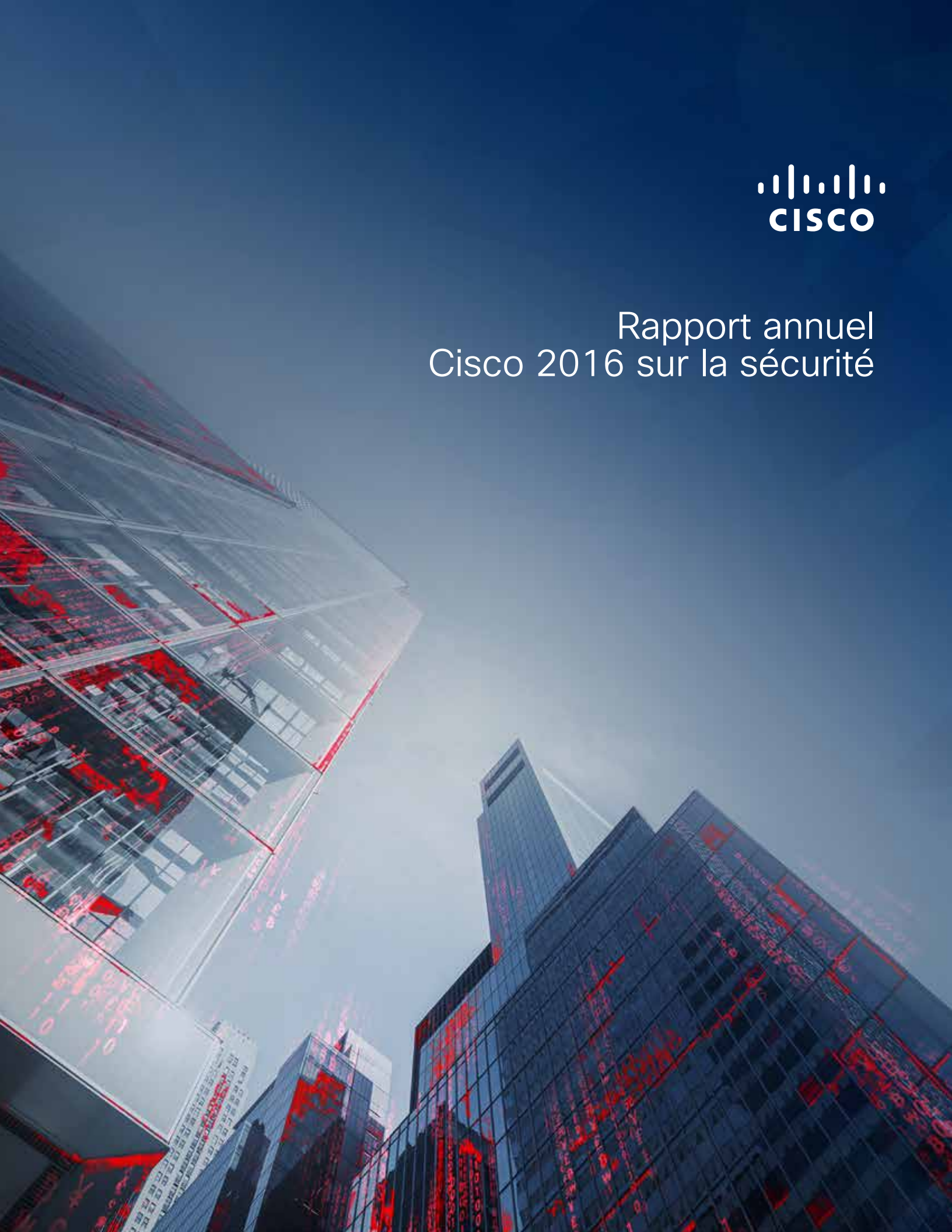


Rapport annuel Cisco 2016 sur la sécurité

Synthèse

Les professionnels de la sécurité doivent repenser leurs stratégies de défense.

Les cybercriminels et les acteurs de la protection élaborent des technologies et des tactiques qui gagnent en complexité. De leur côté, les hackers construisent de solides infrastructures de back-end destinées à exécuter et à sous-tendre leurs campagnes. Les cybercriminels optimisent leurs techniques visant à extorquer de l'argent à leurs victimes et à échapper à la détection tout en continuant à dérober des données et la propriété intellectuelle.

Le rapport annuel Cisco 2016 sur la sécurité présente les résultats de recherches, d'analyses et de perspectives menées par Cisco Security Research, et met en exergue les défis que rencontrent les acteurs de la protection dans leurs tentatives pour détecter et bloquer des pirates qui utilisent un arsenal d'outils diversifié et en constante évolution. Le rapport fait également part de la recherche menée par des experts externes tels que Level 3 Threat Research Labs, afin de mieux expliciter les tendances actuelles en termes de menace.

Les données compilées par les chercheurs Cisco illustrent les changements observés dans la durée ; nous en analysons la signification et expliquons comment les professionnels de la sécurité doivent répondre aux menaces.

Dans ce rapport, nous présentons et abordons les points ci-après :

LA VEILLE SUR LES MENACES

Cette section examine certaines des tendances les plus intéressantes en matière de cybersécurité identifiées par nos chercheurs. Elle décrit également les vecteurs d'attaque Web, les méthodes d'attaque Web et les vulnérabilités. Nous y abordons aussi les menaces en voie d'évolution, comme les « logiciels rançonneurs ». Pour dégager les tendances de l'année 2015, le département Cisco Security Research a analysé des données télémétriques recueillies dans le monde entier.

CONNAISSANCE DE L'INDUSTRIE

Cette section examine les tendances de sécurité qui affectent les entreprises, notamment le recours croissant au cryptage, et les risques de sécurité potentiels inhérents. Nous observons les faiblesses dans la manière dont les PME protègent leurs réseaux. Nous présentons des recherches portant sur des entreprises dont l'infrastructure informatique repose sur des composants logiciels obsolètes, sans assistance ou en fin de vie.

ENQUÊTE SUR L'EFFICACITÉ DES MESURES DE SÉCURITÉ

Cette section présente les résultats de la deuxième enquête sur l'efficacité des mesures de sécurité conduite par Cisco, axée sur la perception qu'ont les professionnels de la sécurité quant à la situation de la sécurité dans leurs entreprises. En comparant les résultats de l'enquête 2015 à ceux de 2014, Cisco a identifié que les responsables de la sécurité et les responsables des équipes chargées de la sécurité sont moins confiants sur le fait que leur infrastructure de sécurité est à jour, ou qu'ils sont en mesure de contrer les attaques. Cependant, l'enquête révèle également que les entreprises intensifient la formation et d'autres processus de sécurité afin de renforcer leurs réseaux. Les résultats de cette enquête sont présentés en exclusivité dans le rapport annuel 2016 de Cisco sur la sécurité.

PERSPECTIVES

Cette section fournit un aperçu du paysage géopolitique affectant la sécurité. Nous abordons ici les résultats de deux études de Cisco : la première examine les préoccupations des dirigeants concernant la cybersécurité ; la seconde met l'accent sur la perception des décideurs informatiques en matière de risque de sécurité et de fiabilité. Nous proposons également une vue actualisée de nos progrès en matière de réduction des délais de détection, et nous insistons sur les avantages à migrer vers une architecture intégrée de défense contre les menaces.

Sommaire

Découvertes et développements majeurs

Découvertes et développements majeurs

Les cybercriminels ont affiné leurs infrastructures back-end pour mener des attaques de manière à accroître leur efficacité et leurs profits.

- Cisco, avec l'aide de Level 3 Threat Research Labs et la coopération de l'hébergeur Limestone Networks, a identifié et écarté la plus grande opération du kit d'exploits Angler aux États-Unis. Les cybercriminels qui en sont à l'origine ciblaient 90 000 victimes par jour et prévoyaient de générer des dizaines de millions de dollars par an.
- SSHPsychos (Group 93), l'un des plus grands botnets de DDoS jamais observés par les chercheurs de Cisco, a été considérablement affaibli par les efforts conjugués de Cisco et de Level 3 Threat Research Labs. Comme le cas Angler mentionné ci-avant, cette réussite illustre la valeur de la collaboration industrielle pour lutter contre les cybercriminels.
- Les extensions malveillantes de navigateur peuvent constituer une source importante de fuites de données pour les entreprises et sont un problème très répandu. Nous estimons que les entreprises étudiées sont affectées, pour plus de 85 % d'entre elles, par des extensions malveillantes de navigateur.
- Les botnets clairement identifiés comme Bedep, Gamarue et Miuref ont représenté la majorité des activités de contrôle-commande de botnets affectant un groupe d'entreprises que nous avons analysées en juillet 2015.
- Les travaux d'analyse conduits par Cisco sur les programmes malveillants identifiés comme « menace connue » ont montré que la plupart de ces programmes, soit 91,3 % d'entre eux, font usage du service DNS pour mener leurs campagnes. Via une enquête rétrospective menée sur les requêtes DNS, Cisco a mis en évidence des résolveurs DNS « sauvages » sur les réseaux des clients. Ceux-ci n'étaient pas au courant que ces résolveurs étaient utilisés par leurs employés dans le cadre de leur infrastructure DNS.
- Les vulnérabilités Adobe Flash continuent d'être exploitées par les cybercriminels. Toutefois, les fournisseurs de logiciels réduisent le risque que les utilisateurs soient exposés à des actions malveillantes via la technologie flash.
- Sur la base de l'observation des tendances 2015, nos chercheurs indiquent que le trafic crypté HTTPS a atteint un tournant : il représentera bientôt la forme dominante du trafic Internet. Bien que le cryptage puisse protéger les consommateurs, il peut également affecter l'efficacité des produits de sécurité, ce qui complique pour la communauté de la sécurité le suivi des menaces. Pour ne rien arranger, certains programmes malveillants peuvent engager des communications cryptées via divers ports.
- Les hackers utilisent pour leurs activités criminelles des sites compromis, créés au moyen de la célèbre plate-forme WordPress de développement Web. Ainsi, ils peuvent mobiliser les ressources serveur et échapper à la détection.

- Les infrastructures informatiques vieillissent de plus en plus, ce qui fragilise davantage les entreprises. Nous avons analysé 115 000 équipements Cisco® sur Internet et découvert que 92 % des appareils de notre échantillon exploitaient un composant logiciel porteur de vulnérabilités connues. En outre, 31 % des équipements Cisco du panel étaient en fin de commercialisation et 8 % étaient en fin de vie.
- En 2015, les responsables de la sécurité se montrent moins confiants dans leurs outils et processus de sécurité qu'en 2014, selon l'enquête 2015 sur l'efficacité des mesures de sécurité de Cisco. Par exemple, en 2015, 59 % des entreprises déclarent que leur infrastructure de sécurité est « très à jour ». En 2014, 64 % des sondés avaient fourni la même réponse. Cependant, leur inquiétude croissante quant à leur sécurité les incite à améliorer leurs moyens de défense.
- L'enquête sur l'efficacité montre que les PME utilisent moins de défenses que les grandes entreprises. Par exemple, en 2015, 48 % des PME ont indiqué utiliser une solution de sécurité Web, contre 59 % en 2014. 29 % ont indiqué avoir utilisé des correctifs et des outils de configuration en 2015, contre 39 % en 2014. Ces faiblesses peuvent mettre en danger les entreprises clientes des PME car les pirates peuvent plus facilement s'introduire dans les réseaux des PME.
- Depuis mai 2015, Cisco a réduit le délai moyen de détection des menaces connues dans nos réseaux à environ 17 heures, moins d'une journée. Cela dépasse largement l'estimation courante sur le marché du délai de détection, qui est de 100 à 200 jours.

L'aspect financier compte : pour les cybercriminels modernes, il est important de gagner de l'argent

L'aspect financier compte : pour les cybercriminels modernes, il est important de gagner de l'argent

Par le passé, de nombreux cybercriminels se dissimulaient dans l'ombre de l'Internet. Ils tentaient d'éviter toute détection en se contentant de brèves incursions sur les réseaux des entreprises pour lancer leurs attaques. Aujourd'hui, certains cybercriminels enhardis s'affichent sur des ressources en ligne légitimes. Ils amenuisent la capacité des serveurs, dérobent des données et exigent des rançons de victimes en ligne dont ils détiennent en otage les informations.

Ces campagnes représentent une escalade inquiétante de la guerre entre les défenseurs et les pirates. Si les pirates trouvent plus de points en ligne à partir desquels opérer, leur impact peut croître de façon exponentielle.

Dans ce rapport, les experts en sécurité Cisco mettent en évidence les tactiques que les criminels utilisent pour bâtir une infrastructure solide afin de rendre leurs campagnes plus efficaces et percutantes. Les cybercriminels continuent d'adopter des méthodes plus efficaces afin d'augmenter leurs profits, beaucoup accordent une attention particulière à l'exploitation des ressources serveur.

L'explosion des logiciels rançonneurs (voir **page 10**) en est un parfait exemple. Les logiciels rançonneurs fournissent aux criminels un moyen simple d'extorquer davantage d'argent directement auprès des utilisateurs. Lorsque les criminels élaborent des campagnes qui compromettent des dizaines de milliers d'utilisateurs chaque jour, avec peu ou pas d'interruption, le « retour sur investissement » de leurs efforts peut être stupéfiant. En plus de développer de meilleures façons de monétiser leurs campagnes, les criminels viennent squatter des ressources légitimes des entreprises.

Les concepteurs de certaines variantes de logiciel rançonneur ainsi que les développeurs d'autres exploits utilisent désormais des sites Web WordPress piratés comme moyen d'occuper de l'espace serveur et d'éviter d'être détectés (voir **page 33**). Citons également SSHPsychos, l'un des plus grands botnets jamais vus par les chercheurs de Cisco, exécuté sur des réseaux standard avec peu d'interférences jusqu'à ce qu'une démarche concertée de Cisco et de Level 3 Threat Research Labs ait convaincu les opérateurs télécoms de bloquer le trafic des créateurs du botnet.

Veille sur les menaces

Veille sur les menaces

Cisco a collecté et analysé un important volume de données télémétriques mondiales pour les besoins de ce rapport. Nos experts travaillent sans relâche sur les menaces nouvelles, comme le trafic de programmes malveillants. Leurs analyses permettent d'avoir une indication du comportement à venir des cybercriminels et aident à détecter les menaces.

Témoignages

Grâce à une collaboration industrielle efficace, Cisco met en échec un kit d'exploits et une campagne de rançonnage à grande échelle particulièrement profitables

Le kit d'exploits Angler est l'un des plus étendus et des plus efficaces qui soient. Il a été associé à plusieurs campagnes de haut vol de malvertising (publicité malveillante) et de rançonnage. Il a largement contribué à l'explosion globale de l'activité de rançonnage que nos experts surveillent étroitement depuis quelques années. Les criminels utilisent les logiciels rançonneurs pour crypter les fichiers des utilisateurs, et ne fournissent les codes de décryptage qu'après que les utilisateurs se sont acquittés d'une « rançon », comprise généralement entre 300 et 500 $.

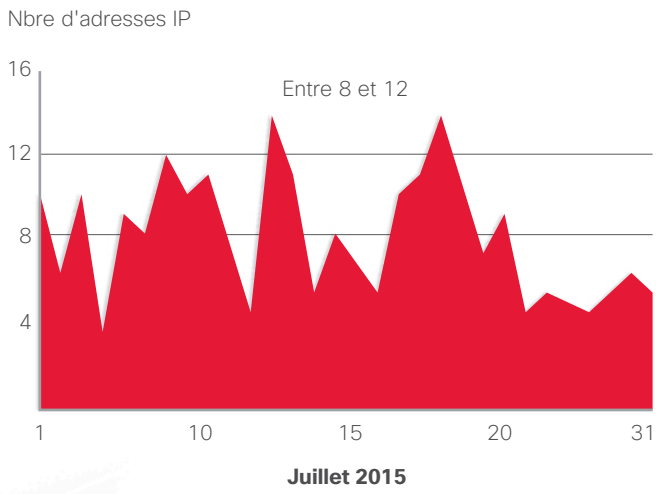
Ainsi que le signalait le rapport semestriel 2015 Cisco sur la cybersécurité, les crypto-monnaies telles que le Bitcoin et les réseaux d'anonymisation tels que Tor permettent aux cyberpirates de se lancer encore plus facilement sur le marché des programmes malveillants et de générer rapidement des revenus. Le gain de popularité des logiciels rançonneurs peut être lié à deux avantages essentiels : l'opération est aisée à mettre en œuvre pour les cybercriminels, et elle procure un accès rapide à la monétisation car les utilisateurs paient directement en crypto-monnaies.

En étudiant Angler et les tendances liées aux logiciels rançonneurs, Cisco a relevé que certains opérateurs du kit d'exploits utilisaient un pourcentage excessif de serveurs proxy mondiaux situés sur des serveurs exploités par Limestone Networks. Cette utilisation des serveurs est un exemple qui illustre bien une autre tendance que nos experts ont observée dans l'économie parallèle récemment : les cybercriminels associent ressources légitimes et ressources malveillantes pour lancer leurs campagnes.

En l'occurrence, l'infrastructure IP sous-tendant Angler n'était pas étendue. Généralement, le nombre quotidien de systèmes actifs oscillait entre 8 et 12. La plupart n'étaient actifs que pour une journée. La Figure 1 montre le nombre d'adresses IP uniques que Cisco a observées au cours de juillet 2015.

Cisco a déterminé que les opérateurs d'Angler changeaient d'adresses IP de manière linéaire pour dissimuler leur activité et empêcher que cesse leur collecte d'argent.

