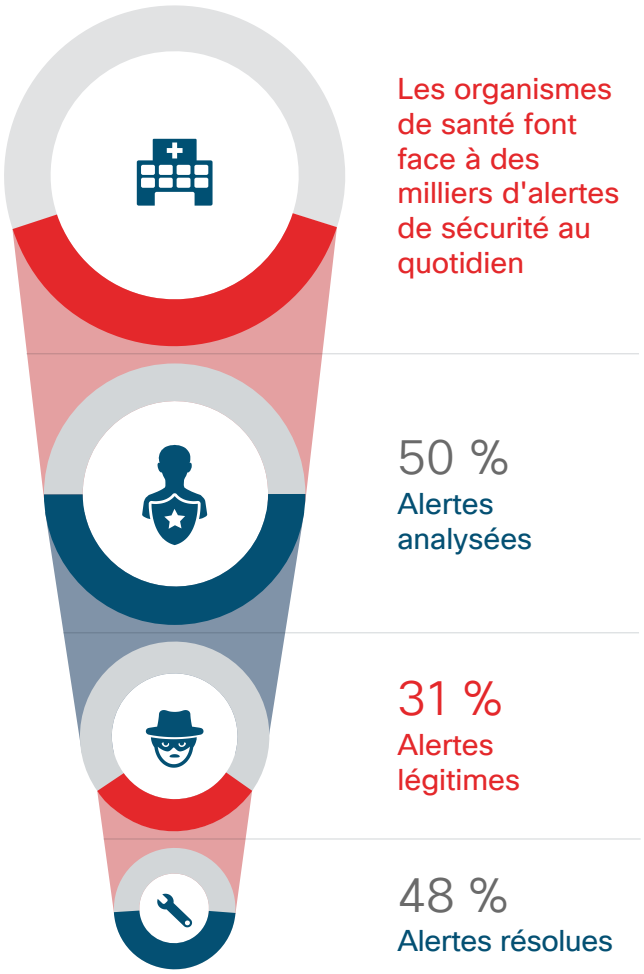


Source : Enquête Cisco 2017 sur l'efficacité des mesures de sécurité

Malheureusement, comme dans plusieurs secteurs, les menaces se multiplient, mais le temps manque et les collaborateurs ne sont pas assez nombreux pour faire des recherches. Plus de 40 % des établissements de santé déclarent recevoir des milliers d'alertes de sécurité chaque jour, mais n'examinent que 50 % d'entre elles (voir Figure 71 à la page suivante). 31 % des alertes analysées par les équipes chargées de la sécurité dans le domaine de la santé sont des menaces légitimes, mais seulement 48 % d'entre elles sont éradiquées.

Les experts de la sécurité Cisco estiment que le nombre d'alertes examinées est probablement bien inférieur à ce que pensent les responsables de la sécurité dans le domaine de la santé. Ces derniers croient aussi peut-être éradiquer les menaces simplement en les bloquant avant qu'elles ne pénètrent sur le réseau. Il n'est pas étonnant non plus que les établissements de santé ne gèrent qu'un si petit nombre d'alertes. En effet, s'ils en analysaient davantage, les activités IT et liées à la sécurité seraient énormément ralenties, ce qui aurait un impact sur leurs autres fonctions.

Figure 71 Des milliers d'alertes déclenchées, mais moins de la moitié corrigée



Source : Enquête Cisco 2017 sur l'efficacité des mesures de sécurité

Les défis à relever par l'équipe encadrante : le manque formation des collaborateurs et la complexité des solutions

La plupart des établissements de santé surmontent les défis liés à la sécurité en associant plusieurs solutions. Presque 60 % d'entre eux affirment utiliser les solutions de plus de six fournisseurs, tandis que 29 % cumulent les solutions de plus de 10 fournisseurs. En outre, deux tiers des responsables de la sécurité déclarent utiliser au moins six produits de sécurité, alors qu'ils sont 41 % à en utiliser plus de 10.

L'abondance évidente de fournisseurs et de produits choisis par les professionnels de la sécurité dans le domaine de la santé peut sans doute s'expliquer par une profonde confusion ou un manque de visibilité sur les outils mis en place. Comme l'ont montré les conclusions de l'enquête sur l'efficacité des mesures de sécurité, les responsables de la sécurité des systèmes d'information (RSSI) et les responsables des opérations de sécurité ont souvent différents points de vue sur leurs outils de sécurité. Les responsables de la sécurité en haut de l'échelle, c'est-à-dire ceux qui ne gèrent pas la sécurité au quotidien, ne savent certainement pas précisément quels outils sont installés sur leur réseau.

Il est extrêmement difficile pour les établissements de santé de répondre tous les jours aux menaces tout en gérant un ensemble complexe de solutions, car ils ne disposent pas d'un nombre suffisant de collaborateurs qualifiés pour le faire. Environ la moitié des professionnels de la sécurité déclarent que moins de 30 employés sont dédiés à la sécurité ; 21 % considèrent le manque de personnel qualifié comme un obstacle majeur à l'adoption de technologies et de processus de sécurité avancés.

Les équipes chargées de la sécurité qui comptent un nombre important de membres sont plutôt rares et ne se trouvent que dans les plus grands établissements. D'après les experts Cisco du domaine de la santé, la définition d'un collaborateur chargé de la sécurité peut varier d'une entreprise à une autre, ce qui change alors l'idée que l'on peut se faire de la taille de l'équipe chargée de la sécurité. Par exemple, un collaborateur IT peut être considéré comme un membre de cette équipe ou ne la rejoindre que temporairement.

