



Cisco 2018
Rapport annuel sur la cybersécurité

Sommaire

Synthèse 3

Partie I : l'évolution des attaques 6

L'évolution des malwares	6
Trafic web malveillant chiffré	9
Menaces par e-mail	14
Tactiques de contournement des sandboxes	22
Détournement des services cloud et d'autres ressources légitimes.....	24
IoT et attaques DDoS	31
Vulnérabilités et correctifs	38

Partie II : les acteurs de la protection..... 46

Le coût des attaques	46
Défis et obstacles	47
Complexité de l'orchestration de plusieurs fournisseurs	48
Impact : la méfiance du public due aux failles de sécurité se traduit par un risque de pertes plus élevé	50
Services : tenir compte des utilisateurs, des politiques et de la technologie.....	53
Attentes : investir dans la technologie et la formation	54

Conclusion 57

À propos de Cisco 60

Annexe 65

Synthèse

Et si les entreprises pouvaient prévoir l'avenir ? Si elles savaient qu'une attaque était imminente, elles pourraient l'arrêter, ou en atténuer l'impact, et protéger leurs ressources les plus importantes. Le fait est que les entreprises peuvent voir ce qui se profile à l'horizon. De nombreux indices sont visibles et évidents.

Les hackers disposent de l'expertise et des outils nécessaires pour démanteler les infrastructures et les systèmes stratégiques et paralyser des régions entières. Mais lorsque les nouvelles font état de cyberattaques destructrices, comme celles qui ont lieu en Ukraine ou ailleurs dans le monde, certains responsables sécurité peuvent d'abord penser : « Le marché, la région ou l'environnement technologique de notre entreprise n'était pas une cible, alors nous ne sommes probablement pas en danger. »

En ignorant ces campagnes éloignées et en se laissant happer par la défense quotidienne de leur infrastructure, les responsables sécurité peuvent sous-estimer l'ampleur et la vitesse à laquelle les hackers amassent et perfectionnent leurs armes informatiques.

Depuis des années, Cisco met en garde les entreprises contre l'augmentation des activités cybercriminelles dans le monde entier. À ce sujet, dans notre tout dernier rapport annuel sur la cybersécurité, nous présentons les données et analyses des experts Cisco ainsi que de plusieurs de nos partenaires technologiques sur le comportement des hackers observé au cours des 12 à 18 derniers mois. Bon nombre des sujets abordés dans le rapport s'articulent autour de trois thèmes généraux :

1. Les malwares atteignent des niveaux de sophistication et d'impact inédits.

L'évolution des malwares (page 6) a été l'un des développements les plus significatifs dans l'évolution des attaques en 2017. L'avènement des cryptovirus ransomwares basés sur le réseau élimine toute nécessité d'une intervention humaine pour lancer des campagnes de ransomwares. Et pour certains hackers, le prix à gagner n'est pas la rançon elle-même, mais l'effacement des systèmes et des données, sur le modèle de Nyetya, un malware déguisé en ransomware conçu pour effacer les données (voir la page 6). Selon les experts Cisco, les malwares qui se propagent automatiquement sont dangereux et seraient capables de bloquer tout Internet.

2. Les hackers contournent de mieux en mieux les systèmes de sécurité et détournent de plus en plus les services cloud et autres technologies légitimes pour leurs activités malveillantes.

En plus de développer des menaces qui peuvent contourner des environnements de sandboxing de plus en plus sophistiqués (page 22), les hackers ont de plus en plus recours au chiffrement pour échapper aux détections (page 9). Le chiffrement a pour but de renforcer la sécurité, mais c'est également un outil puissant pour les hackers pour dissimuler les activités de contrôle-commande (C2) et obtenir plus de temps pour opérer et provoquer des dégâts.

Les cybercriminels adoptent également les canaux C2 qui s'appuient sur des services Internet légitimes comme Google, Dropbox et GitHub (voir la page 24). Cela rend presque impossible l'identification du trafic malveillant.

De plus, de nombreux hackers lancent maintenant plusieurs campagnes à partir d'un même domaine (page 26) afin d'optimiser leur retour sur investissement. Ils réutilisent également les ressources de l'infrastructure, comme les adresses e-mail des inscrits, les numéros de systèmes autonomes (ASN) et les serveurs de noms.

3. Les hackers exploitent les failles de sécurité non défendues, dont beaucoup sont dues à l'expansion de l'Internet des objets (IoT) et à l'utilisation des services cloud.

Les entreprises déplacent rapidement des appareils connectés à l'IoT, mais ne prêtent souvent guère attention à leur sécurité. Les appareils IoT non patchés et non surveillés offrent aux hackers la possibilité d'infiltrer les réseaux (page 34). De plus, les entreprises dotées d'appareils IoT susceptibles d'être attaqués semblent, d'après notre enquête, peu motivées à l'idée d'accélérer la mise en place de correctifs (page 42). Voir ignorer l'existence même de ces appareils vulnérables au sein de leur réseau .

Pendant ce temps, **les botnets IoT se développent** parallèlement à l'IoT et deviennent de plus en plus perfectionnés et automatisés. À mesure qu'ils se développent, les hackers les utilisent pour lancer des attaques par déni de service distribué (DDoS) ([page 31](#)).

Les cybercriminels profitent également du fait que les équipes de sécurité ont **du mal à défendre à la fois les environnements IoT et cloud**. L'une des raisons réside dans le manque de clarté quant au choix des responsables de la protection de ces environnements (voir la [page 42](#)).

Recommandations pour les entreprises

Quand les hackers frappent, les acteurs de la protection peuvent-ils revenir rapidement à une situation normale ? Les conclusions de l'**Enquête Cisco 2018 sur l'efficacité des mesures de sécurité**, menée auprès de 3 600 personnes interrogées dans 26 pays, démontrent que les entreprises ont beaucoup de défis à relever (voir la [page 46](#)).

Dans tous les cas, ces dernières doivent savoir qu'améliorer leur stratégie en matière de sécurité et respecter les bonnes pratiques les plus courantes peut réduire l'exposition aux nouveaux risques, ralentir la progression des hackers et renforcer la visibilité sur les menaces. Ce qu'elles doivent envisager :

- Implémenter des outils de première ligne de défense évolutifs, comme les plates-formes de sécurité cloud.
- Confirmer le respect des politiques et pratiques de l'entreprise en matière de correctifs pour les appliances, les systèmes et les applications.
- Segmenter le réseau pour réduire l'exposition aux attaques.
- Adopter des outils de nouvelle génération pour surveiller les processus au niveau des terminaux.

- Accéder rapidement à des données et à des processus précis de Threat Intelligence qui permettent d'intégrer les données dans les workflows de surveillance et de gestion de la sécurité.
- Effectuer des analyses plus approfondies et plus avancées.
- Passer en revue et mettre en pratique les procédures d'intervention en matière de sécurité.
- Enregistrer régulièrement les données et tester les procédures de restauration. Ce sont des processus essentiels dans un monde où les vers ransomwares basés sur le réseau et les armes cybérétiques évoluent rapidement.
- Examiner les tests d'efficacité effectués par des tiers sur les technologies de sécurité afin de réduire les risques d'attaques de la chaîne d'approvisionnement.
- Analyser la sécurité des systèmes d'administration des microservices, des services cloud et des applications.
- Examiner les systèmes de sécurité et considérer l'utilisation d'analyses SSL et, si possible, de fonctions de déchiffrement SSL.

Les entreprises doivent également envisager d'adopter des technologies de sécurité avancées, utilisant notamment l'apprentissage automatique et l'intelligence artificielle. Face à des malwares qui chiffrent leurs communications et à des utilisateurs internes non autorisés qui envoient des données sensibles par le biais des systèmes cloud de l'entreprise, les équipes de sécurité ont besoin d'outils efficaces pour empêcher ou détecter l'utilisation du chiffrement pour dissimuler les activités malveillantes.

À propos de ce rapport

Le **rappor annuel Cisco 2018 sur la cybersécurité** présente les dernières avancées en matière de sécurité destinées à aider les entreprises et les utilisateurs à se défendre contre les hackers. Nous examinons également les techniques et les stratégies que les hackers utilisent pour percer ces défenses et échapper aux détections.

Le rapport présente également les principales conclusions de l'**Enquête 2018 de Cisco sur l'efficacité des mesures de sécurité**, qui examine les mesures de sécurité et la perception du niveau de préparation dans les entreprises.

Partie I :

L'évolution des attaques

Partie I : l'évolution des attaques

Les malwares atteignent des niveaux de sophistication et d'impact inédits. La diversité et le nombre grandissants des types et familles de malwares réduisent la marge de manœuvre et le temps d'anticipation des entreprises face aux menaces.

ÉVOLUTION DES MALWARES

L'évolution des ransomwares représentait l'un des développements les plus importants en 2017. Avec l'avènement des vers ransomwares basés sur le réseau, il n'y a plus besoin d'intervention humaine pour lancer des campagnes de ransomware. Et pour certains hackers, le but n'est pas la rançon, mais la destruction des systèmes et des données. Nous nous attendons à ce que cette activité progresse davantage dans l'année qui vient.

En 2018, les entreprises doivent se préparer à faire face à de nouvelles menaces dites « autopropagées » basées sur le réseau.

Nous nous y attendions, mais les hackers ont fait considérablement évoluer les ransomwares en 2017. Après SamSam en mars 2016¹, la première attaque de grande envergure utilisant le vecteur réseau pour répandre des ransomwares et supprimer ainsi toute intervention humaine du processus d'infection, les experts en sécurité de Cisco savaient que ce ne serait qu'une question de temps avant que les hackers trouvent un moyen d'automatiser cette technique. Ils savaient que les cybercriminels renforceraient leurs malwares en les associant à des fonctionnalités caractéristiques des infections par vers pour causer des dégâts considérables.

Cette évolution des malwares a été rapide. En mai 2017, le cryptovirus ransomware WannaCry s'est propagé comme un feu de forêt sur Internet.² Pour cela, il a profité d'une faille de sécurité de Microsoft Windows appelée **EternalBlue**, qui a été divulguée par le groupe de hackers Shadow Brokers à la mi-avril 2017.

WannaCry a rapporté plus de 143 000 \$ en bitcoins. Compte tenu du délai et en estimant que la valeur cumulée des bitcoins initialement versés dans les portefeuilles était de 93 531 \$, les experts Cisco estiment qu'environ 312 paiements de rançons ont été effectués. À titre de comparaison, le kit d'exploit Angler, lorsqu'il était actif, présentait des gains d'environ 100 millions de dollars par an à l'échelle mondiale.

Il n'a pas été démontré que les auteurs de WannaCry suivaient réellement les dommages causés ni le paiement des rançons. Le nombre d'utilisateurs ayant reçu des clés de déchiffrement après avoir effectué un paiement est également inconnu. (WannaCry continue de se répandre aujourd'hui et les utilisateurs continuent de payer des rançons en vain.) En raison du très faible rendement de WannaCry en tant que ransomware, le gouvernement américain et de nombreux experts en sécurité pensent que la demande de rançon sert à dissimuler le véritable but du virus : l'effacement des données.

Nyetya (également connu sous le nom de NotPetya) a fait son apparition en juin 2017.³ Ce malware conçu pour effacer les données s'est également déguisé en ransomware et a également exploité les vulnérabilités d'exécution du code à distance appelées « EternalBlue » et « EternalRomance » (également divulguées par le groupe Shadow Brokers) et d'autres vecteurs impliquant la collecte d'identifiants

1 SamSam : *The Doctor Will See You, After He Pays the Ransom*, blog Cisco Talos, mars 2016 : blog.talosintelligence.com/2016/03/samsam-ransomware.html.

2 Player 3 Has Entered the Game : *Say Hello to 'WannaCry'*, blog Cisco Talos, mai 2017 : blog.talosintelligence.com/2017/05/wannacry.html.

3 New Ransomware Variant 'Nyetya' Compromises Systems Worldwide, blog Cisco Talos, juin 2017 : blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html.

sans rapport avec les révélations du groupe Shadow Brokers.⁴ Nyetya a été déployé par le biais des mises à jour logicielles d'un progiciel fiscal utilisé par plus de 80 % des entreprises en Ukraine et installé sur plus d'un million d'ordinateurs.⁵ La cyberpolice ukrainienne a confirmé que cette attaque avait touché plus de 2 000 entreprises du pays.⁶

Avant l'avènement des ransomwares à propagation automatique, les malwares étaient diffusés de trois façons : par téléchargement de type « drive-by », par e-mail ou par support physique, comme un périphérique USB malveillant. Toutes ces méthodes nécessitaient une intervention humaine pour infecter un appareil ou un système avec un ransomware. Avec les nouveaux vecteurs utilisés par les hackers, un poste de travail actif et non corrigé suffit pour lancer une campagne de ransomwares basés sur le réseau.

Les responsables sécurité peuvent considérer les infections par vers comme un type de menace appartenant au passé, car leur nombre parmi les failles et de vulnérabilités courantes (CVE) a diminué au fur et à mesure que les niveaux de sécurité des produits ont augmenté. Toutefois, selon les experts Cisco, les malwares à propagation automatique représentent une menace considérable et ont même le potentiel de bloquer tout Internet. WannaCry et Nyetya ne sont qu'un avant-goût des menaces qui se profilent. C'est pourquoi les entreprises doivent se préparer.

Les attaques WannaCry et Nyetya auraient pu être évitées, ou leur impact atténué, si un plus grand nombre d'entreprises avaient appliqué les bonnes pratiques de base en matière de sécurité telles que l'application de correctifs des vulnérabilités, la mise en place de processus et de politiques appropriés pour les interventions en cas d'incident et la segmentation du réseau.

Pour plus de conseils sur comment se protéger des vers ransomwares automatisés basés sur le réseau, consultez *Back to Basics : Worm Defense in the Ransomware Age* sur le blog Cisco Talos.

Le maillon faible en matière de sécurité : la chaîne d'approvisionnement

Nyetya ciblait également la chaîne d'approvisionnement, comme de nombreuses menaces observées par les experts Cisco en 2017. L'une des raisons pour lesquelles Nyetya a réussi à infecter si rapidement autant de machines, c'est que les utilisateurs ne voyaient pas la mise à jour automatique d'un logiciel comme un risque ou, dans certains cas, ne se rendaient même pas compte qu'ils recevaient des mises à jour malveillantes.

Une autre attaque de la chaîne d'approvisionnement a eu lieu en septembre 2017. Elle concernait les serveurs de téléchargement utilisés par un fournisseur de logiciels pour distribuer un progiciel légitime connu sous le nom de CCleaner.⁷ Les fichiers binaires de CCleaner, qui contenaient une « back door » de type cheval de Troie, ont été signés à l'aide d'un certificat valide. Les utilisateurs étaient ainsi confortés, à tort, dans la certitude que le logiciel utilisé était sécurisé. Les hackers à l'origine de cette campagne visaient les grandes entreprises technologiques où le logiciel était utilisé, soit officiellement soit par des utilisateurs individuels.

Les attaques de la chaîne d'approvisionnement semblent être de plus en plus rapides et complexes. Elles peuvent avoir un impact considérable sur les ordinateurs et persister pendant des mois, voire des années. Les entreprises doivent être conscientes du risque potentiel lié à l'utilisation de logiciels ou de matériel provenant de fournisseurs qui n'ont pas une attitude responsable en matière de sécurité. Faites appel à des fournisseurs qui proposent des listes de failles et de vulnérabilités courantes (CVE), traitent rapidement les vulnérabilités et veillent à ce que leurs systèmes ne puissent pas être attaqués. De plus, les utilisateurs devraient prendre le temps d'analyser les nouveaux logiciels avant de les télécharger pour vérifier qu'ils ne contiennent pas de malwares.

Segmenter le réseau pour les logiciels dont la sécurisation est incomplète peut aider à limiter les dégâts causés par les attaques ciblant la chaîne d'approvisionnement, en les empêchant de se propager dans toute l'entreprise.

4 Ibid.

5 Ukraine scrambles to contain new cyber threat after 'NotPetya' attack, par Jack Stubbs et Matthias Williams, Reuters, juillet 2017 : reuters.com/article/us-cyber-attack-ukraine-backdoor/ukraine-scrambles-to-contain-new-cyber-threat-after-notpetya-attack-idUSKBN19Q14P.

6 The MeDoc Connection, blog Cisco Talos, juillet 2017 : blog.talosintelligence.com/2017/07/the-medoc-connection.html.

7 CCleaner Command and Control Causes Concern, blog Cisco Talos, septembre 2017 : blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html.

L'importance de l'intégrité dans les rapports d'informations sur les programmes malveillants

Toutes les entreprises qui communiquent des informations sur les malwares à leurs clients ou au public, quel que soit le canal employé, devraient appliquer des directives visant à assurer l'exactitude de leurs rapports. Même si tous les faits ne sont pas clairs, les entreprises peuvent toujours communiquer ce qu'elles savent et éviter les suppositions. Il vaut mieux avoir raison que d'être le premier.

Par exemple, lors de l'attaque de WannaCry en mai 2017, la communauté de spécialistes ne savait pas bien au départ comment le ransomware infiltrait les systèmes. Plusieurs entreprises du secteur public et du secteur privé signalaienr qu'une campagne de phishing avec pièces jointes malveillantes était à l'origine de l'attaque. En fait, la menace basée sur le réseau recherchait et infectait les ports SMB (Microsoft Windows Server Message Block) accessibles au public et vulnérables.

Les chercheurs en sécurité Cisco ont rapidement averti la communauté que les e-mails soupçonnés d'être liés à la campagne WannaCry étaient probablement des spams émis

par le bot Necurs qui propageaient le ransomware « Jaff ». Quelques jours plus tard, la communauté de sécurité concluait que les e-mails suspects contenaient Jaff et non WannaCry. Pendant tout ce temps, les utilisateurs ont pris des dispositions en se basant sur une information incapable de les aider à se protéger contre l'avancée fulgurante de WannaCry.

Le chaos qui a suivi l'épisode WannaCry rappelle à la communauté de sécurité qu'il faut éviter de communiquer des faits inexacts sur l'origine et la nature des cyberattaques. Dans les premières heures d'une campagne, on cherche à arrêter les hackers et à protéger les utilisateurs le plus rapidement possible. Dans la panique, on risque de publier, surtout sur les réseaux sociaux, des informations qui pourraient brouiller les esprits et empêcher les utilisateurs de défendre leurs systèmes.

Pour de plus amples informations sur ce sujet, lisez l'article *On Conveying Doubt* (en anglais) sur le blog Cisco Talos.

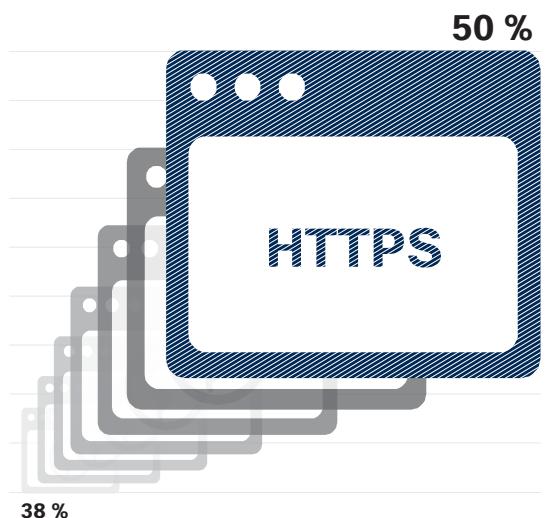
TRAFIG WEB MALVEILLANT CHIFFRÉ

Le volume croissant de trafic web chiffré, qu'il soit légitime ou malveillant, crée encore plus de défis et de confusion pour les entreprises qui tentent d'identifier et de surveiller les menaces potentielles. Le chiffrement a pour but de renforcer la sécurité, mais c'est également un outil puissant pour les hackers pour dissimuler les activités de contrôle-commande (C2) et obtenir plus de temps pour opérer et provoquer des dégâts. Les experts Cisco s'attendent à ce que les hackers aient davantage recours au chiffrement en 2018. Pour s'adapter, les entreprises devront intégrer davantage d'automatisation et d'outils perfectionnés comme l'apprentissage automatique et l'intelligence artificielle pour compléter la prévention, la détection et l'élimination des menaces.

Un point noir pour les entreprises : le trafic web malveillant chiffré

Les experts Cisco indiquent que 50 % du trafic web mondial était chiffré en octobre 2017. Il s'agit d'une augmentation de 12 % par rapport à novembre 2016 (voir la Figure 1). L'un des facteurs qui expliquent cette augmentation est la facilité d'accès à des certificats SSL gratuits ou peu coûteux. Un autre facteur est la signalisation publique par Google Chrome des sites web non chiffrés traitant des informations sensibles, comme les numéros de cartes bancaires des clients ». À moins de prendre le risque de voir baisser de manière significative leur classement sur les pages de recherche Google, les entreprises ont intérêt à se conformer à l'exigence de chiffrement HTTPS de Google.

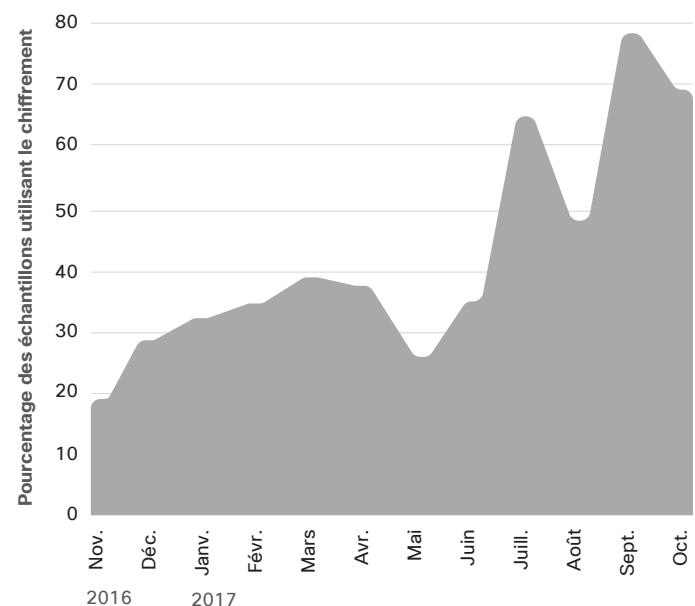
Figure 1 Augmentation du volume du trafic web chiffré mondial



Source : Cisco Security Research

Au fur et à mesure que le volume du trafic web mondial chiffré augmente, les hackers adoptent de plus en plus le chiffrement pour dissimuler leurs activités de type C2. Les experts Cisco ont observé que les communications réseau chiffrées avaient plus que triplé dans les échantillons de malwares inspectés sur une période de 12 mois (voir la Figure 2). Notre analyse de plus de 400 000 fichiers binaires malveillants a révélé qu'environ 70 % d'entre eux avaient eu recours au chiffrement à partir d'octobre 2017.

Figure 2 Augmentation du volume des codes malveillants s'appuyant sur des communications réseau chiffrées



Source : Cisco Security Research

 Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics

L'apprentissage automatique pour se protéger des menaces

Pour surmonter le manque de visibilité dû au chiffrement et réduire la fenêtre d'action des hackers, de plus en plus d'entreprises se tournent vers l'apprentissage automatique et l'intelligence artificielle. Ces fonctionnalités avancées peuvent améliorer les systèmes de sécurité du réseau et, sur le long cours, « apprendre » à détecter automatiquement les tendances inhabituelles du trafic web qui pourraient indiquer une activité malveillante.

L'apprentissage automatique est utile pour détecter automatiquement les menaces « connues-connues », c'est-à-dire les types d'infections qui ont déjà été observées (voir la Figure 3). Mais sa valeur réelle, en particulier dans le cadre de la surveillance du trafic web chiffré, tient à sa capacité à détecter les menaces « connues-inconnues » (variantes inédites de menaces connues, sous-familles de malwares ou nouvelles

menaces connexes) et les menaces « inconnues-inconnues » (malwares totalement nouveaux). Les nouvelles technologies permettent d'identifier des comportements anormaux dans de grands volumes de trafic web chiffré et alerter automatiquement les équipes de sécurité sur la nécessité d'une étude plus approfondie.

Ce dernier point est particulièrement important, étant donné que le manque de personnel qualifié est un obstacle au renforcement des systèmes de sécurité dans de nombreuses entreprises, comme l'indiquent les conclusions de l'Enquête Cisco 2018 sur l'efficacité des mesures de sécurité (voir la page 35). L'automatisation et les outils tels que l'apprentissage automatique et l'intelligence artificielle peuvent aider les entreprises à surmonter leurs lacunes en matière de compétences et de ressources, afin d'identifier et de contrer les menaces connues et émergentes de manière plus efficace.

Figure 3 Apprentissage automatique pour la sécurité réseau : taxonomie



Source : Cisco Security Research

 Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics

i Enquête Cisco 2018 sur l'efficacité des mesures de sécurité : les acteurs de la protection disent se fier plus à l'automatisation et à l'intelligence artificielle

Les RSSI (responsables de la sécurité des systèmes d'information) interrogés dans le cadre de l'Enquête Cisco 2018 sur l'efficacité des mesures de sécurité souhaitent ajouter des outils utilisant l'intelligence artificielle et l'apprentissage automatique à leur infrastructure de sécurité, et pensent que cette dernière gagne en sophistication et en intelligence. Toutefois, ils sont contrariés par le nombre de faux positifs générés par ce type de système et par la charge de travail accrue que cela entraîne pour leurs équipes. Le nombre de faux positifs devrait se réduire au fur et à mesure que les technologies d'apprentissage automatique et d'intelligence artificielle progressent et apprennent en quoi consiste l'activité « normale » dans les environnements réseau qu'elles surveillent.

À la question « Sur quelles technologies automatisées votre entreprise s'appuie-t-elle le plus ? », 39 % des responsables sécurité répondent qu'ils s'appuient entièrement sur l'automatisation, 34 % s'appuient entièrement sur l'apprentissage automatique et 32 % s'appuient entièrement sur l'intelligence artificielle (Figure 4).

Les outils d'analyse des comportements sont également appréciés pour localiser les hackers dans les réseaux : pour 92 % des responsables sécurité, ces outils sont très efficaces ou extrêmement efficaces (Figure 5).