Figure 1 : Nombre d'adresses IP d'Angler par date, juillet 2015



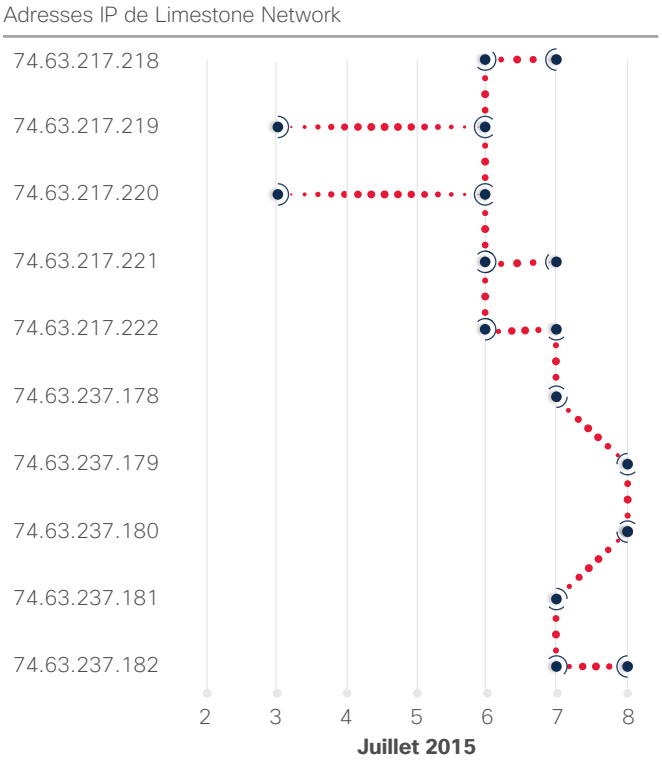
Source : Cisco Security Research

Comme l'illustre la Figure 2, Angler commence par une adresse IP (ici, 74.63.217.218). Lorsque le système compromet les utilisateurs et génère des perturbations que les défenseurs commencent à détecter, les cybercriminels adoptent une adresse IP voisine (74.63.217.219). Cette activité se poursuit dans les blocs contigus de l'espace IP d'un hébergeur unique.

Cisco a analysé les informations IP afin d'identifier les numéros de système autonome (ASN) et les fournisseurs associés aux adresses IP. Nous avons déterminé que la majeure partie du trafic associé à Angler émanait de serveurs exploités par deux hébergeurs légitimes : Limestone Networks et Hetzner (Figure 3). Ils représentaient près de 75 % du volume du trafic global du mois de juillet.

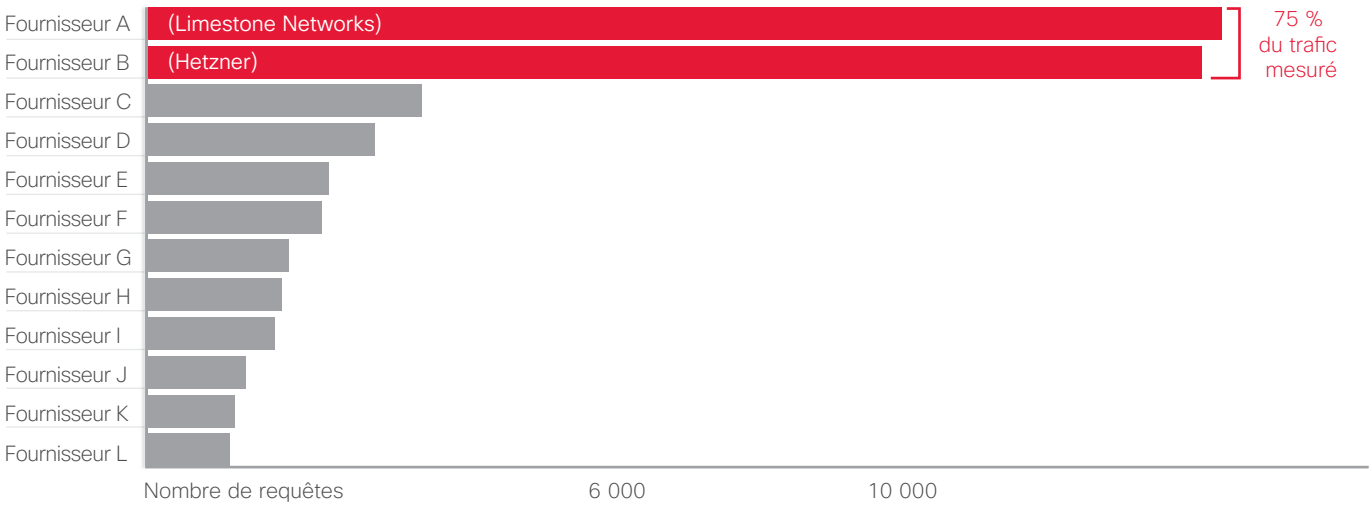
Cisco a tout d'abord contacté Limestone Networks, qui semblait héberger la plus grande partie d'Angler. Limestone a saisi l'opportunité d'apporter sa collaboration. L'entreprise traitait chaque mois un nombre excessif de rétrofacturations de carte de crédit, car les cybercriminels se servaient de cartes bancaires et de noms frauduleux pour acheter en échange de milliers de dollars des plages aléatoires des serveurs.

Figure 2 : Infrastructure d'adresse IP basse sous-tendant Angler



Source : Cisco Security Research

Figure 3 : Requêtes HTTP Angler par fournisseur, juillet 2015



Source : Cisco Security Research

L'approche adoptée par les cybercriminels pour acheter des serveurs permettait difficilement d'associer l'activité frauduleuse à un seul acteur. Par exemple, un criminel peut louer trois ou quatre serveurs un jour, puis utiliser un nom et une carte bancaire différents pour louer trois ou quatre serveurs le lendemain. Ainsi, ils peuvent essentiellement « passer » d'une adresse IP à la suivante lorsque des serveurs compromis ont été identifiés et mis hors ligne par les techniciens.

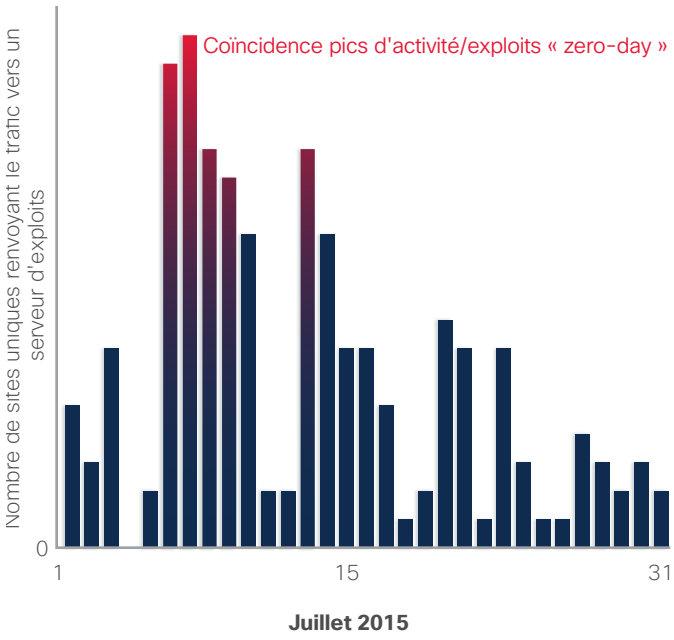
Pour enquêter sur cette activité, Cisco a fait appel à Level 3 Threat Research Labs ainsi qu'à OpenDNS, une entreprise de Cisco. Level 3 Threat Research Labs a été en mesure de fournir une meilleure compréhension globale de la menace, donnant à Cisco la possibilité d'en percevoir un peu mieux la portée et d'en estimer l'envergure à son paroxysme. De son côté, OpenDNS a fourni un éclairage unique sur l'activité des domaines associée à la menace, permettant à Cisco de mieux comprendre comment les techniques telles que le « domain shadowing » étaient utilisées par les pirates.

Les experts Cisco ont ensuite cherché comment, plus précisément, les utilisateurs entraient en contact avec Angler et se voyaient imposer des charges malveillantes. Les experts ont observé des sites Web populaires rediriger des utilisateurs vers le kit d'exploits Angler via des publicités malveillantes. Les fausses publicités ont été diffusées sur des centaines de grands sites d'actualité, d'immobilier et de culture populaire. La communauté de la sécurité désigne habituellement ces sites comme « sites de bonne réputation ».

En outre, les experts Cisco ont découvert d'innombrables exemples de sites Web de petite taille, apparemment aléatoires, opérant le même type de redirection, y compris la notice nécrologique d'une seule personne dans un petit journal rural aux États-Unis. Il est plus que probable que cette dernière stratégie a été conçue pour cibler les personnes âgées. Cette population est généralement plus susceptible d'utiliser les navigateurs Web par défaut, tels que Microsoft Internet Explorer, et est moins consciente de la nécessité de corriger régulièrement les vulnérabilités d'Adobe Flash.

Un autre aspect notable de cette opération Angler réside dans le nombre de prescripteurs uniques et de la faible fréquence avec laquelle ils ont été utilisés (Figure 4). Les internautes ont été redirigés vers le kit d'exploits Angler par plus de 15 000 sites uniques que nous avons identifiés, dont 99,8 % ont été utilisés moins de 10 fois. La plupart des prescripteurs n'étaient donc actifs que pendant une courte période et ont été supprimés après qu'une poignée d'utilisateurs ont été ciblés. Dans notre analyse de juillet 2015, nous avons constaté que les pics d'activité coïncidaient avec les divers exploits « zero-day » de la Hacking Team (CVE-2015-5119, CVE-2015-5122).[1]

Figure 4 : Prescripteurs uniques par jour, juillet 2015



Source : Cisco Security Research

Cisco a déterminé qu'environ 60 % des charges utiles d'Angler produites par cette opération particulière généraient un certain type de variante du logiciel rançonneur (Cryptowall 3.0 dans la plupart des cas). D'autres charges utiles intégraient Bedep, un téléchargeur de programmes malveillants qui est généralement utilisé pour installer un programme malveillant de campagne de fraude au clic. (Voir « Infections touchant les navigateurs : très répandues et source majeure de fuite de données » **page 16**.) Les deux types de programmes malveillants sont conçus pour permettre aux cybercriminels de soutirer beaucoup d'argent auprès des utilisateurs compromis, très rapidement et avec peu ou pas d'efforts.

[1] « Adobe Patches Hacking Team's Flash Player Zero-Day, » par Eduard Kovacs, *SecurityWeek*, 8 juillet 2015 : **http://www.securityweek.com/adobe-patches-hacking-teams-flash-player-zero-day**.

Revenus d'Angler

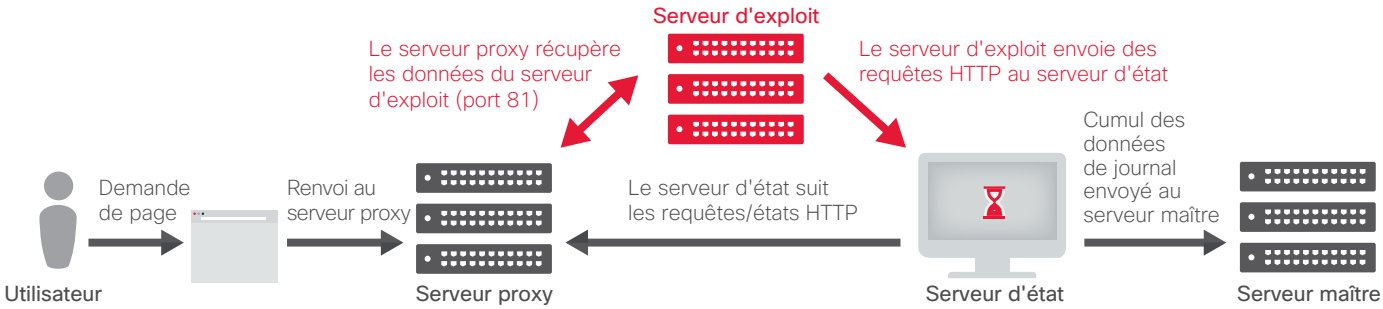
Source : Cisco Security Research

Selon l'enquête de Cisco, le principal acteur responsable de la moitié environ de l'activité du kit d'exploits Angler de cette campagne particulière visait jusqu'à 90 000 victimes par jour. Selon notre estimation, la campagne rapportait aux cybercriminels plus de 30 millions de $ par an.

Vraisemblablement, le réseau externe à Hetzner présentait un taux de réussite similaire. Cela signifie que le cybercriminel à l'initiative de l'opération impliquant les serveurs Limestone Networks et Hetzner était responsable de la moitié de l'activité mondiale d'Angler au moment de l'analyse de Cisco. Les experts de Cisco estiment que cette opération pouvait générer des revenus bruts de 60 millions de dollars par an.

PARTAGER

Figure 5 : Infrastructure back-end d'Angler



Source : Cisco Security Research

Cisco a également découvert que les serveurs auxquels se connectaient les utilisateurs n'hébergeaient pas d'activité malveillante d'Angler. Ils servaient de relais. Un utilisateur entrant dans la chaîne de redirection qui soumet une requête GET pour accéder à une page de destination, sera renvoyé sur le serveur proxy. Le serveur proxy achemine le trafic vers un serveur d'exploits dans un autre pays, chez un autre fournisseur. Au cours de notre recherche, nous avons constaté qu'un seul serveur d'exploits était associé à plusieurs serveurs proxy. (Voir Figure 5.)

Cisco a identifié un serveur d'état qui traitait des tâches telles que la surveillance de l'intégrité. Chaque serveur proxy unique que le serveur d'état surveillait possédait une paire d'URL unique. En cas d'interrogation sur le chemin, le serveur d'état devait renvoyer un code d'état HTTP « 204 ». Les pirates pouvaient identifier de manière unique chaque serveur proxy et s'assurer non seulement qu'il était en fonctionnement, mais que les acteurs de la protection ne l'avaient pas modifié. Au moyen de l'autre URL, les pirates pouvaient collecter les journaux depuis le serveur proxy et déterminer le niveau d'efficacité du fonctionnement du réseau.

La collaboration industrielle s'est avérée être une composante essentielle de la capacité de Cisco à enquêter sur l'activité du kit d'exploits Angler. En définitive, elle a permis de stopper les redirections vers les serveurs proxy Angler chez un opérateur télécoms aux États-Unis. Elle a aussi sensibilisé l'opinion à l'existence d'une activité cybercriminelle hautement sophistiquée qui affectait des milliers d'utilisateurs chaque jour.

PARTAGER

Cisco a travaillé en étroite collaboration avec Limestone Networks pour identifier de nouveaux serveurs dès qu'ils étaient mis en ligne et pour surveiller de près les opérations de désactivation. Après un certain temps, les cybercriminels se sont éloignés de Limestone Networks, et il s'en est suivi une baisse généralisée de l'activité d'Angler.

Pour plus d'informations sur la façon dont Cisco a mis fin à un flot important de revenus internationaux généré par le kit d'exploits Angler, reportez-vous au billet posté sur le blog de Cisco « **Threat Spotlight: Cisco Talos Thwarts Access to Massive International Exploit Kit Generating $60M Annually from Ransomware Alone.** »

Les efforts conjugués des entreprises du secteur contribuent à mettre à mal l'un des plus grands botnets de DDoS sur Internet

Les solutions intégrées de défense contre les menaces peuvent souvent bloquer les attaques importantes avant qu'elles n'affectent les réseaux d'entreprise. Cependant, dans de nombreux cas, l'anéantissement d'une attaque potentiellement massive requiert non seulement des défenses technologiques, mais également une coordination entre les fournisseurs de services, les fournisseurs de solutions de sécurité et les groupes industriels.

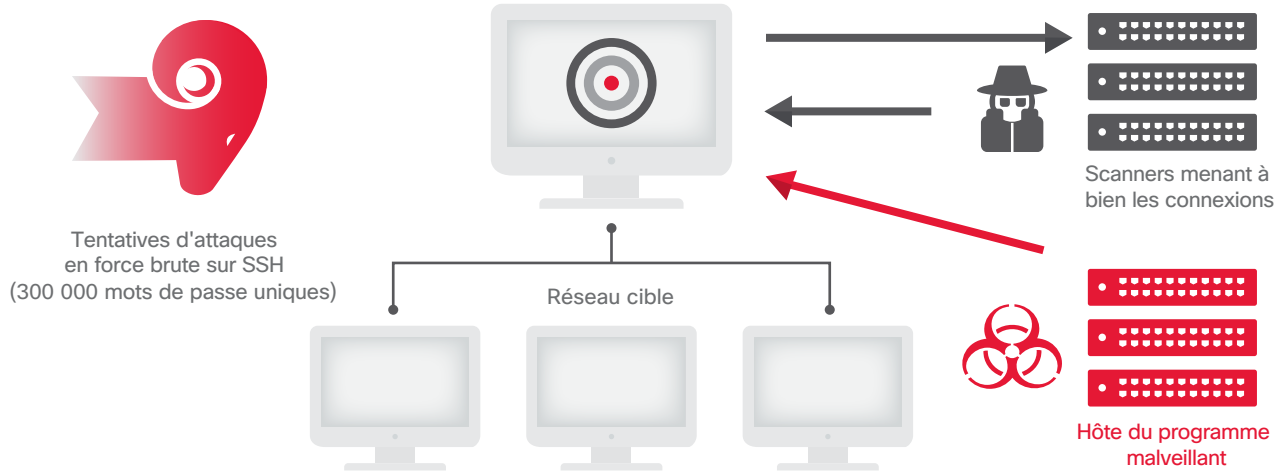
Alors que les cybercriminels tentent de plus en plus de monétiser leurs activités, le secteur technologique doit améliorer ses partenariats pour mettre à bas les campagnes criminelles. SSHPsychos (également appelé Group 93), l'un des plus grands botnets de DDoS jamais observés par les chercheurs de Cisco, a été considérablement affaibli par les efforts conjugués de Cisco et de Level 3 Threat Research Labs.

UNE MENACE UNIQUE

Le réseau SSHPsychos de DDoS représente une menace unique pour diverses raisons. Parce qu'il enrôle des dizaines de milliers de machines réparties sur Internet, il a le pouvoir de lancer une attaque par déni de service distribué (DDoS) qui ne peut être contrée machine par machine. Dans ce cas, le botnet a été créé via des attaques en force brute impliquant le trafic SSH (Secure Shell) (Figure 6). Le protocole SSH permet des communications sécurisées, et il est généralement utilisé à des fins d'administration à distance des systèmes. Par moments, SSHPsychos a occupé plus de 35 % du trafic SSH de l'Internet mondial (Figure 7), selon l'enquête menée par Cisco et Level 3.