Les bénéfices de la segmentation du trafic

Dans le secteur de la santé, l'exigence d'exceptions, qui permet à certains systèmes ou appareils d'adhérer à des protocoles de sécurité différents, amène à s'interroger sur le bien-être et la sécurité des patients. Les équipements médicaux sont onéreux et sont supposés être utilisés pendant plusieurs années. Par conséquent, leurs logiciels et leur système d'exploitation ne sont pas toujours mis à jour régulièrement, d'où la mise en place de certaines exceptions qui leur permettent de fonctionner en toute fiabilité. D'après les experts de la sécurité, la meilleure approche consiste à isoler et à segmenter le trafic entre le réseau et les appareils essentiels. Les établissements de santé peuvent aussi améliorer leur infrastructure de sécurité et leur segmentation du réseau afin de mieux faire face aux exceptions qui imposent des contrôles compensatoires.

En moyenne, les établissements de santé comptent 34 exceptions administratives de sécurité importantes en vigueur ; 47 % de ces exceptions intègrent des contrôles compensatoires. Dans l'idéal, il faudrait tout mettre en œuvre pour réduire au maximum le nombre d'exceptions qui imposent des contrôles compensatoires, parce qu'elles peuvent affaiblir les systèmes de protection.

Transports

Principales problématiques

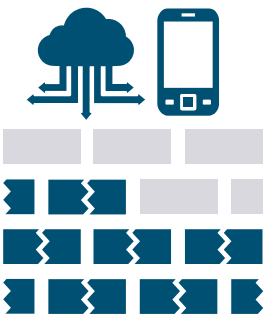
L'infrastructure technologique du secteur des transports reposait traditionnellement sur des systèmes propriétaires fermés. Or, ce secteur est en passe d'effectuer sa transition vers des réseaux connectés modernes et les responsables de la sécurité s'inquiètent de l'exposition aux attaques pendant cette période. Quoi qu'il en soit, la transition vers des systèmes IP connectés s'impose, en raison de la hausse du coût et de la complexité des systèmes existants.

De plus, l'infrastructure de communications existante n'est pas à même de répondre aux demandes des clients qui exigent de nouveaux services de mobilité et de sécurité. Par exemple, les clients veulent interagir sur les réseaux sociaux avec les aéroports, les compagnies aériennes, les entreprises de transport de fret et de voyageurs, les entreprises responsables des routes, les flottes de voitures connectées et les autorités chargées du transport ; acheter des billets via leurs appareils mobiles ou encore utiliser des applications de mobilité dans leurs véhicules. Les employés des entreprises de transport veulent également profiter de la facilité d'utilisation des systèmes connectés, et l'arrivée de la génération Y dans ces entreprises accélère cette demande.

Les menaces persistantes avancées et les appareils connectés comptent parmi les principales menaces

Les sociétés de transport créent des infrastructures connectées complexes et découvrent l'impact d'un réseau toujours plus grand, mais également les différentes menaces qui les accompagnent. Plus d'un tiers des professionnels de la sécurité des transports déclarent que les menaces persistantes avancées et la prolifération du BYOD et des appareils intelligents constituent des risques élevés pour leur entreprise. De plus, 59 % des professionnels de la sécurité affirment que les infrastructures cloud et les terminaux mobiles sont les plus difficiles à protéger contre les attaques (voir Figure 72).

Figure 72 Les infrastructures cloud et les terminaux mobiles sont les plus difficiles à protéger



59 %

des professionnels de la sécurité déclarent que les infrastructures cloud et les appareils mobiles font partie des systèmes les plus difficiles à défendre contre des attaques

Source : Enquête Cisco 2017 sur l'efficacité des mesures de sécurité

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

Afin de favoriser l'accès aux informations, les équipes chargées de la sécurité dans le domaine des transports savent que les données doivent se trouver à la périphérie du réseau et être disponibles en temps réel. Le contrôle de l'accès aux données et la haute disponibilité de ces dernières sont deux préoccupations majeures des responsables de la sécurité.

Ils savent également que ces problèmes vont s'intensifier avec la disparition des systèmes propriétaires fermés. Ils s'attendent ainsi à devoir gérer un très grand nombre de menaces toujours plus complexes. 35 % des professionnels de la sécurité des transports déclarent recevoir des milliers d'alertes quotidiennes, dont 44 % seulement font l'objet d'un examen. Parmi les alertes examinées, 19 % ont été identifiées comme des menaces légitimes, mais seulement 33 % de ces menaces légitimes ont été corrigées.

Le manque de collaborateurs qualifiés dans le domaine de la sécurité encourage l'externalisation

C'est en disposant de collaborateurs qualifiés dans le domaine de la sécurité que les sociétés de transport seront à même de relever les défis auxquels elles doivent faire face, mais celles-ci n'attirent pas forcément les bons candidats. Près de la moitié des équipes chargées de la sécurité dans le secteur des transports compte moins de 30 membres. Le manque d'expertise représente évidemment un inconvénient : 29 % des employés interrogés déclarent que l'absence de collaborateurs qualifiés est un obstacle majeur à l'adoption de procédures et de technologies de sécurité avancée.

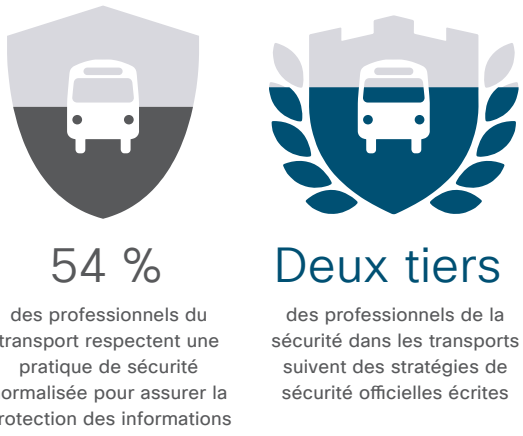
Or, les centres d'opérations de sécurité étant toujours plus sophistiqués et spécifiques, il est fort probable que les entreprises de transport attirent de moins en moins de collaborateurs compétents. Les autorités responsables des transports doivent être capables de recruter, de rémunérer et de fidéliser ces personnes indispensables pour protéger les infrastructures nationales et locales essentielles.