Figure 4 Les entreprises s'appuient fortement sur l'automatisation, l'apprentissage automatique et l'intelligence artificielle

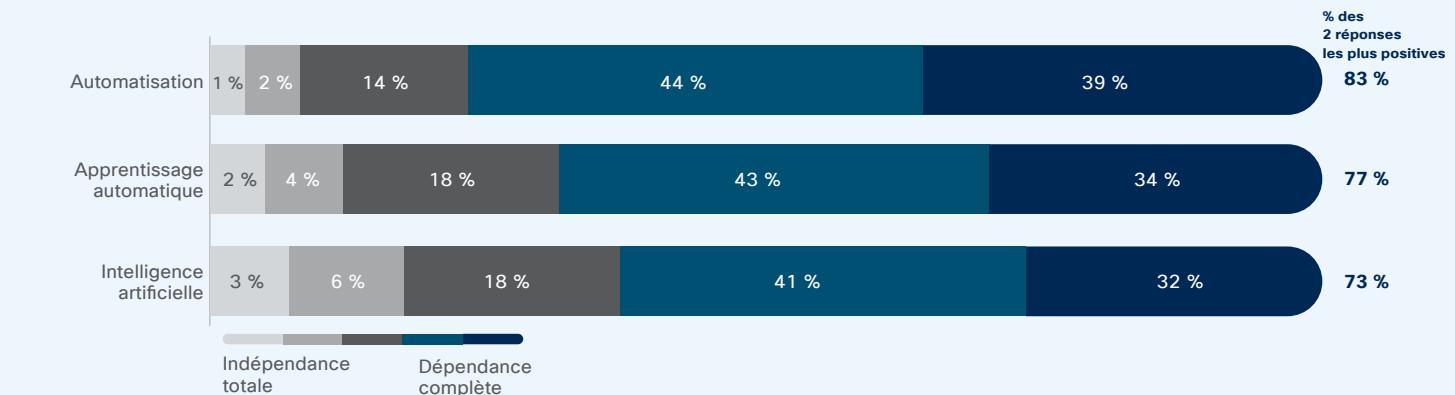
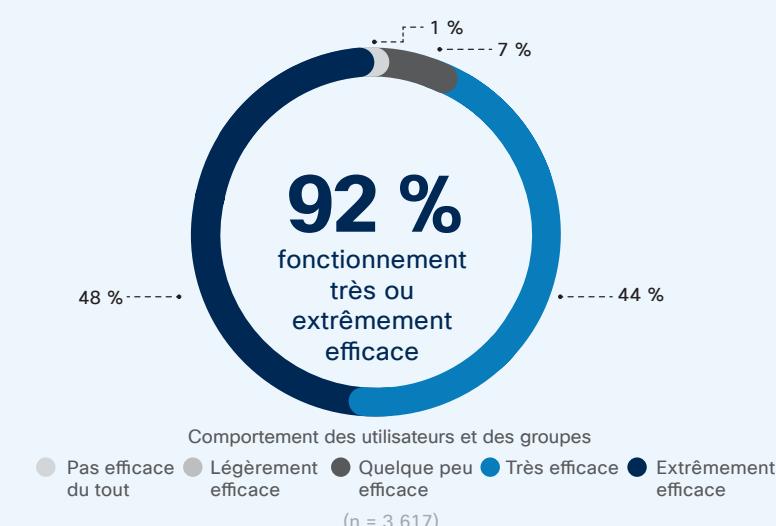


Figure 5 Les outils d'analyse des comportements sont prisés par la plupart des responsables sécurité



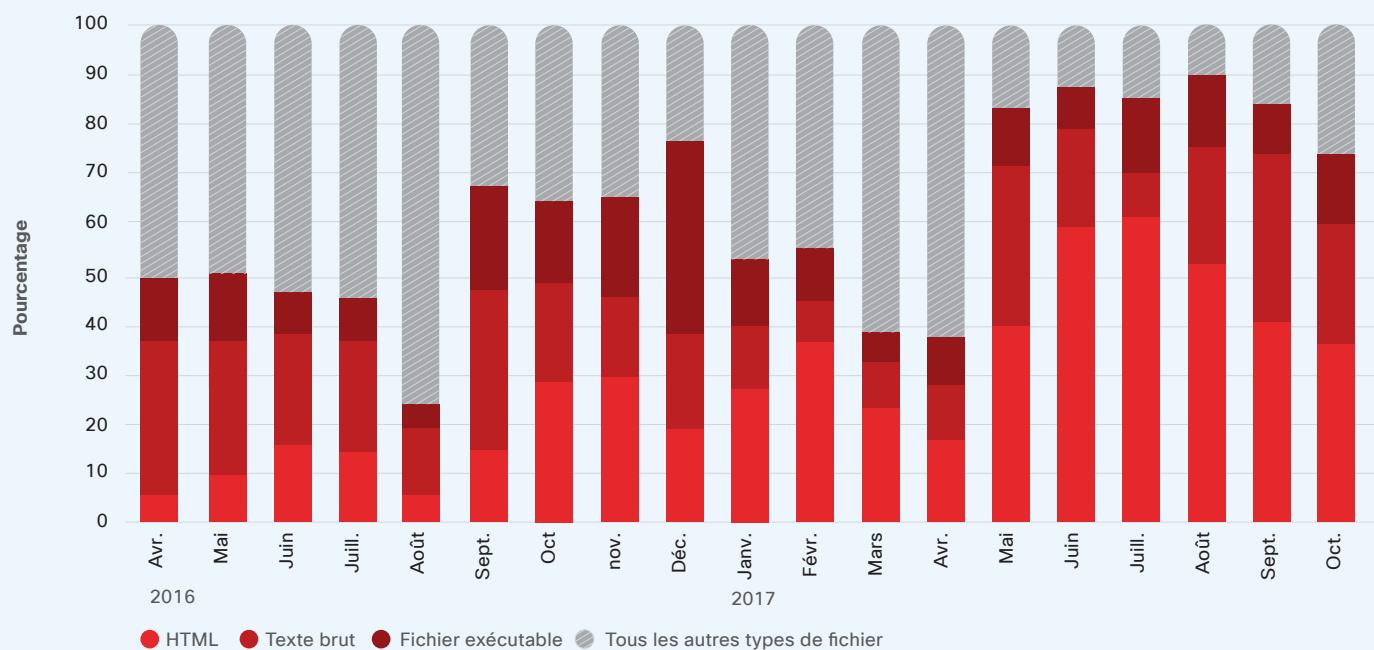
Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics

i) Les méthodes d'attaque sur le web démontrent que les hackers ciblent de plus en plus les navigateurs

Une analyse des méthodes d'attaque sur le web sur une période de 18 mois allant d'avril 2016 à octobre 2017 révèle que les hackers utilisent de plus en plus de contenus web malveillants (Schéma 6). Cette tendance s'aligne sur le ciblage offensif du navigateur Internet Explorer de Microsoft par des kits d'exploit encore actifs.

Les experts Cisco ont constaté que le nombre de détections de contenu web JavaScript malveillant était important et constant au cours de cette période. Cela souligne l'efficacité de cette stratégie pour infecter les navigateurs vulnérables afin de faciliter d'autres activités malveillantes comme la redirection des navigateurs ou les téléchargements de chevaux de Troie.

Figure 6 Blocage des malwares par type de contenu, avril 2016-octobre 2017



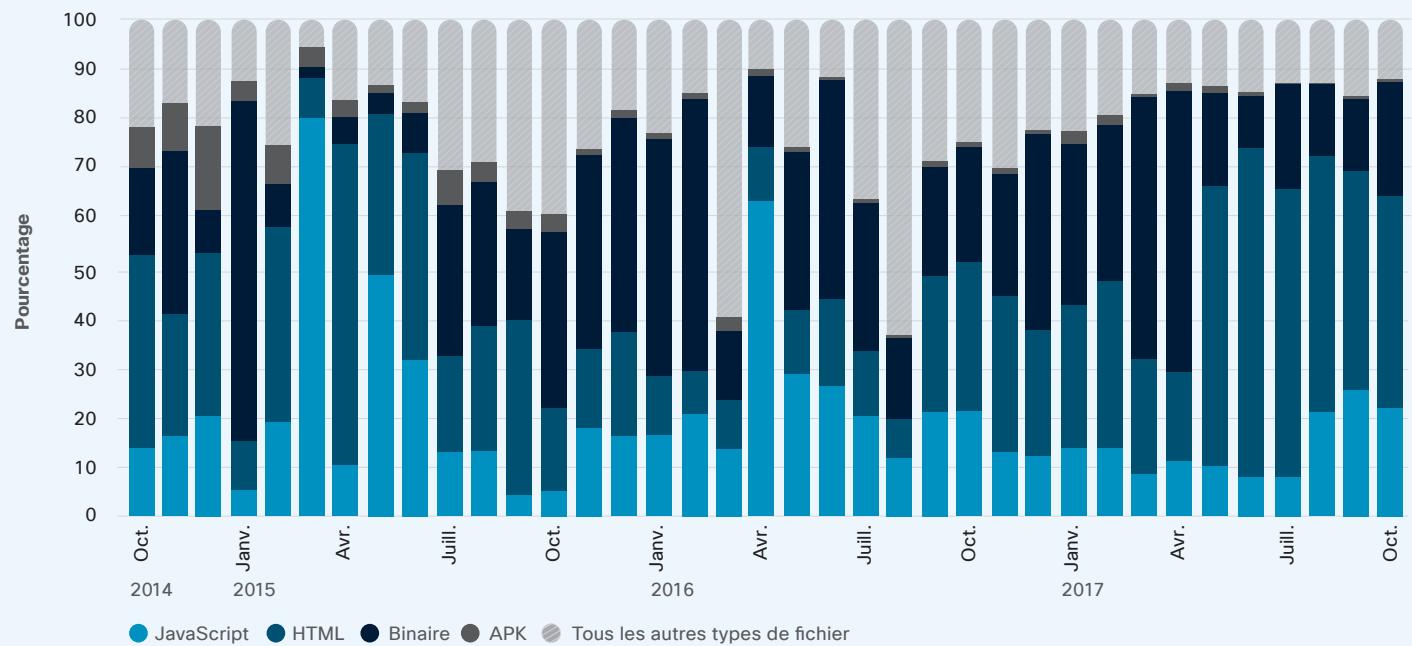
Source: Cisco Security Research

Le schéma 7 fournit un aperçu des méthodes d'attaque sur le web sur une période de trois ans, d'octobre 2014 à octobre 2017. Les hackers ont systématiquement utilisé des fichiers binaires suspects pendant cette période, principalement pour diffuser des logiciels publicitaires et des spywares. Comme mentionné dans le *Rapport Cisco sur la cybersécurité du 1er semestre 2017*, ces types d'applications potentiellement indésirables (PUA) peuvent présenter des risques de sécurité,

tels que l'augmentation des infections par malware et le vol d'informations sur les utilisateurs ou les entreprises.⁸

La vue sur trois ans présentée à la Figure 7 montre également que le volume de contenu web malveillant varie sur le long cours à mesure que les hackers lancent et mettent fin à leurs campagnes et modifient leur tactique pour échapper aux détections.

Figure 7 Blocage des malwares par type de contenu, octobre 2014-octobre 2017



Source : Cisco Security Research

 Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics

⁸ Rapport Cisco sur la cybersécurité du 1er semestre 2017 : cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

MENACES PAR E-MAIL

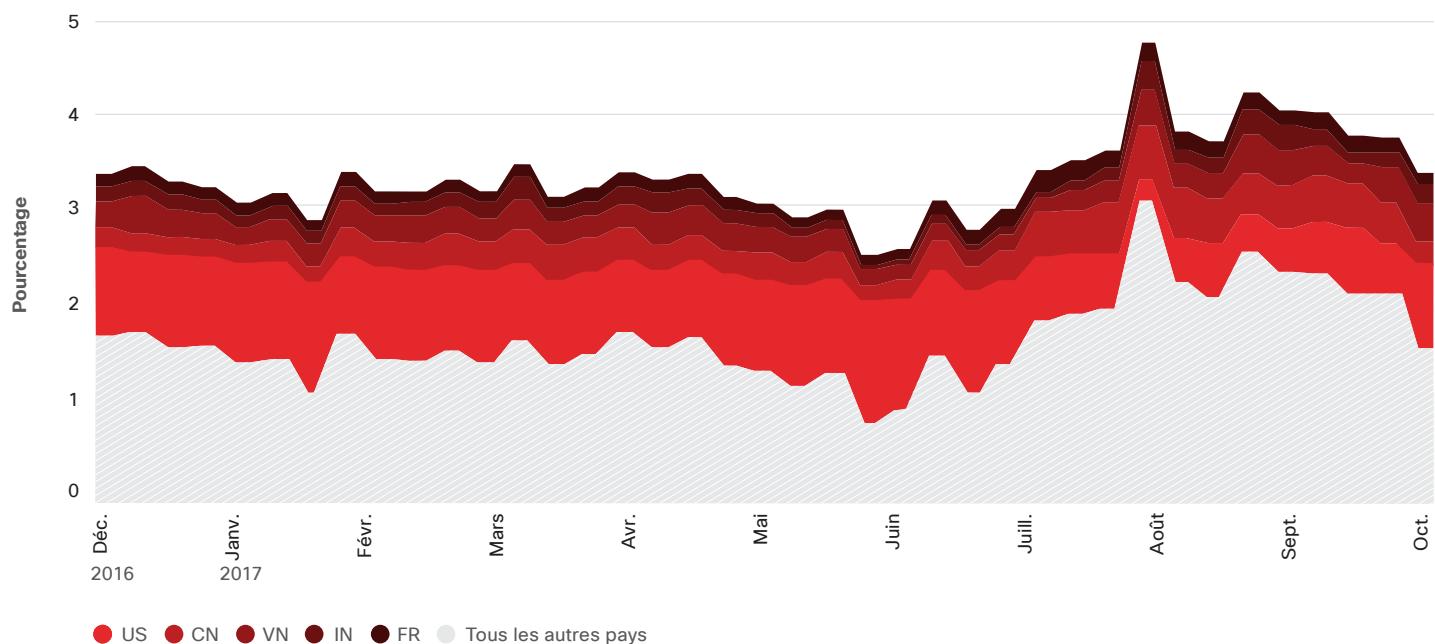
Peu importe l'évolution des menaces, les e-mails et spams malveillants restent des outils essentiels qui permettent aux hackers de distribuer des malwares, car ils acheminent les menaces directement à leur destination. En appliquant la bonne combinaison de techniques d'ingénierie sociale, telles que le phishing et les liens et pièces jointes malveillants, les hackers n'ont qu'à attendre que des utilisateurs sans méfiance activent leurs malwares.

Les fluctuations de l'activité des botnets spammeurs ont un impact sur le volume global

Fin 2016, les experts Cisco ont observé une augmentation notable des campagnes de spams qui semble coïncider avec le déclin des kits d'exploit. Lorsque les kits d'exploit les plus courants comme Angler ont brusquement disparu du marché, les hackers qui les utilisaient se sont tournés en nombre, ou retournés, vers les e-mails malveillants afin de maintenir leur

rentabilité.⁹ Cependant, après cette précipitation initiale, le volume mondial de spams a diminué et s'est stabilisé pendant la majeure partie du premier semestre de 2017. Puis, à la fin mai et au début juin 2017, le volume mondial de spams a chuté avant d'augmenter considérablement entre le milieu et la fin de l'été (voir la Figure 8).

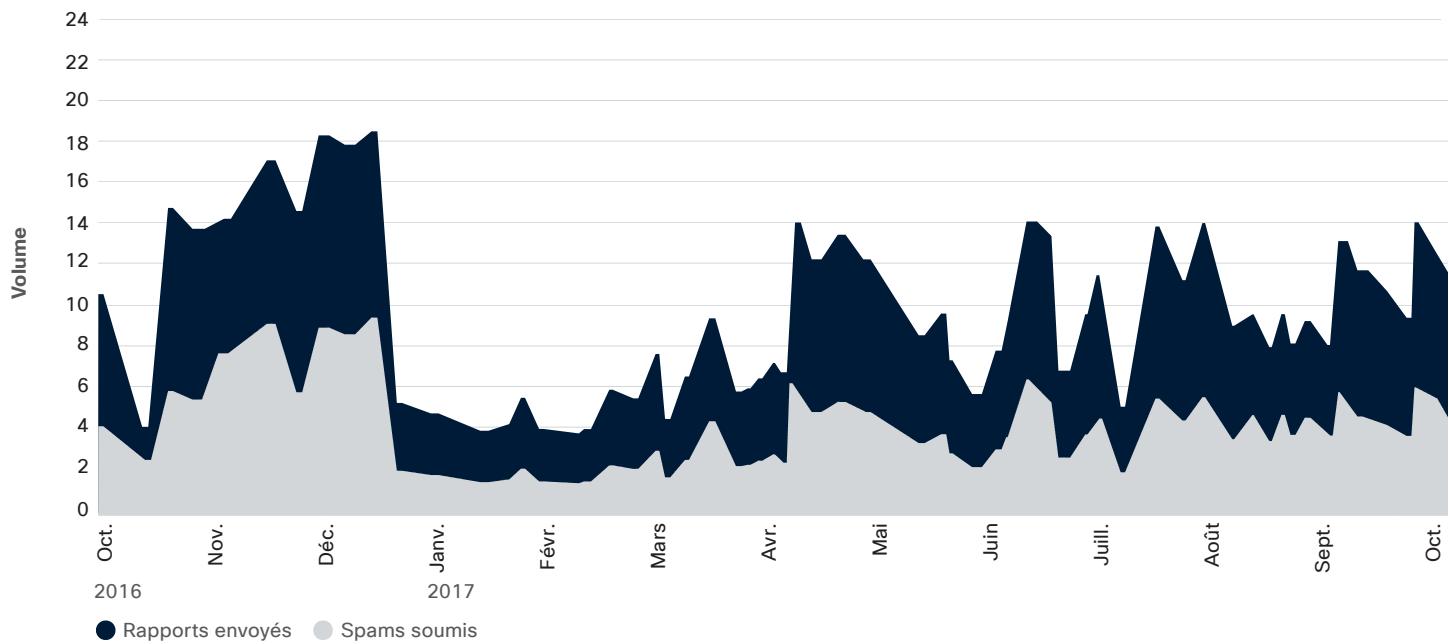
Figure 8 Blocage par réputation des adresses IP par pays, décembre 2016-octobre 2017



Source : Cisco Security Research

⁹ Voir « La recrudescence mondiale du nombre de spams est sans doute liée au déclin des kits d'exploit », p. 18, *Rapport Cisco sur la cybersécurité du 1er semestre 2017* : cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

Figure 9 Activité des botnets spammeurs, octobre 2016–octobre 2017



Source : Cisco SpamCop



Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics

La réduction du volume de spams de janvier à avril 2017 coïncide avec une accalmie de l'activité des botnets spammeurs, comme le montre un graphique interne généré par le service SpamCop de Cisco® (Figure 9).

Les experts Cisco indiquent que le botnet Necurs, un des principaux contributeurs au volume global de spams dans le monde, était actif mais distribuait moins de spams entre janvier et avril. En mai, le botnet diffusait le ransomware Jaff au moyen de campagnes de spams de grande envergure. Les campagnes

comprenaient un fichier PDF intégrant un document Microsoft Office malveillant, et le premier téléchargeur pour le ransomware Jaff.¹⁰ Les experts en sécurité ont découvert une faille dans Jaff, ce qui leur a permis de créer un décrypteur et a forcé les opérateurs de Necurs à revenir rapidement à la distribution de sa menace habituelle, le ransomware Locky.¹¹ Le temps nécessaire aux hackers responsables de Necurs pour se rabattre sur Locky coïncide avec la baisse significative du volume mondial de spams observée au cours des deux premières semaines de juin (Figure 9).

¹⁰ *Jaff Ransomware : Player 2 Has Entered the Game*, de Nick Biasini, Edmund Brumaghin et Warren Mercer, avec la participation de Colin Grady, blog Cisco Talos, mai 2017 : blog.talosintelligence.com/2017/05/jaff-ransomware.html.

¹¹ *Player 1 Limp's Back Into the Ring—Hello Again, Locky !* de Alex Chiu, Warren Mercer et Jaeson Schultz, avec la participation de Sean Baird et Matthew Molyett, blog Cisco Talos, juin 2017 : blog.talosintelligence.com/2017/06/necurs-locky-campaign.html.

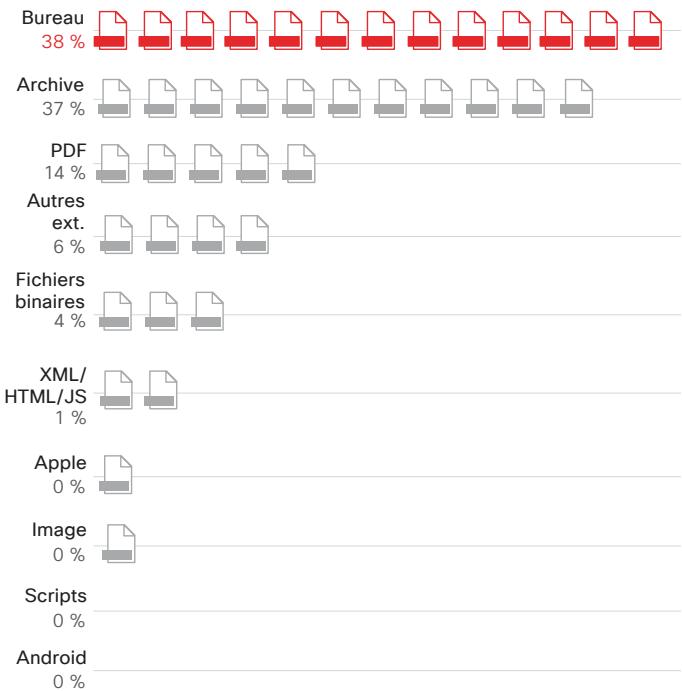
Extensions de fichiers suspectes dans les e-mails : 10 principaux outils des familles de malwares courantes

Les experts Cisco ont analysé les données télémétriques liées aux e-mails de janvier à septembre 2017 pour identifier les types d'extensions de fichiers suspects envoyés par e-mail par les principales familles de malwares. L'analyse a permis d'établir une liste des 10 groupes les plus courants d'extensions de fichiers suspectes (38 %), soit les formats Microsoft Office tels que Word, PowerPoint et Excel (voir la Figure 10).

Les fichiers d'archives, tels que. zip et. jar, représentaient environ 37 % de l'ensemble des extensions de fichiers suspectes observées dans notre étude. Il n'est pas surprenant que les hackers emploient le plus souvent des fichiers d'archives, car ils constituent depuis longtemps des cachettes privilégiées pour les malwares. Les utilisateurs doivent ouvrir les fichiers d'archives pour en voir le contenu, ce qui représente une étape importante dans la chaîne d'infection pour de nombreuses menaces. Les fichiers d'archives malveillants réussissent aussi souvent à déjouer les outils d'analyse automatisés, en particulier lorsqu'ils contiennent des menaces qui nécessitent l'intervention de l'utilisateur pour être activées. Les hackers utilisent également des types de fichiers obscurs, tels que .7z et .rar afin d'échapper aux détections.

Les extensions de fichiers PDF malveillantes complétaient le trio de tête de notre analyse, représentant près de 14 % des extensions de fichiers suspectes observées. (Remarque : la catégorie « Autres extensions » s'applique aux extensions observées dans notre étude qui n'ont pas pu être facilement associées à des types de fichiers connus. Certains types de malwares utilisent des extensions de fichiers aléatoires.)

Figure 10 10 principales extensions de fichiers suspectes, janvier-septembre 2017

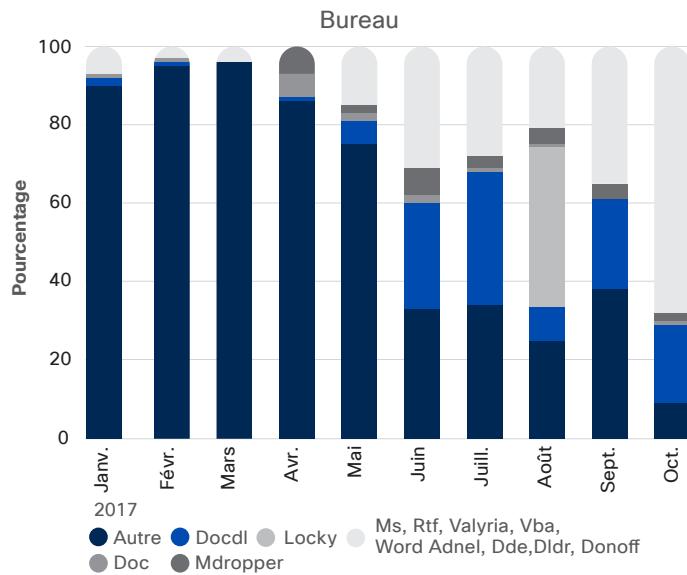


Source : Cisco Security Research

Les Figures 11a-c offrent un aperçu des familles de malwares figurant dans notre enquête qui étaient associées aux trois principaux types d'extensions de fichiers suspectes : fichiers MS Office, archives et PDF. La Figure 12 représente le pourcentage de détections par famille, dans les cas incluant un fichier dont l'extension signalait des données utiles malveillantes. Les pics d'activité correspondent aux campagnes de spams observées durant ces mois-là, selon les experts Cisco. Par exemple, à la fin

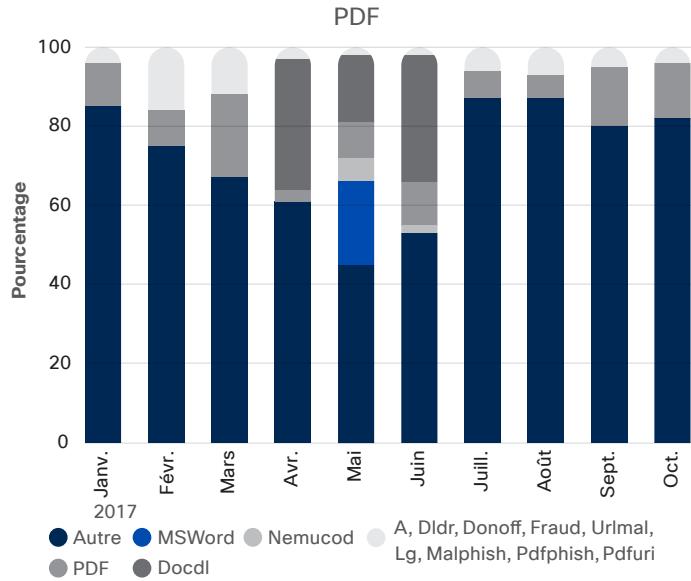
de l'été, d'importantes campagnes de distribution de Nemucod et de Locky, deux menaces qui, souvent, vont de pair, étaient en cours. Nemucod est connu pour envoyer des données utiles malveillantes dans des fichiers d'archives de type .zip qui contiennent du script malveillant, mais ressemblent à des fichiers. doc normaux. (« Dwnldr », comme le montre également la Figure 12, est une variante possible de Nemucod.)

Figure 11a 3 principales relations entre les extensions de fichiers suspectes et les familles de malwares



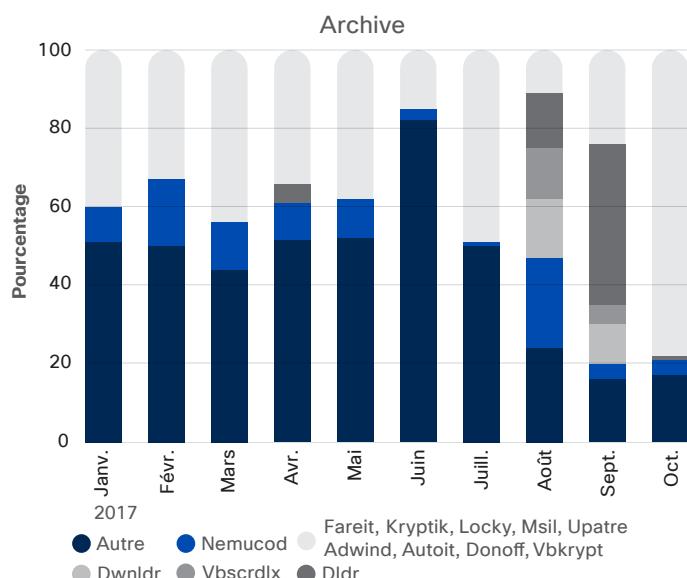
Source : Cisco Security Research

Figure 11b 3 principales relations entre les extensions de fichiers suspectes et les familles de malwares



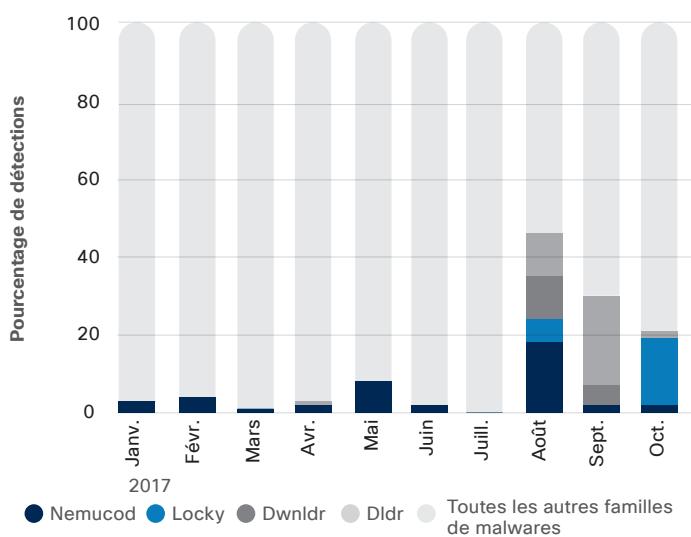
Source : Cisco Security Research

Figure 11c 3 principales relations entre les extensions de fichiers suspectes et les familles de malwares



Source : Cisco Security Research

Figure 12 Profils des principales familles de malwares janvier-octobre 2017



Source : Cisco Security Research

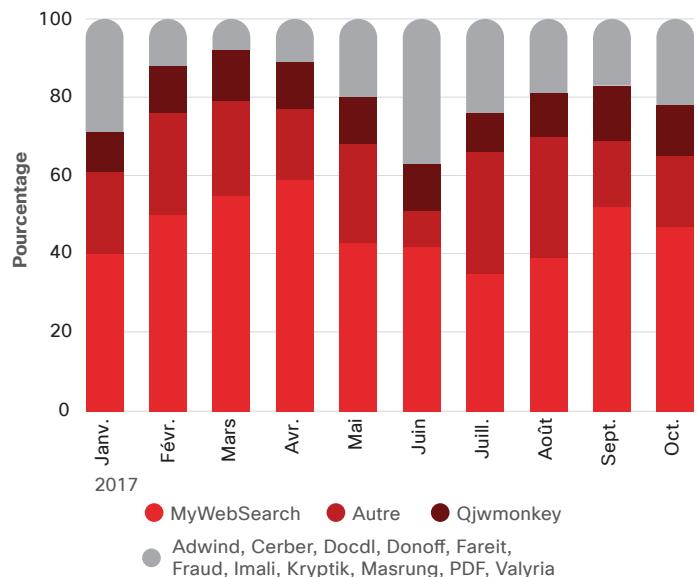
Le spyware MyWebSearch est l'utilisateur le plus actif des « Autres extensions »

Le groupe « Autres extensions » de notre étude comprend plusieurs types de malwares bien connus. Mais MyWebSearch, un logiciel publicitaire malveillant et un mécanisme de piratage des navigateurs qui se présente comme une barre d'outils utile, est l'acteur le plus actif (voir la Figure 13). Il utilise exclusivement des extensions de fichiers .exe, et parfois un seul type par mois. C'est une application potentiellement indésirable (PUA) qui existe depuis plusieurs années et infecte différents types de navigateurs. Elle est souvent associée à des logiciels frauduleux et peut exposer les utilisateurs à des publicités malveillantes.