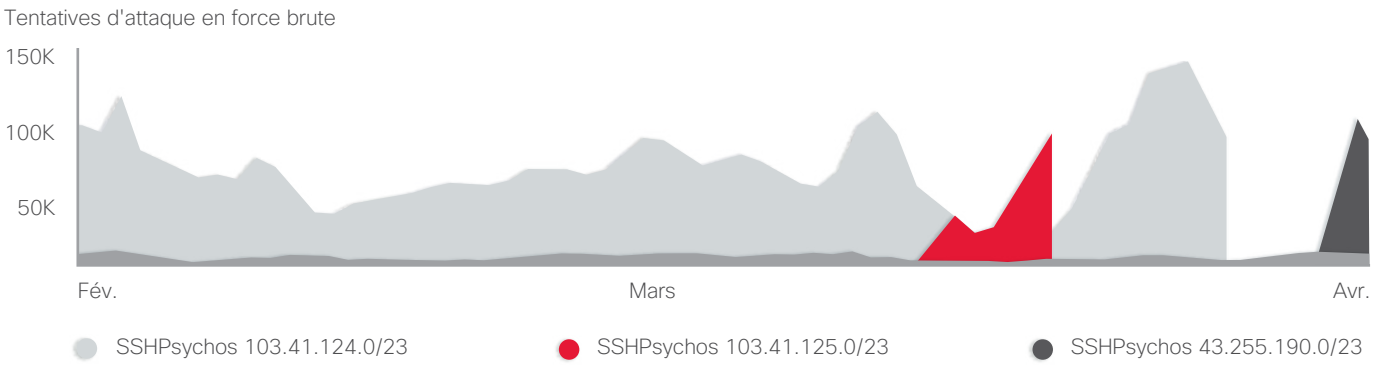
SSHPsychos est opérationnel dans deux pays : la Chine et les États-Unis. Les tentatives de connexion en force, utilisant 300 000 mots de passe uniques, émanaient d'un hébergeur basé en Chine. Lorsque les pirates sont parvenus à se connecter en perçant le mot de passe racine correct, les attaques en force ont cessé. Dans les 24 heures qui ont suivi, les pirates se sont connectés à partir d'une adresse IP aux États-Unis et installé un outil de dissimulation d'activité (« rootkit ») de DDoS sur la machine considérée. Il s'agissait clairement d'une tactique pour atténuer la suspicion des administrateurs réseau. Les cibles du botnet étaient diverses, mais il semble dans de nombreux cas que ce sont de grand fournisseurs de services Internet qui étaient visés.

Figure 6 : SSHPsychos utilise les attaques en force



Source : Cisco Security Research

Figure 7 : À son paroxysme, SSHPsychos a occupé plus de 35 % du trafic de l'Internet mondial



Source : Cisco Security Research

COLLABORATION AVEC DES EXPERTS EN SÉCURITÉ

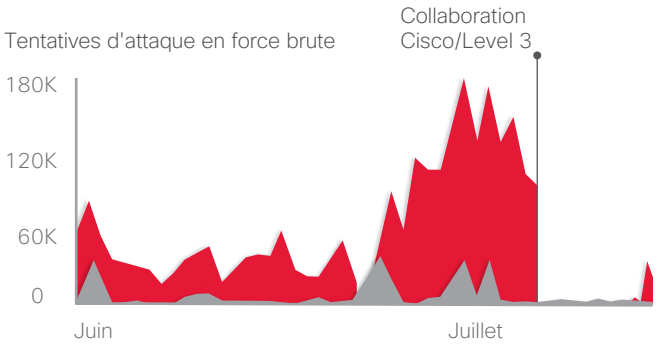
En raison de l'ampleur du réseau DDoS, nos experts pensaient qu'il serait difficile de contenir les dégâts. Il était essentiel de fonctionner en tandem avec une entreprise capable de supprimer efficacement d'Internet le groupe d'attaque en force. Cependant, les fournisseurs de réseaux de base sont réticents quant à filtrer le contenu de leurs clients.

Cisco a contacté Level 3 Threat Research Labs. Level 3 a analysé le trafic au niveau du netblock, ou la plage d'adresses IP, là où il était soupçonné que SSHPsychos réside (103.41.124.0/23). Cela a confirmé qu'aucun trafic légitime n'émanait de cette adresse ou lui était destiné. Le trafic réseau était rerouté vers ses propres réseaux. Le groupe SSHPsychos a contacté les opérateurs télécoms responsables des domaines pertinents pour leur demander de supprimer le trafic réseau.

Les résultats de cette mesure ont été constatés immédiatement (Figure 8). Le réseau initial n'a affiché pratiquement aucune activité. Cependant, un nouveau réseau au netblock 43.255.190.0/23 a affiché un important trafic SSH d'attaque en force. On a constaté le même comportement que celui associé à SSHPsychos. Après cette reprise soudaine d'un trafic assimilé à SSHPsychos, Cisco et Level 3 ont décidé de prendre des mesures à l'encontre de 103.41.124.0/23, ainsi que du nouveau netblock 43.255.190.0/23.

L'anéantissement des netblocks utilisés par SSHPsychos n'a pas définitivement désactivé le réseau DDoS. Il a toutefois certainement ralenti la capacité des pirates à mener à bien leurs opérations, et cela a empêché SSHPsychos de se propager à de nouvelles machines, du moins temporairement.

Figure 8 : Le trafic SSHPsychos chute considérablement après l'intervention



Source : Cisco Security Research

Lorsque les cybercriminels mettent en place de grands réseaux d'attaque, l'industrie de la sécurité doit étudier les moyens de collaborer pour contrer une menace telle que SSHPsychos. Les fournisseurs de domaine de premier niveau, les FAI, les hébergeurs, les résolveurs de DNS et les fournisseurs de solutions de sécurité ne peuvent plus rester les bras croisés lorsque des cybercriminels lancent leurs attaques sur des réseaux censés transporter uniquement du trafic légitime. En d'autres termes, quand des criminels acheminent un trafic malveillant en terrain plus ou moins découvert, l'industrie doit supprimer les passerelles malveillantes menant vers les réseaux légitimes.

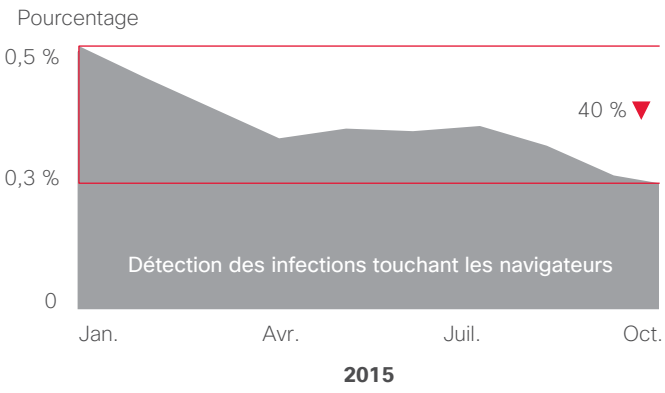
Pour plus d'informations sur la réponse apportée par Cisco et Level 3 Threat Research Labs à la menace SSHPsychos, reportez-vous au billet posté sur le blog de Cisco « **Threat Spotlight: SSHPsychos ».**

Infections touchant les navigateurs : très répandues et source majeure de fuite de données

Les équipes de sécurité considèrent souvent les extensions de navigateur comme une menace sévère. Cependant, elles doivent faire de leur supervision une priorité de manière à pouvoir rapidement identifier et corriger ces types d'infections.

La raison de l'urgence : notre recherche indique que les infections touchant les navigateurs sont bien plus répandues que ne le pensent nombre d'entreprises. De janvier à octobre 2015, nous avons étudié 26 familles d'extension malveillantes de navigateur (Figure 9). En examinant au cours de cette période le profil des infections touchant les navigateurs, le nombre d'infections semble globalement être en recul.

Figure 9 : Infections affectant des navigateurs, janvier à octobre 2015



Source : Cisco Security Research

Ce constat est trompeur, cependant. Le volume croissant du trafic HTTPS au cours des mois considérés a difficilement permis d'identifier des indicateurs de compromission généralement associés aux 26 familles que nous avons suivies, car les informations de l'URL étaient illisibles du fait du cryptage. (Pour plus d'informations sur le cryptage et les défis qu'il représente pour les acteurs de la protection, voir « Cryptage : une tendance à la hausse, et un défi pour les acteurs de la protection », **page 30**.)

Les extensions malveillantes de navigateur peuvent dérober des informations, et peuvent constituer une source importante de fuite de données. Chaque fois qu'un utilisateur ouvre une nouvelle page Web via un navigateur compromis, les extensions malveillantes de ce navigateur collectent des données. Elles exfiltrent bien plus que les détails de base concernant chaque page Web interne ou externe que l'utilisateur consulte. Elles recueillent aussi des informations hautement sensibles incluses dans l'URL. Ces informations peuvent comporter des identifiants, des données clients et des détails sur l'infrastructure ou l'API internes d'une entreprise.

Les extensions malveillantes polyvalentes de navigateur sont installées par le biais de kits logiciels ou de logiciels publicitaires. Elles sont conçues pour générer des revenus en exploitant les utilisateurs de plusieurs façons. Dans un navigateur infecté, elles peuvent amener les utilisateurs à cliquer sur une publicité malveillante, dans l'affichage d'une annonce ou dans une fenêtre contextuelle. Elles peuvent également diffuser le programme malveillant en incitant les utilisateurs à cliquer sur un lien compromis ou à télécharger un fichier infecté présent dans une publicité malveillante. Elles peuvent encore détourner les requêtes de navigation des utilisateurs pour ensuite injecter des pages Web malveillantes dans les pages de résultats du moteur de recherche.

Parmi les 45 entreprises de notre panel, nous avons déterminé chaque mois que plus de 85 % des entreprises ont été affectés par des extensions malveillantes de navigateur. Ce constat souligne la forte évolution à la hausse de ces opérations. Comme les navigateurs infectés sont souvent perçus comme une menace relativement faible, leur état peut passer inaperçu ou n'être pas résolu pendant plusieurs jours, voire davantage, ce qui donne aux cybercriminels plus de temps et d'opportunités pour mener leurs campagnes (voir « Délais de détection : une course pour toujours les réduire », **page 60**).

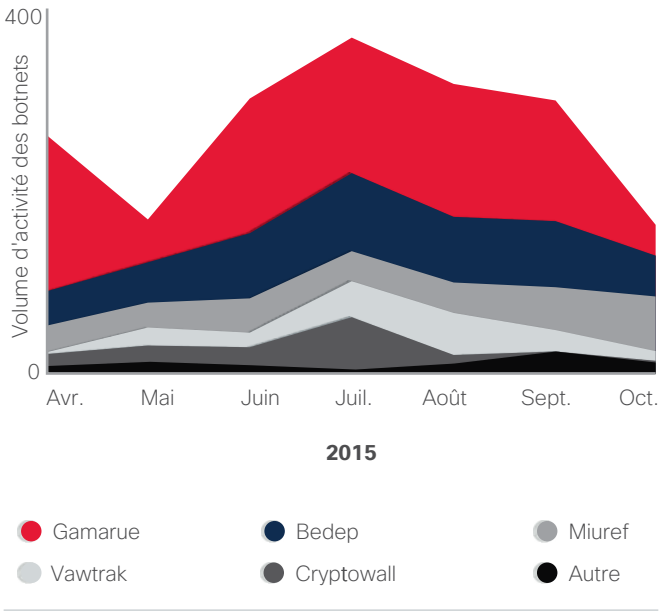
Nous préconisons donc aux équipes de sécurité d'allouer davantage de temps et de ressources à la surveillance de ce risque, et d'envisager d'utiliser plus intensivement l'automatisation afin de hiérarchiser les menaces.

Contrôle et commande des botnets : vue d'ensemble

Un botnet est un réseau d'ordinateurs infectés par un programme malveillant, que des hackers contrôlent collectivement et pilotent dans le but de mener à bien une tâche donnée, telle que l'envoi de spams ou le déclenchement d'une attaque DDoS par exemple. Depuis quelques années, les botnets se multiplient et gagnent en puissance. Afin de mieux comprendre le paysage actuel de la menace à l'échelle internationale, nous avons procédé, d'avril à octobre 2015, à l'analyse de 121 réseaux d'entreprise en y recherchant des preuves d'activité d'un ou de plusieurs des huit botnets les plus courants. Les données ont été standardisées dans le but de fournir un état des lieux de l'activité des botnets (Figure 10).

Gamarue, le dérobeur universel d'informations modulaire qui sévit depuis plusieurs années déjà, est le vecteur de contrôle-commande dont l'activité est ressortie la plus soutenue sur la période.

Figure 10 : Croissance des différentes menaces (taux d'utilisateurs infectés)



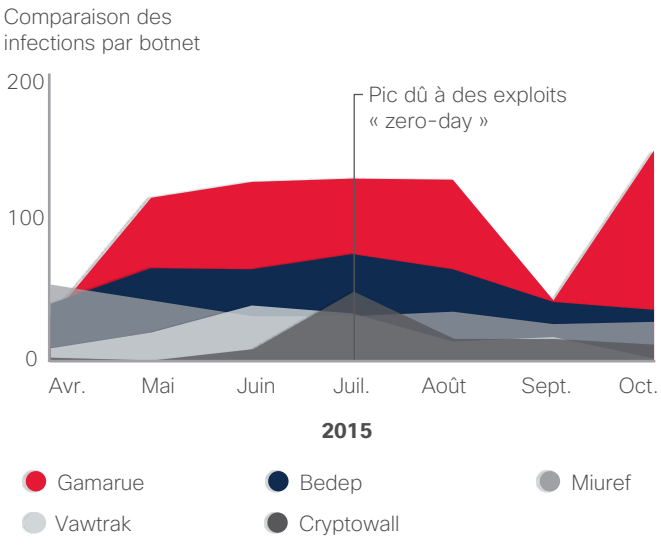
Source : Cisco Security Research

Une hausse significative du nombre d'infections impliquant le rançonneur CryptoWall 3.0 a été observée en juillet. Cette activité est en grande partie imputable au kit d'exploits Angler, connu pour déployer la charge utile CryptoWall. Comme le souligne notre rapport semestriel 2015 sur la cybersécurité, les auteurs d'Angler et de divers autres kits d'exploits ne manquent pas de mettre à profit les « brèches de correction » d'Adobe Flash, créées par le manque d'empressement de nombreux utilisateurs à appliquer les mises à jour publiées par Adobe.[2] Les chercheurs de Cisco attribuent le pic de juillet 2015 à l'exploit « zero-day » Flash CVE-2015-5119 exposé dans le cadre des fuites de la Hacking Team.[3]

Le kit d'exploits Angler intègre également le cheval de Troie Bedep, utilisé pour la mise en œuvre de campagnes de fraude au clic. Une légère augmentation de l'importance de cette menace a également été observée en juillet (Figure 11).

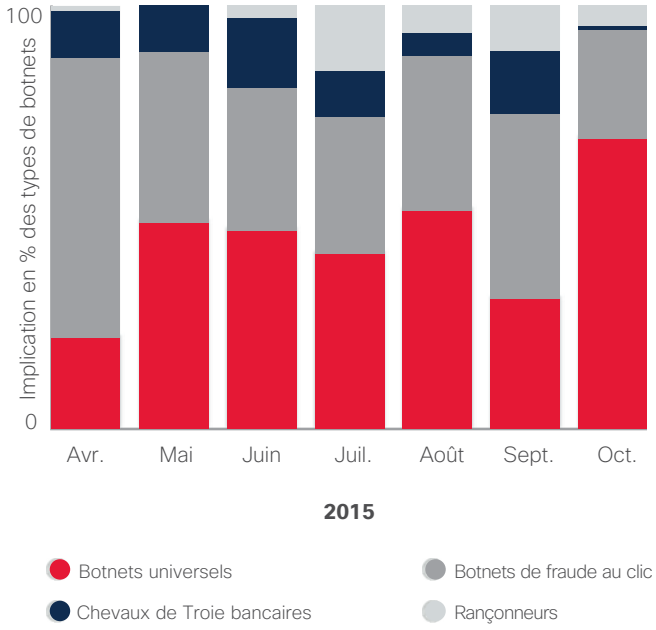
Bedep, Gamarue et Miuref (un autre cheval de Troie et pirateur de navigateurs capable de fraude au clic) représentent à eux trois plus de 65 % de l'activité de contrôle-commande que nous avons relevée dans les réseaux analysés.

Figure 11 : Couverture mensuelle des menaces, basée sur le nombre d'utilisateurs infectés



Source: Cisco Security Research

Figure 12 : Couverture mensuelle des menaces, basée sur les catégories de menaces



Source: Cisco Security Research

Le pourcentage des infections Bedep est resté relativement stable sur toute la période considérée. Parallèlement, une diminution du nombre d'infections Miuref perçues a été observée, laquelle peut être attribuée à l'augmentation du trafic HTTPS, qui a contribué à masquer les indicateurs de compromission de Miuref.

La Figure 12 montre les types de botnets les plus impliqués dans les infections observées sur la période considérée. Les botnets universels tels que Gamarue et Sality arrivent en tête, suivis des botnets de fraude au clic. Les chevaux de Troie bancaires se classent en troisième position, preuve que cette menace, bien qu'elle ne date pas d'hier, reste bien présente.

PARTAGER

[2] Rapport semestriel 2015 Cisco sur la cybersécurité : **http://www.cisco.com/web/offers/lp/2015-midyear-security-report/index.html**.
[3] « Adobe Patches Hacking Team's Flash Player Zero-Day, » par Eduard Kovacs, *SecurityWeek*, 8 juillet 2015 : **http://www.securityweek.com/adobe-patches-hacking-teams-flash-player-zero-day.**

La faille du DNS : des attaques utilisent l'infrastructure DNS à des fins de commande et de contrôle

Les travaux d'analyse conduits par Cisco sur les programmes malveillants identifiés comme « menace connue » ont montré que la plupart de ces programmes, soit 91,3 % d'entre eux, font usage du service DNS de l'une des trois manières suivantes :

- À des fins de contrôle et de commande
- À des fins d'exfiltration de données
- À des fins de redirection du trafic

Pour parvenir à cette conclusion, nous avons étudié les comportements des programmes malveillants de notre échantillon dans divers sandboxes en notre possession. Ceux pour lesquels il a pu être déterminé qu'ils n'utilisaient pas l'infrastructure DNS de quelque manière que ce soit, ou uniquement pour réaliser des « bilans de santé » Internet, ont été retirés de l'échantillon pour l'analyse. Les programmes malveillants restants utilisaient le DNS pour se connecter à des sites identifiés comme dangereux ou considérés comme suspects.

S'il ressort que l'infrastructure DNS est massivement exploitée par les hackers dans le cadre de leurs campagnes, nombreuses sont les entreprises qui omettent de la surveiller de manière appropriée pour se protéger (voire qui ne la surveillent pas du tout). Du fait de ce manque de supervision, l'infrastructure DNS constitue un vecteur de choix pour les pirates. Dans une récente enquête que nous avons réalisée (voir Figure 13), 68 % des professionnels de la sécurité indiquaient que le DNS récursif ne fait l'objet d'aucune surveillance dans leur entreprise. (Les serveurs DNS récursifs fournissent les adresses IP des noms de domaine voulus aux hôtes à l'origine de la requête.)