Les entreprises de ce secteur qui ne disposent pas de l'expertise adéquate en interne sont nombreuses à externaliser. Près de la moitié d'entre elles le fait pour une partie ou même la totalité des tâches liées à la sécurité. Parmi les entreprises qui ont opté pour l'externalisation, 52 % ont fait ce choix dans un souci premier de réduction des coûts et 44 % pour avoir accès à des informations objectives.

En se conformant aux pratiques standardisées en matière de sécurité de l'information, comme les normes ISO 27001 ou NIST 800-53, il est plus facile pour les entreprises de transport de respecter les procédures de référence établies en matière de sécurité. 54 % des professionnels de la sécurité du secteur des transports suivent une politique standardisée de sécurité de l'information et deux tiers suivent des politiques de sécurité formellement définies (voir Figure 73).

Certains signes prouvent également que les sociétés de transport savent qu'il est intéressant d'appliquer des mesures de sécurité à tous les niveaux de l'entreprise et non uniquement des solutions ponctuelles. 75 % des entreprises de transport ont mis en place un centre opérationnel dédié à la sécurité et 14 % envisagent d'en créer un. De plus, près de 90 % des professionnels de la sécurité déclarent que leur entreprise est membre d'un organisme de standardisation ou d'une organisation sectorielle pour la sécurité, comme PT-ISAC ou ST-ISAC.

Figure 73 Le pourcentage de professionnels de la sécurité du secteur des transports qui respectent des pratiques standardisées



Source : Enquête Cisco 2017 sur l'efficacité des mesures de sécurité

Les simulations d'attaques favorisent les améliorations

Le secteur des transports, comme tout autre secteur soumis à des réglementations strictes, étant jugé essentiel, son infrastructure peut donc dicter des décisions relatives à la sécurité. Par exemple, environ 80 % des professionnels de la sécurité de ce secteur simulent au moins une fois par trimestre des attaques contre leur entreprise. En outre, près de la moitié d'entre eux affirme que les résultats de ces simulations donnent lieu à des améliorations considérables en matière de politiques, de procédures et de technologies liées à la sécurité.

Les violations de données rendues publiques encouragent également le changement. 48 % des professionnels de la sécurité du secteur des transports ont été confrontés à la méfiance du public suite à une violation de données. Même si seulement 34 % d'entre eux estiment que ces failles sont à l'origine d'améliorations « majeures », 83 % pensent qu'elles ont donné lieu à des améliorations au minimum « modestes ».

Les failles ont également des conséquences durables sur le secteur, même une fois le problème résolu. 31 % des professionnels de la sécurité déclarent que, au cours de l'année passée, leur entreprise a perdu une partie de son chiffre d'affaires à cause d'attaques, la moyenne s'élevant à 9 %. De plus, 22 % signalent avoir perdu des clients et 27 % ont manqué des opportunités suite à des attaques.

Finances

Principales problématiques

Les entreprises du secteur de la finance sont des cibles très lucratives pour les cybercriminels. La multitude de données clients ainsi que l'accès aux noms d'utilisateur et aux mots de passe des comptes clients est une mine d'or pour les cybercriminels qui n'hésitent pas à lancer de nombreuses attaques contre ces entreprises. Certains créateurs de malwares conçoivent même leurs attaques précisément pour compromettre les réseaux de services financiers, comme le malware Dridex, conçu pour voler des identifiants et le cheval de Troie Zeus.[53] [54]

Dans ce contexte, les professionnels de la sécurité des services financiers savent que leurs solutions de protection doivent être efficaces contre les cybercriminels qui utilisent des malwares sophistiqués. Cependant, ils savent aussi que la complexité de leur infrastructure de sécurité, qui reposent sur de nombreux fournisseurs et produits de sécurité différents, est un obstacle à l'efficacité et favorise la dissimulation des attaques au lieu de les révéler au grand jour. Les équipes responsables de la sécurité ont également la charge d'une tâche fastidieuse : intégrer les applications existantes avec les nouvelles technologies, tout en vérifiant que leur système de sécurité reste performant.

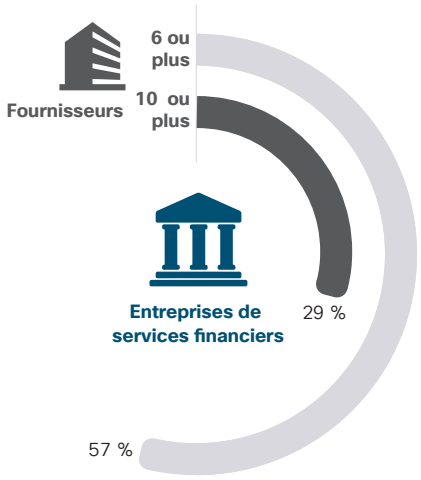
Certaines entreprises du secteur financier qui se sont associées à des entreprises spécialisées dans les technologies financières ont découvert que la surface d'exposition aux attaques risquait de s'étendre et de devenir encore plus complexe. Comment ces partenariats peuvent-ils assurer une protection appropriée des données des clients ? Comment les entreprises de services financiers peuvent-elles s'associer à des tiers tout en respectant des réglementations strictes ? Les réponses à ces questions ont un impact sur la manière dont le secteur relèvera les défis liés à la sécurité qui se poseront dans les années à venir.

En plus de devoir garantir la sécurité de leur réseau, les entreprises de services financiers doivent aussi s'assurer d'être conformes aux réglementations en vigueur. On constate d'ailleurs que, de plus en plus souvent dans divers secteurs soumis à des réglementations strictes, les entreprises pensent qu'il leur suffit de respecter les exigences réglementaires pour résoudre les problèmes liés à la sécurité. Les exigences réglementaires, comme la segmentation du réseau, contribuent, en effet, à la protection des données, mais elles ne représentent qu'une partie de la solution pour stopper les failles et analyser les menaces.

Les environnements multifournisseurs sont synonymes de confusion et non de clarté

Les entreprises de services financiers multiplient souvent les fournisseurs dans leur environnement. 57 % d'entre elles déclarent utiliser des solutions d'au moins six fournisseurs, tandis que 29 % font appel à plus de 10 fournisseurs (voir Figure 74). Deux tiers des entreprises de services financiers sont équipés d'au moins six produits de sécurité et 33 % en utilisent plus de 10.