Notre analyse des types d'extensions de fichiers suspectes montre que, même dans l'environnement de menaces sophistiqué et complexe d'aujourd'hui, l'e-mail reste un canal essentiel à la distribution des malwares. Pour les entreprises, les stratégies de défense de base incluent :

- Implémenter des systèmes de sécurité puissants et complets pour la messagerie.
- Sensibiliser les utilisateurs à l'existence de pièces jointes et de liens malveillants dans les spams et les e-mails de phishing.

Figure 13 MyWebSearch est l'utilisateur le plus actif des « Autres extensions »



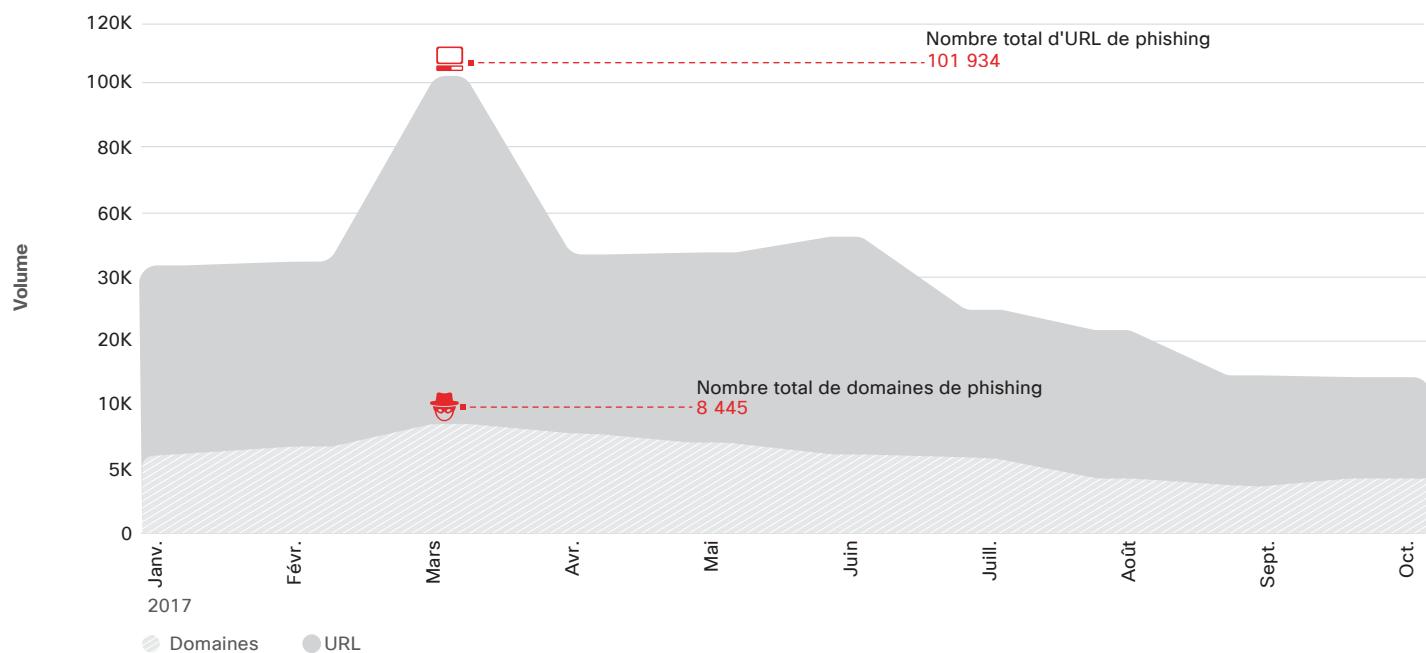
Source : Cisco Security Research

L'ingénierie sociale reste un tremplin important pour les attaques par e-mail

Le phishing et le spear-phishing sont des tactiques bien rodées et très efficaces pour voler les identifiants des utilisateurs ainsi que d'autres informations sensibles. En fait, au cours de ces dernières années, les e-mails de phishing et de spear-phishing ont été à l'origine de certaines failles parmi les plus importantes ayant fait la une des journaux. Parmi deux exemples de 2017, citons une attaque généralisée visant les utilisateurs de Gmail¹² et un piratage des systèmes de distribution d'énergie irlandais.¹³

Pour évaluer la prévalence des URL et des domaines de phishing sur Internet aujourd'hui, les experts Cisco ont examiné des données provenant d'enquêtes sur les e-mails potentiellement catégorisés comme du phishing et signalés par les utilisateurs au moyen de fonctions de Threat Intelligence communautaires anti-phishing. La Figure 14 indique le nombre d'URL et de domaines de phishing observés entre janvier et octobre 2017.

Figure 14 Nombre d'URL et de domaines de phishing observés par mois



Source : Cisco Security Research

Les pics observés en mars et juin peuvent être attribués à deux campagnes différentes. La première semblait cibler les utilisateurs d'un important opérateur de télécommunications. Cette campagne :

- Impliquait 59 651 URL contenant des sous-domaines sous aaaainfomation[dot]org.
- Disposait de sous-domaines qui contenait des chaînes de caractères aléatoires composées de 50 à 62 lettres.

Chaque longueur de sous-domaine (50–62) contenait environ 3 500 URL, ce qui permettait l'utilisation programmable de sous-domaines (par exemple : Cewekonuxykysowegulukzapojygepuqybyteqjohofopefogu[dot]aaaainfomation[dot]org).

Les hackers ont utilisé un service de confidentialité peu coûteux pour enregistrer les domaines observés pendant cette campagne.

12. Massive Phishing Attack Targets Gmail Users, d'Alex Johnson, NBC News, mai 2017 : nbcnews.com/tech/security/massive-phishing-attack-targets-millions-gmail-users-n754501.

13. Hackers target Irish energy networks amid fears of further cyber attacks on UK's crucial infrastructure, de Lizzie Deardon, The Independent, juillet 2017 :

independent.co.uk/news/world/europe/cyber-attacks-uk-hackers-target-irish-energy-network-russia-putin-electricity-supply-board-nuclear-a7843086.html.

Au cours de la deuxième campagne, qui a été plus active en juin, les hackers ont utilisé le nom d'un organisme fiscal légal au Royaume-Uni pour dissimuler leurs agissements. Ils ont employé 12 domaines de premier niveau. Onze de ces domaines correspondaient à des URL comportant six chaînes aléatoires de six caractères (par exemple : jyzwyp[dot]top). Et neuf de ces domaines étaient associés à plus de 1 600 sites de phishing chacun.

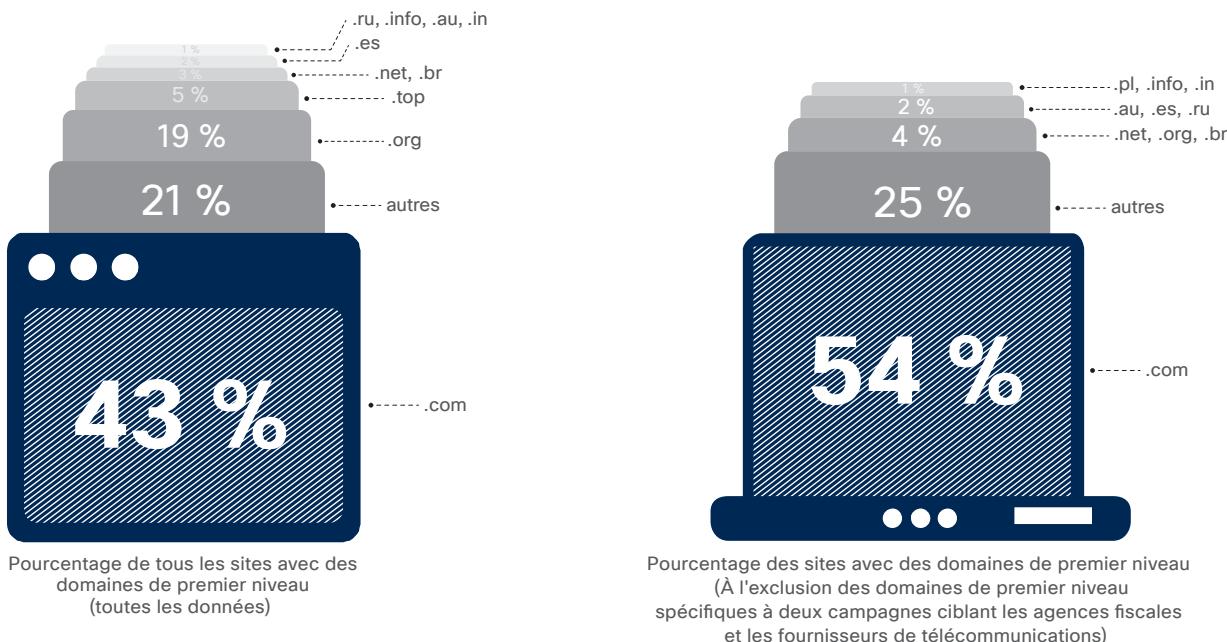
À l'instar de la campagne de mars, les hackers ont enregistré les domaines en utilisant un service de confidentialité pour dissimuler les informations d'enregistrement de domaine. Ils ont enregistré tous les domaines sur une période de deux jours. Le deuxième jour, près de 19 000 URL liées à la campagne ont été observées et toutes ont été découvertes dans un délai de cinq heures (pour en savoir plus sur la rapidité avec laquelle les hackers ont mis à

profit les domaines récemment enregistrés, voir « Utilisation malveillante de ressources légitimes pour les activités de type C2 par porte dérobée », à la [page 24](#)).

Distribution de domaines de premier niveau sur des sites de phishing connus

Notre analyse des sites de phishing au cours de la période de janvier à août 2017 a révélé que les hackers employaient 326 domaines de premier niveau uniques pour ces activités, dont les extensions .com, .org, .top (principalement en raison de la campagne dirigée vers les organismes fiscaux britanniques), ainsi que des domaines de premier plan spécifiques à chaque pays (voir la Figure 15). L'utilisation de domaines de premier plan moins connus peut être bénéfique pour les hackers, car ils sont généralement peu coûteux et offrent souvent une protection de la confidentialité bon marché.

Figure 15 Distribution de domaines de premier niveau sur des sites de phishing connus



Source : Cisco Security Research

Les entreprises doivent continuer à surveiller de près cette « ancienne » menace

En 2017, des dizaines de milliers de tentatives de phishing ont été signalées chaque mois aux services communautaires de Threat Intelligence anti-phishing inclus dans notre analyse. Parmi les tactiques et outils couramment utilisés par les hackers pour mener des campagnes de phishing, citons :

- **L'occupation de domaine :** les noms attribués aux domaines ressemblent à des domaines valides (par exemple : cisc0[dot]com).
- **La dissimulation de domaine :** des sous-domaines sont ajoutés sous un domaine valide à l'insu du propriétaire (par exemple : badstuff[dot]cisco[dot]com).
- **L'enregistrement de domaines malveillants :** un domaine est créé à des fins malveillantes (par exemple : viqbe[dot]top).
- **Les raccourcisseurs d'URL :** une URL malveillante est déguisée avec un raccourcisseur d'URL (par exemple : bitly[dot]com/random-string).

Remarque : dans les données que nous avons examinées, Bitly.com était l'outil de raccourcissement d'URL le plus utilisé par les hackers. Les URL raccourcies malveillantes représentaient 2 % des sites de phishing dans notre étude. Ce chiffre a atteint 3,1 % en août.

- **Les services de sous-domaine :** un site est créé sous un serveur de sous-domaine (par exemple : mybadpage[dot]000webhost[dot]com).

Les hackers à l'origine de phishing et de « spear phishing » affinent en permanence leurs méthodes d'ingénierie sociale pour amener les utilisateurs à cliquer sur des liens malveillants ou à visiter des pages web frauduleuses, puis à fournir des informations d'identification ou d'autres données à haute valeur ajoutée. Il est crucial de continuer à former et à responsabiliser les utilisateurs et de mettre en place des technologies de sécurité de la messagerie pour lutter contre ces menaces.

TACTIQUES DE CONTOURNEMENT DES SANBOXES

Les hackers apprécient tout particulièrement de développer des menaces capables d'échapper aux environnements de sandboxing de plus en plus sophistiqués. Les chercheurs spécialisés Cisco ont analysé des pièces jointes malveillantes conçues pour déjouer les sandboxes et ont découvert que nombre d'échantillons malveillants qui utilisaient une telle technique présentaient des pics acérés, puis étaient rapidement abandonnés. C'est encore un autre exemple qui prouve que les hackers multiplient rapidement les tentatives de contournement des défenses dès qu'ils trouvent une technique efficace.

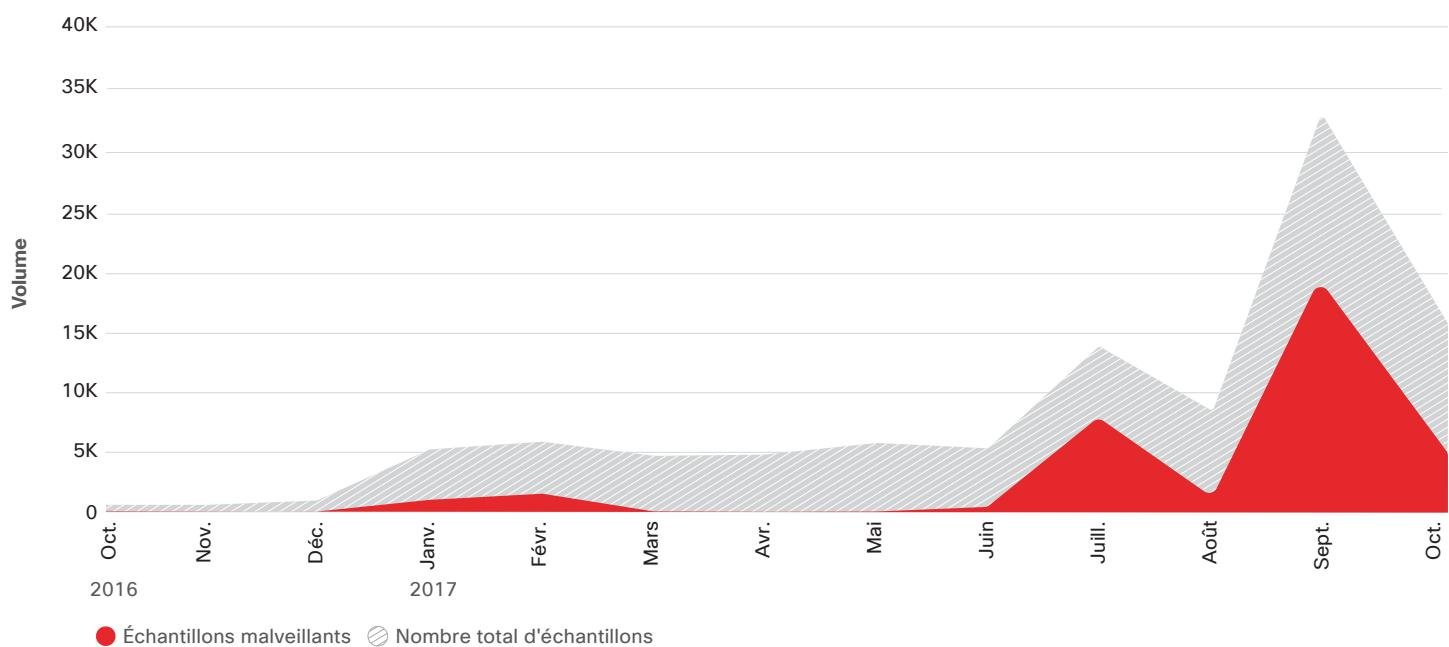
Les concepteurs de malwares arrivent à duper les sandboxes

En septembre 2017, les chercheurs Cisco ont remarqué qu'un grand nombre d'échantillons diffusaient une charge utile malveillante après la fermeture d'un document (Figure 16). Dans ce cas, le programme malveillant est déclenché avec l'événement « document_close ». La technique est efficace car, bien souvent, les documents ne sont pas fermés après avoir été ouverts et analysés par la sandbox. Étant donné que la sandbox ne ferme pas explicitement le document, les pièces jointes sont considérées comme sûres et envoyées aux destinataires. Lorsque le destinataire ouvre la pièce jointe du document, puis referme ensuite le document, la charge utile malveillante se diffuse. Les

sandboxes qui ne détectent pas correctement les actions déclenchées à la fermeture du document peuvent être contournées par le biais de cette technique.

L'événement « document_close » est une option intéressante pour les hackers. Il tire parti de la fonctionnalité de la macro intégrée dans Microsoft Office ainsi que de l'habitude qu'ont les utilisateurs à ouvrir les pièces jointes qu'ils estiment pertinentes. Une fois que les utilisateurs réalisent que la pièce jointe n'est pas pertinente, ils la ferment, ce qui déclenche les macros dans lesquelles le malware est dissimulé.

Figure 16 Volume élevé de documents Microsoft Word malveillants utilisant l'invite de fermeture de fonction observé en septembre 2017



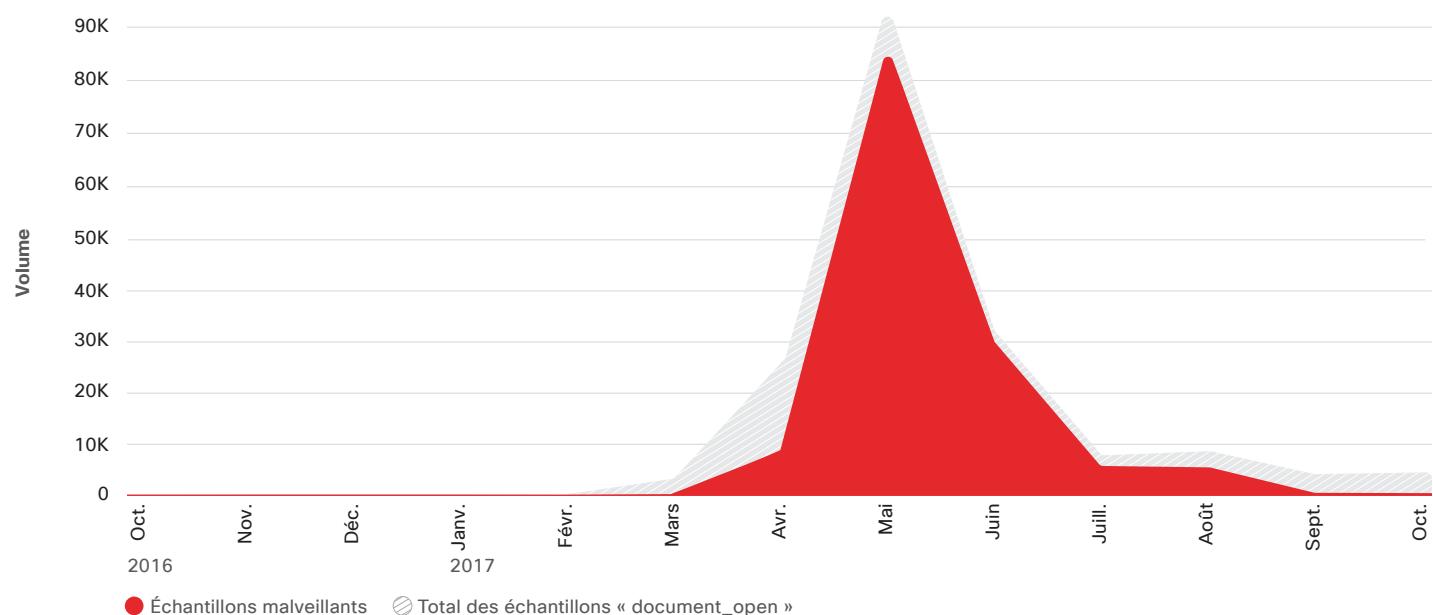
Source : Cisco Security Research

Certains hackers contournent le sandboxing en camouflant le type de document qui renferme la charge utile malveillante. Comme illustré dans la Figure 17, nous avons détecté une attaque importante en mai 2017 qui intégrait des documents Word malveillants dans des documents PDF. Il était possible de contourner les sandboxes qui se contentent de détecter et d'ouvrir le fichier PDF au lieu d'ouvrir et d'analyser aussi le document Word incorporé. Le document PDF incitait généralement l'utilisateur à cliquer sur un lien pour ouvrir le

document Word, ce qui déclenchait le comportement malveillant. Les sandboxes qui n'ouvrent et n'analysent pas les documents incorporés dans les fichiers PDF peuvent être contournées grâce à cette technique.

Après avoir observé un pic d'échantillons malveillants dans ces fichiers PDF, nos chercheurs spécialisés ont redéfini la sandbox pour détecter si les fichiers PDF contenait des actions ou incitaient à ouvrir des documents Word intégrés.

Figure 17 Attaque de grande ampleur en mai 2017 impliquant des documents PDF avec documents Word malveillants incorporés



Source : Cisco Security Research

Les pics d'échantillons malveillants qui utilisent différentes techniques de contournement des sandboxes mettent en évidence la volonté des hackers d'appliquer une méthode qui semble porter ses fruits pour eux ou pour d'autres cybercriminels. En outre, si des hackers se donnent la peine de créer des programmes malveillants et l'infrastructure associée, ils attendent un retour sur investissement. S'ils pensent que le malware peut déjouer les tests des sandboxes, ils augmenteront le nombre de tentatives d'attaques et ainsi d'utilisateurs infectés.

Les chercheurs Cisco recommandent d'utiliser une sandbox qui englobe des fonctionnalités « sensibles au contexte » pour s'assurer que le malware qui utilise les tactiques décrites ci-dessus ne réussisse pas à contourner l'analyse de la sandbox. Par exemple, la technologie de sandboxing devrait tenir compte des métadonnées des échantillons qu'elle analyse, par exemple en déterminant si l'échantillon intègre une action à la fermeture du document.

DÉTOURNEMENT DES SERVICES CLOUD ET D'AUTRES RESSOURCES LÉGITIMES

À mesure que les applications, les données et les identités basculent vers le cloud, les équipes de sécurité doivent gérer les risques liés à la perte de contrôle du périmètre réseau classique. Les hackers profitent du fait que les équipes de sécurité ont du mal à protéger des environnements IoT et cloud en pleine croissance. L'une des raisons est qu'elles ne savent pas qui est précisément chargé de protéger ces environnements.

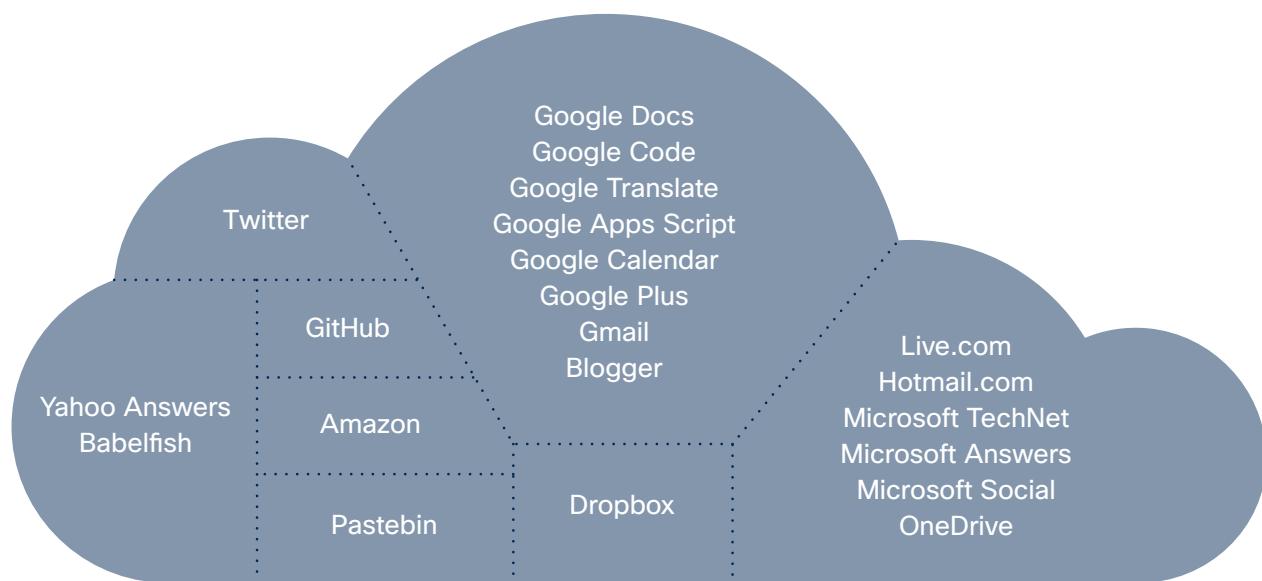
Pour relever ce challenge, les entreprises devront combiner des bonnes pratiques, des technologies de sécurité avancées comme l'apprentissage automatique, et même certaines méthodologies expérimentales, en fonction des services qu'elles utilisent pour mener à bien leurs activités et de l'évolution des menaces dans cet espace.

L'utilisation malveillante de ressources légitimes pour les activités de type C2 par porte dérobée

Lorsque les hackers utilisent des services légitimes pour des activités de type contrôle-commande (C2), les équipes de sécurité ne parviennent quasiment jamais à identifier le trafic réseau malveillant car il imite le comportement du trafic réseau légitime. Les hackers se couvrent à l'aide du « bruit » d'Internet, parce qu'un très grand nombre d'utilisateurs font appel aujourd'hui à des services comme Google Docs et Dropbox dans le cadre de leur travail, que ces services soient ou non proposés ou systématiquement approuvés par leurs employeurs.

La Figure 18 présente plusieurs services légitimes bien connus que les chercheurs et Anomali, un partenaire Cisco fournisseur de Threat Intelligence, ont observé dans des activités de C2 par porte dérobée¹⁴ au cours des dernières années. (Remarque : ces types de services étaient confrontés à un dilemme dans le cadre de la lutte contre les abus : comme il était plus difficile pour les utilisateurs de créer des comptes et d'utiliser leurs services, leur capacité à générer des revenus s'en trouvait affectée.)

Figure 18 Exemples de services légitimes utilisés par des malwares pour des activités de type C2



Source : Anomali

¹⁴ Anomali définit un schéma de C2 comme suit : « l'ensemble des adresses IP, des domaines, des services légitimes et des systèmes distants qui font partie de... l'architecture de communication » du malware.

D'après les recherches d'Anomali, les auteurs de menaces persistantes avancées et les groupes soutenus par un État faisaient partie des premiers hackers à utiliser des services légitimes pour les activités de type C2. Cependant, cette technique sophistiquée est désormais exploitée par un plus grand nombre de hackers de l'économie parallèle. En effet, en utilisant des services légitimes pour les activités de type C2, les hackers peuvent facilement :

- Créer de nouveaux comptes sur ces services.
- Créer une page web accessible publiquement sur Internet.
- Contourner le chiffrement des protocoles de C2. (Au lieu d'ajouter le chiffrement à des serveurs de C2 ou de l'intégrer dans le programme malveillant, les hackers peuvent simplement adopter le certificat SSL d'un service légitime.)
- Adapter et transformer des ressources à la volée. (Les hackers peuvent réutiliser des implants d'attaques sans réutiliser des adresses IP ou DNS, par exemple.)
- Limiter les risques d'avoir à détruire leur infrastructure. (Les hackers qui utilisent des services légitimes pour leurs activités de type C2 n'ont pas besoin de coder en dur le malware avec des adresses IP ou des domaines. Au terme de leur opération, il suffit de désactiver leurs pages de services légitimes et personne ne découvrira jamais les adresses IP.)
- Les hackers apprécient cette technique, car elle leur permet de réduire leurs frais et améliore leur retour sur investissement.

Cette utilisation de services légitimes pour des activités de type C2 pose des défis de taille aux acteurs de la protection :

Les services légitimes sont difficiles à bloquer

D'un point de vue purement professionnel, est-ce que les entreprises peuvent envisager de bloquer des services légitimes comme Twitter ou Google ?

Les services légitimes sont souvent chiffrés et donc difficiles à inspecter par nature

Le déchiffrement SSL est onéreux et difficile à mettre en œuvre. Le malware dissimule ses communications dans le trafic chiffré. Il est donc plus difficile, voire impossible, pour les équipes de sécurité d'identifier le trafic malveillant.

L'utilisation de services légitimes permet de manipuler les informations relatives au domaine et au certificat, et complique l'attribution

Les hackers n'ont pas besoin d'enregistrer des domaines car le compte du service légitime est considéré comme l'adresse de C2 initiale. Ils n'ont pas non plus besoin de continuer à enregistrer des certificats SSL ou d'utiliser des certificats SSL autosignés pour les activités de type C2. Ces deux tendances auront évidemment un impact négatif sur les flux d'indicateurs pour le filtrage par réputation et la création de listes noires d'indicateurs, qui dépendent des domaines et des certificats qui viennent d'être créés ou enregistrés et des adresses IP qui y sont connectées.