Figure 13 : Surveillance des menaces du DNS récursif

91,3 %
des programmes malveillants exploitent l'infrastructure DNS pour leurs attaques

68 %
des entreprises ne surveillent pas le DNS récursif

Source : Cisco Security Research

Mais pourquoi tant d'entreprises ne traitent-elles pas cette faille de sécurité que représente leur infrastructure DNS ? Cette situation est principalement due au fait que les spécialistes de la sécurité et les experts DNS de l'entreprise, généralement rattachés à des entités informatiques différentes, n'interagissent que très rarement.

Et pourtant, ils le devraient. La surveillance de l'infrastructure DNS est essentielle pour détecter et bloquer les infections qui utilisent le DNS pour l'une des trois activités mentionnées plus haut. Elle constitue également une première étape importante pour la cartographie des divers autres composants exploitables pour étudier plus en détail une attaque, depuis la détermination du type d'infrastructure utilisé par l'attaque jusqu'à l'identification de son origine.

Cependant, la surveillance du DNS demande bien plus qu'une collaboration efficace entre les équipes sécurité et DNS. Elle nécessite également l'alignement de la bonne technologie et de la bonne expertise pour l'analyse des corrélations. (Pour plus d'informations, voir la section « Grâce à une collaboration industrielle efficace, Cisco met en échec un kit d'exploits et une campagne de rançonnage à grande échelle particulièrement profitables », **page 10**, qui explique comment OpenDNS a aidé Cisco à acquérir une plus grande visibilité sur les adresses IP utilisées par le kit d'exploits Angler.)

ANALYSE RÉTROSPECTIVE DU DNS

L'enquête rétrospective menée par Cisco sur les requêtes DNS et le trafic TCP et UDP ultérieur permet d'identifier les sources de programmes malveillants : serveurs de contrôle-commande, sites Web et points de distribution, notamment. Cette enquête rétrospective détecte également le contenu à risque élevé en tirant profit de listes de menaces, de rapports communautaires sur les menaces, des données de tendances disponibles sur les cyber-compromissions et de toute l'expertise de Cisco s'agissant des vulnérabilités particulières qui touchent le secteur du client.

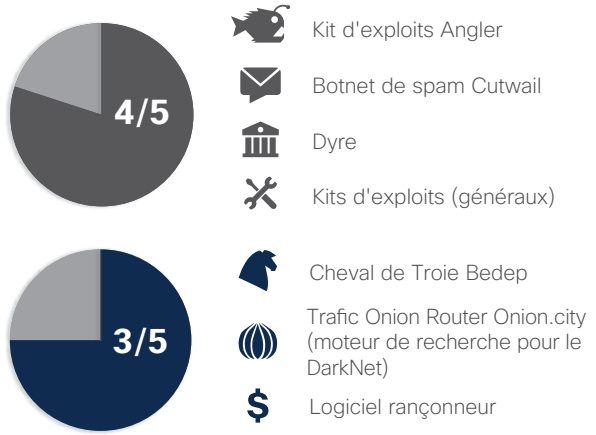
Notre reporting rétrospectif aide à identifier les tentatives d'exfiltration de données « low and slow » couramment associées aux menaces persistantes avancées (APT) et qui, dans la plupart des cas, ne sont pas capturées par les technologies traditionnelles de détection des menaces. L'analyse passe au crible les communications sortantes et vise à détecter les anomalies présentes dans cette énorme quantité de trafic. Cette approche « inside out » permet de mettre à jour de possibles compromissions de données et activités réseau néfastes qui risqueraient de passer inaperçues avec les approches traditionnelles.

C'est de cette manière que nous avons découvert des résolveurs DNS « sauvages » chez plusieurs de nos clients. Ceux-ci n'étaient pas au courant que ces résolveurs étaient utilisés par leurs employés dans le cadre de leur infrastructure DNS. À défaut de gérer et de surveiller activement le recours par ses employés à des résolveurs DNS, l'entreprise s'expose à des risques de comportements malveillants, d'empoisonnement du cache DNS ou de redirection DNS, par exemple.

Outre la découverte et l'identification de ces résolveurs DNS indésirables, l'enquête rétrospective a également mis en lumière les problèmes suivants sur les réseaux concernés :

- Mise au jour de l'espace d'adressage du client sur des listes de blocage de spams et de programmes malveillants tiers
- Balisage de l'espace d'adressage du client pour les serveurs de contrôle-commande connus Zeus et Palevo
- Campagnes d'attaques actives (CTB-Locker, Angler et DarkHotel, notamment)
- Activités suspectes (utilisation du Tor, transferts automatiques d'e-mails et conversions de documents en ligne, notamment)
- Tunnellisation DNS généralisée vers des domaines enregistrés en Chine
- « Typosquatting »[4] du DNS
- Contournement de l'infrastructure DNS de confiance de l'entreprise par les clients internes

Pour un échantillon représentatif de clients du service Cisco Custom Threat Intelligence, couvrant différents secteurs, la présence des types de programmes malveillants suivants a par ailleurs été relevée dans un certain nombre de cas :



[4] Le « typosquatting » consiste à enregistrer un nom de domaine similaire à un nom de domaine existant ; c'est une stratégie utilisée par des pirates pour cibler des utilisateurs qui commettent une faute de frappe par inadvertance dans la saisie de noms de domaine.

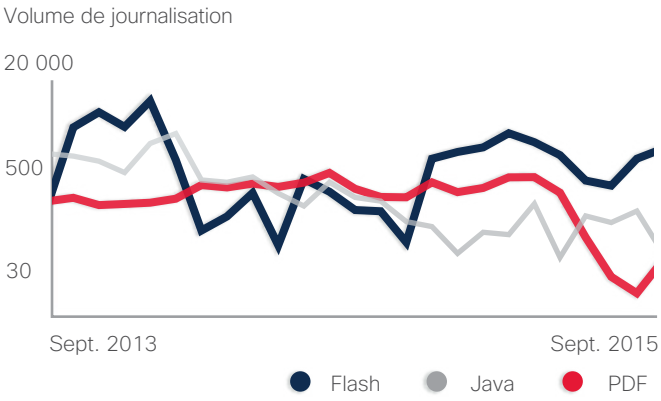
Analyse des menaces

Vecteurs d'attaque Web

ADOBE FLASH : SUR LE DÉCLIN, FINALEMENT

Bien que le volume global de contenu Flash ait diminué au cours de l'année passée (voir la section suivante, **« Tendances observées sur les contenus Adobe Flash et PDF »**), celui-ci demeure encore aujourd'hui un vecteur largement exploité par les développeurs de kits d'exploits. En fait, le volume d'attaques exploitant les vulnérabilités Flash n'a pas connu d'évolution notable sur l'année 2015 (Figure 14). Flash devrait rester un vecteur d'attaque privilégié pendant un certain temps encore, sachant que les auteurs du kit d'exploits Angler, notamment, ont fait des vulnérabilités Flash une cible de choix.

Figure 14 : Partage de vecteurs d'attaque, comparaison sur deux années



Source : Cisco Security Research

Les pressions exercées en faveur du retrait d'Adobe Flash de l'expérience de navigation entraînent une diminution du volume de contenus Flash sur le Web (voir la section suivante, **« Tendances observées sur les contenus Adobe Flash et PDF »**). Le phénomène est similaire à celui observé avec le contenu Java ces dernières années, et qui a conduit, par voie de conséquence, à une chute régulière du volume de programmes malveillants Java (les auteurs d'Angler ne prennent du reste même plus la peine d'inclure des exploits Java dans leur kit). Parallèlement, le volume d'attaques exploitant les vulnérabilités PDF est demeuré relativement stable.

Microsoft Silverlight est également moins ciblé comme vecteur d'attaque, de nombreux fournisseurs ayant cessé de prendre en charge l'API qu'utilise Silverlight pour s'intégrer dans les navigateurs. De nombreuses entreprises se détournent désormais de Silverlight pour se doter de technologies HTML5. Microsoft a annoncé qu'aucune nouvelle version de Silverlight ne verrait le jour dans le futur et ne publie plus actuellement que des mises à jour de sécurité.

TENDANCES OBSERVÉES SUR LES CONTENUS ADOBE FLASH ET PDF

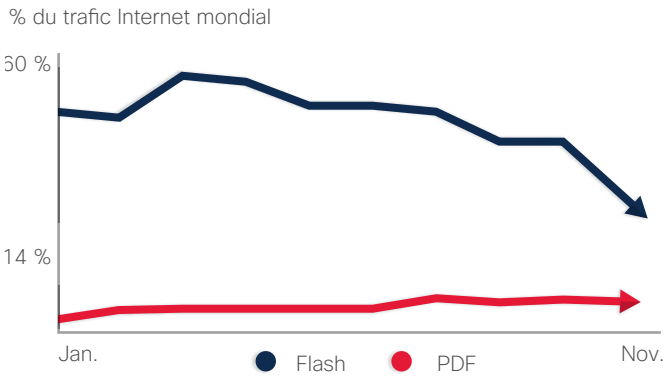
Les chercheurs de Cisco font le constat d'une décroissance généralisée du volume de contenus Adobe Flash sur le Web (Figure 15). Les actions récentes d'Amazon, de Google et de divers autres grands acteurs de l'espace Internet sont un facteur favorable au déclin du contenu Flash. Ces entreprises n'acceptent plus la publicité en ligne qui utilise Flash, ou bien elles la bloquent.

Le contenu PDF, quant à lui, est demeuré relativement stable au cours de l'année passée et l'on peut s'attendre à ce qu'il le reste. Ceci étant, il ne constitue plus un vecteur d'attaque Web majeur depuis quelque temps.

Le déclin du contenu Flash devrait logiquement se poursuivre, voire s'accélérer à court terme maintenant qu'Adobe a annoncé la mise à pied de Flash[5]. Cependant, un certain temps devrait s'écouler avant que le contenu Flash ne disparaisse totalement. Flash est intégré dans de nombreux navigateurs tels que Google Chrome, Microsoft Internet Explorer ou encore Microsoft Edge, et reste très largement utilisé pour le contenu Web, y compris les jeux et la vidéo.

Toutefois, avec l'adoption dans les années à venir de nouvelles technologies (plates-formes mobiles et HTML5, notamment), le futur à plus long terme des vecteurs d'attaque Web tels que Java, Flash et Silverlight s'annonce bien sombre. Au fil du temps, ils seront de moins en moins utilisés. Ces vecteurs seront de moins en moins intéressants pour des hackers mus par la cupidité, qui concentrent essentiellement leurs efforts sur les vecteurs qui leur permettent de toucher facilement de vastes populations d'utilisateurs et de générer des revenus rapidement.

Figure 15 : Pourcentage du trafic global pour Flash et PDF

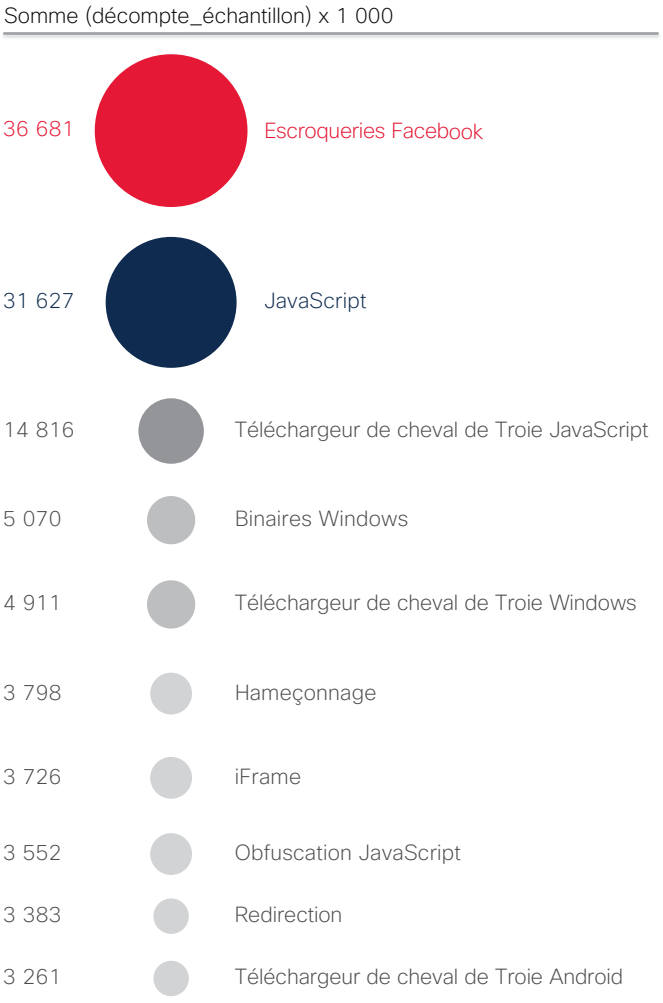


Source : Cisco Security Research

Méthodes d'attaque Web

Les Figures 16 et 17 nous renseignent sur les divers types de techniques que les hackers utilisent pour accéder aux réseaux des entreprises. La Figure 16 présente les programmes malveillants les plus couramment observés : logiciels publicitaires, logiciels espions, logiciels de redirection malveillants, exploits iFrame et logiciels de hameçonnage.

Figure 16 : Logiciels malveillants les plus couramment observés



Source : Cisco Security Research

[5] « Adobe News: Flash, HTML5 and Open Web Standards, » Adobe, 30 novembre 2015 : **http://blogs.adobe.com/conversations/2015/11/flash-html5-and-open-web-standards.html**.

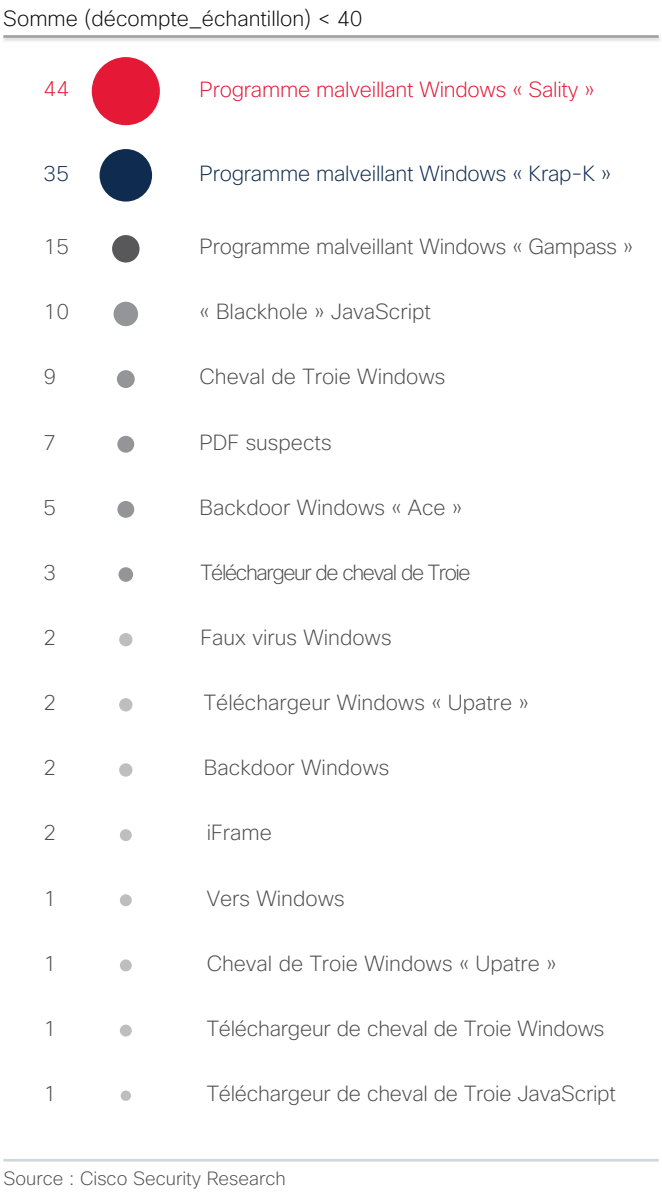
La Figure 16 reflète la palette des principaux types d'outils malveillants utilisés par les cybercriminels pour l'accès initial. Ces méthodes éprouvées particulièrement économiques leur permettent de compromettre relativement facilement de vastes populations d'utilisateurs. Les exploits JavaScript et les escroqueries Facebook (ingénierie sociale) sont les méthodes d'attaque les plus fréquemment utilisées, d'après nos recherches.

La Figure 17 présente les méthodes d'attaque de plus faible volume observées. À noter qu'un « volume plus faible » ne signifie pas « moins efficace. » D'après Cisco Security Research, les méthodes d'attaque de plus faible volume peuvent représenter des menaces émergentes ou des campagnes extrêmement ciblées.

La plupart de ces techniques plus sophistiquées sont conçues pour tirer le maximum des utilisateurs compromis. Leur objectif est de dérober des données de grande valeur ou de rendre inutilisables les ressources numériques de l'utilisateur dans le but de l'amener à payer une rançon.

Par conséquent, lors de la surveillance des programmes malveillants Web, il n'est pas suffisant de se concentrer simplement sur les types d'attaque les plus souvent observés. L'ensemble des attaques doit être pris en compte.