Figure 74 Le pourcentage d'entreprises de services financiers qui utilisent les solutions d'au moins 6 fournisseurs



Source : Enquête Cisco 2017 sur l'efficacité des mesures de sécurité

D'après les experts de la sécurité Cisco, il n'est pas rare de trouver les produits de près de 30 fournisseurs dans une seule entreprise de ce secteur. Pour répondre rapidement et efficacement aux nouveaux types de menaces, ces entreprises doivent s'efforcer de simplifier leur architecture de sécurité : moins d'outils et plus d'intégration. En effet, les différents produits opèrent souvent en silos : ils sont efficaces individuellement, mais sans intégration en vue de partager et de mettre en corrélation leurs informations liées à la sécurité, les équipes dédiées passent leur temps à gérer des rapports et des alertes en conflit.

53 « Dridex Attacks Target Corporate Accounting », par Martin Nystrom, blog Cisco Security, 4 mars 2015 : blogs.cisco.com/security/dridex-attacks-target-corporate-accounting.
54 « Zeus Trojan Analysis », par Alex Kirk, blog Cisco Talos : talosintelligence.com/zeus_trojan.

La multiplication des produits empêche également les professionnels de la sécurité d'analyser les menaces. 46 % des entreprises du secteur financier déclarent recevoir des milliers d'alertes quotidiennes, dont 55 % seulement font l'objet d'un examen. 28 % des menaces examinées sont considérées comme légitimes, mais seulement 43 % des menaces légitimes sont éradiquées.

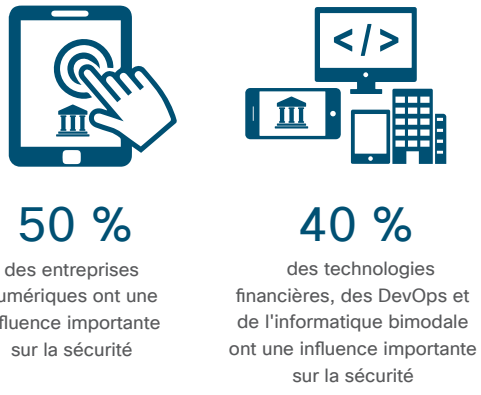
Le nombre élevé d'alertes est dû au manque d'intégration des produits de plusieurs fournisseurs. Les équipes chargées de la gestion des incidents ne parviennent pas toujours à identifier les alertes en double ou celles moins prioritaires. Sans intégration, les équipes responsables de la sécurité sont limitées en termes de mise en corrélation et d'analyse des menaces.

La transformation numérique comme moteur d'améliorations

Les entreprises de services financiers s'associent avec des entreprises spécialisées dans les technologies financières et découvrent de nouvelles méthodes pour renforcer leur sécurité, comme la formalisation des responsabilités en vue de protéger les données. Près de la moitié des entreprises du secteur financier déclarent que l'activité numérique a une très grande incidence sur la sécurité. De même, environ 40 % estiment que les entreprises spécialisées dans les technologies financières, les processus DevOps et l'IT bimodal influencent très sensiblement les mesures de sécurité (voir Figure 75).

Par exemple, une entreprise de services financiers associée à un partenaire spécialisé dans les technologies financières doit choisir la méthode à appliquer pour protéger les données de ses clients, notamment dans un environnement cloud. Les partenaires détermineront également les processus conjoints qui permettent d'éviter les incidents et, en cas d'incident, les méthodes de riposte à mettre en œuvre.

Figure 75 L'impact du numérique sur la sécurité



Source : Enquête Cisco 2017 sur l'efficacité des mesures de sécurité

Téléchargez les graphiques du rapport 2017 à l'adresse : **cisco.com/go/mcr2017graphics**

Accélérer l'adoption des standards

À l'ère du numérique, si les entreprises de services financiers veulent répondre aux demandes de leurs clients en toute sécurité, elles doivent être capables d'adopter plus rapidement de nouvelles politiques et de nouveaux processus. à ce jour, 63 % des établissements financiers ont mis en place des politiques de sécurité formelles écrites. 48 % seulement suivent une pratique normalisée de politique de sécurité des informations, comme ISO 27001 ou NIST 800-53. Les services financiers sont plutôt conservateurs, c'est pourquoi les équipes IT et celles chargées de la sécurité doivent avancer en douceur lorsqu'elles envisagent d'ajouter de nouveaux standards à une stratégie de sécurité existante.

Il serait également judicieux pour les entreprises de services financiers de demander à leurs fournisseurs de respecter des pratiques professionnelles établies. Par exemple, seules 37 % d'entre elles imposent à leurs fournisseurs de se conformer au standard ISO 27001 pour travailler avec elles.

D'après les experts de la sécurité Cisco, plus la politique de sécurité d'une entreprise est mature, plus celle-ci peut se permettre d'être exigeante avec ses fournisseurs : les grandes entreprises bien établies sont plus à même d'imposer leurs conditions aux fournisseurs que les plus petites structures.

Conclusion

Conclusion

Cisco publie des rapports annuels et semestriels sur la cybersécurité depuis près de dix ans. Le principal objectif de ces rapports est d'informer les équipes de sécurité et les entreprises des nouvelles menaces et vulnérabilités connues et émergentes, et de leur préconiser des mesures pour améliorer la sécurité et la résilience aux cyberattaques.

La diversité de contenus présentés par nos chercheurs spécialistes des menaces et nos partenaires technologiques dans ce rapport témoigne de la complexité des menaces modernes. L'étude montre également que les acteurs de la protection ont non seulement gagné du terrain sur les hackers, mais sont également parvenus à mieux comprendre comment et où les cybercriminels agissent.