Il est difficile de détecter l'utilisation de services légitimes pour des activités de type C2. Toutefois, les chercheurs Anomali recommandent aux acteurs de la protection d'appliquer des méthodologies expérimentales. Ils pourraient, par exemple, identifier les programmes malveillants qui utilisent des services légitimes pour les activités de C2 en recherchant les éléments suivants :

- Des connexions à des services légitimes hors d'un navigateur ou d'une application
- Des tailles de réponse uniques ou faibles provenant de services légitimes
- Des échanges de certificats trop réguliers avec des services légitimes
- Des lots d'échantillons de sandboxing pour des appels DNS suspects aux services légitimes

Tous ces comportements uniques méritent une analyse plus poussée des processus et des programmes sources.¹⁵

¹⁵ Pour en savoir plus sur ces méthodes expérimentales et sur la manière dont les hackers utilisent des services légitimes pour leurs activités de type C2, téléchargez le document de recherche d'Anomali, *Rise of Legitimate Services for Backdoor Command and Control*, disponible à cette adresse : Anomali.Cdn.rackfoundry.net/files/Anomali-Labs-Reports/legit-services.pdf.

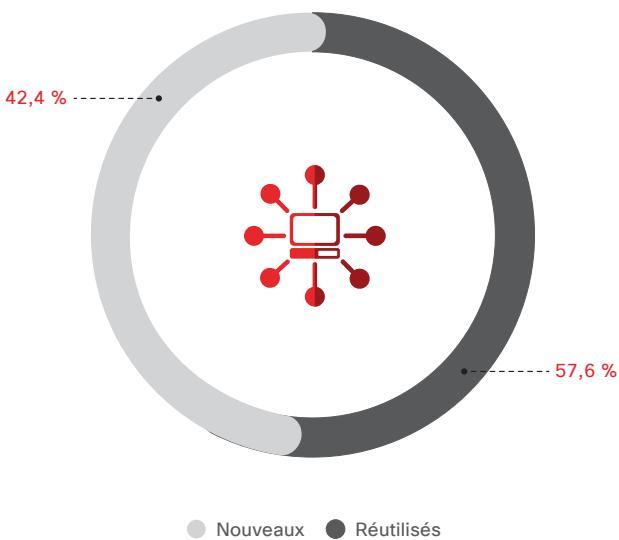
Tirer pleinement parti des ressources

Les chercheurs Cisco en matière de sécurité ont analysé les noms de requêtes uniques récemment détectés (domaines) associés à des requêtes DNS effectuées pendant sept jours en août 2017. Sachez que l'expression « récemment détecté » dans ce cas ne dépend pas du tout de la date de création d'un domaine. Elle fait référence à la première fois qu'une technologie de sécurité cloud Cisco a « repéré » un domaine au cours de la période d'observation.

Cette recherche vise à mieux comprendre à quelle fréquence les hackers utilisent et réutilisent des domaines enregistrés dans leurs attaques. Cerner le comportement du hacker au niveau du domaine peut aider les acteurs de la protection à identifier les domaines malveillants et les sous-domaines associés, qui doivent être bloqués à l'aide d'outils de première ligne de défense, comme les plates-formes de sécurité cloud.

Pour que nos chercheurs puissent uniquement se concentrer sur le groupe principal de domaines enregistrés uniques (environ 4 millions au total), les sous-domaines ont été supprimés du jeu de domaines récemment détectés. Seul un faible pourcentage de domaines enregistrés de cet échantillon a été désigné comme malveillant. Parmi les domaines enregistrés malveillants, plus de la moitié (environ 58 %) étaient réutilisés, comme illustré dans la Figure 19.

Figure 19 Pourcentage de nouveaux domaines par rapport aux domaines réutilisés



Source : Cisco Security Research

Ces résultats suggèrent que, même si la plupart des hackers créent de nouveaux domaines pour leurs campagnes, ils sont nombreux à essayer d'obtenir le meilleur retour sur investissement en lançant plusieurs campagnes à partir d'un seul domaine. L'enregistrement d'un domaine peut être coûteux, surtout vu l'ampleur des campagnes des hackers et les systèmes de détection à contourner.

Un cinquième des domaines malveillants est utilisé rapidement

Les hackers attendent souvent le bon moment pour utiliser un domaine : plusieurs jours, mois, voire plusieurs années après l'enregistrement. Cependant, les chercheurs Cisco ont observé qu'un pourcentage significatif de domaines malveillants (environ 20 %) était utilisé dans des campagnes moins d'une semaine après leur enregistrement (voir Figure 20).

Figure 20 Délais après enregistrement des domaines malveillants

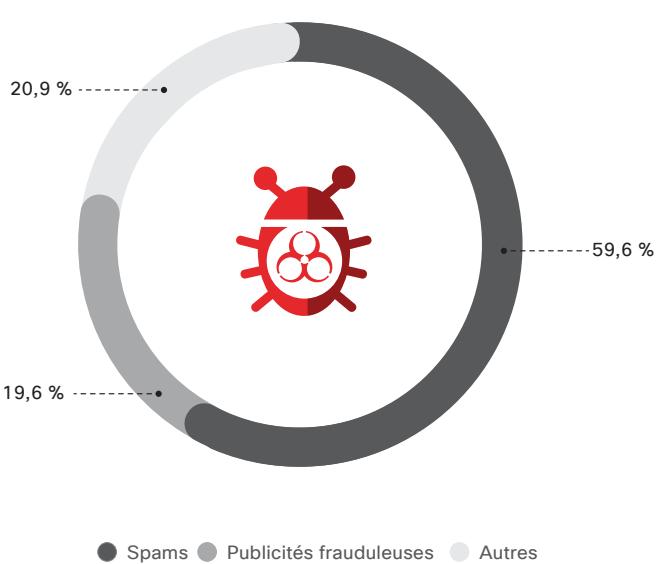


Source : Cisco Security Research

Bon nombre de nouveaux domaines sont liés à des campagnes de publicité malveillante

La plupart des domaines malveillants que nous avons analysés étaient associés à des campagnes de spam (environ 60 %). Presque un cinquième des domaines était relié à des campagnes de publicité malveillante (voir Figure 21). Les publicités malveillantes sont devenues indispensables pour diriger les utilisateurs vers des kits d'exploit, notamment ceux qui diffusent des ransomwares.

Figure 21 Catégories d'attaques



Source : Cisco Security Research

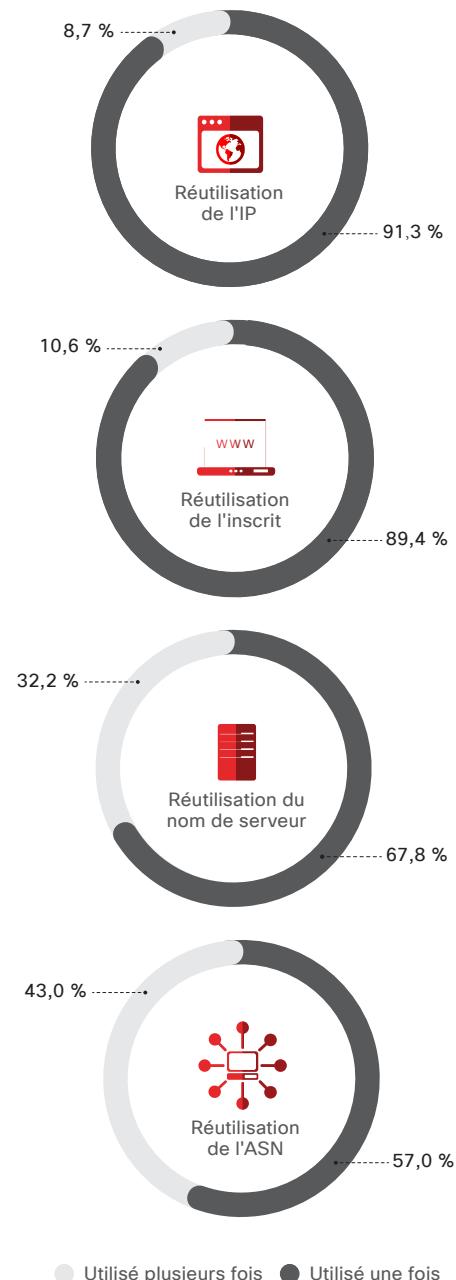
Certaines techniques bien rodées relatives aux domaines servent à créer des campagnes de publicité malveillante, comme la dissimulation de domaine. Avec cette technique, les hackers volent les informations d'identification de comptes de domaine légitimes pour créer des sous-domaines qui dirigent vers des serveurs malveillants. Une autre tactique consiste à utiliser les services DNS dynamiques gratuits pour générer des sous-domaines et des domaines malveillants. Les hackers peuvent ainsi fournir des charges utiles malveillantes à partir d'adresses IP d'hébergement qui changent constamment, soit des ordinateurs infectés, soit des sites web publics compromis.

Les domaines réutilisent les ressources de l'infrastructure

Les domaines enregistrés malveillants de notre échantillon semblaient également réutiliser des ressources de l'infrastructure, comme les adresses e-mail des inscrits, les adresses IP, les

numéros de systèmes autonomes et les serveurs de noms (voir Figure 22). Cela prouve encore une fois que les hackers essaient de tirer le meilleur parti de leurs investissements dans les nouveaux domaines et de préserver leurs ressources, d'après nos chercheurs. Par exemple, une même adresse IP peut être utilisée par plusieurs domaines. Par conséquent, un cybercriminel qui planifie une campagne pourrait décider d'investir dans quelques adresses IP et une série de noms de domaine à la place de serveurs qui coûtent plus cher.

Figure 22 Réutilisation de l'infrastructure par des domaines enregistrés malveillants



Source : Cisco Security Research

Les ressources réutilisées par les domaines enregistrés vous indiquent si le domaine est susceptible d'être malveillant. Par exemple, les adresses e-mail ou les adresses IP des inscrits sont généralement peu réutilisées. Dans le cas contraire, cela suggère un comportement suspect. Les acteurs de la protection savent pertinemment qu'en bloquant ces domaines, les activités de l'entreprise n'en seront pas impactées.

Dans la plupart des cas, il ne sera pas possible de réaliser un blocage statique des numéros de systèmes autonomes et des serveurs de noms. Cependant, les techniques de réutilisation des domaines enregistrés méritent d'être analysées pour savoir si certains domaines doivent être bloqués.

À l'aide d'outils intelligents de sécurité cloud qui agissent comme une première ligne de défense et qui identifient et analysent les éventuels sous-domaines et domaines malveillants, les équipes

de sécurité peuvent suivre la piste d'un hacker et répondre aux questions suivantes :

- Quelle adresse IP le domaine traduit-il ?
- Quel numéro de système autonome est associé à cette adresse IP ?
- Qui a enregistré le domaine ?
- Quels autres domaines sont associés à ce domaine ?

Les réponses peuvent aider les acteurs de la protection à affiner les politiques de sécurité et à bloquer les attaques, mais également à empêcher les utilisateurs de se connecter à des destinations malveillantes sur Internet alors qu'ils sont connectés au réseau de l'entreprise.

Les technologies DevOps, cibles des ransomwares

En 2017, les attaques de ransomwares DevOps se sont multipliées, à commencer par une campagne en janvier qui a ciblé une plate-forme open source de base de données, MongoDB.¹⁶ Des hackers ont chiffré des instances MongoDB publiques, puis ont demandé de payer une rançon en échange des clés et des logiciels de déchiffrement. Peu après, ils ont décidé de compromettre des bases de données, telles que CouchDB et Elasticsearch, à l'aide d'un ransomware ciblé sur les serveurs.

Rapid7 est un partenaire Cisco et fournisseur de solutions d'analyse et de données de sécurité. Comme l'ont expliqué les chercheurs de Rapid7 dans notre *rapport Cisco du 1er semestre 2017 sur la cybersécurité*, les services DevOps sont souvent déployés de façon incorrecte ou intentionnellement laissés ouverts pour faciliter l'accès des utilisateurs légitimes, mais ils restent également ouverts aux attaques.

Rapid7 analyse régulièrement Internet à la recherche de ces technologies et a catalogué les instances ouvertes et les instances rançonnées. Certains services DevOps qu'ils ont repérés lors de leurs analyses peuvent contenir des

informations personnelles identifiables, basées sur les noms des tables exposées sur Internet.

Afin de réduire le risque d'exposition aux attaques de ransomwares DevOps, les entreprises qui utilisent des instances Internet publiques de technologies DevOps devraient :

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

Pour plus d'informations sur les recherches de Rapid7, consultez la section « Ne laissez pas les technologies de DevOps mettre en danger votre entreprise » dans le *rapport Cisco du 1er semestre 2017 sur la cybersécurité*.

¹⁶ « 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](http://www.pcworld.com/article/3157417/security/after-mongodb-ransomware-groups-hit-exposed-elasticsearch-clusters.html).

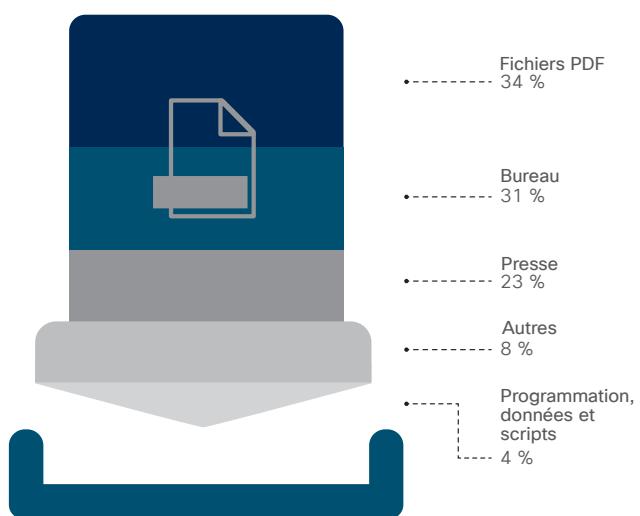
Menaces internes : tirer parti du cloud

Dans les précédents rapports de sécurité, nous avons parlé des atouts des autorisations OAuth et des priviléges de super utilisateur qui permettent de déterminer qui peut entrer dans les réseaux et comment accéder aux données.¹⁷ Pour examiner de manière plus poussée l'impact de l'activité des utilisateurs sur la sécurité, les chercheurs Cisco ont récemment analysé les tendances d'exfiltration des données. Ils ont utilisé un algorithme d'apprentissage automatique pour dresser le profil de 150 000 utilisateurs dans 34 pays qui font tous appel à des opérateurs cloud, de janvier à juin 2017. L'algorithme a pris en compte le volume de documents téléchargés, mais aussi des variables comme l'heure à laquelle les téléchargements ont été effectués, les adresses IP et les emplacements.

Après avoir profilé les utilisateurs pendant six mois, nos chercheurs ont étudié les anomalies pendant 1 mois et demi. Il en ressort que 0,5 % des utilisateurs sont à l'origine de téléchargements suspects. Ce chiffre est relativement faible, mais ces utilisateurs ont téléchargé au total plus de 3,9 millions de documents depuis les systèmes cloud de l'entreprise, soit une moyenne de 5 200 documents par utilisateur sur 1 mois et demi. Parmi les téléchargements suspects, 62 % ont été effectués en dehors des heures d'ouverture normales et 40 % ont eu lieu le week-end.

Les chercheurs Cisco ont également réalisé une analyse du texte des titres des 3,9 millions de documents téléchargés de manière suspecte.

Figure 23 Documents les plus couramment téléchargés



Source : Cisco Security Research

Un des mots-clés qui apparaissait le plus souvent dans les titres des documents était « données ». D'autres mots-clés très souvent associés au terme « données » étaient « collaborateur » et « client ». Les téléchargements concernaient à 34 % des documents PDF et à 31 % des documents Microsoft Office (voir Figure 23).

Les algorithmes d'apprentissage automatique ont permis d'obtenir une visibilité plus nuancée sur l'activité des utilisateurs dans le cloud, qui allait au-delà du nombre de téléchargements. D'après notre analyse, 23 % des utilisateurs ont réalisé des téléchargements suspects plus de trois fois, en commençant généralement par un petit nombre de documents. Le volume augmentait progressivement à chaque fois jusqu'à atteindre un pic (Figure 24).

Les algorithmes d'apprentissage automatique promettent une meilleure visibilité sur le comportement du cloud et des utilisateurs. Si les acteurs de la protection peuvent prévoir le comportement des utilisateurs en matière de téléchargements, ils évitent de consacrer du temps à rechercher les comportements légitimes. Ils peuvent également intervenir pour arrêter une attaque éventuelle ou une exfiltration potentielle des données avant qu'elles ne se produisent.

Figure 24 Les algorithmes d'apprentissage automatique capturent les comportements de téléchargement suspects



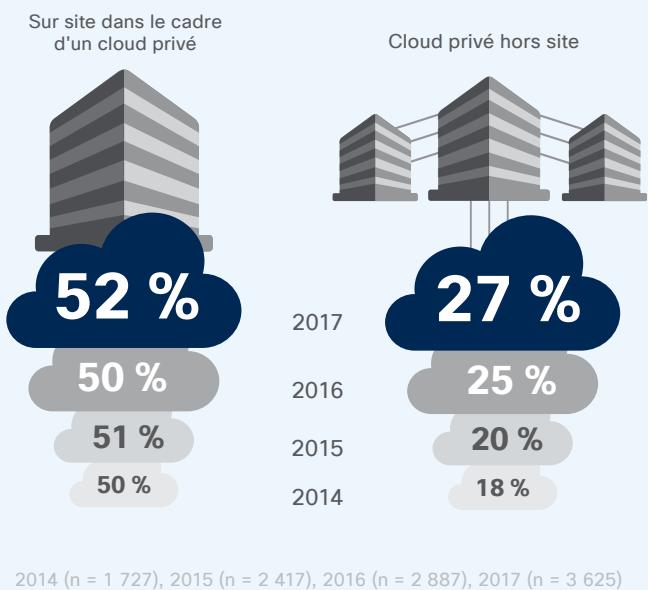
Source : Cisco Security Research

17 Rapport Cisco du 1er semestre 2017 sur la cybersécurité : cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

i Enquête Cisco 2018 sur l'efficacité des mesures de sécurité : la sécurité est perçue comme le principal bénéfice de l'hébergement des réseaux dans le cloud

L'infrastructure cloud et sur site est de plus en plus utilisée, d'après l'Enquête Cisco 2018 sur l'efficacité des mesures de sécurité, même si de nombreuses entreprises hébergent toujours leur réseau sur site. Dans l'enquête 2017, 27 % des responsables sécurité utilisaient des clouds privés hors site, par rapport à 25 % en 2016 et 20 % en 2015 (Figure 25). 52 % indiquaient que leurs réseaux étaient hébergés sur site dans le cadre d'un cloud privé.

Figure 25 Plus d'entreprises utilisent des clouds privés



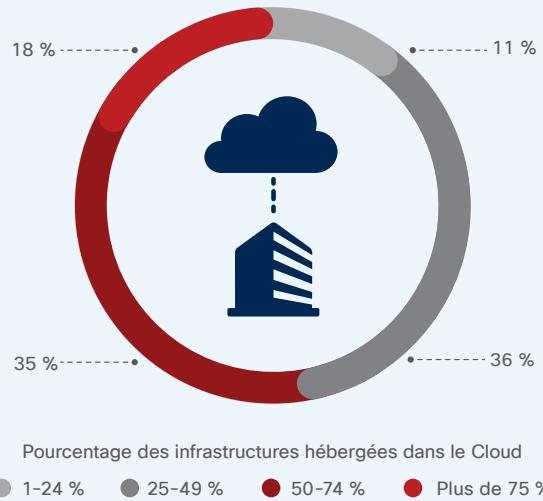
Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Parmi les entreprises utilisant le cloud, 36 % hébergent entre 25 et 49 % de leur infrastructure dans le cloud, tandis que 35 % y hébergent entre 50 et 74 % de leur infrastructure (Figure 26).

Pour le personnel de sécurité, le principal bénéfice d'héberger les réseaux dans le cloud est de renforcer leur protection. 57 % hébergent des réseaux dans le cloud pour améliorer la sécurité des données, 48 % pour l'évolutivité et 46 % pour la facilité d'utilisation (Figure 27).

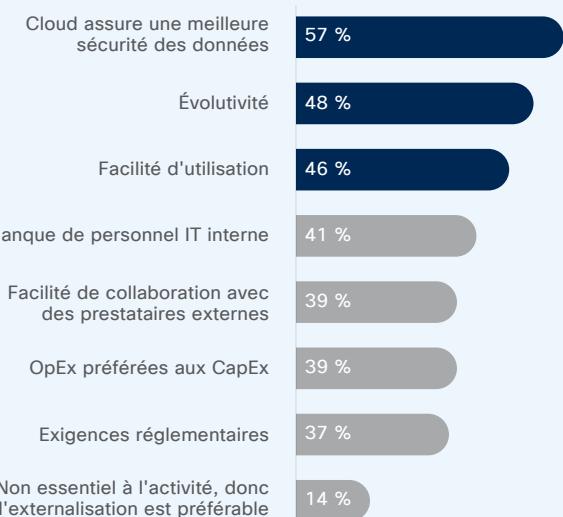
Les personnes interrogées ont également indiqué qu'elles cherchaient peut-être à investir dans des solutions de courtage de services de sécurité pour l'accès au cloud (CASB) pour renforcer la sécurité des environnements cloud.

Figure 26 53 % des entreprises hébergent au moins la moitié de leur infrastructure dans le cloud



Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Figure 27 57 % pensent que le cloud accroît la sécurité des données



Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics

IoT ET ATTAQUES DDoS

L'IoT poursuit son évolution, mais les hackers exploitent déjà les faiblesses de sécurité des appareils connectés à l'IoT pour accéder aux systèmes, notamment aux systèmes de contrôle industriels qui prennent en charge les infrastructures essentielles. Les botnets IoT gagnent également en taille et en puissance. Ils sont désormais capables de lancer de puissantes attaques qui pourraient gravement perturber Internet. Les hackers se sont fixé un nouvel objectif : exploiter davantage la couche applicative. Toutefois, de nombreux responsables sécurité ne connaissent pas, ou ignorent la menace que représentent les botnets IoT. Les entreprises continuent d'ajouter des appareils connectés à l'IoT à leurs environnements IT sans trop se soucier de la sécurité. Pire encore, elles ne prennent pas le temps d'évaluer le nombre d'objets IoT connectés à leurs réseaux. Il est donc très facile pour les hackers de prendre le contrôle de l'IoT.

Peu d'entreprises considèrent les botnets IoT comme une menace imminente, alors qu'elles devraient

Les botnets IoT suivent le même rythme que l'IoT. Ces botnets gagnent en maturité et évoluent de plus en plus, ce qui pousse les hackers à les utiliser pour lancer des attaques DDoS de plus grande ampleur. Radware, un partenaire Cisco, a analysé trois des plus grands botnets IoT, à savoir Mirai, Brickerbot et Hajime, dans le *rapport Cisco du 1er semestre 2017 sur la cybersécurité* et reparle des botnets IoT dans notre dernier rapport pour mettre l'accent sur la gravité de cette menace.¹⁸ Ses recherches démontrent que seulement 13 % des entreprises estiment que les botnets IoT constitueront une menace majeure en 2018.

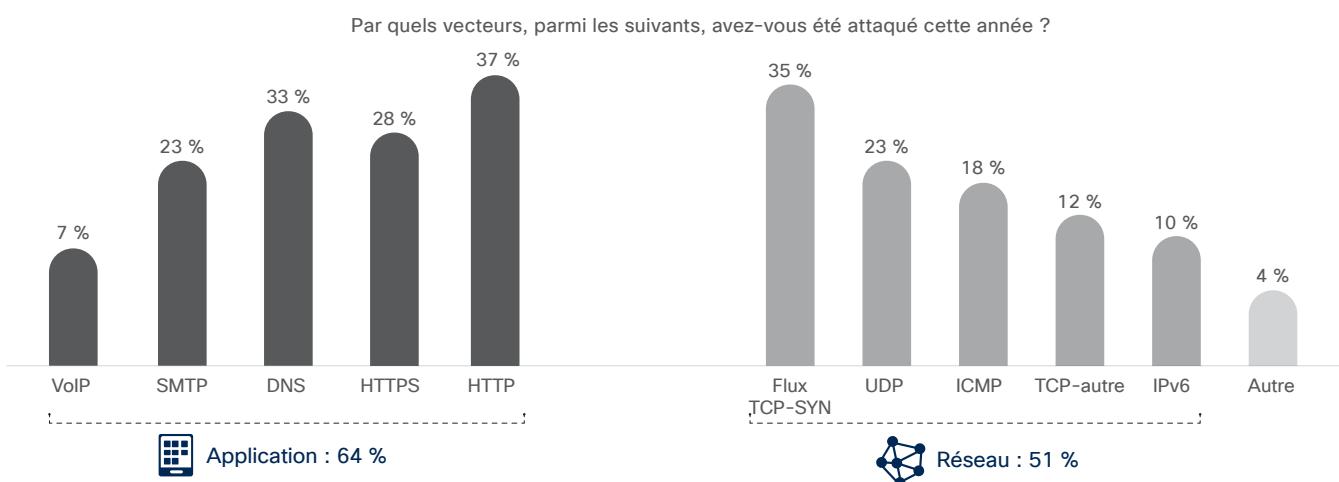
Les botnets IoT sont en plein essor parce que les entreprises et les utilisateurs déploient rapidement des appareils connectés à l'IoT peu coûteux sans se préoccuper de la sécurité. Les appareils connectés à l'IoT sont des systèmes basés sur Linux et Unix, qui sont donc souvent la cible des fichiers binaires ELF. Il est également plus facile de prendre le contrôle de ces appareils plutôt qu'un ordinateur, ce qui signifie que les hackers peuvent créer aisément et rapidement une gigantesque armée.

Les appareils connectés à l'IoT fonctionnent 24 h/24 et peuvent s'activer en quelques minutes. En outre, à mesure que les hackers augmentent la taille de leurs botnets IoT, ils investissent dans du code et des malwares plus sophistiqués pour créer des attaques DDoS plus avancées.

Les attaques DDoS sur les applications sont plus nombreuses que les attaques DDoS contre le réseau

Les attaques de la couche applicative sont de plus en plus fréquentes, alors que les attaques de la couche réseau sont en baisse (voir Figure 28). Les chercheurs Radware estiment que ce changement peut être attribué à l'évolution des botnets IoT. Cette tendance est préoccupante parce que la couche applicative est très diverse et intègre un grand nombre d'appareils, ce qui signifie que les attaques qui ciblent cette couche pourraient potentiellement bloquer de grandes parties d'Internet.

Figure 28 Les attaques par déni de service sur les applications ont augmenté en 2017



Source : Radware

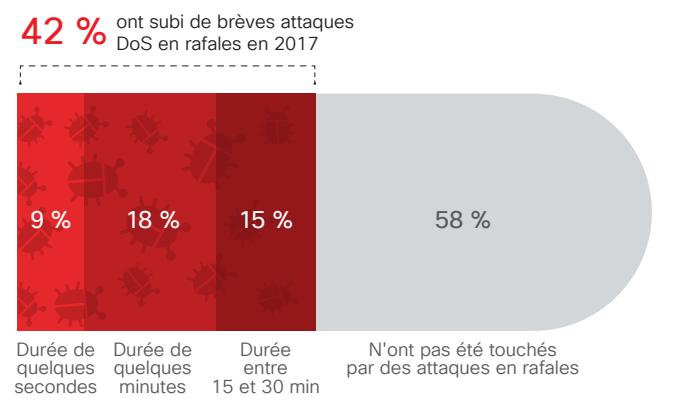
¹⁸ Pour en savoir plus sur l'étude Radware sur les botnets IoT, consultez la section « The IoT is only just emerging but the IoT botnets are already here » p. 39 du *rapport Cisco du 1er semestre 2017 sur la cybersécurité* : cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

Les hackers se tournent de plus en plus vers la couche applicative car la couche réseau a déjà été largement exploitée, d'après les chercheurs Radware. La création de botnets IoT exige également moins de ressources que les botnets de PC. Les hackers peuvent ainsi investir davantage de ressources dans le développement de codes et de malwares sophistiqués. Les opérateurs du botnet multivecteur Mirai, connu pour ses attaques avancées contre les applications, consentent ce type d'investissement.

Des campagnes d'« attaques éclair » de plus en plus complexes, fréquentes et longues

En 2017, Radware a observé une tendance significative en matière d'attaque DDoS : la multiplication des attaques éclair de plus en plus complexes, fréquentes et longues. 42 % des entreprises examinées par Radware ont subi ce type d'attaque DDoS en 2017 (Figure 29). Dans la plupart des cas, il s'agissait d'attaques récurrentes ne durant que quelques minutes.