Figure 17 : Méthodes d'attaque de plus faible volume observées



Source : Cisco Security Research

Actualité des menaces

ADOBE FLASH, CHAMPION DES VULNÉRABILITÉS

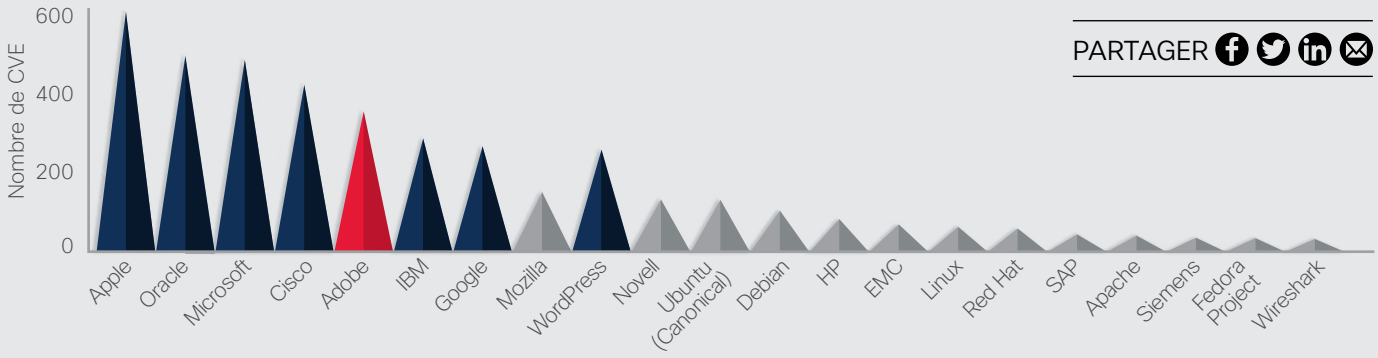
La plate-forme Adobe Flash est depuis plusieurs années un vecteur d'attaque très prisé par les cybercriminels. Des vulnérabilités Flash figurent toujours fréquemment en bonne place sur les listes d'alertes urgentes. Une bonne nouvelle cependant : en 2015, les fournisseurs des produits dans lesquels ces exploits surviennent généralement, tels que les navigateurs Web, ont reconnu cette faiblesse et prennent désormais des mesures pour réduire les possibilités offertes aux hackers.

En 2016, les criminels sont plus susceptibles de concentrer leurs exploits et attaques sur les utilisateurs d'Adobe Flash. Certaines de ces vulnérabilités Flash sont mises à profit par des exploits disponibles gratuitement en ligne ou à la vente en tant qu'éléments de kits d'exploits. (Comme indiqué **page 21**, le volume de contenus de type Flash a diminué, mais Flash reste un vecteur d'attaque majeur.)

Dans l'esprit des mesures prises pour réduire l'impact de Java, autre vecteur d'attaque courant, de nombreux navigateurs Web bloquent ou « sandboxent » Flash afin de protéger les utilisateurs. Bien qu'il s'agisse là d'une évolution positive, il est important de comprendre que les hackers continueront pendant un certain temps encore à lancer des exploits avec succès. Ils savent que nombreux sont les utilisateurs qui négligent de mettre à jour leur navigateur comme il le faudrait, et ils continueront à lancer des exploits destinés à d'anciennes versions des logiciels de navigation.

Cependant, les chercheurs de Cisco estiment que les protections désormais intégrées dans un certain nombre de navigateurs Web et de systèmes d'exploitation d'usage courant vont amoindrir l'intérêt de Flash pour les cybercriminels. Dans la mesure où les hackers recherchent une efficacité maximale (une rentabilité élevée, notamment), il est peu probable qu'ils continuent à s'investir dans des attaques moins susceptibles de produire les fruits escomptés.

Figure 18 : Nombre total de CVE par constructeur



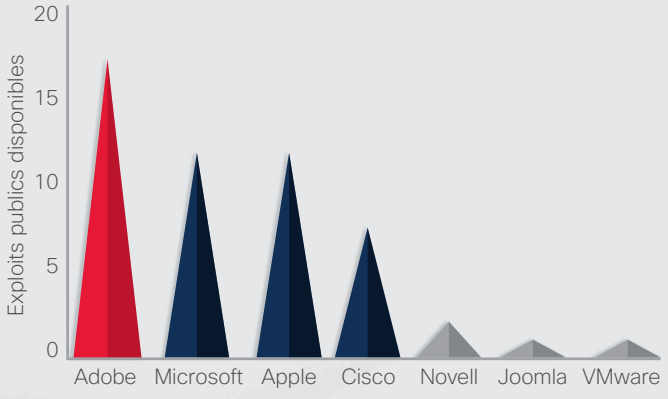
Source : Cisco Security Research, National Vulnerability Database

Le graphique ci-dessus montre le nombre de CVE publiés en 2015 par constructeur. À noter que l'importance d'Adobe n'est pas trop marquée dans ce graphique, car la marque figure dans le graphique de droite, affichant les vulnérabilités pour lesquelles des exploits sont disponibles.

En outre, WordPress affiche uniquement 12 vulnérabilités en 2015 pour son propre produit. Les 240 vulnérabilités supplémentaires sont issues de modules et de scripts créés par des contributeurs tiers.

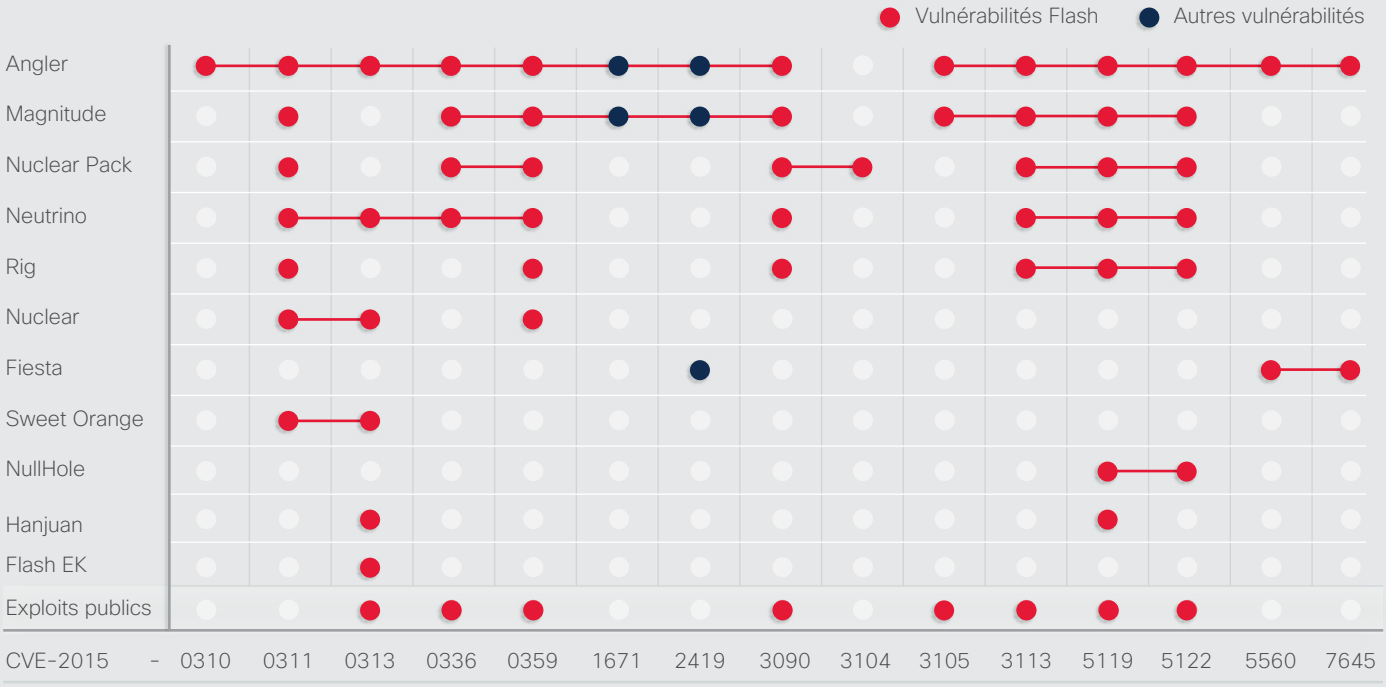
Comme l'illustre la Figure 20, les listes de vulnérabilités et les exploits qui y sont associés peuvent servir de support aux professionnels de la sécurité. Ils les utilisent pour gérer et hiérarchiser les vulnérabilités à haut risque et les plus courantes, afin de les corriger plus rapidement que les vulnérabilités à moindre risque. Consultez le site Web CVE Details **(https://www.cvedetails.com/top-50-products.php)** pour plus d'informations sur les CVE par constructeur.

Figure 19 : Nombre d'exploits publics disponibles selon les vulnérabilités par constructeur



Source : Cisco Security Research, Metasploit, Exploit DB

Figure 20 : Vulnérabilités courantes



Source : Cisco Security Research

La Figure 20 présente des vulnérabilités à haut risque, et indique si une vulnérabilité fait partie d'un kit d'exploits à louer (voir ligne « Flash EK ») ou correspond à des exploits publiquement disponibles (voir ligne « Exploits publics »). Les vulnérabilités pour lesquelles il existe des exploits fonctionnels sont celles qu'il est prioritaire de corriger.

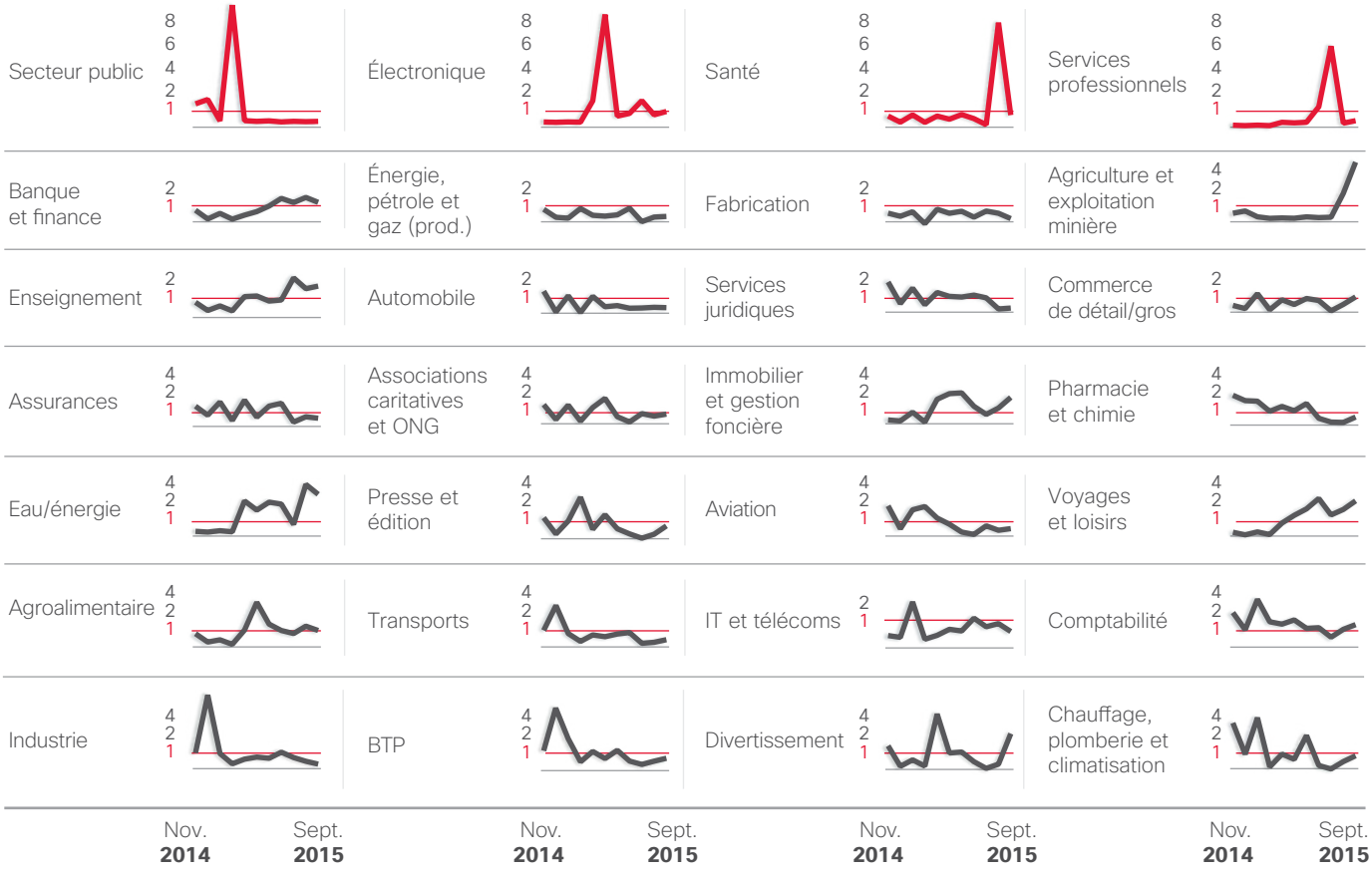
Cette liste peut servir aux professionnels de la sécurité à hiérarchiser leurs activités de correction et « d'assainissement ». L'existence d'un exploit pour un produit donné (soit publiquement, soit au sein d'un kit d'exploits) ne signifie pas nécessairement que des attaques se produisent.

Risque sectoriel d'exposition aux programmes malveillants

Pour le suivi des secteurs présentant un risque élevé d'exposition aux attaques de programmes malveillants, nous avons examiné les volumes respectifs de trafic d'attaque (« taux de blocage ») et de trafic « normal » ou prévu.

La Figure 21 présente 28 secteurs importants et la part de leur activité de blocage respective au regard du trafic réseau normal. Un ratio de 1 indique que le nombre de blocages est proportionnel au volume du trafic observé. Un ratio supérieur à 1 représente un taux de blocage supérieur à la normale et un ratio inférieur à 1 représente un taux de blocage inférieur à la normale.

Figure 21 : Taux de blocage mensuels par secteur, novembre 2014-septembre 2015

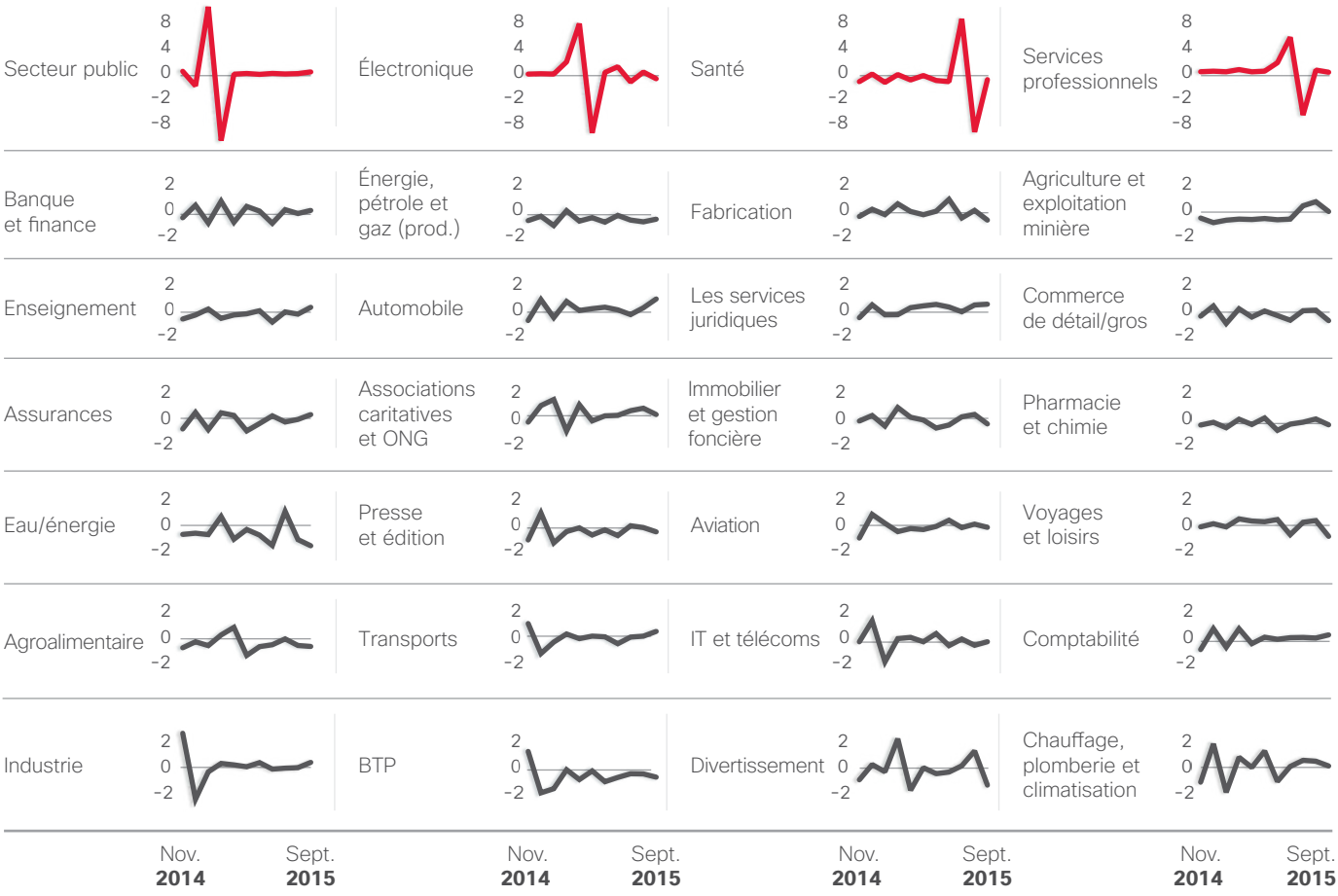


Source : Cisco Security Research

La Figure 22 montre à quel point l'intérêt des hackers pour certains secteurs spécifiques peut être fluctuant. (Zéro = aucune évolution nette.) Entre janvier et mars 2015, c'est le Secteur public qui affichait le taux de blocage le plus élevé. De mars à mai, c'est l'Électronique qui a pris le relais. Dans le milieu de l'été, c'est dans les Services professionnels qu'ont été relevés le plus de blocages. Et durant l'automne 2015, c'est la Santé qui damait le pion à tous les autres secteurs en termes de nombre de blocages.

Selon notre enquête, ces secteurs à forte activité de blocage en 2015 ont tous les quatre été victimes d'attaques par cheval de Troie. Le secteur public a également dû faire face à un nombre élevé d'attaques par injection PHP, tandis que les services professionnels ont été victimes de nombreuses attaques iFrame.