Cependant, avec le développement de l'IoT, nous pensons que les acteurs de la protection auront des difficultés à maintenir leur avance. Comme indiqué dans l'introduction de ce rapport, certains signes montrent que de nouveaux types d'attaques (plus malveillantes et destructrices que les campagnes antérieures) sont en cours de développement. Les hackers mettent au point des attaques parfaitement planifiées pour un maximum d'impact, conçues pour bloquer le fonctionnement de toute entreprise, quelle que soit sa taille. Ils savent qu'aucune entreprise n'a conçu de plan d'urgence pour reconstruire ses installations IT ou OT à partir de zéro, et ils sont déterminés à utiliser cette faiblesse à leur avantage.

C'est pourquoi il n'a jamais été aussi important pour les entreprises de faire de la cybersécurité une priorité absolue. Elles doivent investir dans des outils automatisés qui permettent aux équipes de sécurité de rester constamment informées des alertes, de gagner en visibilité, de gérer leurs réseaux désormais dynamiques, et de détecter les véritables attaques pour mieux y répondre. Elles doivent aussi consacrer tout le temps et les ressources nécessaires pour s'assurer qu'elles savent toujours exactement ce qui se trouve dans leur environnement IT, et que tout y est déployé correctement et de façon sécurisée, et constamment mis à jour.

La communauté des spécialistes de la sécurité, quant à elle, doit réfléchir et discuter davantage des moyens de créer un écosystème ouvert qui permettra aux clients de mettre en œuvre des solutions de sécurité plus efficaces pour leur entreprise et d'exploiter pleinement les investissements existants. Dans cet écosystème, toutes les solutions de sécurité doivent communiquer entre elles et fonctionner conjointement pour protéger les utilisateurs et les entreprises. Les acteurs de la protection doivent tous se préparer à affronter des attaques puissantes qui cibleront les environnements IoT et infliger des dommages considérables aux entreprises qui les utilisent.

Il est temps pour les responsables de la sécurité de s'inviter à la table des dirigeants de l'entreprise

La dernière enquête Cisco sur l'efficacité des mesures de sécurité a révélé que la sécurité était une priorité pour les dirigeants de nombreuses entreprises. De même, selon les professionnels de la sécurité, leur direction met la sécurité en tête de liste des objectifs de l'entreprise. Cependant, le nombre de professionnels à l'affirmer diminue, car ils ne sont plus que 59 % en 2016, contre 61 % en 2015 et 63 % en 2014.

Toutefois, cette baisse de confiance n'est peut-être pas justifiée. Les RSSI ne sont pas toujours conscients que leur direction considère la cybersécurité comme une priorité tout en étant en attente de recommandations fortes sur ce sujet. En fait, ils veulent avoir plus d'informations de meilleure qualité.

D'après une enquête sur la gouvernance des entreprises publiques en 2016-2017 réalisée par la National Association of Corporate Directors (NACD),[55] près d'un quart des conseils d'administration n'est pas satisfait des rapports liés à la cybersécurité fournis par leur direction. Ils signalent que les informations reçues ne permettent pas de réaliser une évaluation précise, ne sont pas transparentes concernant les problèmes et sont difficiles à interpréter. Dans le même rapport, 14 % seulement des personnes ayant répondu avaient le sentiment que leur conseil d'administration comprenait globalement les problèmes de cybersécurité.

Les spécialistes de la sécurité de SAINT Corporation, fournisseur de solutions de sécurité et partenaire de Cisco, suggèrent que les RSSI ont les moyens de combler ces lacunes de connaissances. Mais pour cela, ils doivent :

- S'efforcer de fournir des informations utiles et exploitables pour l'entreprise. Les rapports sur la cybersécurité et les cybermenaces de l'entreprise ne doivent pas être trop techniques. Ils doivent faire un parallèle entre ces problèmes et les risques traditionnels auxquels l'entreprise est confrontée, et les relier aux priorités de l'entreprise et aux résultats souhaités. Il ne faut pas non plus oublier de préciser que la cybersécurité peut stimuler la croissance et représenter un atout concurrentiel pour l'entreprise.
- Lorsque vous signalez une cyberattaque à la direction et au conseil d'administration, présentez en termes clairs l'impact sur l'entreprise (par exemple, le nombre de collaborateurs ou de clients affectés, le type d'informations à haute valeur ajoutée touchées), les mesures que l'équipe chargée de la sécurité doit mettre en œuvre pour contenir et analyser la menace, et le temps nécessaire pour rétablir un fonctionnement normal.
- Solliciter l'implication d'autres responsables de l'entreprise, notamment ceux qui ne font pas partie du département technologique. En collaborant régulièrement avec les différents responsables de l'entreprise (directeur du service informatique, directeur du service technologique, directeur des audits et directeur de la gestion des risques), les RSSI peuvent améliorer la communication directe avec la direction et le conseil d'administration. Ils ont également l'opportunité de prendre une place de choix à la table des discussions pour parler de la stratégie de cybersécurité et participer au développement d'un programme de sécurité complet pour l'entreprise.

Les RSSI ont souvent des difficultés à financer durablement les initiatives de sécurité. Mais là encore, ils ne réalisent pas forcément que c'est le moment idéal pour discuter des budgets avec la direction. L'enquête 2017 sur les tendances IT de Society for Information Management (SIM) révèle que la cybersécurité est aujourd'hui le troisième poste d'investissement le plus important des entreprises.[56] En 2013, elle n'arrivait qu'au 14e rang. Les personnes interrogées dans le cadre de l'enquête SIM (responsables IT) ont également classé la cybersécurité en deuxième position des domaines IT qui méritent davantage d'investissements et en tête de la liste des technologies de l'information qu'elles estiment « personnellement les plus préoccupantes ».[57]

55 Les données, les informations et le contenu sont directement issus de l'enquête sur la gouvernance des entreprises publiques de 2016-2017 réalisée par la National Association of Corporate Directors (NACD), avec son autorisation. Vous pouvez télécharger l'enquête auprès de la NACD à cette adresse nacdonline.org/Resources/publicsurvey.cfm?ItemNumber=36843.
56 Enquête sur les tendances IT de Society for Information Management, Kappelman, L. A. et autres (2017). Vous pouvez télécharger cette enquête sur le site SIM à cette adresse simnet.org/members/group_content_view.asp?group=140286&id=442564.
57 Ibid.