Figure 29 Attaques DDoS en rafale récurrentes



Source : Radware

Les attaques éclair visent généralement les opérateurs télécoms et les sites web de jeux parce qu'ils sont sensibles à la disponibilité et sont incapables de faire face longtemps à de telles manœuvres. Des pics de trafic rapides ou aléatoires pendant plusieurs jours ou même plusieurs semaines peuvent empêcher ces entreprises de réagir, d'où de graves interruptions.

Les chercheurs Radware déclarent que les attaques éclair :

- Sont composées de plusieurs vecteurs changeants. Les attaques sont réparties géographiquement et prennent la forme d'une série durable d'inondations SYN, ACK et UDP (User Datagram Protocol) précises de grande ampleur sur plusieurs ports.

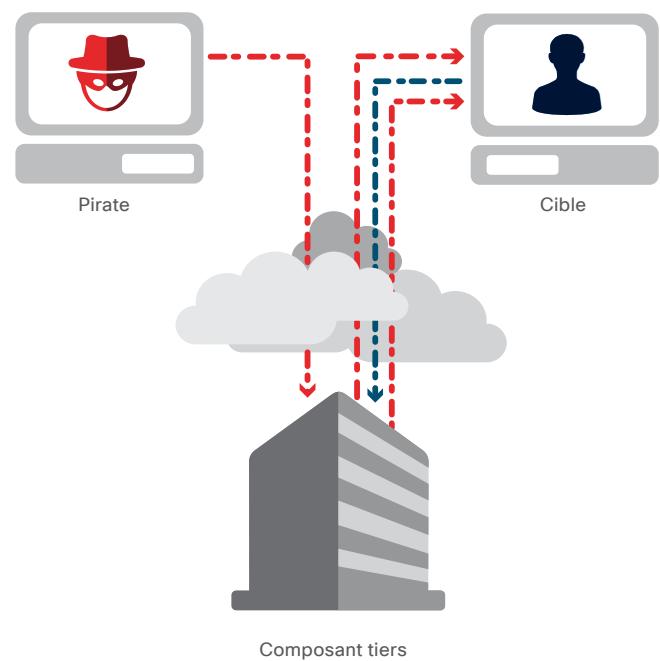
- Combinent des attaques de grande ampleur de durées variables, des pics de trafic de 2 à 50 secondes toutes les cinq à 15 minutes environ.
- Sont souvent associées avec d'autres attaques DDoS longue durée.

La croissance des attaques par amplification et réflexion

Radware a observé une autre tendance au cours de l'année 2017 : la multiplication des attaques DDoS par amplification et réflexion contre un large éventail de services. Selon Radware, deux entreprises sur cinq ont été victimes d'une telle attaque en 2017. Un tiers de ces entreprises ont déclaré être incapables d'éliminer ces attaques.

Une attaque par amplification et réflexion utilise un composant tiers potentiellement légitime pour envoyer du trafic malveillant à une cible, en dissimulant l'identité de l'intrus. Les hackers envoient des paquets à des serveurs de réflexion en utilisant l'adresse IP de l'utilisateur cible comme adresse IP source. Ils peuvent donc submerger indirectement la cible avec des paquets de réponse et épouser son taux d'utilisation de ressources (voir Figure 30).

Figure 30 Attaques par amplification et réflexion



Source : Radware

Pour exécuter une attaque par amplification et réflexion, les hackers ont besoin d'une bande passante plus élevée que leurs cibles. C'est là que les serveurs de réflexion entrent en jeu : le hacker se contente de refléter le trafic en provenance d'une ou de plusieurs machines tierces. Étant donné que ce sont des serveurs ordinaires, ce type d'attaque est particulièrement difficile à maîtriser. Voici quelques exemples fréquents :

Les attaques par réflexion et amplification DNS

Cette attaque sophistiquée par déni de service est amplifiée par le comportement du serveur DNS. Une requête DNS standard est plus petite que la réponse DNS. Dans le cas d'une attaque par réflexion et amplification DNS, le hacker sélectionne avec soin une requête DNS qui implique une réponse jusqu'à 80 fois plus longue que la requête (par exemple, « ANY »). Il envoie ensuite cette requête par l'intermédiaire d'un botnet à des serveurs DNS tiers, tout en dissimulant l'adresse IP source avec l'adresse IP de l'utilisateur cible. Les serveurs DNS tiers envoient leurs réponses à l'adresse IP de la cible. Grâce à cette technique, un botnet relativement petit peut transmettre un énorme flux de réponses volumineuses à la cible.

La réflexion NTP

Ce type d'attaque par amplification exploite les serveurs NTP (Network Time Protocol) accessibles au public pour submerger et épuiser les systèmes de défense avec du trafic UDP. NTP est un ancien protocole réseau dédié à la synchronisation d'horloge entre des systèmes informatiques sur des réseaux à commutation de paquets. Il est encore largement utilisé sur Internet par des ordinateurs de bureau, des serveurs et même des téléphones pour réaliser la synchronisation d'horloge. Plusieurs anciennes versions de serveurs NTP contiennent une commande appelée monlist, qui envoie au demandeur une liste des 600 derniers hôtes connectés au serveur interrogé.

Dans un scénario basique, le hacker envoie à plusieurs reprises la requête « get monlist » à un serveur NTP aléatoire et usurpe l'adresse IP source du serveur à l'origine de la demande pour en faire le serveur cible. Les réponses du serveur NTP sont ensuite envoyées au serveur cible, ce qui provoque une augmentation considérable du trafic UDP depuis le port source 123.

La réflexion SSDP

Cette attaque exploite le protocole SSDP (Simple Service Discovery Protocol), utilisé par les appareils UPnP (Universal Plug-and-Play) pour signaler leur existence. Il contribue également à détecter et contrôler les services et les appareils en réseau, tels que les caméras, les imprimantes connectées et beaucoup d'autres équipements électroniques.

Lorsqu'un appareil UPnP est connecté à un réseau et qu'il reçoit une adresse IP, il peut annoncer ses services à d'autres ordinateurs du réseau en envoyant un message dans un paquet IP multicast. Lorsqu'un ordinateur reçoit le message de l'appareil, il demande une description complète de ses services. L'appareil UPnP répond alors directement à cet ordinateur en lui transmettant une liste complète de tous les services qu'il propose.

Comme dans le cas des attaques DDoS par amplification NTP et DNS, le hacker peut utiliser un petit botnet à qui seront transmises les demandes finales de services. Il ne reste plus au hacker qu'à remplacer l'adresse IP source par l'adresse IP de l'utilisateur cible et à diriger les réponses directement vers la cible.

Les acteurs de la protection doivent remédier aux « fuites »

Un « chemin de fuite », tel que défini par Lumeta, partenaire Cisco, est une violation d'une politique ou d'une segmentation, ou une connexion non autorisée ou mal configurée à Internet sur un réseau d'entreprise, notamment depuis le cloud, qui autorise le transfert du trafic vers un emplacement sur Internet, comme un site web malveillant. Ces connexions inattendues peuvent également se produire en interne entre deux segments de réseau différents qui ne devraient pas communiquer l'un avec l'autre. Par exemple, dans des environnements stratégiques, un chemin de fuite entre l'atelier de fabrication et les systèmes IT commerciaux pourrait être le signe d'une activité malveillante. Les fuites peuvent également provenir de routeurs et de commutateurs mal configurés.

Les appareils, dont les autorisations ne sont pas correctement configurées ou sont ouvertes et non gérées, sont vulnérables aux attaques. Les appareils et les réseaux associés au « Shadow IT » ou à un environnement IT non autorisé permettent aussi aux hackers de mettre en place facilement un chemin de fuite parce qu'ils ne sont habituellement ni gérés ni corrigés. Lumeta estime

qu'environ 40 % des réseaux dynamiques, des terminaux et des infrastructures cloud dans les entreprises sont à l'origine d'angles morts considérables et ne sont pas surveillés en temps réel par les équipes de sécurité.

Il est essentiel de détecter les chemins de fuite existants car ils peuvent être exploités à tout moment. Cependant, il est aussi important de repérer les nouveaux chemins de fuite en temps réel, car ils constituent des indicateurs de compromission immédiats et sont associés à des attaques plus sophistiquées, comme les ransomwares.

Lumeta a récemment analysé l'infrastructure IT de plus de 200 entreprises dans plusieurs secteurs et a constaté une grande différence en matière de visibilité sur les terminaux. Ces résultats prouvent également que de nombreuses entreprises sous-estiment largement le nombre de terminaux dans leurs environnements IT (voir Figure 31). Le manque d'informations sur le nombre d'appareils IoT compatibles avec IP connectés au réseau explique souvent la sous-estimation des terminaux.

Figure 31 Vue d'ensemble des angles morts de l'infrastructure dans différents secteurs

Clients réels de Lumeta	Secteur public	Santé	Technologies	Secteur financier
Terminaux présumés	150 000	60 000	8 000	600 000
Terminaux détectés	170 000	89 860	14 000	1 200 000
Manque de visibilité sur les terminaux	12 %	33 %	43 %	50 %
Réseaux non gérés	3 278	24	5	771
Appareils de transfert non autorisés ou non sécurisés	520	75	2 026	420
Réseaux connus mais inaccessibles	33 256	4	16 828	45
Fuites sur Internet identifiées lors du déploiement	3 000	120	9 400	220

Source : Lumeta

Les chercheurs Lumeta estiment que les chemins de fuite sont en hausse, en particulier dans les environnements cloud, où la visibilité sur le réseau est moindre et où les contrôles de sécurité sont limités.

Les hackers n'utilisent pas toujours immédiatement les chemins de fuite qu'ils créent ou trouvent. En temps voulu, ils les utilisent pour installer des programmes malveillants ou des ransomwares, voler des informations et plus encore. Les chercheurs Lumeta expliquent que les chemins de fuite passent souvent inaperçus parce que les hackers savent très bien chiffrer et dissimuler leurs activités, en utilisant TOR par exemple. Ils s'efforcent aussi d'utiliser les chemins de fuite de manière judicieuse, pour ne pas éveiller les soupçons des équipes de sécurité.

Les chercheurs Lumeta déclarent que les lacunes des équipes de sécurité, à savoir le manque de connaissances fondamentales sur les réseaux, peuvent interférer avec la capacité des entreprises à rechercher et à corriger les problèmes de fuite rapidement. Une meilleure collaboration entre les équipes chargées des réseaux et de la sécurité peut contribuer à détecter et éliminer les chemins de fuite plus rapidement.

Les outils d'automatisation qui fournissent des informations sur le réseau peuvent également donner aux analystes de sécurité un aperçu des chemins de fuite potentiels. En outre, implémenter des politiques de segmentation appropriées peut aider les équipes de sécurité à déterminer rapidement si une communication imprévue entre des réseaux ou des appareils est malveillante.

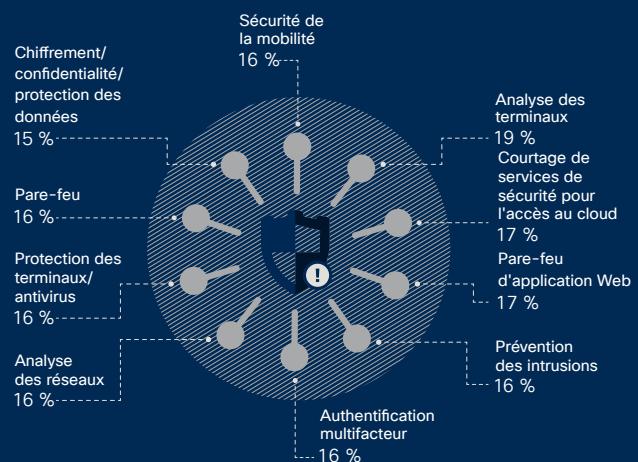
Enquête Cisco 2018 sur l'efficacité des mesures de sécurité : le manque de personnel de sécurité empêche de nombreuses entreprises d'implémenter de nouvelles cyberfonctionnalités

Le manque cruel de personnel demeure un obstacle de taille pour les acteurs de la protection. Comme remarqué ci-dessus, le manque de compétence peut limiter une entreprise dans ses capacités d'enquête et de résolution de certains types de menace.

Aussi, sans les bonnes compétences, les acteurs de la protection sont incapables de déployer de nouvelles technologies et de nouveaux processus qui pourraient renforcer leurs systèmes de sécurité (Figure 32).

De nombreux responsables sécurité interrogés dans le cadre de l'Enquête Cisco 2018 sur l'efficacité des mesures de sécurité ont indiqué que, dans l'idéal, ils souhaiteraient automatiser ou sous-traiter plus d'activités de routine afin de pouvoir recentrer leurs équipes sur des activités plus importantes.

Figure 32 Les principales fonctionnalités que les entreprises renforcerait si elles disposaient de plus de personnel



Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics

Les vulnérabilités des systèmes de contrôle industriels mettent les infrastructures stratégiques en péril

Les systèmes de contrôle industriel (ICS) sont au cœur de tous les systèmes de contrôle des processus et de la fabrication. Les ICS se connectent à d'autres systèmes électroniques qui font partie du processus de contrôle, ce qui crée un écosystème ultraconnecté d'appareils vulnérables que les hackers ne manquent pas de cibler.

Ces cyberpirates qui veulent cibler les ICS pour paralyser les infrastructures stratégiques s'emploient activement à rechercher et créer des points d'entrée illégaux pour faciliter les attaques futures, selon TrapX Security, un partenaire de Cisco qui développe des dispositifs de cybersécurité ayant recours à la tromperie. Ces hackers potentiels comptent dans leurs rangs des experts dotés d'une connaissance pointue des systèmes informatiques, ainsi que des architectures d'ICS et de leurs processus. Certains savent même programmer des sous-systèmes et des contrôleurs de gestion du cycle de vie des produits (ou PLM, Product Lifecycle Management).

Les experts de la cybersécurité de TrapX ont récemment étudié plusieurs cyberattaques qui ont visé les ICS de clients spécifiques pour mettre en évidence les problèmes inattendus que présente la défense des ICS. Deux de ces incidents, décrits ci-dessous, ont eu lieu en 2017 et font toujours l'objet d'une analyse.

Cible : grande société internationale de traitement des eaux et des déchets

Les hackers ont utilisé le serveur de zone démilitarisée (DMZ) de l'entreprise comme point d'entrée pour attaquer le réseau interne. L'équipe en charge de la sécurité a reçu des alertes de la technologie de défense intégrée à la DMZ du réseau. Ce sous-réseau physique ou logique protège les réseaux internes des réseaux non approuvés, tels qu'Internet et protège ainsi les infrastructures internes. L'enquête a révélé que :

- Le serveur DMZ a été attaqué en raison d'une mauvaise configuration autorisant les connexions RDP.
- Le serveur a été attaqué et contrôlé à partir de plusieurs adresses IP, qui étaient reliées à des hackers politiques hostiles à la société.

- Ces derniers ont ainsi pu lancer des attaques de grande ampleur contre plusieurs usines de la société à partir du réseau interne compromis.

Cible : centrale électrique

Les ressources stratégiques de cette centrale comprennent une très grande infrastructure ICS et les systèmes d'acquisition et de surveillance des données nécessaires pour gérer et exécuter les processus de ces ressources. La centrale est considérée comme une infrastructure nationale sensible, contrôlée et surveillée par l'agence responsable de la sécurité nationale. Elle fait donc l'objet d'une haute sécurité.

Le RSSI impliqué a décidé de mettre en œuvre la technologie de défense fondée sur la tromperie afin de protéger les ressources informatiques standard de la centrale contre les attaques de ransomware. La technologie a également été appliquée dans l'infrastructure ICS. Peu après, l'équipe en charge des opérations de sécurité a reçu plusieurs alertes indiquant une faille dans les systèmes de fonctionnement de l'infrastructure stratégique de la centrale. L'enquête immédiate menée par l'équipe a conclu ce qui suit :

- Un appareil dans le réseau de contrôle des processus a tenté d'interagir avec les pièges de tromperie camouflés en tant que contrôleurs PLM. Il s'agissait d'une tentative active de cartographier et de connaître la nature exacte de chaque contrôleur PLM sur le réseau.
- L'appareil compromis aurait normalement dû être fermé, mais un prestataire de maintenance n'a pas fermé la connexion à la fin de son intervention. À cause de cet oubli, le réseau de contrôle des processus était vulnérable aux attaques.
- Les informations recueillies par les hackers étaient exactement celles dont ils avaient besoin pour nuire gravement à l'activité de la centrale et potentiellement à son fonctionnement.

Recommendations

De nombreuses failles de systèmes ICS commencent par la compromission des serveurs et des ressources informatiques vulnérables sur le réseau d'une entreprise. Les experts en cybersécurité de TrapX conseillent aux entreprises de prendre les mesures suivantes pour réduire les risques et assurer l'intégrité des opérations au sein de leurs installations :

- Examiner les systèmes et leurs fournisseurs et vérifier que tous les correctifs et les mises à jour sont bien appliqués sans délai. (Si des correctifs ne sont pas disponibles, envisager la migration vers une nouvelle technologie.)
- Réduire l'utilisation de clés USB et de lecteurs de DVD.
- Isoler les systèmes ICS des réseaux informatiques. Éviter les connexions directes entre les deux. Cela inclut les connexions réseau, les ordinateurs portables et les clés USB.

- Mettre en œuvre des politiques qui limitent fortement l'utilisation des réseaux ICS à d'autres choses que les opérations essentielles. Réduire l'accès aux postes de travail et moniteurs ICS avec un navigateur Internet externe. Prévoir l'échec de ces politiques et les plans de secours associés.
- Rechercher et éliminer les mots de passe intégrés ou les mots de passe par défaut dans le réseau de production. Et dans la mesure du possible, mettre en œuvre l'authentification à deux facteurs.
- Examiner les plans de reprise sur sinistre suite à une cyberattaque majeure.

Pour d'autres études de cas, voir le document de recherche de TrapX Security, *Anatomie d'une attaque : les systèmes de contrôle industriels sont assiégés*.

Enquête Cisco 2018 sur l'efficacité des mesures de sécurité : plus d'attaques prévues au niveau des technologies opérationnelles (OT) et de l'IoT

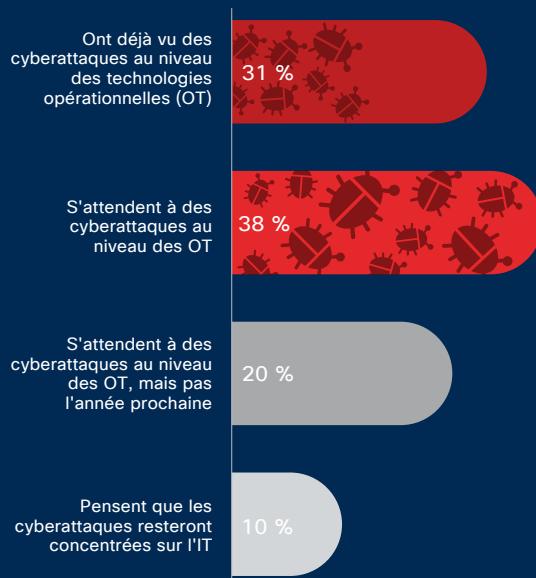
Les attaques ciblant les technologies opérationnelles (OT) telles que les systèmes de contrôle industriel (ICS) ou les appareils connectés à l'IoT sont encore rares, si bien que de nombreux responsables sécurité n'en ont pas encore fait l'expérience eux-mêmes. Toutefois, d'après les études menées pour **l'Enquête Cisco 2018 sur l'efficacité des mesures de sécurité**, ils s'attendent à subir de telles attaques à l'avenir et réfléchissent à la manière dont ils y feront face.

Les responsables sécurité savent que ces systèmes sont vulnérables, avec souvent peu de protection ainsi que des logiciels non corrigés et obsolètes.

Selon une des personnes interrogées : « Nous utilisons encore des appareils OT qui ont 25 ans, et des compresseurs et des machines qui ont 40 ans. Les professionnels IT ont l'habitude des calendriers de gestion des logiciels. Ils me disent « Prévenez-moi quand Windows X ne sera plus pris en charge », ou encore « Tiens, cette version d'Oracle arrive en fin de vie ». Dans les environnements OT, ce n'est pas du tout le cas. »

Peu de responsables sécurité peuvent parler en toute connaissance de cause des problèmes qu'ils ont avec la sécurité des OT de leur entreprise, soit parce qu'ils ont peu d'infrastructures OT ou ne prévoient pas d'en ajouter particulièrement, soit parce que la mise en œuvre de l'IoT est trop récente. Parmi ces professionnels, 31 % ont répondu que leur entreprise avait déjà subi une attaque sur leur infrastructure OT, tandis que 38 % s'attendent à ce que les attaques passent de l'IT à l'OT dans l'année (Figure 33).

Figure 33 31 % des entreprises ont subi une attaque sur leur infrastructure OT



Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

 Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics

VULNÉRABILITÉS ET CORRECTIFS

En raison de la multitude des préoccupations de sécurité, les acteurs de la protection peuvent perdre de vue les vulnérabilités dont pâtit leur technologie. Mais vous pouvez être sûr que ce n'est pas le cas pour les hackers qui vont chercher à exploiter ces faiblesses potentielles pour lancer des attaques.

Il fut un temps où appliquer des correctifs aux vulnérabilités connues dans les 30 jours était considéré comme une bonne pratique. Aujourd'hui, un tel délai peut augmenter les risques qu'une entreprise soit la cible d'une attaque, car les hackers ont un temps d'avance pour exploiter activement les vulnérabilités. Les entreprises doivent également éviter de négliger les petites, mais néanmoins sérieuses, failles de sécurité que peuvent exploiter les cybercriminels, surtout pendant la phase de reconnaissance des attaques, lorsqu'ils recherchent le moyen de pénétrer dans les systèmes.

Les erreurs de type dépassement de mémoire tampon et Apache Struts sont les principales vulnérabilités constatées en 2017

Les erreurs de dépassement de mémoire tampon arrivent en tête de la liste des catégories de vulnérabilité CWE (Common Weakness Enumeration) prises en compte par Cisco en 2017, bien que d'autres catégories aient connu une tendance à la

hausse ou la baisse. Les vulnérabilités de validation des entrées ont augmenté, alors que les erreurs de mémoire tampon ont diminué (Figure 34).

Figure 34 Activité des catégories de menace CWE

Catégorie de menace	Janvier-septembre 2016	Janvier-septembre 2017	Variation
CWE-119 : erreurs de mémoire tampon	493	403	(-22 %)
CWE-20 : validation des entrées	227	268	+15 %
CWE-264 : autorisations, privilèges et contrôle d'accès	137	163	+18 %
CWE-200 : fuite/divulgation d'informations	125	250	+100 %
CWE-310 : problèmes de cryptographie	27	17	(-37 %)
CWE-78 : injections de commande SE	7	15	+114 %
CWE-59 : suivi de lien	5	0	

Source : Cisco Security Research

L'étude des alertes critiques (Figure 35) montre que les vulnérabilités Apache Struts étaient encore importantes en 2017. Apache Struts est un framework open source largement utilisé qui sert à créer des applications Java. Les vulnérabilités Apache Struts étaient à l'origine de failles de sécurité qui impliquaient des courtiers de données de premier plan en 2017.

Bien qu'Apache identifie les vulnérabilités et propose des correctifs rapidement, il n'est pas aisément d'appliquer des correctifs aux solutions d'infrastructure tels qu'Apache Struts sans perturber les performances du réseau. Comme le soulignent les rapports

précédents sur la sécurité de Cisco,¹⁹ des vulnérabilités de logiciels tiers ou open source peuvent nécessiter l'application manuelle de correctifs, ce qui n'est pas aussi systématique que l'application automatique de correctifs par les fournisseurs de logiciels standard. Cela donne aux cybercriminels plus de temps pour lancer des attaques.

Une analyse approfondie des systèmes d'exploitation, bibliothèque et fichiers individuels compris, peut fournir aux entreprises un inventaire des composants des solutions open-source.

Figure 35 Alertes critiques et activité des attaques

Vulnérabilités critiques				Activités d'attaque	
Mises à jour critiques Oracle, vulnérabilités OIT Plusieurs CVE	Vulnérabilités sur Open SSL Plusieurs CVE	Vulnérabilités sur Open SSL CVE-2017-3733	Vulnérabilités d'exécution du code à distance Apache Struts 2 CVE-2017-5638	Publication de Vault 7 par WikiLeaks Plusieurs CVE	Activité WannaCry MS17-010 Multiple CVEs
18 janvier	26 janvier	6 février	6 mars	7 mars	17 mai
Microsoft Windows Graphics CVE-2017-0108	Vulnérabilités du service Microsoft Windows Server Message Block pour exécuter du code arbitraire CVE-2017-0145	Vulnérabilités du protocole NTP (Network Time Protocol) Plusieurs CVE	Services IIS WebDav de Microsoft CVE-2017-7269	Campagnes internationales continues Operation Cloud Hopper	Divulgation par le Shadow Brokers Group des exploits d'Equation
14 mars	14 mars	21 mars	29 mars	6 avril	8 avril
Microsoft Office (attaque Dridex) CVE-2017-0199				Vulnérabilité du plug-in REST d'Apache Struts pour exécuter du code arbitraire pour transmettre du contenu XML CVE-2017-9805	Vulnérabilité de Microsoft .NET Framework pour exécuter du code arbitraire CVE-2017-8759
11 avril				6 septembre	12 septembre

Source : Cisco Security Research



Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics

19 Rapport du 1er semestre 2017 sur la cybersécurité de Cisco : cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

Les vulnérabilités de l'IoT et des bibliothèques ont pris de l'ampleur en 2017

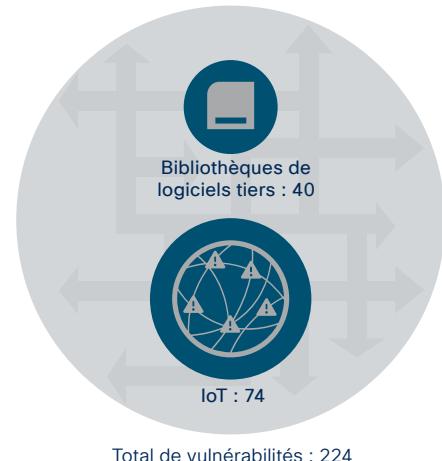
Entre le 1er octobre 2016 et le 30 septembre 2017, les experts de la cybersécurité de Cisco ont découvert 224 nouvelles vulnérabilités dans des produits autres que Cisco, dont 40 étaient associées à des bibliothèques de logiciels tiers incluses dans ces produits, et 74 étaient associées à des objets connectés (Figure 36).

Le nombre relativement important de vulnérabilités dans les bibliothèques souligne la nécessité d'examiner de façon plus approfondie les solutions tierces qui constituent l'ossature de nombreux réseaux d'entreprise. Les entreprises doivent tenir compte du fait que les bibliothèques de logiciels tiers peuvent être la cible des hackers ; il ne suffit pas de simplement s'assurer que la dernière version du logiciel est utilisée, ou qu'aucune faille ou vulnérabilité courante (CVE) ouverte n'a été signalée. Les équipes de sécurité doivent vérifier régulièrement que les derniers correctifs sont installés et examiner les pratiques de sécurité des fournisseurs tiers. Elles peuvent, par exemple, demander que les fournisseurs fournissent des avis de cycle de vie de développement sécurisé.

Une autre bonne pratique de vérification des logiciels tiers est de veiller à ce que les fonctions de mise à jour automatique et de vérification des mises à jour s'exécutent en toute sécurité. Par exemple, lorsqu'une mise à jour est lancée, les responsables sécurité doivent s'assurer que la communication nécessaire à celle-ci a lieu sur un canal sécurisé (par exemple, SSL) et que le

logiciel mis à jour est signé numériquement. Les deux sont nécessaires : si seules les signatures numériques sont utilisées, un hacker peut intercepter le trafic et remplacer une mise à jour par une version antérieure du logiciel qui est signé numériquement, mais qui peut contenir des failles. Si seul un canal sécurisé est utilisé, un hacker peut compromettre le serveur de mise à jour du fournisseur et remplacer la mise à jour par un logiciel malveillant.

Figure 36 Vulnérabilités des bibliothèques tierces et de l'IoT



Source : Cisco Security Research

i Vulnérabilités Spectre et Meltdown : une préparation proactive peut accélérer la résolution

L'annonce en janvier 2018 de l'existence des vulnérabilités Spectre et Meltdown, qui peuvent être exploitées pour compromettre les données sur des plates-formes utilisant les processeurs d'aujourd'hui, a soulevé des inquiétudes sur la capacité des responsables sécurité à protéger les données contre de telles attaques. Les hackers pourraient profiter de ces vulnérabilités pour afficher les données des applications dans la mémoire sur le jeu de composants. Sachant que les microprocesseurs concernés se trouvent partout, des téléphones portables au matériel des serveurs, le risque de dégâts à très grande échelle est bien présent.