Figure 22 : Taux de blocage relatif par secteur, comparaison entre deux mois



Source : Cisco Security Research

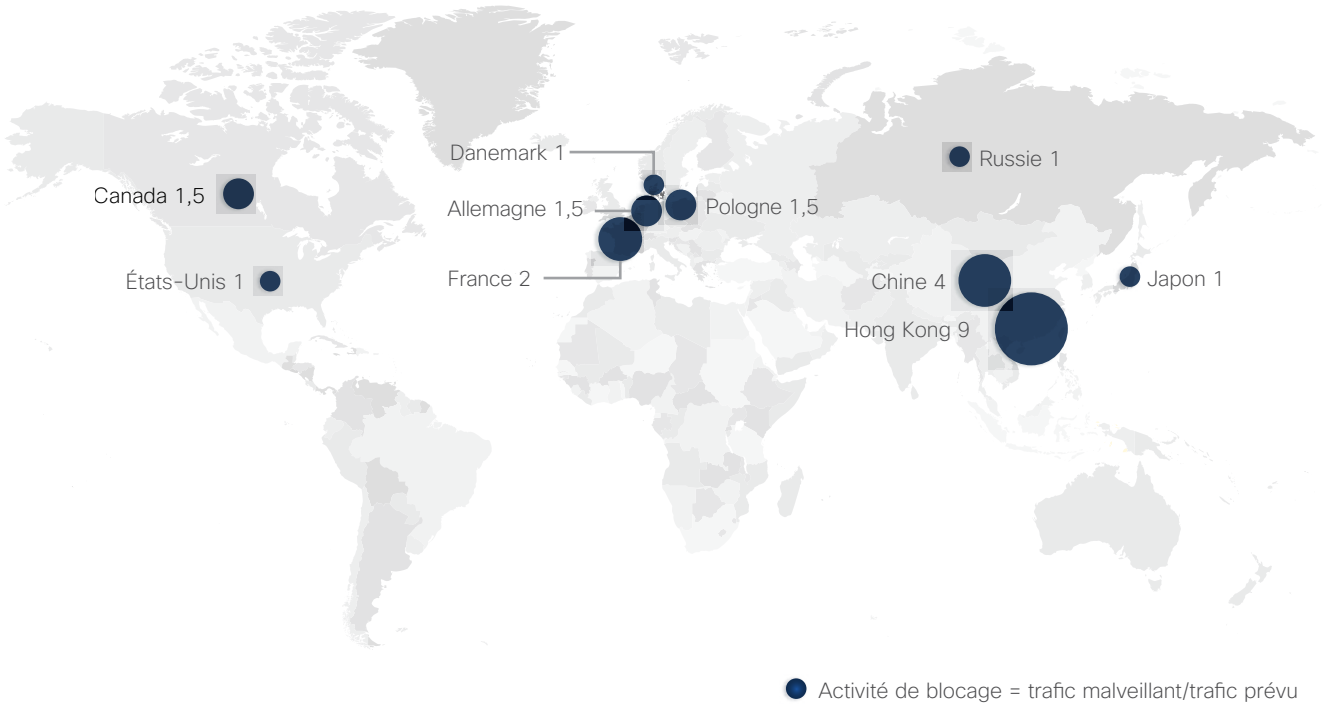
PARTAGER

Activité de blocage Web : répartition géographique

Nous avons également examiné les sites de départ des activités de blocage basées sur des programmes malveillants, par pays ou la région, comme le montre la Figure 23. Les pays ont été sélectionnés pour l'enquête en fonction du volume de trafic Internet. Un taux de blocage de 1 indique que le nombre de blocages observés est proportionnel à la taille du réseau.

Les pays et régions où les activités de blocage sont supérieures au taux normal ont probablement de nombreux hôtes et serveurs Web présentant des failles sur leurs réseaux. Les acteurs malveillants ne respectent pas les frontières géographiques et hébergeront les programmes malveillants là où ils s'avèrent les plus efficaces.

Figure 23 : Blocages Web par pays ou région



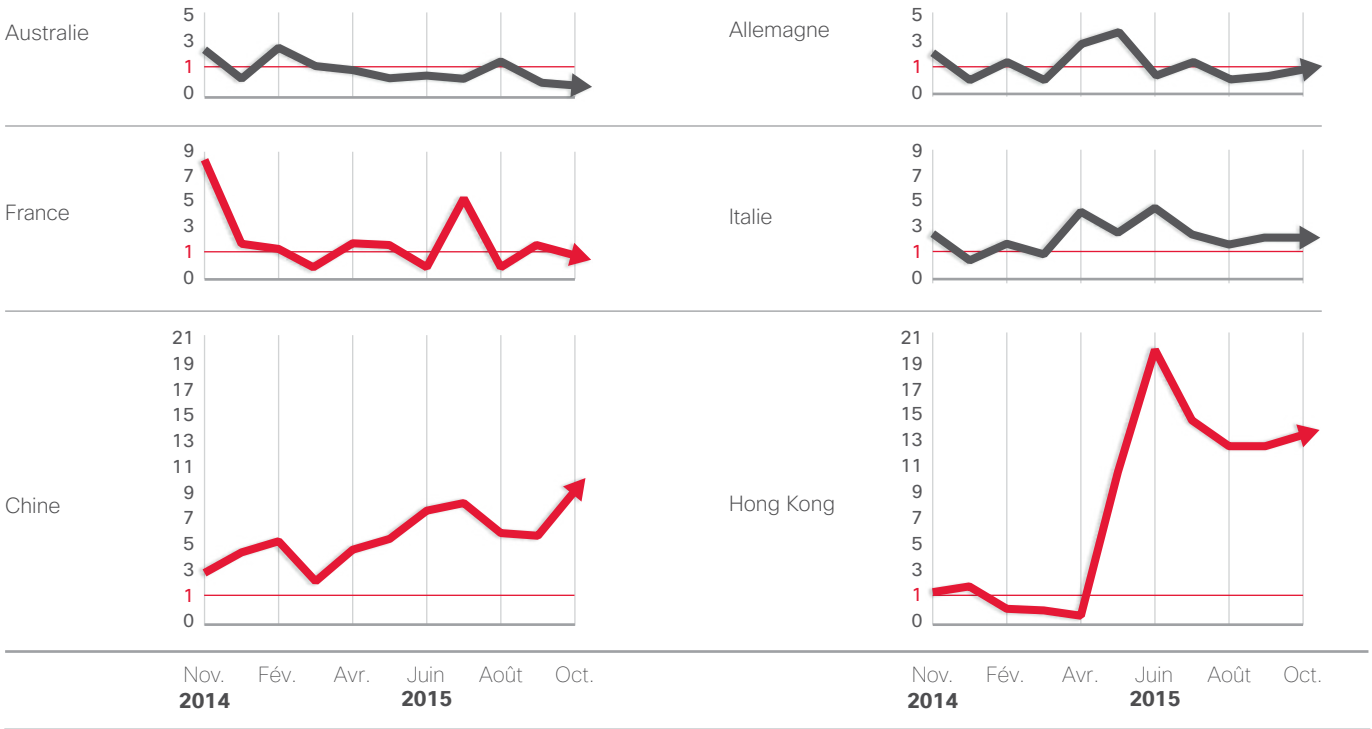
Source : Cisco Security Research

Une présence dans des réseaux de grande taille commercialement viables qui traitent un grand volume de trafic Internet est un autre facteur d'activités de blocage élevées. C'est pourquoi Hong Kong arrive en haut de notre classement.

La Figure 24, qui illustre une comparaison mois par mois des blocages Web par pays ou par région de novembre 2014 à octobre 2015, apporte un éclairage supplémentaire à ces résultats.

À noter que Hong Kong a enregistré une activité anormalement élevée de blocage Web au début du printemps 2015, à l'instar de la France. Depuis lors, les deux pays ont connu une baisse significative de l'activité de blocage Web. Cependant, parce que les taux d'activités en début d'année étaient si anormalement élevés, la récente chute d'activité ne fait pas beaucoup baisser Hong Kong dans le classement par rapport au printemps. Le pic des activités de blocage en France est revenu à la normale au milieu de l'été.

Figure 24 : Blocages Web par pays ou région, entre deux mois, novembre 2014-octobre 2015



Source : Cisco Security Research

Connaissance de l'industrie

Analyse du secteur

Cisco mène des études et des analyses sur les tendances et pratiques en matière de sécurité. Paradoxalement, certaines de ces approches peuvent compliquer la détection des menaces pour les acteurs de la protection, et faire courir aux entreprises et aux utilisateurs des risques de compromission ou d'attaque plus élevés.

Cryptage : une tendance à la hausse, et un défi pour les acteurs de la protection

Le cryptage est un bon choix. Les entreprises ont besoin de protéger leurs données sensibles, notamment la propriété intellectuelle, ainsi que la confidentialité des données de leurs clients. Les annonceurs doivent quant à eux préserver l'intégrité de leur contenu publicitaire et de leurs analyses back-end.

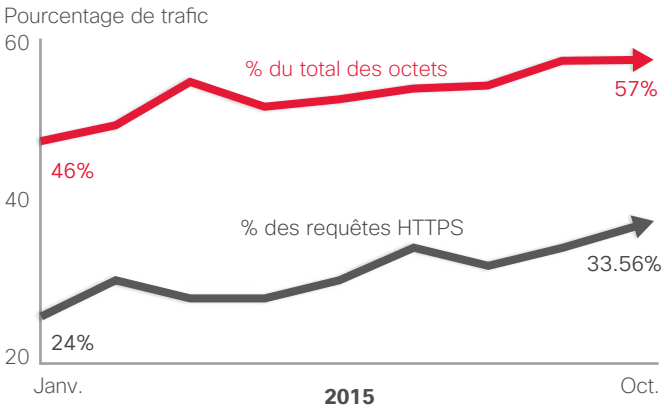
Mais le cryptage peut néanmoins entraîner des problèmes de sécurité en donnant, par exemple, un faux sentiment de sécurité aux entreprises. Si les entreprises ont fait des progrès dans le cryptage des informations transmises entre entités, elles négligent bien souvent la protection des données au repos. La plupart des atteintes à la sécurité les plus marquantes de ces dernières années ont profité des données non cryptées stockées dans le data center et autres systèmes internes. Pour les cyberpirates, cela équivaut à suivre un camion de marchandises sécurisé jusqu'à un entrepôt non verrouillé.

Les entreprises doivent également comprendre que le cryptage de bout en bout peut nuire à l'efficacité de certains produits de sécurité. Le cryptage masque en effet les indicateurs de compromission utilisés pour identifier et suivre les activités malveillantes.

Mais il n'y a aucune raison de ne pas crypter les données sensibles. Les outils de sécurité et leurs opérateurs doivent s'adapter aux réalités du monde actuel en recueillant les en-têtes et autres éléments non cryptés du flux de données, en combinaison avec d'autres sources d'informations contextuelles, pour analyser le trafic crypté. Les outils qui s'appuient sur la visibilité des charges utiles, comme la capture complète des paquets, sont de moins en moins efficaces. L'exécution de Cisco NetFlow et d'autres solutions d'analyse des métadonnées est aujourd'hui une nécessité.

Au vu des tendances 2015, nos experts estiment que le volume de trafic crypté, en particulier HTTPS, a franchi une étape charnière. Même s'il ne représente pas encore la majorité des transactions, il deviendra bientôt la principale forme de trafic sur Internet. Nos études montrent en définitive qu'il compte déjà pour plus de 50 % des octets transmis (Figure 25). Ceci est dû à la charge supplémentaire induite par HTTPS et aux plus grands volumes de contenu envoyés via ce protocole, comme les transferts vers des sites de stockage de fichiers.

Figure 25 : Pourcentages de trafic SSL



Source : Cisco Security Research

Pour chaque transaction Web, un certain nombre d'octets sont envoyés (sortants) et reçus (entrants). Les requêtes sortantes des transactions HTTPS contiennent environ 2 000 octets de plus que les requêtes HTTP sortantes. Les requêtes HTTPS entrantes induisent elles aussi une charge supplémentaire, mais la différence s'estompe avec des réponses volumineuses.

En additionnant les octets entrants et sortants par transaction Web, nous pouvons déterminer le pourcentage total d'octets cryptés via HTTPS pour chaque transaction Web. En raison de l'augmentation du trafic HTTPS et de la charge supplémentaire induite, les octets HTTPS représentaient 57 % de l'ensemble du trafic Web en octobre 2015 (Figure 25), contre 46 % en janvier.

Une analyse du trafic Web nous a également permis de déterminer que les requêtes HTTPS avaient augmenté de manière progressive, mais significative, depuis janvier 2015. Comme le montre la Figure 25, 24 % de requêtes HTTPS ont été observées en janvier, le reste utilisant le protocole HTTP.

En octobre, ce chiffre est passé à 33,56 %. Nous avons en outre constaté une hausse du pourcentage d'octets HTTPS entrants. Cela a été le cas tout au long de l'année. La hausse du trafic HTTPS augmente les besoins en bande passante. 5 Kbit/s supplémentaires sont ainsi requis par transaction.

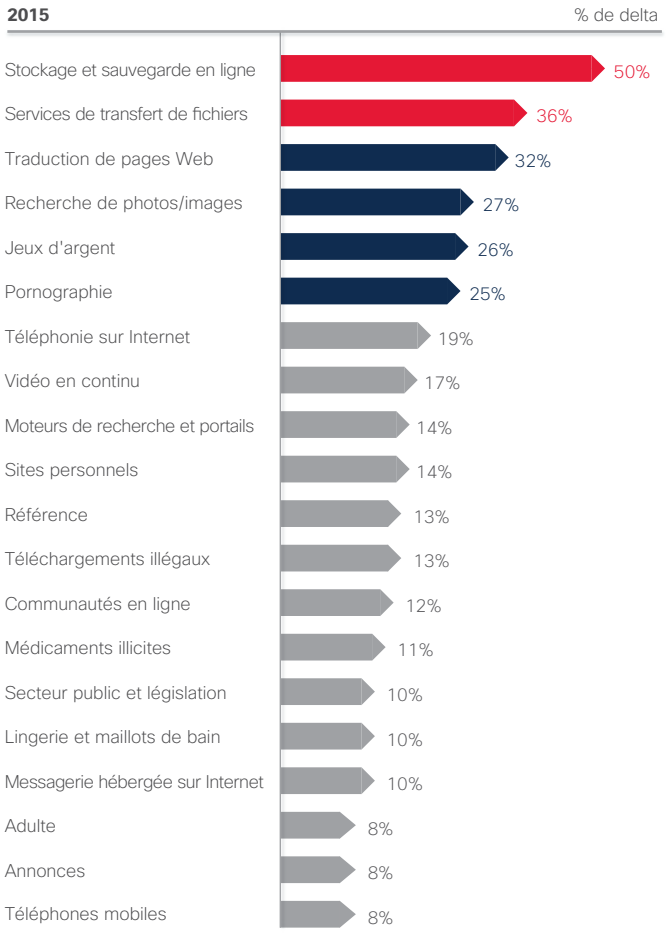
Nous attribuons principalement l'augmentation globale du trafic Web crypté aux facteurs suivants :

- **Hausse du trafic des applications mobiles qui, par nature, cryptent les données**
- **Téléchargements accrus de vidéos cryptées par les utilisateurs**
- **Augmentation des requêtes vers des serveurs de stockage et de sauvegarde hébergeant des « données au repos », des cibles privilégiées pour les hackers**

En fait, la Figure 26 montre que les requêtes HTTPS à destination des ressources de stockage et de sauvegarde en ligne ont augmenté de 50 % depuis le début 2015. Les services de transfert de fichiers ont également enregistré une nette hausse d'activité au cours de la même période (36 %).

Enfin, on constate à la fois une augmentation du nombre de transactions cryptées et d'octets cryptés par transaction. Ces deux aspects présentent aussi bien des avantages que des risques pour la sécurité, et nécessitent le recours à un système intégré de défense offrant une meilleure visibilité.

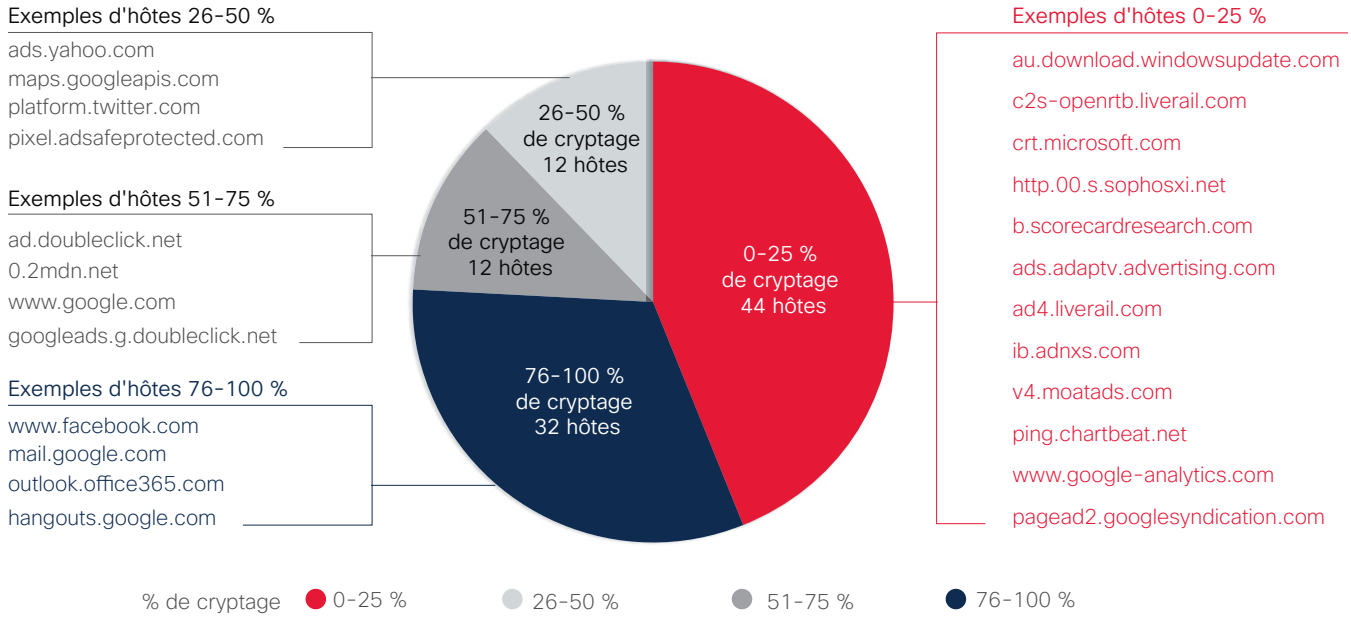
Figure 26 : Requêtes HTTPS : principales évolutions de janvier à septembre 2015



Source : Cisco Security Research

PARTAGER

Figure 27 : Principaux hôtes cryptant le trafic HTTPS



Source : Cisco Security Research

L'analyse des principaux domaines par requêtes (Figure 27) montre qu'un grand nombre des principales pages de contenu Google et Facebook sont cryptées. En général, seuls 10 % de leur trafic publicitaire sont cryptés.