À propos de Cisco

À propos de Cisco

Cisco crée des solutions de cybersécurité intelligentes qui ont une utilisation concrète. Nous proposons désormais l'une des gammes de solutions de protection avancée les plus complètes du marché couvrant un vaste éventail de vecteurs d'attaque. Notre approche axée sur les attaques et les aspects opérationnels réduit la complexité et la fragmentation, tout en vous apportant une visibilité avancée, un contrôle systématique et une protection renforcée avant, pendant et après l'attaque.

Les chercheurs de Cisco CSI, notre écosystème de sécurité adaptative collective, regroupent l'ensemble de la Threat Intelligence déduite des données télémétriques émanant des nombreux appareils et capteurs, des flux publics et privés, et de la communauté open source. Tous les jours, des milliards de requêtes web et des millions d'e-mails, d'échantillons de malwares et de données sur les intrusions dans les réseaux sont collectés.

Notre infrastructure et nos systèmes sophistiqués analysent ces données télémétriques pour permettre aux chercheurs et aux systèmes automatisés de détecter les attaques et d'en identifier les causes et l'envergure où qu'elles se produisent : réseaux, Internet, data centers, terminaux, appareils mobiles, systèmes virtuels, e-mails et cloud. L'analyse de ces données nous permet de renforcer en temps réel la sécurité des produits et des services que nos clients utilisent dans le monde entier.

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

Les participants au rapport Cisco du 1er semestre 2017 sur la cybersécurité

Cisco Cloudlock

Cisco CloudLock propose des solutions de courtage de services de sécurité pour l'accès au cloud (CASB), qui permettent aux entreprises d'utiliser le cloud en toute sécurité. Il offre contrôle et visibilité sur les utilisateurs, les données et les applications des environnements SaaS (Software-as-a-service), PaaS (Platform-as-a-service) et IaaS (Infrastructure-as-a-service). CloudLock fournit également des informations exploitables en matière de cybersécurité en s'appuyant sur les analyses de données fournies par les spécialistes de CyberLab et celles basées sur le crowdsourcing.

Équipe Cisco chargée de traiter les incidents liés à la sécurité informatique (CSIRT, Computer Security Incident Response Team)

L'équipe Cisco CSIRT fait partie du service chargé des investigations du bureau Corporate Security Programs Office. Elle offre des services sur mesure de surveillance de la sécurité afin de protéger Cisco contre les cyberattaques et la perte de ressources intellectuelles. Par ailleurs, cette équipe interne est dédiée aux recherches et aux investigations sur les cyberattaques. Sa principale mission consiste à assurer la protection des données, des systèmes et de l'entreprise en faisant des recherches complètes sur les incidents informatiques. Elle contribue aussi à empêcher de tels incidents en réalisant une analyse proactive des menaces, en planifiant leur correction, en examinant les tendances liées aux incidents et en contrôlant l'architecture dédiée à la sécurité.

Services de traitement des incidents liés à la sécurité de Cisco (CSIRS, Cisco Security Incident Response Services)

L'équipe des services de traitement des incidents de sécurité de Cisco (CSIRS) se compose de spécialistes mondiaux qui sont chargés d'aider les clients de Cisco avant, pendant et après une attaque. Elle tire parti des meilleurs experts, de solutions de sécurité professionnelles, de techniques de riposte de pointe et de bonnes pratiques issues d'années de lutte contre les hackers afin de s'assurer que nos clients puissent se protéger de manière proactive et répondre rapidement à une attaque.

Cognitive Threat Analytics

Le service Cognitive Threat Analytics (CTA) de Cisco est un service cloud qui détecte les attaques, les programmes malveillants opérant à l'intérieur des réseaux protégés et d'autres attaques, au moyen d'analyses statistiques des données du trafic réseau. En procédant à une analyse de comportement et à une détection des anomalies, la solution identifie les symptômes d'une infection par programme malveillant ou d'une violation des données, et comble les failles des défenses périmétriques. Cisco Cognitive Threat Analytics utilise des fonctions évoluées de modélisation statistique et d'apprentissage automatique pour identifier indépendamment de nouvelles attaques, exploiter les informations recueillies et s'adapter progressivement.

Commercial West Sales

Le département Commercial West Sales est chargé d'engager des conversations sur la sécurité avec les clients Cisco, de leur organiser des ateliers SAFE et de conseiller leurs responsables de la sécurité pour renforcer la protection de leur entreprise et réduire les risques.

Global Government Affairs

Cisco est impliqué à différents niveaux auprès des gouvernements pour les aider à façonner des politiques publiques et des réglementations qui soutiennent le secteur technologique et aident les gouvernements à atteindre leurs objectifs. L'équipe des affaires gouvernementales mondiales (Global Government Affairs) influence les politiques publiques et les réglementations en faveur de la technologie. Travaillant en étroite collaboration avec les industriels et les associations commerciales, l'équipe établit des relations avec les leaders gouvernementaux afin d'influer sur les politiques qui affectent l'activité de Cisco et sur l'adoption générale des TIC, en cherchant à influencer les décisions politiques à l'échelle mondiale, nationale et locale. L'équipe se compose d'anciens élus, parlementaires, membres d'organismes de réglementation, représentants du gouvernement américain ainsi que de personnes travaillant dans des organismes publics qui soutiennent Cisco dans la promotion et la protection des technologies dans le monde entier.

Global Industrial Marketing

L'équipe Cisco Global Industrial Marketing œuvre dans le domaine de l'industrie, dans les secteurs pétrolier et gazier, et dans les services publics. Elle est chargée d'influencer la vision globale de chaque secteur avec des promesses, des solutions et des campagnes de commercialisation différenciées pour aider les clients à s'engager sur la voie du numérique. L'équipe collabore également avec des clients, des homologues, des équipes de gestion des comptes, des analystes, la presse et d'autres collaborateurs externes et internes. Elle se sert d'analyses en temps réel pour établir des stratégies propres au secteur, des stratégies de mise sur le marché, des plans et des messages ciblés.