Les risques posés par les vulnérabilités Spectre et Meltdown soulignent l'importance de communiquer avec les entreprises de sécurité pour échanger des solutions telles que les corrections ainsi que pour s'assurer que les fournisseurs tiers (ceux de la chaîne d'approvisionnement ou les opérateurs cloud, par exemple) suivent les bonnes pratiques pour remédier à ces failles de sécurité. Les équipes de réponse aux incidents liés à la sécurité des produits (comme l'équipe PSIRT de Cisco) sont formées pour agir rapidement après l'annonce des vulnérabilités, mettre au point des correctifs et conseiller les clients sur les moyens d'éviter les risques.

Les entreprises doivent se préparer à d'autres vulnérabilités du type Spectre et Meltdown, au lieu d'espérer ne plus jamais voir ce type de failles. Il est essentiel de se préparer à de telles éventualités et de mettre en place des systèmes pour limiter les dégâts potentiels. Par exemple, les équipes de sécurité doivent faire l'inventaire des appareils sous leur contrôle et documenter les configurations des fonctionnalités utilisées, puisque certaines vulnérabilités dépendent de la configuration et affectent la sécurité uniquement si certaines fonctionnalités sont activées.

Elles doivent également se renseigner auprès des prestataires tiers, tels que les fournisseurs de cloud, pour connaître leurs processus de correction et de mise à jour. Les entreprises doivent ensuite réclamer de la transparence de la part de leurs fournisseurs de cloud sur leur manière de résoudre les vulnérabilités et sur leur rapidité d'action après une alerte. Mais en fin de compte, c'est bien aux entreprises elles-mêmes que revient la responsabilité de se préparer correctement : elles doivent communiquer avec les équipes PSIRT et établir des processus pour réagir rapidement en cas de vulnérabilité.

Pour en savoir plus, lisez l'article de blog de Talos sur Spectre et Meltdown.

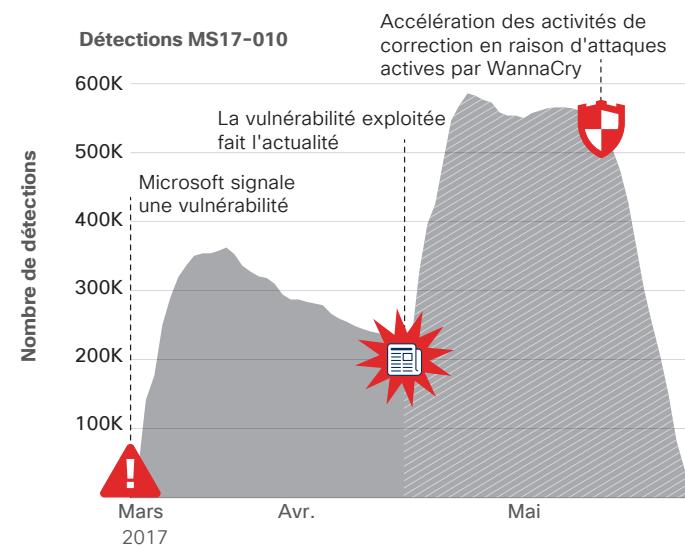
Les exploits actifs nécessitent des corrections rapides, sauf dans le cas des objets connectés

Qualys, Inc., un partenaire de Cisco et un fournisseur de solutions de sécurité et de conformité basées sur le cloud, s'est penché sur le comportement de gestion des correctifs des entreprises avant et après la campagne WannaCry qui a touché de nombreuses entreprises partout dans le monde en mai 2017.

Le cryptovirus ransomware WannaCry qui, selon de nombreux experts, a été conçu pour effacer les données, a profité d'une faille de sécurité de Microsoft Windows appelée EternalBlue. Cette vulnérabilité a été divulguée par le groupe de hackers Shadow Brokers en avril 2017. (Pour en savoir plus sur ce sujet, voir « Le danger est là : en 2018, les entreprises doivent se préparer à faire face à de nouvelles menaces en réseau qui se propagent automatiquement » à la [page 6](#).)

Le 14 mars 2017, Microsoft a publié une mise à jour de sécurité (MS17-010) pour corriger une vulnérabilité critique dans son logiciel Microsoft Windows SMB Server. La Figure 37 illustre le pic du nombre d'appareils détectés avec la vulnérabilité et la baisse graduelle entre mi-mars et mi-avril lorsque les entreprises ont analysé leurs systèmes et appliqué le correctif.

Figure 37 Correctifs avant et après la campagne WannaCry



Source : Qualys

 Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics

Cependant, un nombre important d'appareils n'étaient toujours pas corrigés mi-avril. Puis, le 14 avril, le groupe Shadow Brokers a lancé un exploit ciblant cette vulnérabilité connue dans différentes versions de Microsoft Windows. La Figure 37 montre que le nombre d'appareils détectés avec la vulnérabilité a presque doublé peu après, car les entreprises ont appris l'impact potentiel de l'exploit sur les versions prises en charge ou non de Windows via un contrôle distant de Qualys qui a utilisé une partie du code de l'exploit.

Mais même après le lancement de l'exploit, la correction généralisée n'a pas eu lieu avant mi-mai, après la diffusion de l'attaque WannaCry dans la presse mondiale. La Figure 37 montre la hausse brutale des corrections après cette campagne. Dès fin mai, il restait peu d'appareils non corrigés.

L'étude de Qualys sur le comportement de correction de ses clients indique qu'il faut qu'un événement majeur se produise pour que les entreprises corrige les vulnérabilités critiques, même avoir connaissance d'une attaque active ne suffit pas à accélérer la correction. Et dans le cas de la campagne WannaCry, les entreprises avaient accès au correctif pour la vulnérabilité de Microsoft pendant deux mois avant le déclenchement des attaques du ransomware.

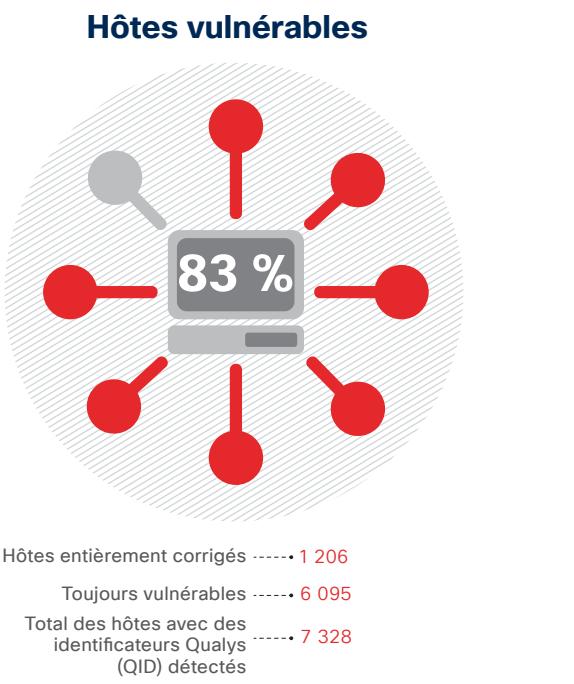
En outre, selon les experts de Cisco et du partenaire de Qualys Lumeta, des terminaux inconnus, non managés, non autorisés et fantômes n'ont pas été corrigés. Les hackers ont pu tirer parti de ces failles. En raison de cet oubli, les scanners de vulnérabilités n'ont pas pu évaluer ces systèmes et recommander de leur appliquer des correctifs, ils n'étaient donc pas protégés contre WannaCry.

L'application de correctifs est encore plus lente ou ne s'effectue pas du tout pour les objets connectés

Qualys a également examiné les tendances en matière de correction pour les objets connectés. Les appareils de l'échantillon examiné comprenaient des systèmes de climatisation, des serrures de porte, des panneaux de contrôle d'alarme incendie et des lecteurs de cartes activés par adresse IP.

Les experts ont surtout examiné les objets connectés vulnérables à plusieurs menaces connues, notamment le malware Devil's Ivy qui exploite une vulnérabilité dans un morceau de code appelé gSOAP qui est largement utilisé dans les produits de sécurité physique, et Mirai, un botnet visant l'IoT qui se connecte aux machines ciblées via des attaques brutales contre les serveurs Telnet.

Figure 38 Tendances en matière de correction des appareils connectés à l'IoT



Source : Qualys

Qualys a détecté 7 328 appareils infectés au total, mais seuls 1 206 avaient été corrigés (voir la Figure 38). Cela signifie que 83 % des objets IoT de l'échantillon comportaient encore des vulnérabilités critiques. Bien que Qualys n'ait pas pu prouver que des cybercriminels ciblaient activement ces vulnérabilités, les entreprises n'en demeurent pas moins susceptibles d'être attaquées. Cependant, elles ne semblent pas pressées de corriger ces vulnérabilités.

Il existe plusieurs explications possibles à cette inertie selon Qualys. Certains appareils ne peuvent pas être mis à jour. D'autres peuvent nécessiter l'intervention directe du fournisseur. En outre, il n'est pas toujours facile de savoir qui dans l'entreprise est chargé de la maintenance des objets connectés. Par exemple, une équipe d'ingénieurs qui s'occupe du système de climatisation de la société peut ne pas connaître les risques informatiques qu'encourt ce système, ou même ne pas savoir que le système est activé par adresse IP.

Plus préoccupant encore, est le faible nombre d'objets connectés détectés par Qualys. Le nombre réel est susceptible d'être beaucoup plus élevé, car les entreprises ne savent tout simplement pas combien d'objets sont connectés à leur réseau. Ce manque de visibilité les expose à des attaques (voir [page 34](#) pour en savoir plus sur ce sujet).

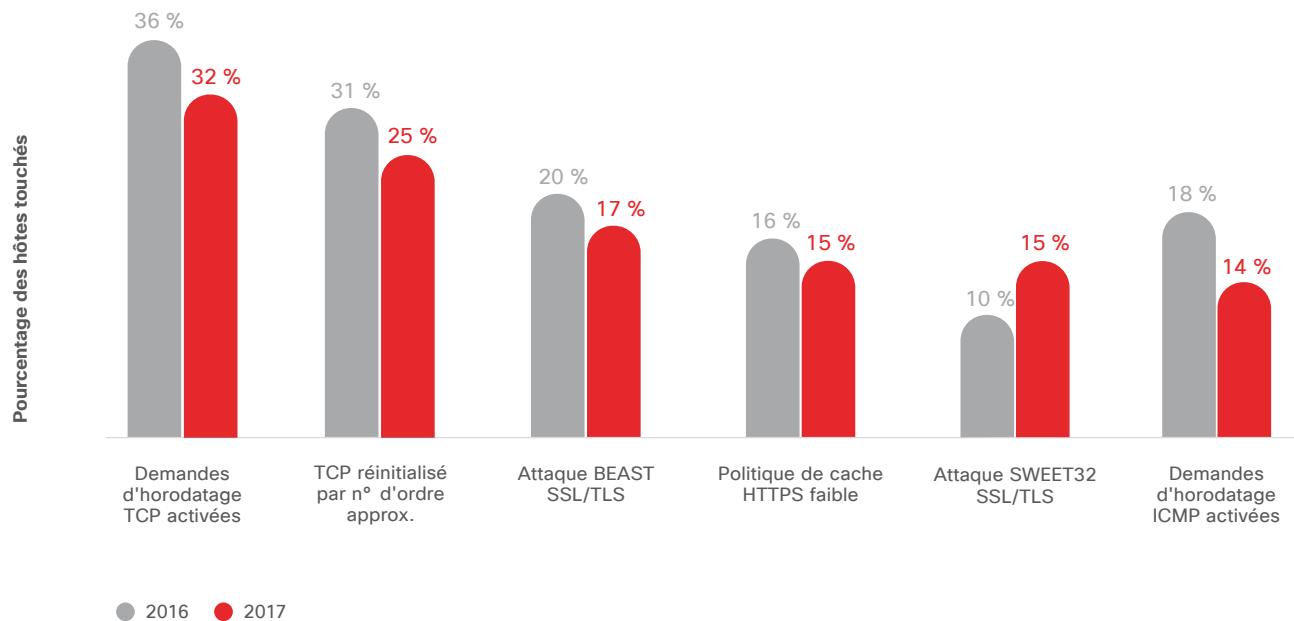
La première étape pour répondre à ce problème est de répertorier tous les appareils connectés sur le réseau. Les entreprises peuvent alors déterminer si les appareils sont analysables, si leurs fournisseurs les prennent toujours en charge et à quels employés ils appartiennent. Les entreprises peuvent également améliorer la sécurité des objets connectés en les traitant de la même manière que les autres appareils informatiques, pour mettre à jour leur micrologiciel et leur appliquer régulièrement des correctifs.

Les vulnérabilités courantes sont de faible gravité mais présentent un risque élevé

Les vulnérabilités de faible gravité restent non corrigées pendant des années, car les entreprises ne savent pas qu'elles existent, ou bien elles considèrent qu'elles ne présentent pas de risques importants, selon les experts de la sécurité de SAINT Corporation, une société de solutions de sécurité et partenaire de Cisco. Toutefois, ces petites failles de sécurité mais néanmoins sérieuses peuvent permettre à des hackers de pénétrer dans les systèmes.

Les experts de SAINT ont examiné les données de vulnérabilité collectées auprès de plus de 10 000 hôtes en 2016 et 2017. La société a dressé une liste des principales vulnérabilités détectées le plus souvent dans toutes les entreprises incluses dans l'étude, qui montre que les vulnérabilités de faible gravité sont les plus courantes (voir Figure 39). (Remarque : certaines entreprises incluses dans l'étude disposaient de plusieurs hôtes.)

Figure 39 Les vulnérabilités de faible gravité sont le plus souvent détectées, 2016–2017



Source : SAINT Corporation

Les trois principales vulnérabilités de faible gravité de la Figure 39 sont décrites ci-dessous pour expliquer en quoi elles sont utiles aux hackers :

Demandes d'horodatage TCP activées

Les horodatages TCP indiquent depuis combien de temps une machine fonctionne, ou quand elle a été redémarrée pour la dernière fois. À partir de ces informations, les hackers peuvent déterminer quel type de vulnérabilités corrigibles ils peuvent exploiter sur la machine. En outre, les programmes logiciels peuvent utiliser l'horodatage du système pour amorcer un générateur de nombres aléatoires afin de créer des clés de chiffrement.

TCP réinitialisé par un numéro d'ordre approximatif

Des hackers peuvent deviner à distance les numéros d'ordre et provoquer un déni de service pour les connexions TCP permanentes en injectant à plusieurs reprises un paquet TCP RST, surtout dans les protocoles qui utilisent des connexions à longue durée, comme le protocole BGP (Border Gateway Protocol).

Attaque « BEAST »

Un hacker peut utiliser la vulnérabilité BEAST (Browser Exploit Against SSL/TLS) pour lancer une attaque MiTM (man-in-the-middle ou homme du milieu) afin de « lire » le contenu protégé qui est échangé entre les parties. (Remarque : il s'agit d'une attaque compliquée à exécuter, car le hacker doit également avoir le contrôle du navigateur côté client pour pouvoir lire et injecter des paquets de données très rapidement.)

Les experts de la sécurité de SAINT n'ont pas détecté d'attaques exploitant ces vulnérabilités de faible gravité au cours de leur analyse.

Les vulnérabilités présentées dans la Figure 39 sont connues de la communauté de cybersécurité, mais certaines d'entre elles ne sont en général pas repérées ou provoquent un échec automatique lors d'un contrôle de conformité courant, par exemple un audit de vérification de la sécurité des données lors de paiements par carte bancaire selon le standard PCI-DSS (Payment Card Industry Data Security Standard). Ces vulnérabilités ne sont en fait pas considérées comme critiques selon les normes en vigueur dans ce secteur d'activité. Chaque secteur définit le caractère critique des vulnérabilités différemment.

En outre, la plupart des vulnérabilités fréquentes de faible gravité présentées dans la Figure 39 sont parfois difficiles à corriger ou ne peuvent pas être corrigées du tout via la gestion des correctifs, en raison de problèmes de configuration ou de problèmes de certificat de sécurité (par exemple, faible chiffrement SSL ou certificat SSL autosigné).

Les entreprises doivent agir rapidement pour corriger les vulnérabilités de faible gravité qui peuvent présenter des risques. Elles doivent évaluer et identifier les priorités de correction en fonction de leur perception des risques, et non en fonction d'évaluations d'organismes tiers, de systèmes de notation utilisés partiellement, pour obtenir par exemple un score CVSS de base, ou encore de certaines évaluations de conformité. Les entreprises connaissent mieux que quiconque leur environnement et leurs stratégies de gestion des risques.

Partie II : les acteurs de la protection

Partie II : les acteurs de la protection

Nous savons que les hackers modifient et adaptent leurs techniques plus rapidement que les entreprises. Ils développent et testent également leurs exploits, stratégies de contournement et compétences en situation réelle, afin de pouvoir lancer des attaques de plus grande ampleur. Quand les hackers frappent, les acteurs de la protection sont-ils prêts à y remédier rapidement ? Cela dépend en grande partie des mesures qu'ils prennent aujourd'hui pour renforcer leur sécurité.

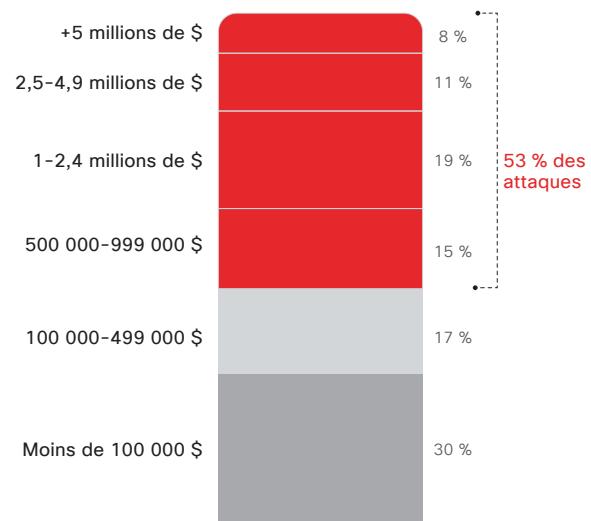
D'après nos recherches dans le cadre de notre enquête 2018 sur l'efficacité des mesures de sécurité, les acteurs de la protection ont beaucoup de travail devant eux et de nombreux défis à relever. Pour savoir comment les acteurs de la protection perçoivent les mesures adoptées par leur entreprise en matière de sécurité, nous avons interrogé des responsables de la sécurité des systèmes d'information (RSSI) et des responsables des opérations de sécurité (SecOps) d'entreprises de différentes tailles, dans plusieurs pays, sur leurs ressources et procédures de sécurité.

L'enquête donne des informations sur les pratiques actuelles en matière de sécurité. Elle compare également les résultats avec ceux des enquêtes réalisées en 2015, 2016 et 2017. Plus de 3 600 personnes ont été interrogées dans 26 pays pour mener à bien cette recherche.

Le coût des attaques

La crainte des failles de sécurité repose sur le coût financier des attaques, qui n'est plus hypothétique. Les failles de sécurité ont des conséquences économiques désastreuses pour les entreprises, dont elles peuvent mettre des mois voire des années à se remettre. Selon les participants à l'étude, plus de la moitié (53 %) de toutes les attaques ont entraîné des pertes financières de plus de 500 000 dollars (pertes de chiffre d'affaires, de clients et d'opportunités commerciales ou coûts directs) voir la Figure 40.

Figure 40 53 % des attaques causent au moins 500 000 \$ de dégâts



Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

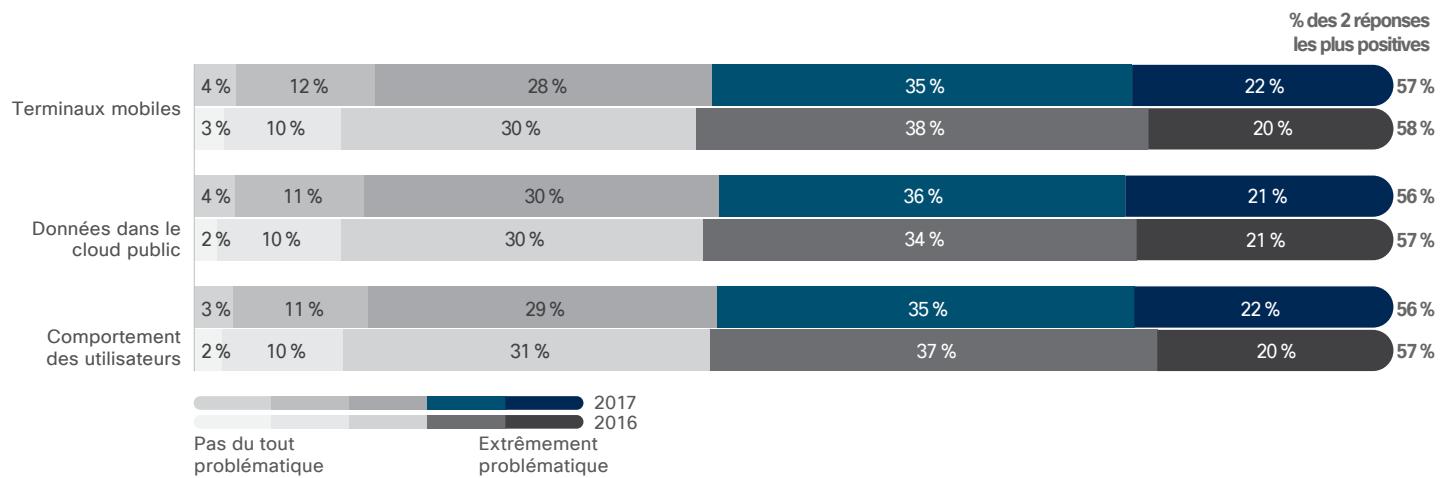
 Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics

Défis et obstacles

Dans leurs efforts pour protéger leurs entreprises, les équipes de sécurité font face à de nombreux obstacles. Les entreprises doivent défendre plusieurs domaines et fonctions, ce qui accroît les problèmes de sécurité. Les appareils mobiles, les données

dans le cloud public et le comportement des utilisateurs présentent les plus grands risques et sont les plus difficiles à protéger (Figure 41).

Figure 41 Les domaines les plus difficiles à défendre : les terminaux mobiles et les données dans le cloud



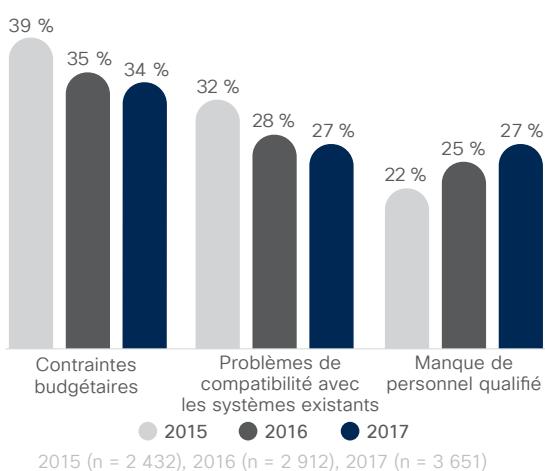
Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité



Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics

Les responsables sécurité citent le budget, l'interopérabilité et le personnel comme principales contraintes pour gérer la sécurité (Figure 42). Le manque de personnel qualifié est également cité comme un obstacle à l'adoption de processus et de technologies de sécurité avancés. En 2017, 27 % des personnes interrogées ont indiqué que le manque de personnel qualifié était un obstacle, comparé à 25 % en 2016 et 22 % en 2015.

Figure 42 Le plus grand obstacle à la sécurité : les contraintes budgétaires



Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Le manque de personnel qualifié arrive en tête des obstacles cités dans tous les secteurs d'activité et dans toutes les régions. « Si je pouvais agiter une baguette magique et obtenir 10 % de personnes en plus pour soulager le personnel déjà sous pression pour répondre à la forte demande de services, je serais très, très heureux, » a déclaré un RSSI d'une grande entreprise de services professionnels.

Bien que le manque de personnel qualifié constitue un défi permanent, les entreprises indiquent qu'elles recherchent et embauchent plus de ressources pour leurs équipes de sécurité. En 2017, le nombre médian de responsables sécurité dans les entreprises était 40, contre 33 en 2016 (Figure 43), ce qui représente une forte augmentation.

Figure 43 Les entreprises embauchent plus de responsables sécurité



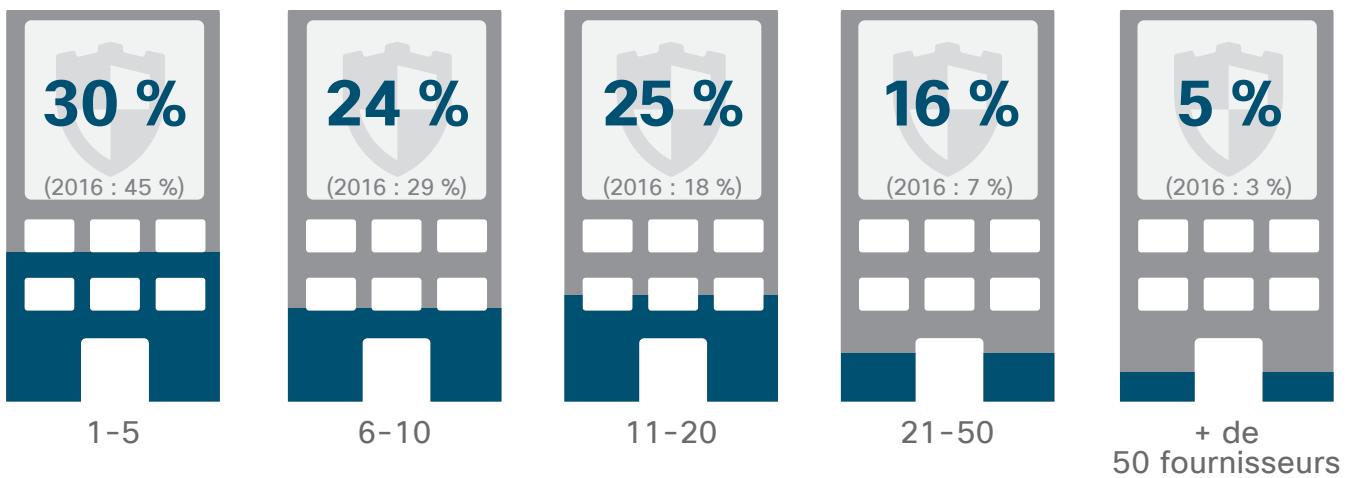
Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Complexité de l'orchestration de plusieurs fournisseurs

Les acteurs de la protection mettent en œuvre un mélange complexe de produits provenant de différents fournisseurs : un arsenal d'outils qui peut complexifier plutôt que simplifier l'environnement de sécurité. Cette complexité a de nombreux effets en aval sur la capacité d'une entreprise à se défendre contre les attaques, notamment l'augmentation du risque de pertes.

En 2017, 25 % des responsables sécurité ont indiqué avoir utilisé des produits de 11 à 20 fournisseurs contre 18 % en 2016. Toujours en 2017, 16 % des personnes interrogées ont indiqué avoir utilisé des produits de 21 à 50 fournisseurs contre 7 % en 2016 (Figure 44).

Figure 44 Les entreprises ont fait appel à plus de fournisseurs de solutions de sécurité en 2017

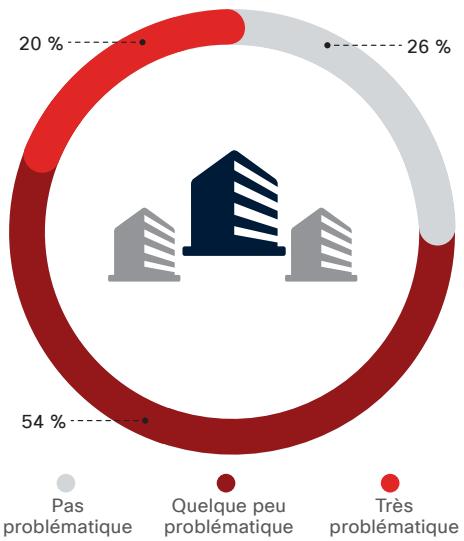


Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

 Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics

À mesure que le nombre de fournisseurs augmente, il devient plus problématique d'orchestrer les alertes émises par les solutions de ces fournisseurs. Comme l'indique la Figure 45, 54 % des responsables sécurité ont déclaré que gérer les alertes émises par les solutions de plusieurs fournisseurs est problématique, et très problématique pour 20 % d'entre eux.