Peu importent les difficultés de mise en œuvre, le cryptage des données est indispensable pour faire face aux menaces actuelles. Les cyberpirates étant passés maîtres dans l'art de contourner les contrôles d'accès, les utilisateurs ne peuvent pas se permettre de laisser des informations critiques sans protection à quelque étape du stockage ou du transfert que ce soit.

C'est pourquoi il est essentiel que les équipes de sécurité surveillent les schémas de trafic Web afin d'identifier toute requête HTTPS en provenance ou à destination de sites suspects. Attention : ne surveillez pas le trafic crypté sur un ensemble prédéfini de ports. Comme expliqué dans la section suivante, nos études montrent que les programmes malveillants tendent à initier des communications cryptées sur des ports variés.

LE FACTEUR D'ENTROPIE

Un haut niveau d'entropie est un bon indicateur de communication ou de transfert de fichiers cryptés ou compressés.[6] La bonne nouvelle, pour les équipes de sécurité, est que l'entropie est relativement facile à surveiller, car elle ne requiert aucune connaissance des protocoles cryptographiques sous-jacents.

Pendant trois mois à compter du 1er juin 2015, les ex perts en sécurité Cisco ont observé 7 480 178 flux issus d'un panel de 598 138 programmes malveillants présentant un indice de dangerosité de 100. Nous avons noté 958 851 flux à entropie élevée sur cette période, soit 12,82 %.

Nous avons également identifié 917 052 flux transmis via le protocole TLS (Transport Layer Security), soit 12,26 %. De plus, 8 419 flux TLS ont transité via un port autre que le port HTTP 443 utilisé par défaut pour le trafic sécurisé. Le programme malveillant observé s'est notamment servi des ports 21, 53, 80 et 500 pour communiquer.

Comme le volume de trafic Internet crypté continue d'augmenter, il est de plus en plus important pour les entreprises d'adopter une architecture intégrée de défense contre les menaces (voir la section « Les six principes d'une solution intégrée de défense contre les menaces », **page 62**). Les solutions ponctuelles n'identifient pas efficacement les menaces potentielles au sein du trafic crypté. Les plates-formes de sécurité intégrées offrent aux équipes de sécurité davantage de visibilité sur les équipements ou les réseaux, ce qui facilite la détection des activités suspectes.

[6] Entropie : en informatique, l'entropie (absence d'ordre ou de prévisibilité) désigne le caractère aléatoire recueilli par un système d'exploitation ou une application en vue d'une utilisation dans la cryptographie ou à d'autres fins exigeant des données aléatoires.

Vers une plus grande adoption du cryptage : enquête de cas

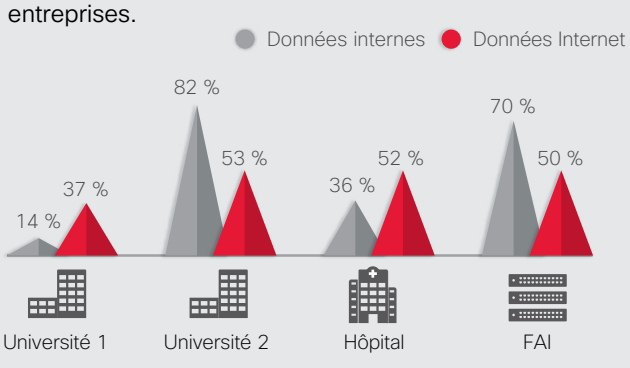
Lancope, une entreprise Cisco, a examiné le taux de cryptage du trafic interne et Internet dans trois secteurs d'activité (deux universités, un hôpital et un fournisseur d'accès à Internet, tous basés aux États-Unis).

Dans l'une des universités, Lancope a découvert que la quasi-totalité du trafic interne (82 %), et 53 % du trafic Internet, étaient cryptés. Ces résultats confirment les tendances observées par Lancope dans d'autres secteurs d'activité.

Seules 36 % des données internes de l'hôpital étaient cryptées. En revanche, plus de la moitié (52 %) du trafic Internet était crypté.

Chez le fournisseur d'accès à Internet de premier plan, 70 % du trafic interne, et 50 % du trafic Internet, étaient cryptés.

L'enquête de Lancope montre une large adoption du cryptage pour les données en mouvement dans différents secteurs. Cisco recommande la même approche pour le cryptage des données au repos afin de limiter l'impact des atteintes à la sécurité des entreprises.



Source : Lancope Threat Research Labs

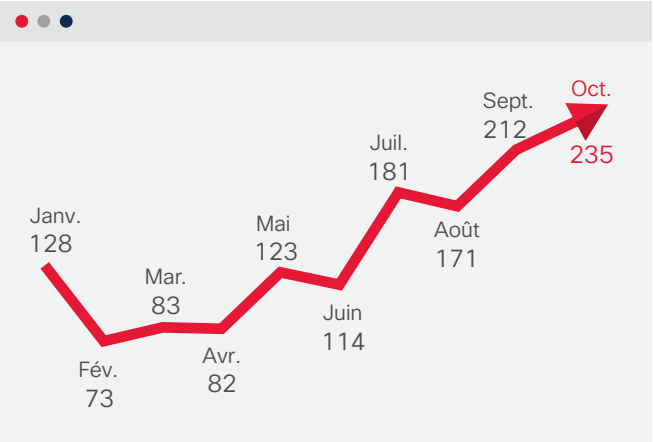
Augmentation de l'activité des cybercriminels sur les serveurs WordPress

Comme indiqué dans l'introduction de ce rapport, les cybercriminels recherchent en permanence de nouveaux moyens de renforcer l'efficacité de leurs activités, d'en réduire les coûts et de passer entre les mailles du filet. C'est pourquoi ils se tournent de plus en plus vers les sites Web créés sous WordPress, une plate-forme populaire de développement de sites Web et de blogs, lesquels leur facilitent grandement la tâche. Les sites WordPress permettent aux hackers de prendre le contrôle d'un flux constant de serveurs compromis et de créer une infrastructure propice au rançonnage, à la fraude bancaire et à l'hameçonnage. Internet regorge de sites laissés à l'abandon, créés avec WordPress, dont la sécurité n'est pas actualisée. À mesure que de nouvelles menaces voient le jour, ces sites sont souvent compromis et intégrés dans les campagnes d'attaques.

En analysant les systèmes exploités par les logiciels rançonneurs et autres programmes malveillants, les experts en sécurité Cisco ont constaté que de nombreux cybercriminels réorientaient désormais leur activité en ligne vers des serveurs WordPress compromis. Le nombre de domaines WordPress utilisés par les cybercriminels a ainsi augmenté de 221 % entre février et octobre 2015 (voir la Figure 28).

Selon les experts Cisco, ce changement de cible est dû à plusieurs raisons. Lorsque les logiciels rançonneurs utilisent d'autres outils pour transmettre les clés de cryptage ou autres informations de commande et de contrôle (CnC), ces communications peuvent être détectées ou bloquées, ce qui empêche l'exécution du processus de cryptage. En revanche, l'envoi des clés de cryptage par le biais de serveurs WordPress compromis peut sembler normal et permet de mener à bien le cryptage. En d'autres termes, les sites WordPress agissent comme des agents de relais.

Figure 28 : Nombre de domaines WordPress utilisés par les développeurs de programmes malveillants



Source : Cisco Security Research

Pour éviter les inconvénients des autres technologies, les cybercriminels se sont tournés vers WordPress, qu'ils utilisent pour héberger les charges utiles des programmes malveillants ainsi que les serveurs de commande et de contrôle. Les sites WordPress leur offrent plusieurs avantages. Par exemple, les nombreux sites abandonnés présentent un faible niveau de sécurité et constituent par conséquent des proies faciles.

L'utilisation de systèmes compromis à des fins malveillantes présente néanmoins un inconvénient : la mise à l'arrêt éventuelle des serveurs piratés une fois l'incident détecté. Si cela se produit au milieu d'une campagne d'attaque, le téléchargeur du programme malveillant risque de ne pas pouvoir récupérer sa charge utile, ou bien le programme malveillant peut être dans l'incapacité de communiquer avec ses serveurs de commande et de contrôle. Les experts en sécurité Cisco ont constaté que le programme malveillant contournait ce problème en utilisant plusieurs serveurs WordPress. Ils ont même découvert des listes de serveurs WordPress compromis stockées sur des sites de partage de données tels que Pastebin.

Le programme malveillant se servait de ces listes pour trouver des serveurs de commande et de contrôle opérationnels lui permettant de poursuivre ses opérations même en cas d'arrêt d'un serveur compromis. Nos experts ont également identifié des téléchargeurs de programmes malveillants contenant une liste de sites WordPress sur lesquels des charges utiles étaient stockées. En cas de non-fonctionnement d'un site de téléchargement, le programme malveillant téléchargeait les charges utiles néfastes à partir du serveur WordPress opérationnel suivant.

En général, les sites WordPress compromis n'exécutaient pas la dernière version de WordPress, étaient protégés par des mots de passe administrateur faibles et utilisaient des plug-ins non à jour des correctifs de sécurité.

Ces vulnérabilités permettaient aux cyberpirates de s'approprier les serveurs WordPress et de les utiliser en tant qu'infrastructure de programme malveillant (voir la Figure 29).

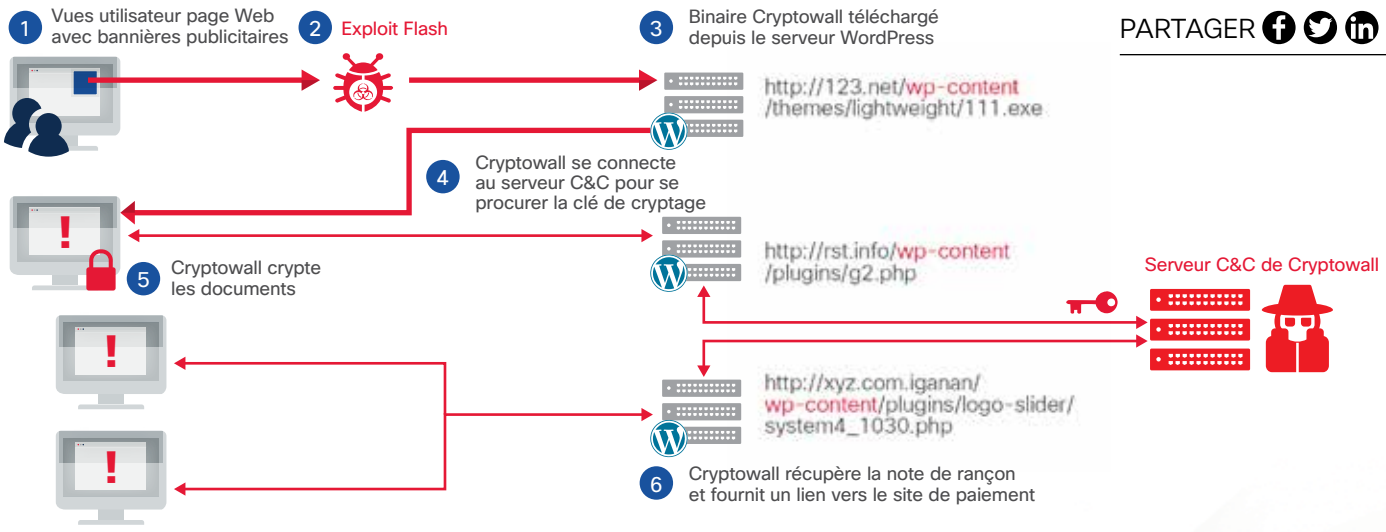
Les experts Cisco ont identifié certains des logiciels et types de fichiers généralement hébergés sur les sites WordPress compromis :

- Fichiers exécutables correspondant aux charges utiles dont se servent les kits d'exploits pour les attaques
- Fichiers de configuration de logiciels malveillants tels que Dridex et Dyre
- Code de proxy relayant les communications de commande et de contrôle pour masquer l'infrastructure de commande et de contrôle
- Pages Web d'hameçonnage pour collecter les noms d'utilisateur et mots de passe
- Scripts HTML qui redirigent le trafic vers des serveurs hébergeant des kits d'exploits

Les experts Cisco ont en outre identifié de nombreuses familles de programmes malveillants qui utilisent des sites WordPress compromis pour leur infrastructure :

- Infostealer Dridex
- Module de vol de mots de passe Poney
- Logiciel de rançonnage TeslaCrypt
- Logiciel de rançonnage Cryptowall 3.0
- Logiciel de rançonnage TorrentLocker
- Botnet de spam Andromeda
- Diffuseur de chevaux de Troie Bartallex
- Infostealer Necurs
- Fausses pages de connexion

Figure 29 : De compromission des sites WordPress



Source : Cisco Security Research

Les professionnels de la sécurité inquiets des risques liés à l'exploitation de WordPress par les cybercriminels ont tout intérêt à s'orienter vers une solution de sécurité web qui examine le contenu provenant de sites créés sous WordPress. Ce trafic pourra être considéré comme suspect si le réseau télécharge des programmes, plutôt que des pages Web et des images, à partir des sites WordPress (bien que ces derniers puissent également héberger des programmes légitimes).

Infrastructure vieillissante : un problème qui remonte à 10 ans

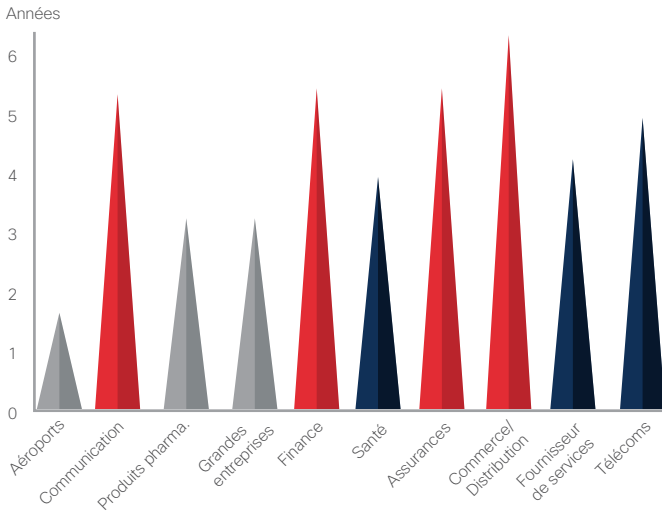
Aujourd'hui, toutes les entreprises peuvent, en quelque sorte, être qualifiées de sociétés informatiques dans la mesure où elles dépendent de leur infrastructure informatique et de technologies opérationnelles (OT) pour être connectées, numérisées et performantes. Elles doivent par conséquent placer la sécurité informatique en tête de leurs priorités. Nombre d'entre elles s'appuient cependant sur des infrastructures réseau non cyber-résilientes dont les composants sont anciens, obsolètes et exécutent des systèmes d'exploitation vulnérables.

Nous avons récemment analysé 115 000 équipements Cisco sur Internet et dans des environnements clients afin d'attirer l'attention sur les risques de sécurité que présentent les infrastructures vieillissantes, de même que l'absence de correction des vulnérabilités.

Les 115 000 équipements observés lors de cet échantillonnage d'une journée ont été identifiés en analysant Internet, puis en examinant les équipements de « l'extérieur vers l'intérieur » (depuis Internet vers l'entreprise). Notre analyse a permis de déterminer que 106 000 des 115 000 équipements contenaient un logiciel présentant des vulnérabilités connues. Cela signifie que, parmi notre échantillon, 92 % des équipements Cisco sur Internet sont exposés à des vulnérabilités connues.

Cisco a en outre découvert que la version du logiciel exécutée sur ces équipements présentait, en moyenne, 26 vulnérabilités. Il est également apparu que de nombreuses entreprises utilisaient des logiciels obsolètes dans leur infrastructure réseau (Figure 30). Certains clients des secteurs de la finance, de la santé et du commerce de détail exécutaient des versions de nos logiciels datant de plus de 6 ans.

Figure 30 : Âge moyen des logiciels (en années)

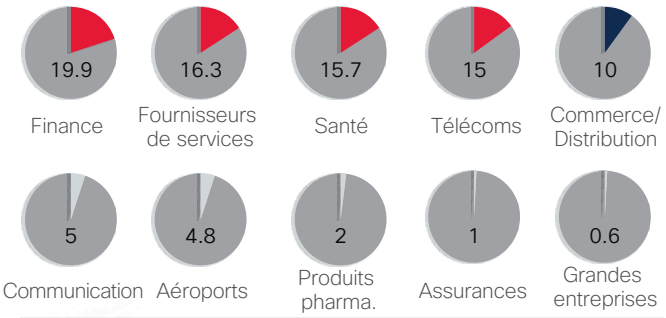


Source : Cisco Security Research

Nous nous sommes par ailleurs aperçus qu'un grand nombre des équipements d'infrastructure analysés avaient atteint leur date de fin de prise en charge, autrement dit qu'il était impossible de les mettre à jour afin de renforcer leur sécurité (Figure 31). Ils ne reçoivent même plus de correctifs contre les vulnérabilités connues, si bien qu'ils ne sont pas informés des nouvelles menaces. Les clients ont été avertis de ce problème.

8 % des 115 000 équipements analysés étaient arrivés en

Figure 31 : Pourcentage d'équipements d'infrastructure en fin de prise en charge



Source : Cisco Security Research

Pour plus d'informations sur ce sujet, consultez les articles du blog Cisco dédié à la sécurité :

- **« IT Security: When Maturity Is Overrated »**
- **« Evolution of Attacks on Cisco IOS Devices »**
- **« SYNful Knock: Detecting and Mitigating Cisco IOS Software Attacks »**

fin de vie, et 31 % ne bénéficieront plus d'aucune prise en charge d'ici un à quatre ans.

Une infrastructure informatique vieillissante et obsolète rend les entreprises vulnérables. Plus on se rapproche de l'Internet des objets (IoT), et de l'Internet of Everything (IoE), plus il est important pour les entreprises de s'assurer qu'elles s'appuient sur une infrastructure réseau sécurisée afin de garantir l'intégrité des données et des communications qui transitent sur le réseau. Il s'agit là d'une condition essentielle à la réussite de la technologie IoE émergente.

De nombreux clients Cisco ont mis en place leur infrastructure réseau il y a dix ans. À cette époque, peu d'entreprises ont réalisé qu'elles dépendraient entièrement de cette infrastructure. Il leur était également difficile de prévoir que leur infrastructure deviendrait la cible privilégiée des hackers.

Les entreprises évitent généralement de mettre à jour leur infrastructure, une opération coûteuse, qui nécessite en outre l'arrêt du réseau. Dans certains cas, une simple mise à jour ne suffit même pas. Certains produits sont si anciens qu'ils ne peuvent plus être mis à niveau pour intégrer les dernières solutions de sécurité nécessaires à la protection de l'entreprise.