IPTG Connected Car

L'équipe IPTG Connected Car est chargée d'aider les constructeurs automobiles à connecter, converger, sécuriser et numériser les réseaux intégrés dans les véhicules vers IP.

IoT

Le groupe dédié aux technologies de sécurité développe des outils, des processus et de la documentation pour identifier et éradiquer les menaces dans les environnements connectés.

Équipe Portfolio Solutions Marketing Team

L'équipe Portfolio Solutions Marketing Team est chargée de créer et de diffuser des messages et du contenu liés à la sécurité qui présentent et préconisent la gamme de solutions Cisco intégrées complètes.

U.S. Public Sector Organization

Le département Cisco U.S. Public Sector Organization transforme la manière dont les clients Cisco protègent, équipent et forment les utilisateurs aux États-Unis. Nous connectons les personnes et la technologie dans les administrations fédérales, régionales et locales ainsi que sur le marché de l'éducation. Par ailleurs, nous innovons à tous les niveaux, depuis la satisfaction de nos clients jusqu'à l'excellence opérationnelle et la réussite de nos missions. Nous guidons nos clients en décryptant les challenges auxquels leur entreprise est confrontée, en personnalisant des solutions qui répondent à leurs besoins spécifiques, en nouant des relations, en simplifiant la technologie et en influençant considérablement leur mission aux États-Unis et dans le monde entier.

Security Business Group Technical Marketing

L'équipe dédiée au marketing technique du groupe Security Business Group met à disposition un savoir-faire technique et spécialisé très poussé qui s'avère bien utile pour toutes les décisions relatives à la gestion des produits liés à la sécurité. Cette équipe composée d'experts techniques très qualifiés apporte son soutien à de nombreuses équipes Cisco dans le domaine de l'ingénierie, du marketing, des ventes et des services. Elle les aide à relever et à expliquer les challenges technologiques les plus complexes et les plus sophistiqués afin de mieux protéger les clients Cisco. Très sollicités pour leurs connaissances poussées, les membres de cette équipe participent à de nombreuses publications et conférences.

Security Research and Operations (SR&O)

Le département Security Research & Operations (SR&O) est responsable de la gestion des menaces et des vulnérabilités pour tous les produits et services Cisco, y compris pour l'équipe PSIRT, leader du secteur, en charge des incidents liés à la sécurité des produits. Le département SR&O aide les clients à comprendre ces menaces en perpétuelle évolution dans le cadre d'événements tels que Cisco Live et Black Hat, mais aussi par le biais d'une collaboration entre Cisco et les acteurs du secteur. Le département SR&O propose de nouveaux services, par exemple le service de Threat Intelligence personnalisée, qui permet d'identifier des indicateurs de compromission non encore détectés ou traités par les infrastructures de sécurité existantes.

Département Security and Trust

Le département Security and Trust de Cisco souligne l'implication de Cisco pour répondre à deux des enjeux les plus critiques, et qui constituent une priorité pour les dirigeants et leaders du monde entier. Le département a pour principales tâches la protection des clients publics et privés de Cisco, l'établissement d'un cycle de développement sécurisé et de systèmes fiables sur toute la gamme de produits et services Cisco, ainsi que la protection de l'entreprise Cisco contre des menaces en perpétuelle évolution. Cisco adopte une approche holistique de la sécurité et de la fiabilité, qui implique les personnes, les politiques, les processus et la technologie. Le département pousse à l'excellence opérationnelle dans tous les domaines : sécurité des systèmes d'information, fiabilité de l'ingénierie, protection et confidentialité des données, sécurité du cloud, transparence et validation, recherche sur la sécurité avancée et organismes publics. Pour en savoir plus, rendez-vous sur trust.cisco.com.

Talos Security Intelligence and Research Group

Talos, département de Cisco chargé des informations sur les menaces, réunit l'élite des experts de la sécurité chargés d'assurer une protection de qualité des clients, des produits et des services Cisco. Talos se compose des meilleurs spécialistes de la cybersécurité, lesquels exploitent des systèmes sophistiqués afin d'établir un panorama des menaces permettant aux produits Cisco de détecter et d'analyser les menaces connues et émergentes, et d'y répondre. Talos respecte les règles officielles de Snort.org, ClamAV et SpamCop ; son équipe est la source principale d'informations sur les menaces pour l'écosystème Cisco CSI.

Les partenaires technologiques du rapport Cisco du 1er semestre 2017 sur la cybersécurité

ANOMALI™

La suite Anomali de solutions de Threat Intelligence permet aux entreprises de détecter, d'analyser et de contrer les menaces de cybersécurité actives. La plate-forme primée de Threat Intelligence ThreatStream regroupe et optimise des millions d'indicateurs de menaces afin de créer une « liste noire des cyberattaques ». Anomali s'intègre avec l'infrastructure interne pour identifier les nouvelles attaques, recherche les failles qui se sont produites au cours de l'année et permet aux équipes responsables de la sécurité de cerner et de contenir rapidement les menaces. Anomali propose également un outil gratuit, STAXX, qui collecte et partage de la Threat Intelligence, et offre également un flux d'informations gratuit prêt à l'emploi, Anomali Limo. Pour en savoir plus, rendez-vous sur anomali.com et suivez-nous sur Twitter : @anomali.

FLASHPOINT

Flashpoint propose des informations sur les risques qui permettent aux entités commerciales et aux départements d'une entreprise de prendre de meilleures décisions et de réduire les risques. Sa technologie, son expertise et ses données inédites sur le dark web et le deep web aident les clients à collecter des informations sur les risques et à protéger leur activité. Pour en savoir plus, rendez-vous sur flashpoint-intel.com.