Figure 45 Le défi de l'orchestration des alertes



Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

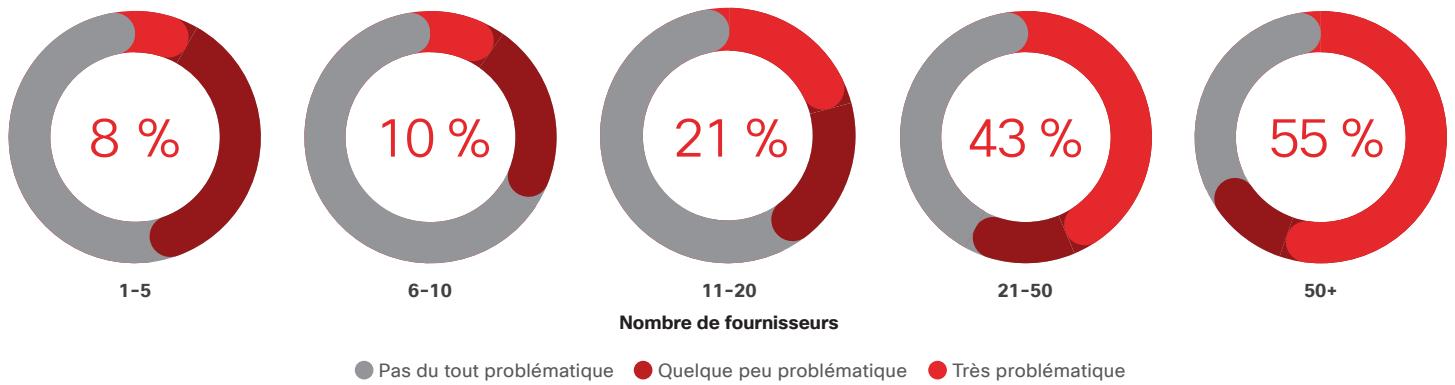
Les équipes de sécurité rencontrent des difficultés pour orchestrer les alertes émises par les solutions de plusieurs fournisseurs

Comme le montre la Figure 46, parmi les entreprises utilisant les produits de seulement 1 à 5 fournisseurs, 8 % ont indiqué qu'orchestrer les alertes est très problématique. Parmi les

entreprises qui utilisent plus de 50 fournisseurs, 55 % ont indiqué que cette orchestration est très problématique.

Lorsque les entreprises ne peuvent pas orchestrer et comprendre les alertes qu'elles reçoivent, les menaces légitimes passent à travers les mailles du filet.

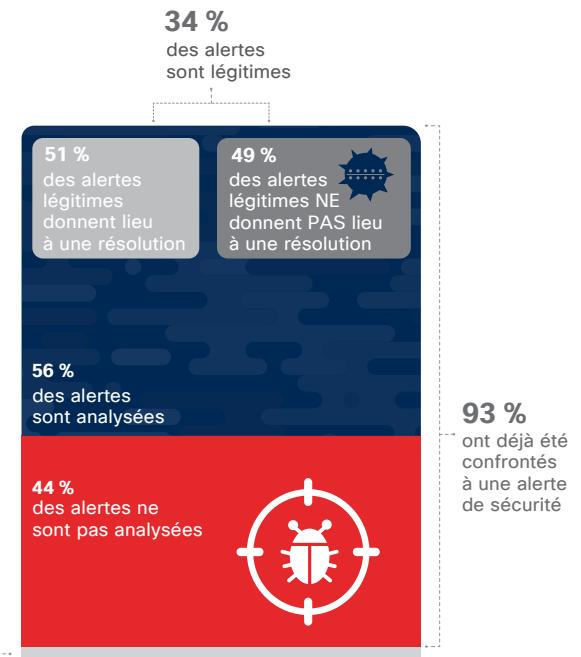
Figure 46 Plus il y a de fournisseurs de solutions de sécurité, plus l'orchestration des alertes est complexe



Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics

Figure 47 De nombreuses alertes de sécurité ne sont pas analysées ou traitées

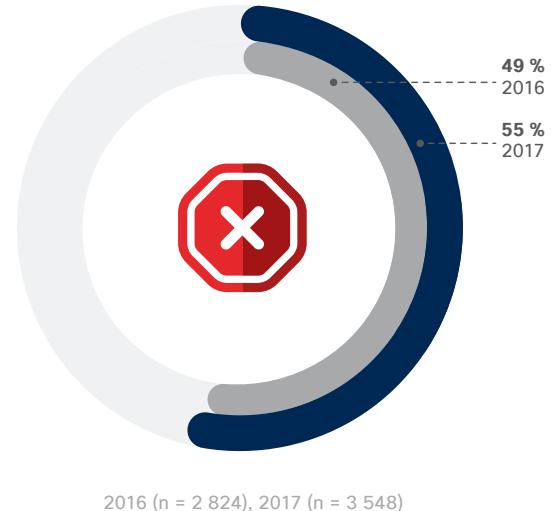


Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Impact : la méfiance du public due aux failles de sécurité se traduit par un risque de pertes plus élevé

« Il existe deux types de sociétés : celles qui ont été attaquées et celles qui ne savent pas qu'elles ont été attaquées, » indique un participant à l'étude sur l'efficacité des mesures de sécurité. (La réponse fait écho à une citation bien connue de l'ancien PDG de Cisco, John Chambers : « Il existe deux types de sociétés : celles qui ont été piratées et celles qui ne savent pas qu'elles ont été piratées. ») Bien que les entreprises tentent de relever les défis de la sécurité de demain avec une préparation adéquate, les responsables sécurité s'attendent à ce qu'elles soient victimes d'une faille qui entraînera la méfiance du public à leur égard. 55 % des personnes interrogées ont indiqué que leur entreprise a dû faire face à la méfiance du public suite à une faille l'an dernier (Figure 48).

Figure 48 55 % des entreprises ont dû faire face à la méfiance du public après une faille de sécurité



Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité



Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics



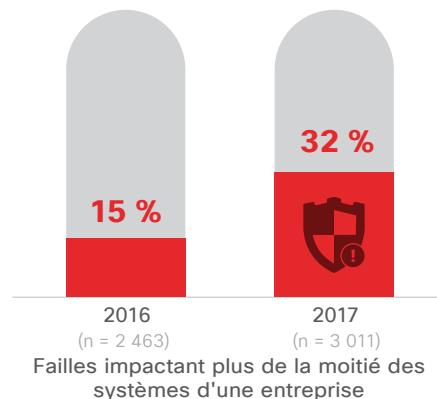
« D'ici peu, presque toutes les entreprises Fortune 500 auront été attaquées au cours des derniers 24 mois, ce sera devenu normal. Il faut s'y préparer, surtout du point de vue du marketing et des relations publiques. »

– Une personne interrogée pendant l'enquête

Les entreprises ont signalé beaucoup plus de failles de sécurité concernant plus de 50 % des systèmes (Figure 49), par rapport à l'étude de l'an dernier. En 2017, 32 % des responsables sécurité ont déclaré avoir détecté des failles de sécurité sur plus de la moitié de leurs systèmes, contre 15 % en 2016. Les secteurs des entreprises les plus touchées par les failles de sécurité sont les opérations, les finances, la propriété intellectuelle et la réputation de la marque (Figure 50).

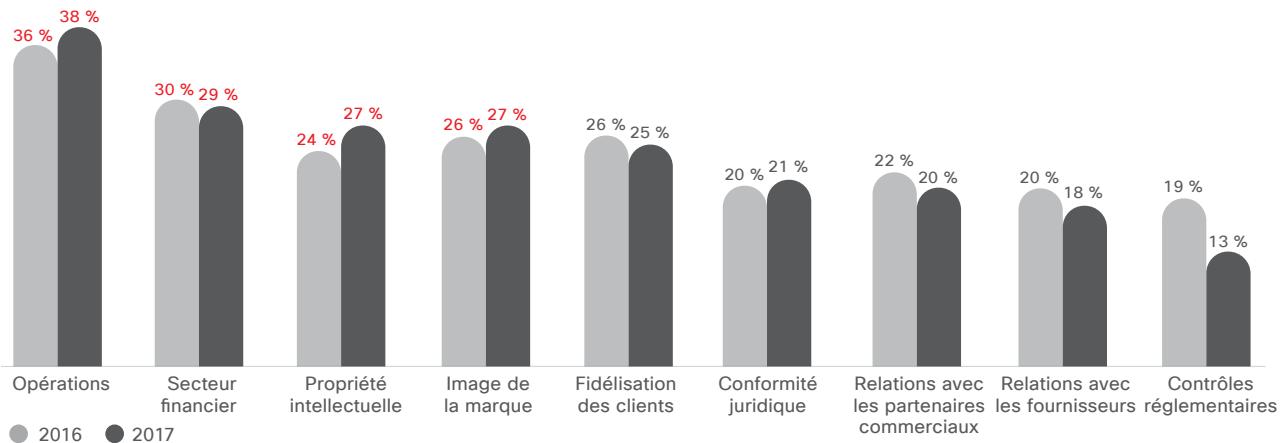
Dans les environnements de sécurité complexes, les entreprises sont plus susceptibles de traiter des failles de sécurité. Parmi les entreprises utilisant les solutions de 1 à 5 fournisseurs, 28 % ont indiqué avoir dû faire face à la méfiance du public après une faille et 80 % pour celles qui ont recours à plus de 50 fournisseurs (Figure 51). Cela est peut-être dû à la visibilité accrue des menaces en raison du plus grand nombre de produits.

Figure 49 Forte augmentation des failles de sécurité affectant plus de 50 % des systèmes



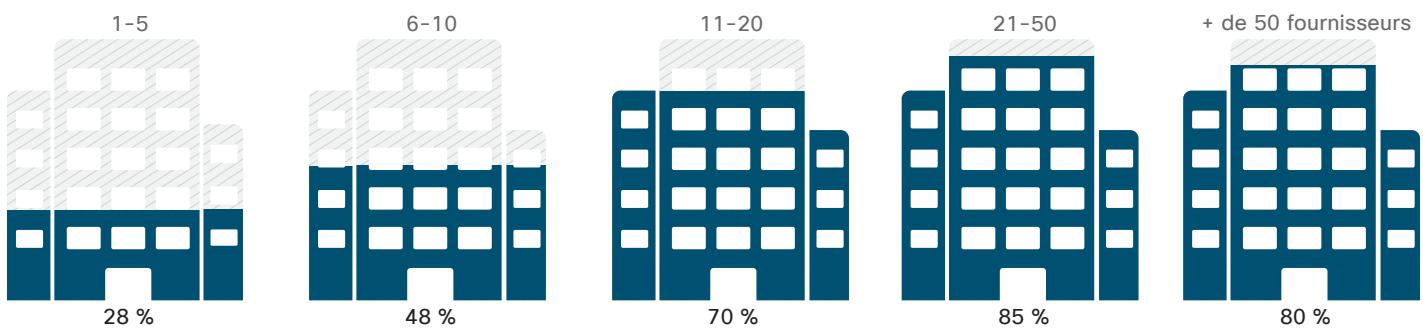
Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Figure 50 Les environnements d'exploitation et financiers sont les plus susceptibles d'être affectés par les failles



Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Figure 51 80 % des entreprises qui ont recours à plus de 50 fournisseurs ont dû faire face à la méfiance des clients après une faille rendue publique



Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics

La valeur d'une infrastructure intégrée

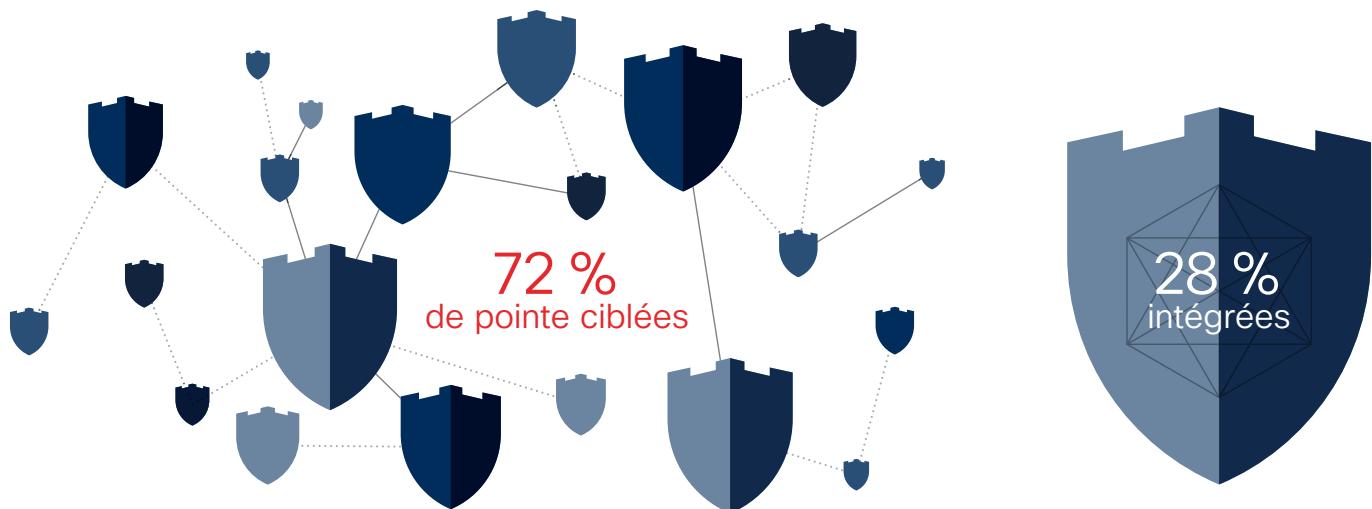
Pourquoi utiliser plusieurs solutions de différents fournisseurs si l'environnement qui en résulte est difficile à gérer ? L'approche, qui consiste à ce que les équipes de sécurité choisissent la meilleure solution pour chaque besoin de sécurité, est l'une des principales raisons. Les responsables sécurité qui appliquent cette approche pensent également qu'elle est plus rentable, comme le montre l'étude sur l'efficacité des mesures de sécurité.

La comparaison entre les solutions ciblées haut de gamme et les solutions intégrées montre que 72 % des professionnels de sécurité achètent des solutions ponctuelles de pointe pour répondre à des besoins spécifiques, contre 28 % qui achètent des produits destinés à fonctionner ensemble en tant que solution intégrée (voir la Figure 52). Parmi les entreprises qui préfèrent les solutions de pointe ciblées, 57 % citent la rentabilité, tandis que 39 % indiquent que cette approche est plus facile à mettre en œuvre.

Fait intéressant, les entreprises qui adoptent une approche intégrée de la sécurité citent des raisons semblables pour leur choix. 56 % affirment qu'une approche intégrée est plus rentable. 47 % pensent qu'elle est plus facile à mettre en œuvre.

La facilité de mise en œuvre est de plus en plus citée comme un facteur favorisant l'utilisation d'une approche d'architecture intégrée : seulement 33 % des entreprises affirmaient que la facilité de mise en œuvre était une raison de choisir une approche intégrée en 2016, contre 47 % en 2017. Bien que les solutions d'un seul fournisseur puissent ne pas être pratiques pour toutes les entreprises, les acheteurs des solutions doivent veiller à ce qu'elles fonctionnent ensemble pour réduire les risques et accroître l'efficacité.

Figure 52 72 % achètent des solutions haut de gamme ciblées pour répondre à leurs besoins spécifiques



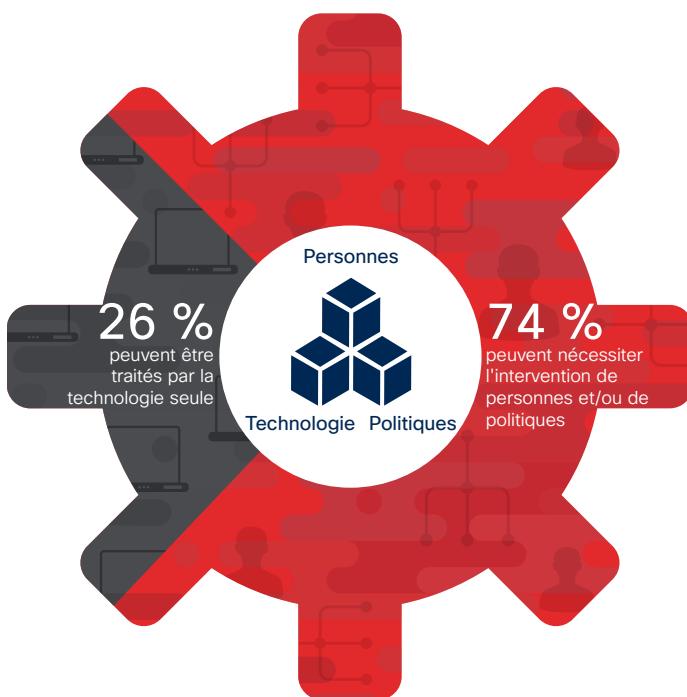
Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Services : tenir compte des utilisateurs, des politiques et de la technologie

Face à des pertes potentielles et un impact négatif sur les systèmes, les entreprises ne doivent pas compter uniquement sur la technologie pour se défendre. Par conséquent, elles doivent examiner d'autres possibilités pour améliorer la sécurité, notamment en appliquant des politiques ou en formant les utilisateurs. Cette approche globale de la sécurité est visible dans les problèmes identifiés au cours d'une évaluation de la sécurité sur la base des données collectées (appelée évaluation « Red Team ») assurée par l'équipe des services Cisco de conseil avancés pour la sécurité.

En examinant les données des recommandations de plusieurs évaluations Red Team réalisées en 2017, les agents de l'équipe chargée des services ont identifié trois principales capacités de défense : les personnes, les politiques et la technologie. En utilisant uniquement la technologie pour corriger les vulnérabilités de sécurité, une entreprise résoudrait seulement 26 % des problèmes identifiés par les simulations d'attaque réalisées lors des évaluations « Red Team ». Par conséquent, 74 % des problèmes ne sont pas résolus (voir la Figure 53). De même, si les entreprises utilisaient uniquement des politiques pour résoudre les problèmes de sécurité, seulement 10 % des problèmes seraient résolus, et 4 % avec la formation des personnes uniquement. Les trois domaines de défense doivent par conséquent être pris en compte en même temps.

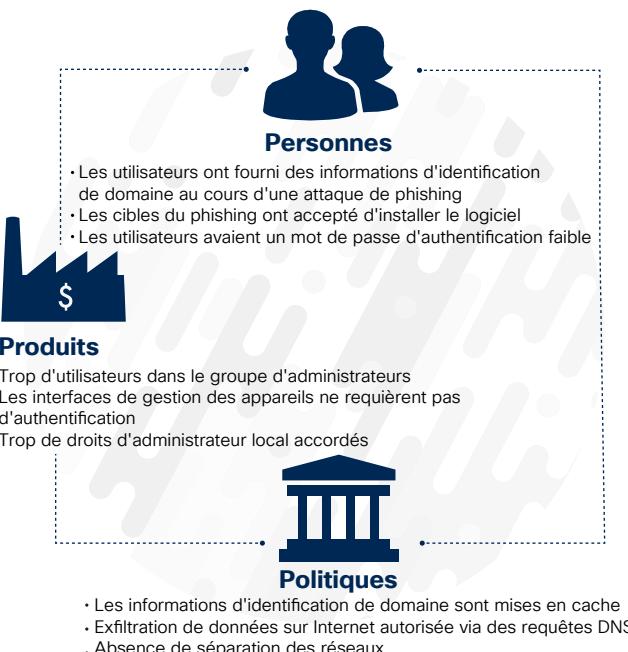
Figure 53 Seulement 26 % des problèmes de sécurité peuvent être traités par les produits seuls



Source : Cisco Security Research

La Figure 54 montre des exemples de problèmes identifiés par catégorie lors des simulations. Certains problèmes, tels que les mots de passe faibles, concernent les trois catégories. Le renforcement des mots de passe peut nécessiter des améliorations au niveau des personnes (formation des utilisateurs), des produits (configuration des serveurs pour utiliser des mots de passe plus complexes) et des politiques (garantissant l'utilisation de mots de passe plus sécurisés).

Figure 54 Types de problèmes découverts lors des simulations d'attaque, classés par type de résolution



Source : Cisco Security Research

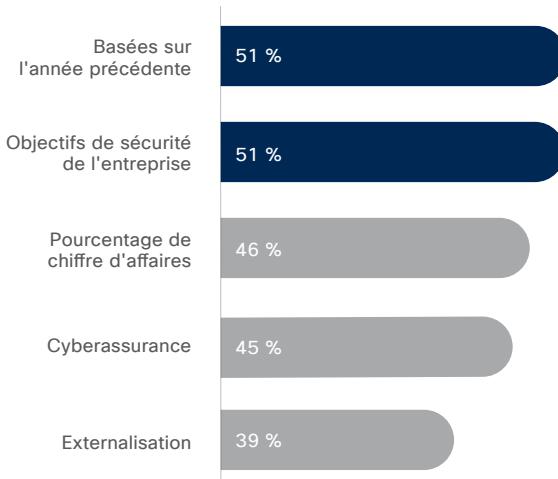
Les entreprises peuvent augmenter leurs chances de gérer avec succès les trois facteurs si elles intègrent la sécurité à tous les niveaux de leur activité et non ici et là. Elles doivent également éviter de compter uniquement sur des produits ou des améliorations techniques pour corriger les failles de sécurité. Pour que les produits soient efficaces, les entreprises doivent comprendre la technologie et mettre en œuvre des politiques et des processus appropriés.

Attentes : investir dans la technologie et la formation

Les responsables sécurité estiment que les menaces pesant sur leur entreprise continueront à être complexes et difficiles à traiter. Ils s'attendent à ce que les cybercriminels développent des moyens toujours plus sophistiqués et nuisibles pour attaquer les réseaux. Ils savent aussi que l'espace de travail moderne crée des conditions favorables aux attaques : la mobilité des collaborateurs et l'adoption d'objets connectés offrent de nouvelles possibilités aux hackers. En plus de l'augmentation des menaces, de nombreux responsables sécurité s'attendent à être de plus en plus sous surveillance, par les régulateurs, les dirigeants, les décideurs, les partenaires et les clients.

Pour réduire la probabilité des risques et des pertes, les acteurs de la protection doivent déterminer où investir les ressources limitées dont ils disposent. Pour l'essentiel, les responsables sécurité estiment que les budgets de sécurité resteront relativement stables, à moins qu'une importante faille rendue publique n'entraîne une remise en cause des technologies et des processus et de nouvelles dépenses en la matière. 51 % des responsables sécurité ont déclaré que les dépenses en matière de sécurité reposent sur les budgets des années précédentes, tandis que pour un pourcentage égal des personnes interrogées les budgets dépendent des objectifs fixés (Figure 55). La plupart des responsables de la sécurité considèrent que leur entreprise dépense suffisamment dans la sécurité.

Figure 55 Pour 51 %, les dépenses de sécurité sont déterminées par les budgets précédents

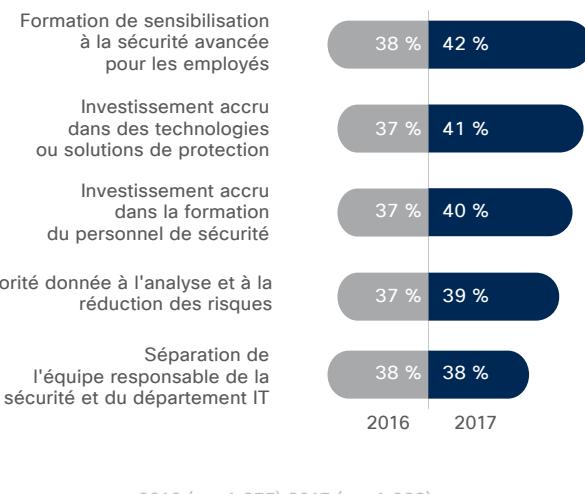


Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Lors de la planification des budgets, de nombreuses entreprises ont recours systématiquement à des listes de souhaits élaborés dans le cadre de plans de sécurité complets, afin de hiérarchiser les investissements à mesure que des ressources deviennent disponibles. Les investissements peuvent être redéfinis si de nouvelles vulnérabilités sont exposées, que ce soit à la suite d'un incident interne, d'une faille très médiatisée ou d'une évaluation courante des risques réalisée par un prestataire tiers.

En fait, il semble que ce soit surtout les failles qui favorisent les investissements futurs et par conséquent les améliorations dans la technologie et les processus. En 2017, 41 % des responsables sécurité ont déclaré que les failles de sécurité ont donné lieu à une augmentation des investissements dans les technologies et les solutions de sécurité, contre 37 % en 2016 (Figure 56). 40 % ont déclaré que les failles de sécurité sont à l'origine d'une augmentation des investissements dans la formation du personnel de sécurité, contre 37 % en 2016.

Figure 56 Les failles de sécurité donnent lieu à plus d'investissements dans les technologies et la formation



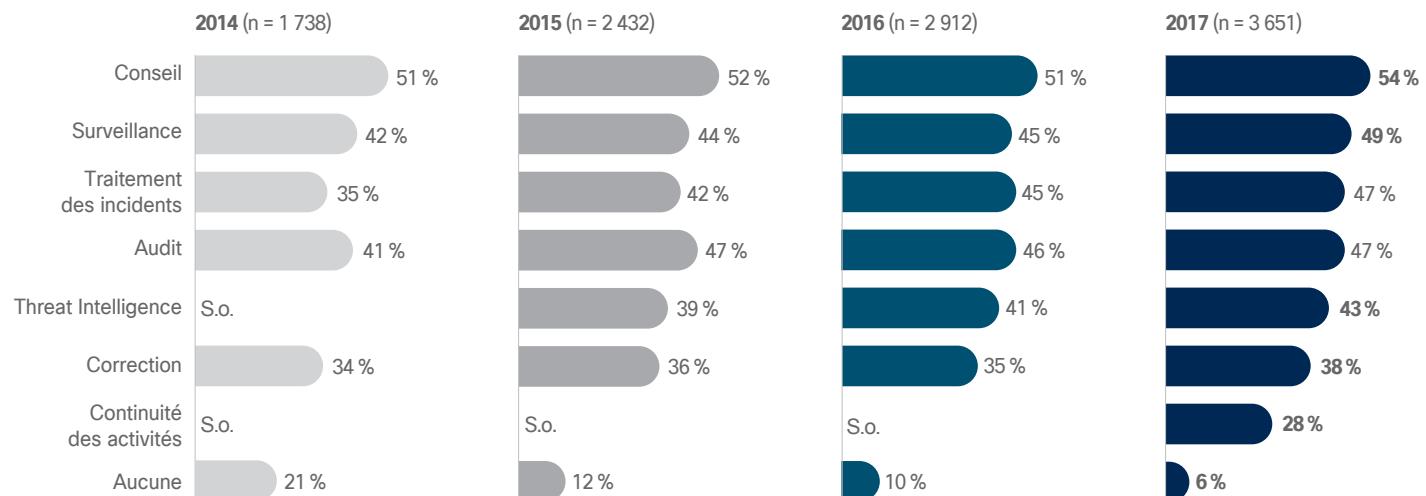
Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

 Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics

Les responsables sécurité s'attendent à dépenser plus dans des outils qui utilisent l'intelligence artificielle et l'apprentissage automatique en vue d'améliorer les défenses tout en supportant la charge de travail. En outre, ils prévoient d'investir dans des outils qui fourniront des protections pour les systèmes stratégiques, avec notamment des services d'infrastructure stratégique.

Pour étirer les ressources et renforcer les défenses, les entreprises intensifient leur recours à l'externalisation. Parmi les responsables sécurité, 49 % ont déclaré avoir externalisé les services de surveillance en 2017, contre 44 % en 2015 ; et 47 % ont déclaré avoir externalisé les réponses aux incidents en 2017, contre 42 % en 2015 (Figure 57).

Figure 57 L'externalisation de la surveillance et de la gestion des incidents augmente chaque année



Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité



Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics

i D'autres résultats de l'Enquête Cisco 2018 sur l'efficacité des mesures de sécurité sont fournis en annexe à la page 64.

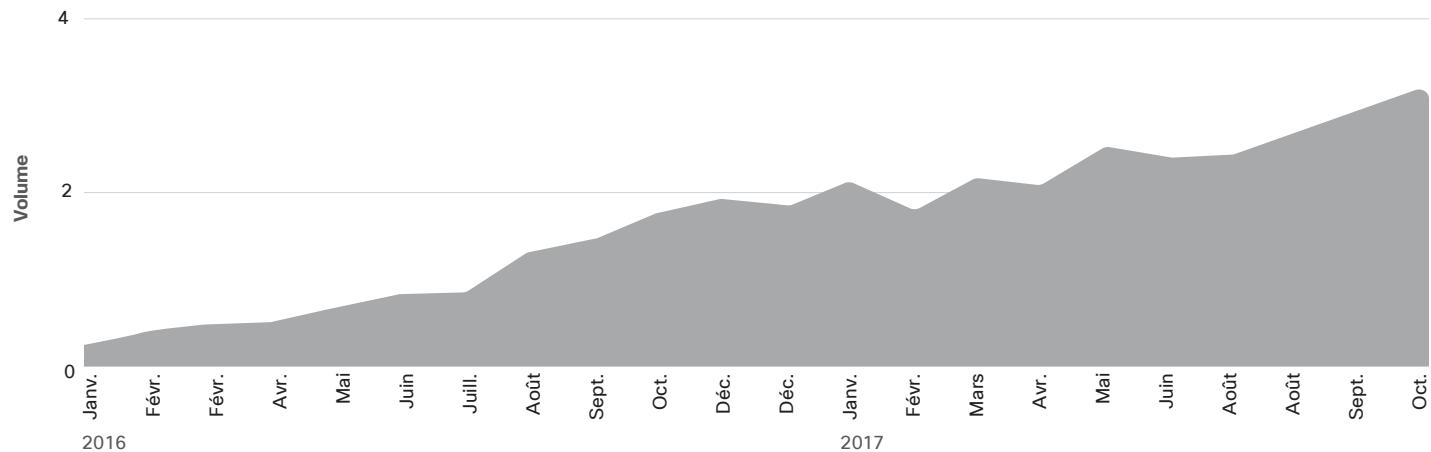
Conclusion

Conclusion

Le nombre de menaces modernes augmente et les hackers savent éviter la détection. Ils disposent d'outils plus efficaces, comme le chiffrement et savent mettre en œuvre des tactiques toujours plus sophistiquées et intelligentes, telles que le détournement de services Internet légitimes, pour dissimuler leur activité et contrer les technologies de sécurité classiques. De plus, ils changent constamment de tactiques pour que leurs malwares continuent à être efficaces. Même l'identification des menaces connues de la communauté de sécurité peut prendre beaucoup de temps.

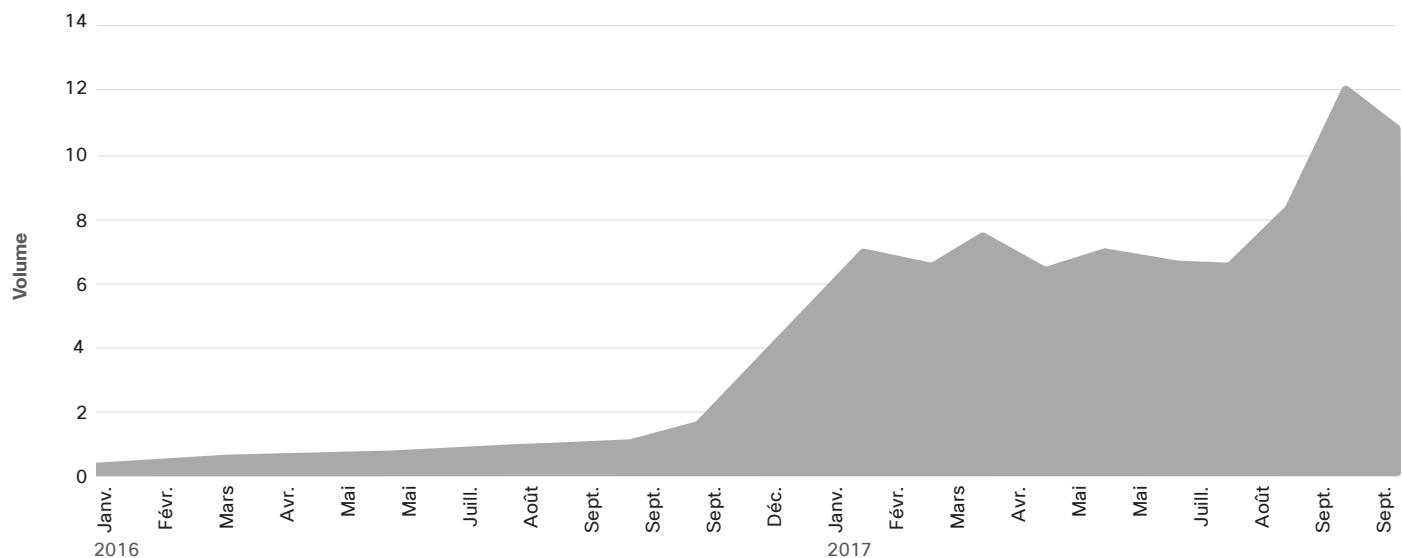
Une des raisons pour lesquelles les acteurs de la protection ont du mal à juguler les attaques et à réellement voir et comprendre l'évolution des menaces, est qu'ils ne parviennent pas à prendre la mesure du volume de trafic potentiellement malveillant auquel ils sont confrontés. Notre recherche montre que le volume du nombre total d'événements détectés par les produits de sécurité des terminaux basés sur le cloud Cisco a quadruplé de janvier 2016 à octobre 2017 (voir Figure 58). Le « nombre total d'événements » indique le nombre de tous les événements, inoffensifs ou malveillants, détectés par nos produits de sécurité des terminaux basé sur le cloud au cours de la période observée.

Figure 58 Nombre total d'événements



Source : Cisco Security Research

Figure 59 Volume global des malwares



Source : Cisco Security Research

Nos solutions de sécurité ont également constaté une multiplication par onze du volume global de malware pendant la même période, comme le montre la Figure 59.

L'augmentation en volume du nombre de logiciels malveillants impacte le temps de détection des menaces, qui est un indicateur important de mesure des performances de leurs défenses.

Le délai de détection médian selon Cisco qui est d'environ 4,6 heures pour la période de novembre 2016 à octobre 2017 illustre les difficultés rencontrées pour identifier rapidement les menaces qui évoluent constamment. Pourtant, ce chiffre est bien inférieur au délai de détection médian de 39 heures que nous avions indiqué lors de notre première évaluation en novembre 2015, et au délai moyen de 14 heures indiqué dans le

Rapport annuel Cisco 2017 sur la cybersécurité pour la période de novembre 2015 à octobre 2016.²⁰

L'utilisation des technologies de sécurité cloud a été un facteur déterminant grâce auquel Cisco est parvenu à maintenir à un niveau bas ses délais de détection médians. Le cloud permet d'adapter les performances à l'augmentation constante du volume des événements et du nombre de malware ciblant les terminaux. Les solutions de sécurité locales sont incapables d'offrir la même souplesse. Concevoir une solution pouvant traiter plus de 10 fois le volume des activités malveillantes sur une période de deux ans, et maintenir ou augmenter les délais de réponse, serait très difficile et coûteux pour toute entreprise.



Pour Cisco, le terme « délai de détection » désigne le laps de temps entre une compromission et l'identification 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 le téléchargement d'un fichier malveillant et le moment où la menace est détectée. Cette mesure concerne les fichiers malveillants non classés au moment de la détection.

Le délai de détection médian correspond à la moyenne des valeurs médianes mensuelles au cours de la période observée.

²⁰ Rapport annuel Cisco 2017 sur la cybersécurité : cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2017.html.

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 menaces 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 veille 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 programmes malveillants 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, data centers, terminaux, terminaux 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 CONTRIBUTEURS AU RAPPORT ANNUEL CISCO 2018 SUR LA CYBERSÉCURITÉ

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 annuel Cisco 2018 sur la cybersécurité**. 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.

Cisco Advanced Malware Protection (AMP) for Endpoints

Cisco AMP for Endpoints fournit des fonctionnalités automatisées de prévention, de détection et de gestion des incidents dans une même solution. Il recherche en permanence les signes d'activité malveillante pour détecter les menaces qui contournent la sécurité et présentent le plus grand risque pour l'entreprise. Il utilise une variété de techniques de détection, dont le sandboxing avancé, la prévention des exploits et l'apprentissage automatique pour détecter et éliminer rapidement les menaces. Cisco AMP for Endpoints est la seule solution qui assure une sécurité rétrospective pour réagir rapidement et identifier la portée, le point d'origine et la méthode pour endiguer la menace et protéger l'entreprise.

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.

Cisco Cognitive Threat Analytics

Cognitive Threat Analytics (CTA) de Cisco est un service cloud qui détecte les failles, les malwares opérant à l'intérieur des réseaux protégés et d'autres menaces, 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 périphériques. 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.

Équipe Cisco chargée de traiter les incidents liés à la sécurité des produits (PSIRT)

Cisco PSIRT (Product Security Incident Response) est une équipe mondiale chargée de collecter, d'analyser et de publier les informations sur les problèmes et les vulnérabilités liés à la sécurité qui touchent les produits et les réseaux Cisco. L'équipe reçoit des signalements de la part de chercheurs indépendants, d'entreprises du secteur, de fournisseurs tiers, de clients ou de toute autre source concernée par la sécurité des produits et des réseaux.

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 liés à la 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.

Groupe de recherche Cisco Talos

Composé de chercheurs, d'analystes et de techniciens d'excellence, le groupe de recherche Cisco Talos est l'une des plus vastes équipes au monde de Threat Intelligence dédiée aux entreprises. Ces équipes utilisent des systèmes sophistiqués et des données télémétriques de pointe pour produire des informations rapides, exactes et exploitables par les clients, produits et services de Cisco. Le groupe Talos protège les clients de Cisco contre les menaces connues et émergentes, détecte de nouvelles vulnérabilités dans les logiciels courants et arrête les menaces à la source avant qu'elles fassent d'autres dégâts ailleurs sur Internet. Les informations du centre Talos alimentent les produits Cisco dédiés à la détection, à l'analyse et à la protection contre les menaces connues et émergentes. Talos maintient à jour les jeux de règles officiels de Snort.org, ClamAV et SpamCop, et publie de nombreuses études et outils d'analyse open source.

Cisco Threat Grid

Cisco Threat Grid est une plate-forme d'analyse des malwares et de Threat Intelligence. Elle réalise des analyses statiques et dynamiques des échantillons suspects issus de nos clients et de nos intégrations de produits partout dans le monde. Des centaines de milliers d'échantillons, comprenant de nombreux types de fichiers différents, sont envoyés tous les jours via le portail cloud Threat Grid ou automatiquement via l'API Threat Grid. Cette plate-forme peut également être déployée en tant qu'appliance sur site.

Cisco Umbrella

Cisco Umbrella est une passerelle Internet sécurisée constituant la première ligne de défense contre les menaces qui circulent sur Internet, où que se trouvent les utilisateurs. Umbrella s'intègre avec l'accès Internet, ce qui lui confère une visibilité complète sur les activités de tous les sites, appareils et utilisateurs. En analysant ces activités, Umbrella détecte automatiquement les infrastructures d'attaque mises en place pour les menaces d'aujourd'hui et de demain, et bloque de façon proactive les requêtes avant qu'une connexion soit établie.

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 Cisco

PSIRT. 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 de Cisco qui permet d'identifier des indicateurs de compromission non encore détectés ou traités par les infrastructures de sécurité existantes.

Security and Trust Organization

Le département Security and Trust de Cisco souligne notre engagement à répondre à deux des enjeux les plus critiques 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.

Les partenaires technologiques du Rapport annuel Cisco 2018 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 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](https://twitter.com/@anomali).

LUMETA

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 de réseau connues, inconnues, fantômes et non autorisées plus efficacement que les autres solutions du marché, tout en proposant la surveillance en temps réel des terminaux et du réseau afin de détecter les modifications non autorisées, d'éviter les fuites de données, d'assurer une bonne segmentation du réseau et de détecter les comportements suspects sur les éléments de 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 à la demande de fonctions de sécurité adaptative essentielles 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.



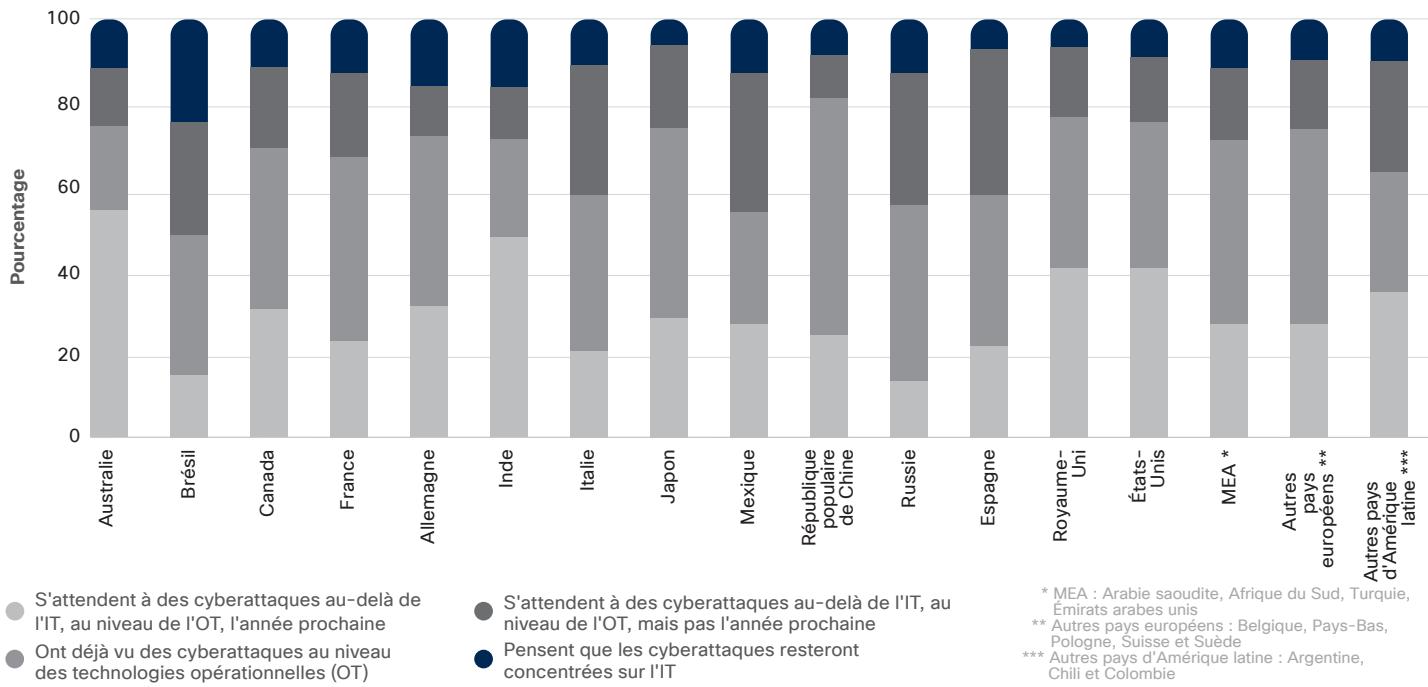
SAINT Corporation, leader dans le domaine des solutions intégrées de gestion des vulnérabilités de nouvelle génération, aide les entreprises et les institutions publiques à identifier les risques à tous les niveaux. Grâce à SAINT, l'accès, la sécurité et la confidentialité peuvent coexister pour le bénéfice 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.



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.

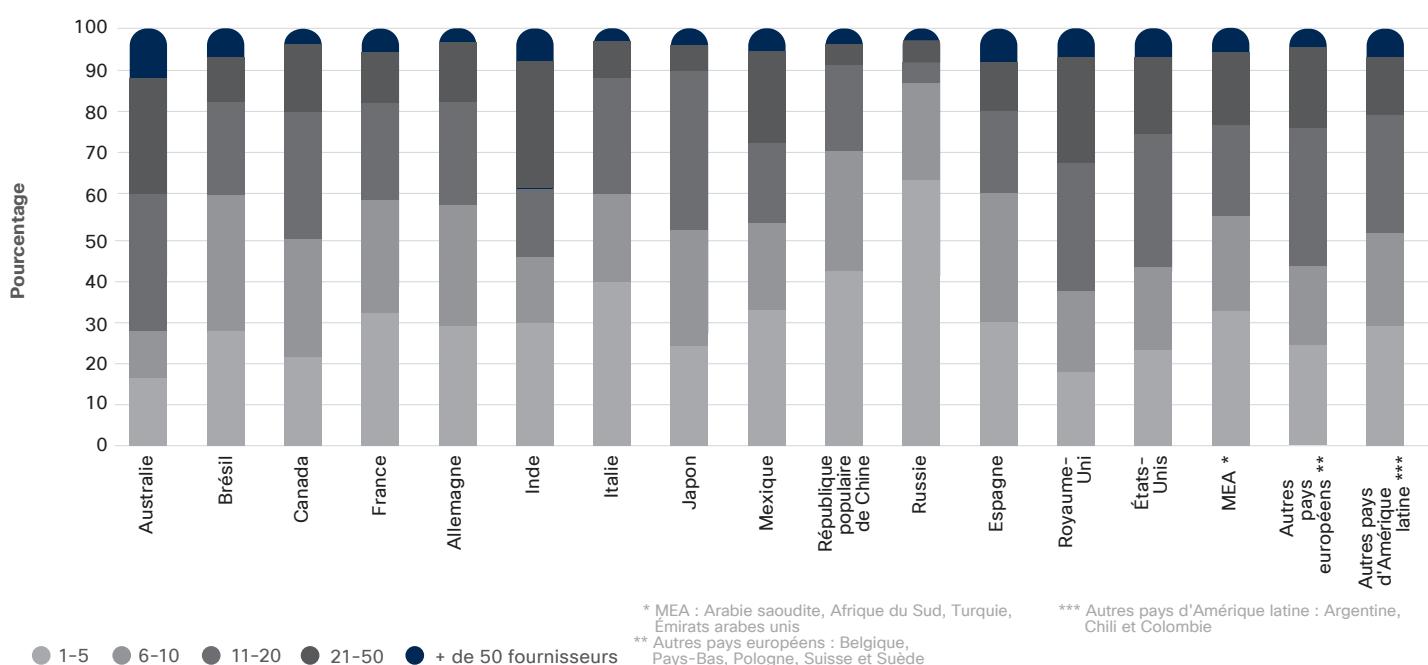
Annexe

Figure 60 Estimations des cyberattaques au niveau de l'OT et de l'IoT, par pays ou région



Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Figure 61 Nombre de fournisseurs de solutions de sécurité dans l'environnement, par pays ou région

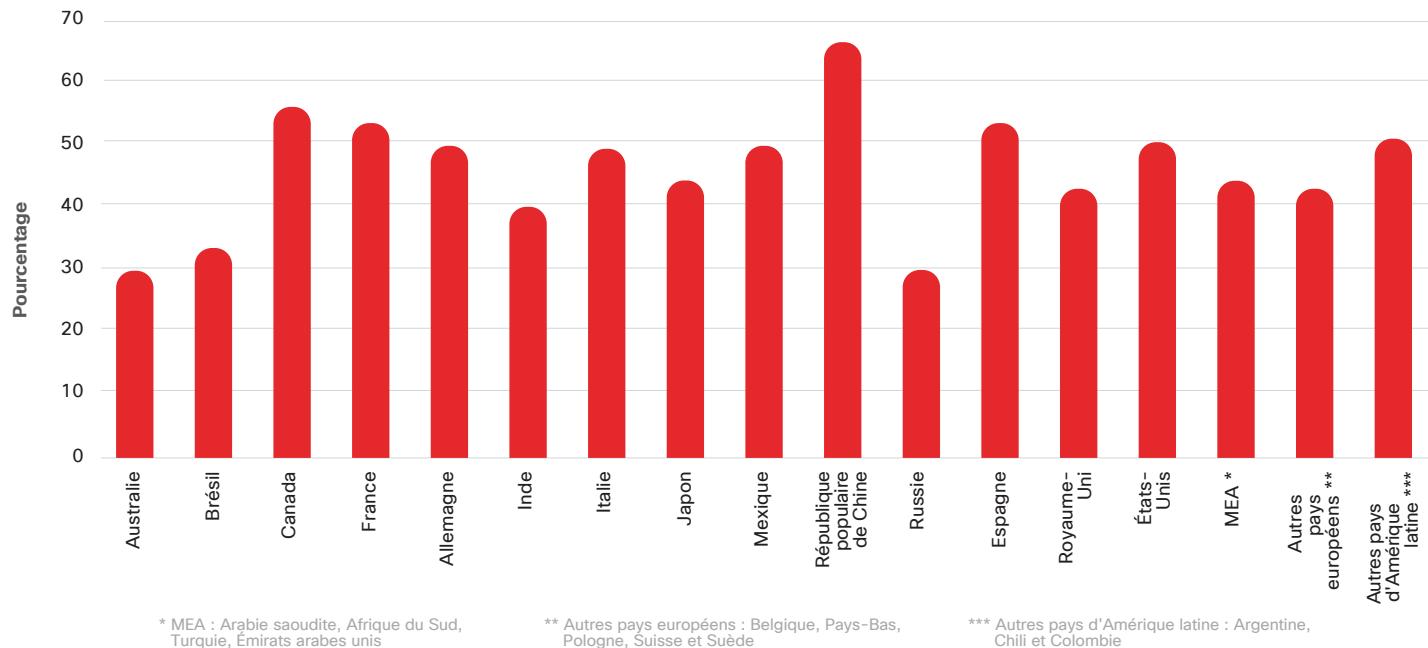


Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité



Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics

Figure 62 Pourcentage des alertes analysées, par pays ou région



Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Figure 63 Obstacles à l'adoption de processus et de technologies de sécurité avancés, par pays ou région

Quels sont pour vous les principaux obstacles à l'adoption de processus et technologies de sécurité avancés ?

	Australie	Brésil	Canada	France	Allemagne	Inde	Italie	Japon	Mexique	République populaire de Chine	Russie	Espagne	Royaume-Uni	États-Unis	MEA*	Autres pays européens**	Autres pays d'Amérique latine***
Contraintes budgétaires	23 %	35 %	29 %	33 %	25 %	36 %	38 %	31 %	31 %	38 %	60 %	33 %	27 %	34 %	36 %	37 %	35 %
Autres priorités	28 %	11 %	29 %	27 %	28 %	26 %	24 %	27 %	16 %	27 %	20 %	18 %	32 %	32 %	25 %	18 %	24 %
Manque de personnel qualifié	25 %	28 %	19 %	22 %	24 %	31 %	24 %	28 %	30 %	25 %	35 %	33 %	31 %	26 %	25 %	23 %	26 %
Manque de connaissances sur les technologies et les processus de sécurité avancée	26 %	26 %	24 %	21 %	22 %	24 %	21 %	26 %	23 %	29 %	18 %	21 %	27 %	22 %	22 %	17 %	21 %
Problèmes de compatibilité avec les systèmes légaux	27 %	19 %	30 %	27 %	30 %	30 %	22 %	23 %	32 %	40 %	25 %	25 %	24 %	28 %	30 %	25 %	28 %
Exigences de certification	33 %	27 %	29 %	29 %	24 %	27 %	27 %	22 %	27 %	23 %	22 %	27 %	27 %	30 %	24 %	33 %	21 %
Attitude/culture de l'entreprise en matière de sécurité	30 %	23 %	25 %	20 %	16 %	26 %	17 %	21 %	26 %	17 %	19 %	24 %	28 %	25 %	20 %	20 %	27 %
Réticence à l'achat avant que les produits aient fait leurs preuves sur le marché	19 %	20 %	23 %	26 %	25 %	29 %	20 %	28 %	15 %	16 %	17 %	20 %	21 %	22 %	22 %	21 %	25 %
Charge de travail trop importante pour accepter de nouvelles responsabilités	22 %	16 %	28 %	18 %	28 %	28 %	26 %	27 %	23 %	21 %	15 %	28 %	22 %	22 %	20 %	17 %	19 %
L'entreprise n'est pas une cible de choix pour les hackers	25 %	18 %	21 %	22 %	24 %	17 %	14 %	20 %	12 %	16 %	11 %	13 %	21 %	21 %	21 %	20 %	16 %
La sécurité n'est pas considérée comme une haute priorité par la direction	22 %	10 %	17 %	17 %	20 %	13 %	13 %	23 %	15 %	18 %	11 %	11 %	19 %	19 %	17 %	19 %	21 %

* MEA : Arabie saoudite, Afrique du Sud, Turquie, Emirats arabes unis

** Autres pays européens : Belgique, Pays-Bas, Pologne, Suisse et Suède

*** Autres pays d'Amérique latine : Argentine, Chili et Colombie

Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité



Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics

Figure 64 Achat de solutions de défense contre les menaces, par pays ou région

Qu'est-ce qui définit le mieux l'approche de votre entreprise concernant l'achat de solutions de défense contre les menaces ?

Pays	N=	Achète en général des produits de pointe ciblés pour répondre à des besoins spécifiques	Achète en général des produits conçus pour fonctionner ensemble
Australie	203	86	14
Brésil	197	72	28
Canada	185	67	33
France	191	59	41
Allemagne	195	69	31
Inde	199	78	22
Italie	201	71	29
Japon	223	72	28
Mexique	198	77	23
République populaire de Chine	205	63	37
Russie	196	58	42
Espagne	148	70	30
Royaume-Uni	194	76	24
États-Unis	393	81	19
MEA*	249	69	31
Autres pays européens **	199	73	27
Autres pays d'Amérique latine ***	196	71	29

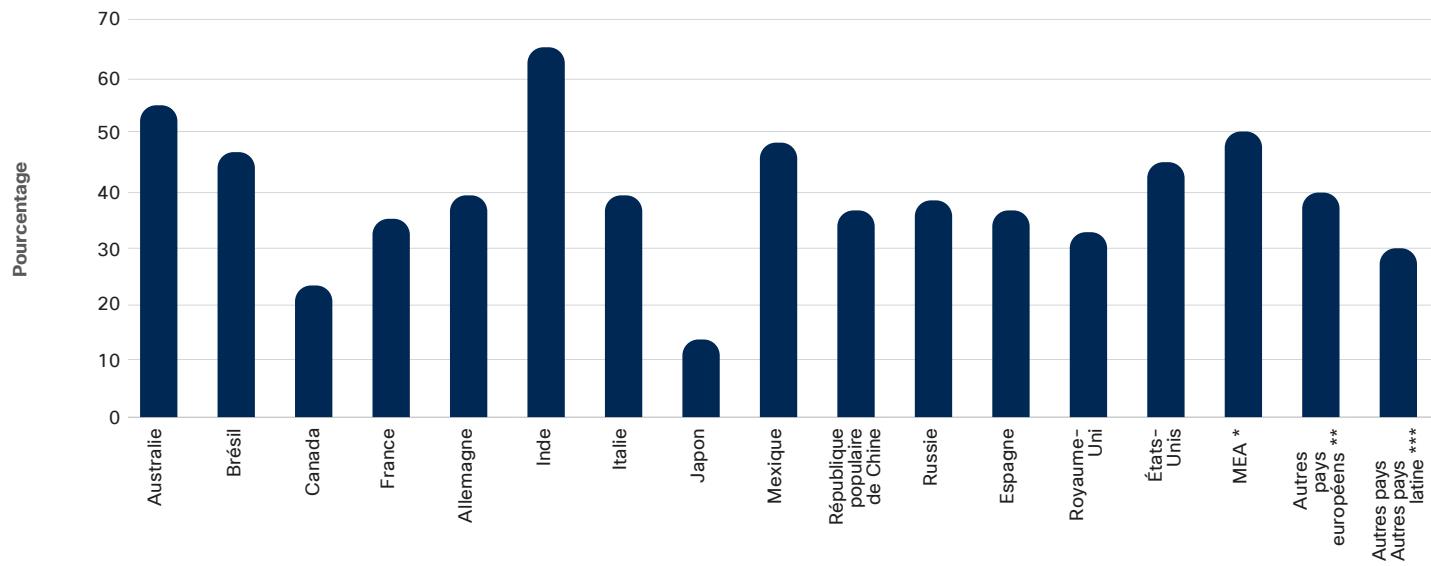
* MEA : Arabie saoudite, Afrique du Sud, Turquie, Émirats arabes unis

** Autres pays européens : Belgique, Pays-Bas, Pologne, Suisse et Suède

*** Autres pays d'Amérique latine : Argentine, Chili et Colombie

Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

Figure 65 Pourcentage des entreprises estimant très bien respecter le cadre InfoSec standardisé, par pays ou région



* MEA : Arabie saoudite, Afrique du Sud, Turquie, Émirats arabes unis

** Autres pays européens : Belgique, Pays-Bas, Pologne, Suisse et Suède

*** Autres pays d'Amérique latine : Argentine, Chili et Colombie

Source : Enquête Cisco 2018 sur l'efficacité des mesures de sécurité

 Téléchargez les graphiques pour 2018 à l'adresse : cisco.com/go/acr2018graphics

Télécharger les graphiques

Vous pouvez télécharger tous les graphiques de ce rapport à l'adresse : cisco.com/go/mcr2018graphics.

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, Californie

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 bureaux à travers le monde. Leurs adresses, numéros de téléphone et numéros de fax sont répertoriés sur le site web www.cisco.com/go/offices.

Publié en février 2018

© 2018 Cisco et/ou ses filiales. Tous droits réservés.

Cisco et le logo Cisco sont des marques commerciales ou déposées de Cisco et/ou de ses filiales aux États-Unis et dans d'autres pays. Pour consulter la liste des marques commerciales de Cisco, visitez : www.cisco.com/go/trademarks. Les autres marques commerciales mentionnées dans ce document sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat entre Cisco et toute autre entreprise. (1110R)

Adobe, Acrobat et Flash sont des marques déposées ou des marques commerciales d'Adobe Systems Incorporated aux États-Unis et/ou dans d'autres pays.