Lumeta fournit des informations contextuelles essentielles qui aident les équipes chargées de la sécurité et du réseau à éviter les failles. Lumeta détecte les infrastructures réseau connues, inconnues, fantômes et non autorisées, tout en proposant la surveillance en temps réel des terminaux et du réseau, et une analyse de la segmentation pour les éléments réseau dynamiques, les terminaux, les machines virtuelles et les infrastructures basées dans le cloud. Pour en savoir plus, rendez-vous sur lumeta.com.

Qualys, Inc. (NASDAQ : QLYS) est un fournisseur leader et avant-gardiste de solutions de conformité et de sécurité basées dans le cloud. Il compte plus de 9 300 clients dans plus de 100 pays, dont une majorité fait partie des classements Forbes Global 100 et Fortune 100. La plate-forme cloud et la suite intégrée de solutions Qualys permettent aux entreprises de simplifier les opérations de sécurité et de réduire le coût de la mise en conformité. En effet, les clients bénéficient d'une sécurité adaptative essentielle à la demande et sont en mesure d'automatiser tout le processus d'audit, de mise en conformité et de protection des systèmes IT et des applications web. Créée en 1999, l'entreprise Qualys a conclu des partenariats stratégiques avec des prestataires de services managés leaders et des entreprises de conseils dans le monde entier. Pour en savoir plus, rendez-vous sur qualys.com.

Radware (NASDAQ : RDWR) est un leader mondial dans le domaine des solutions de cybersécurité et des applications pour les data centers virtuels, cloud et sous forme logicielle. Sa gamme de solutions primées assure un excellent niveau de service à plus de 10 000 entreprises et opérateurs dans le monde entier. Pour obtenir d'autres informations et ressources spécialisées sur la sécurité, visitez le centre de sécurité en ligne Radware qui propose une analyse complète des outils, des tendances et des menaces liés aux attaques par déni de service (DDoS) : security.radware.com.

Les professionnels de la sécurité et de l'informatique du monde entier font confiance à Rapid7 (NASDAQ : RPD) pour gérer les risques, simplifier une infrastructure IT moderne complexe et stimuler l'innovation. Les analyses Rapid7 transforment les innombrables données sur la sécurité et l'IT en informations exploitables, nécessaires pour développer et exécuter en toute sécurité des réseaux et des applications IT sophistiqués. La recherche, la technologie et les services Rapid7 permettent de gérer les vulnérabilités, de tester les intrusions, de protéger les applications, de détecter et d'éradiquer les attaques et de gérer les événements pour plus de 6 300 entreprises dans plus de 120 pays, dont 39 % appartiennent au classement Fortune 1000. Pour en savoir plus, rendez-vous sur rapid7.com.

Les solutions de sécurité RSA dédiées aux entreprises aident les clients à établir rapidement un lien entre les incidents liés à la sécurité et le contexte afin de déployer des mesures correctives efficaces et de protéger les ressources essentielles. Grâce à des solutions primées qui assurent une détection et une riposte rapides, le contrôle des identités et des accès, la protection contre la fraude et la gestion des risques, les clients RSA peuvent tirer leur épingle du jeu dans un environnement très risqué. Pour en savoir plus, rendez-vous sur rsa.com.

SAINT Corporation, leader dans le domaine des solutions intégrées de gestion des vulnérabilités de nouvelle génération, aide les entreprises et les institutions publiques à identifier les risques à tous les niveaux. Grâce à SAINT, l'accès, la sécurité et la confidentialité peuvent coexister pour le bénéfice de tous. Par ailleurs, ses clients peuvent renforcer la sécurité de leurs systèmes d'information, tout en réduisant le coût total de possession. Pour en savoir plus, rendez-vous sur saintcorporation.com.

ThreatConnect® met à la disposition des entreprises une solution de protection puissante contre les cybermenaces et les aide à prendre des décisions stratégiques en toute confiance. Reposant sur la seule plate-forme de sécurité extensible et axée sur les informations du secteur, ThreatConnect propose une suite de produits conçus pour répondre aux besoins des équipes responsable de la sécurité en matière d'agrégation, d'analyse et d'automatisation de la Threat Intelligence, quel que soit leur niveau de maturité. Plus de 1 600 entreprises et agences du monde entier ont déployé la plate-forme ThreatConnect pour intégrer pleinement une solution de Threat Intelligence exploitable avec leurs technologies de sécurité, leurs équipes et leurs processus, d'où une réduction du délai entre la détection et la riposte, et une meilleure protection des ressources. Pour en savoir plus, rendez-vous sur threatconnect.com.

TrapX Security propose des solutions de sécurité automatisées pour une détection et une protection adaptatives qui interceptent les menaces en temps réel, tout en fournissant les informations exploitables nécessaires pour bloquer les hackers. TrapX DeceptionGrid™ permet aux entreprises de détecter, de capturer et d'analyser les malwares de type « zero-day » utilisés par les menaces persistantes avancées les plus efficaces au monde. Les entreprises, quel que soit leur secteur, tirent parti de TrapX pour renforcer leur écosystème IT et réduire les risques de compromissions, de violations des données et de non-conformité qui peuvent s'avérer coûteux et perturber leur activité. Les systèmes de défense TrapX sont intégrés au cœur du réseau et de l'infrastructure principale, sans avoir besoin d'agents ou de configuration spéciale. En regroupant d'excellentes fonctionnalités de détection des malwares, de Threat Intelligence, d'analyse et de mise en place de mesures correctives dans une seule plate-forme, vous limitez la complexité et les coûts. Pour en savoir plus, rendez-vous sur trapx.com.

Télécharger les graphiques

Vous pouvez télécharger tous les graphiques de ce rapport à l'adresse : cisco.com/go/mcr2017graphics.

Mises à jour et corrections

Pour consulter les mises à jour de ce rapport et connaître les corrections apportées aux informations, rendez-vous sur : cisco.com/go/errata.

Siège social aux États-Unis
Cisco Systems, Inc.
San José. CA

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

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

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et de fax sont répertoriés sur le site web de Cisco, à l'adresse : www.cisco.com/go/offices.