Ces constatations montrent à quel point il est important d'actualiser l'infrastructure. Les entreprises doivent planifier des mises à jour régulières et prendre le contrôle de leur infrastructure critique de manière proactive, avant qu'un hacker ne le fasse à leur place.

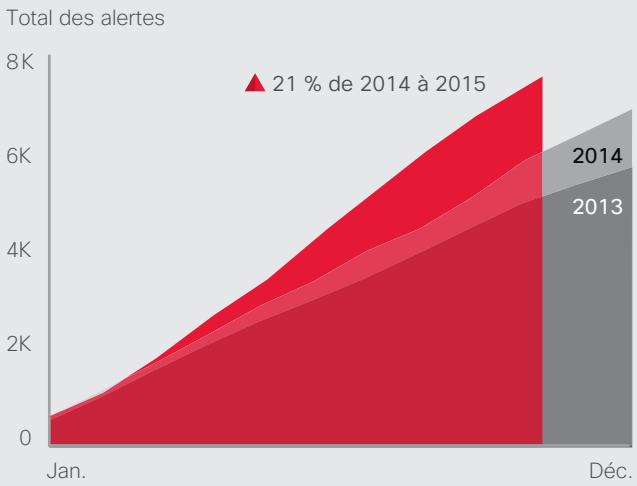
Le nombre total d'alertes cumulées montre une tendance croissante à la gestion des vulnérabilités

L'utilisation d'infrastructures vieillissantes est la porte ouverte aux cyberattaques. Cependant, l'augmentation des alertes cumulées, qui regroupent les vulnérabilités des solutions open source et propriétaires, est un signe que le secteur de la technologie se mobilise pour barrer la route aux cybercriminels.

Le total des alertes cumulées a augmenté de 21 % entre 2014 et 2015. De juillet à septembre 2015, cette hausse a été particulièrement marquée. Cette recrudescence est en grande partie due aux mises à jour logicielles majeures publiées par des éditeurs tels que Microsoft et Apple, car les mises à jour de produits permettent de mieux signaler les vulnérabilités logicielles.

Les principaux éditeurs de logiciels publient désormais davantage de correctifs et de mises à niveau, et le font de manière plus transparente. Ce volume croissant pousse les entreprises à automatiser la gestion des vulnérabilités à l'aide de plates-formes de gestion et d'informations de vieille qui les aident à gérer l'inventaire des logiciels et des systèmes, les vulnérabilités ainsi que la veille sur les menaces. Ces systèmes et API (Application Programming Interface) permettent aux grandes et petites entreprises de gérer la sécurité de manière plus efficace et rapide.

Figure 32 : Nombre total d'alertes annuelles cumulées



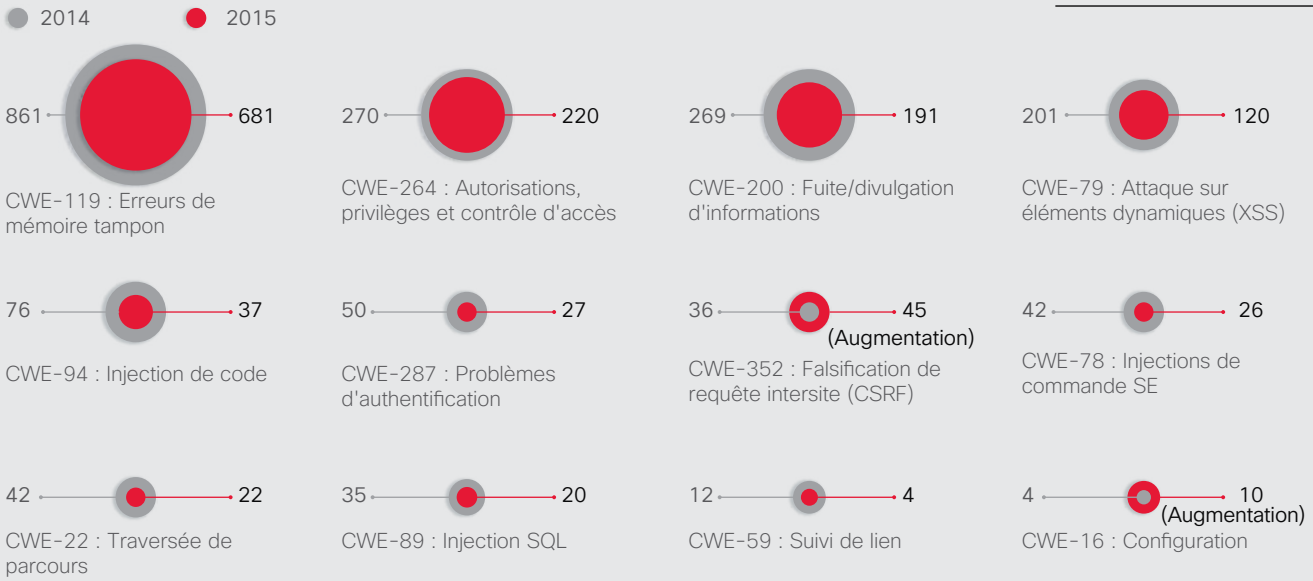
Source : Cisco Security Research

Catégories de menaces : erreurs de tampon et fuites/divulgation d'informations en baisse

Si l'on examine les catégories courantes de vulnérabilités, on constate que celles de type XSS (Cross-Site Scripting) ont baissé de 47 % entre 2014 et 2015 (Figure 33). Cette diminution peut s'expliquer par la plus grande attention portée aux tests de vulnérabilité. Les éditeurs ont développé leur expertise. Ils sont aujourd'hui plus à même d'identifier ces vulnérabilités spécifiques et d'y remédier avant la commercialisation de leurs produits.

Les vulnérabilités de type fuite/divulgation d'informations ont chuté de 15 % en 2015. Ces vulnérabilités concernent la divulgation involontaire de données à des tiers non explicitement autorisés à y accéder. Les éditeurs accordent plus d'attention aux contrôles permettant d'autoriser ou d'interdire l'accès aux données, ce qui contribue à réduire la fréquence de ces vulnérabilités courantes.

Figure 33 : Nombre de vulnérabilités par catégories courantes



Source : Cisco Security Research

Les petites et moyennes entreprises sont-elles un maillon faible en termes de sécurité ?

Les PME jouent un rôle essentiel dans les économies nationales. Elles ont également la responsabilité de protéger de tout piratage les données que leur confient leurs clients. Toutefois, comme expliqué dans l'enquête 2015 de Cisco sur l'efficacité des mesures de sécurité (voir **page 41**), leurs défenses contre les hackers ne sont pas à la hauteur de la tâche. Ces faiblesses peuvent à leur tour mettre en danger leurs entreprises clientes. Les hackers capables de s'introduire dans le réseau d'une PME peuvent également se frayer un chemin vers le réseau d'un de ses clients.

Si l'on en juge par les résultats de l'enquête 2014 de Cisco sur l'efficacité des mesures de sécurité, les PME utilisent moins de processus d'analyse des compromissions, et moins d'outils de défense contre les menaces, que l'année dernière. Par exemple, en 2015, 48 % des PME ont indiqué utiliser une solution de sécurité Web, contre 59 % en 2014. Seules 29 % ont reconnu avoir utilisé des correctifs et des outils de configuration en 2015, contre 39 % en 2014.

De plus, parmi les PME interrogées dépourvues de responsable de la sécurité, près d'un quart ne se considèrent pas comme des cibles de choix pour les cybercriminels. Ce point de vue témoigne d'un excès de confiance dans leur capacité à déjouer les attaques en ligne sophistiquées d'aujourd'hui ou, plus probablement, de la conviction qu'elles ne feront jamais l'objet d'attaques.

LES PME MOINS SUSCEPTIBLES DE METTRE EN PLACE DES ÉQUIPES DE GESTION DES INCIDENTS

Les PME sont moins susceptibles que les grandes entreprises de disposer d'équipes de gestion des incidents et des informations sur les menaces. Cela peut être dû à des contraintes budgétaires. Les personnes interrogées ont en effet désigné les problèmes de budget comme l'un des principaux obstacles à l'adoption de processus et de technologies de sécurité avancés. Ces deux équipes sont présentes dans 72 % des grandes entreprises (de plus de 1 000 employés) et dans 67 % des entreprises de moins de 500 employés.

Les PME exécutent par ailleurs moins de processus d'analyse des compromissions, d'élimination de la cause d'un incident et de rétablissement des systèmes dans l'état où ils se trouvaient avant l'incident (Figure 35). Par exemple, 53 % des entreprises de plus de 10 000 employés procèdent à une analyse du trafic réseau pour identifier les systèmes compromis, contre 43 % des entreprises de moins de 500 employés. 60 % des entreprises de plus de 10 000 employés appliquent des correctifs et des mises à jour aux applications jugées vulnérables, contre 51 % des entreprises de moins de 500 employés.

L'utilisation de certaines solutions de défense contre les menaces est en baisse dans les PME. Par exemple, 52 % des PME ont eu recours à des solutions de sécurité mobile en 2014, contre seulement 42 % en 2015. 48 % ont utilisé un logiciel d'analyse des vulnérabilités en 2014, contre 40 % en 2015 (voir la Figure 36).

Figure 34 : Principaux obstacles pour les PME

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

Taille de l'entreprise	250-499	500-999	1 000-9 999	10 000+
Contraintes budgétaires	40 %	39 %	39 %	41 %
Problèmes de compatibilité avec les systèmes existants	34 %	30 %	32 %	34 %
Autres priorités	25 %	25 %	24 %	24 %

Source : Enquête 2015 de Cisco sur l'efficacité des mesures de sécurité

Figure 36 : Baisse de l'utilisation de solutions de défense par les PME en 2015

Quels moyens de défense contre les menaces à la sécurité votre entreprise utilise-t-elle actuellement, le cas échéant ?

	2014	2015
Sécurité mobile	52 %	42 %
Réseau sans fil sécurisé	51 %	41 %
Analyse des vulnérabilités	48 %	40 %
VPN	46 %	36 %
Gestion des systèmes de gestion des informations et des événements de sécurité (SIEM)	42 %	35 %
Tests de pénétration	38 %	32 %
Analyse des réseaux	41 %	29 %
Application de correctifs et configuration	39 %	29 %
Analyse des terminaux	31 %	23 %

Source : Enquête 2015 de Cisco sur l'efficacité des mesures de sécurité

Figure 35 : Les PME utilisent moins de processus de sécurité que les grandes entreprises

Quels processus, le cas échéant, votre entreprise utilise-t-elle pour analyser les systèmes infectés ?

Taille de l'entreprise	250-499	500-999	1 000-9 999	10 000+
Analyse de la mémoire	36 %	36 %	35 %	34 %
Analyse des flux réseau	43 %	47 %	52 %	53 %
Analyse de corrélation entre journaux et événements	34 %	34 %	40 %	42 %
Équipes externes (tierces) d'analyse/de résolution des incidents	40 %	32 %	34 %	39 %
Analyse des journaux système	47 %	51 %	55 %	59 %
Analyse des registres	43 %	47 %	52 %	53 %
Détection des IOC	31 %	34 %	37 %	36 %

Quels processus votre entreprise utilise-t-elle pour restaurer les systèmes affectés à leurs niveaux de fonctionnement avant incident ?

Application de correctifs et mise à jour des applications jugées vulnérables	51 %	53 %	57 %	60 %
Mise en œuvre de nouveaux contrôles et dispositifs de détection	49 %	55 %	57 %	61 %

Source : Enquête 2015 de Cisco sur l'efficacité des mesures de sécurité

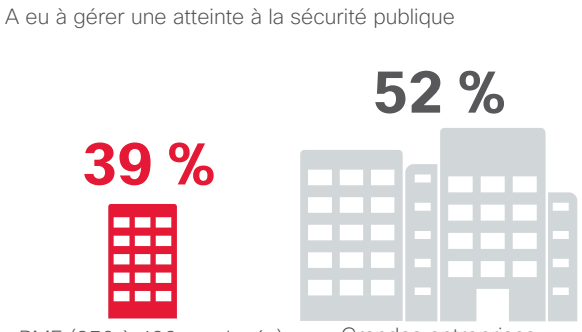
Pourquoi le fait que les PME utilisent moins de solutions de défense que les grandes entreprises est-il si important ? Dans le contexte de la sécurité actuel, où les cybercriminels mettent au point des tactiques de plus en plus sophistiquées pour s'introduire dans les réseaux sans se faire repérer, aucune entreprise ne peut se permettre de laisser ses réseaux sans protection, ni de renoncer à utiliser des processus permettant de déterminer comment une attaque a eu lieu afin d'éviter qu'elle ne se reproduise.

De plus, les PME ne semblent pas réaliser que leur propre vulnérabilité met en danger leurs clients grands comptes et leurs réseaux. Aujourd'hui, les cybercriminels s'introduisent souvent dans un réseau afin de s'en prendre à un autre réseau plus lucratif. Les PME peuvent constituer le point d'entrée de ce type d'attaque.

LES PME SONT MOINS EXPOSÉES AUX ATTEINTES À LA SÉCURITÉ PUBLIQUES

Les PME ont moins de risques que les grandes entreprises d'être victimes d'une atteinte à la sécurité publique, probablement en raison de la moindre envergure de leur réseau. Si 52 % des entreprises de plus de 10 000 employés ont réussi à gérer les répercussions d'une atteinte à la sécurité publique, seules 39 % des entreprises de moins de 500 employés y sont parvenues.

Figure 37 : Les entreprises signalent moins d'atteintes à la sécurité publique

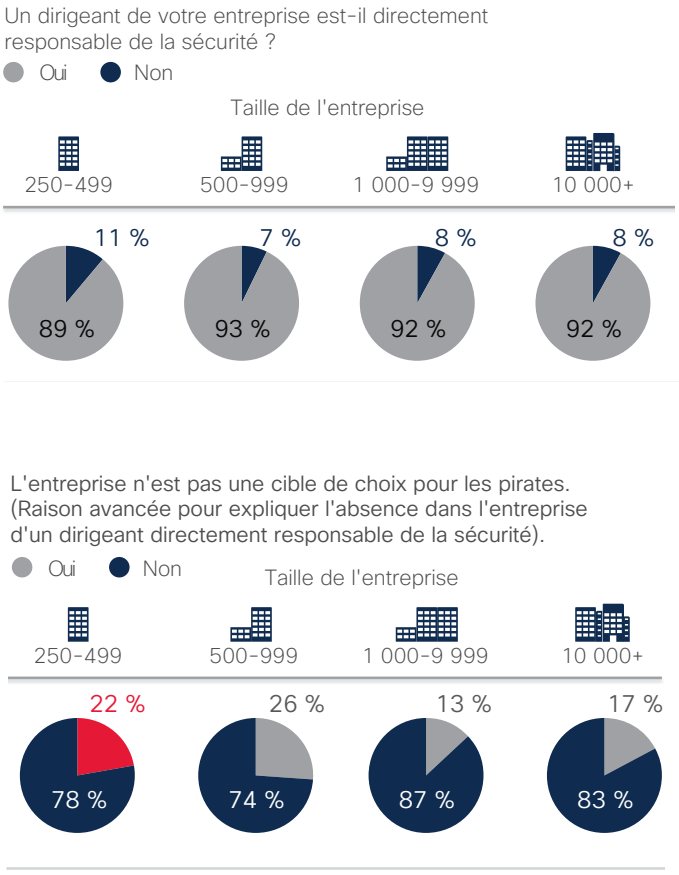


Source : Enquête 2015 de Cisco sur l'efficacité des mesures de sécurité

PARTAGER

Les atteintes à la sécurité publiques perturbent bien entendu l'activité et portent préjudice à l'image de marque, mais offrent néanmoins un avantage : elles encouragent bien souvent les entreprises à examiner de plus près leur système de protection et à le renforcer. Les données de l'enquête Cisco (voir **page 74**) montrent que les grandes entreprises victimes d'une atteinte à la sécurité publique améliorent considérablement leur technologie de sécurité et renforcent leurs processus.

Figure 38 : Les PME ne se considèrent pas comme des cibles de choix



Source : Enquête 2015 de Cisco sur l'efficacité des mesures de sécurité

La perception que les PME ont de leur entreprise en tant que cible potentielle d'attaques peut sembler en décalage avec la réalité du cybercrime. Comme illustré ci-dessus, à la Figure 38, 22 % des entreprises de moins de 500 employés ont indiqué qu'elles ne disposaient d'aucun dirigeant directement responsable de la sécurité dans la mesure où elles ne se considèrent pas comme des cibles de choix.

LES PME SONT PLUS SUSCEPTIBLES D'EXTERNALISER LEURS FONCTIONS DE SÉCURITÉ EN 2015

Même si l'enquête montre que, globalement, de plus en plus de PME sous-traitent certaines de leurs fonctions de sécurité, les PME sont en général moins susceptibles que les grandes entreprises d'externaliser des services tels que le conseil. Par exemple, 55 % des grandes entreprises sous-traitent les services de conseil, contre 46 % des entreprises de moins de 500 employés. 56 % des grandes entreprises externalisent les tâches d'audit de la sécurité, contre 42 % des entreprises de moins de 500 employés (voir la Figure 39).

En 2015, cependant, davantage de PME ont externalisé au moins certains services de sécurité. En 2014, 24 % des PME de moins de 499 employés ont indiqué n'avoir externalisé aucun service. En 2015, cela a été le cas pour seulement 18 % des PME.

Le fait qu'un plus grand nombre de PME choisissent l'externalisation comme mode gestion de la sécurité est une bonne nouvelle. Il indique que les PME recherchent des outils de sécurité réseau flexibles, qui n'alourdissent pas la charge de travail de leurs effectifs restreints et ne pèsent pas sur leurs budgets serrés. Toutefois, les PME peuvent s'imaginer à tort que l'externalisation des processus de sécurité réduira de manière significative les risques d'atteinte à la sécurité du réseau. Elles peuvent aussi placer l'entière responsabilité de la sécurité entre les mains d'un tiers. Un tel point de vue est illusoire étant donné que seul un véritable système intégré de défense contre les menaces, non seulement capable de détecter les attaques et d'en atténuer l'impact, mais aussi de les prévenir, peut offrir aux entreprises un niveau de sécurité adéquat.

Figure 39 : Davantage de PME externalisent leurs services de sécurité en 2015

En matière de sécurité, quels types de services, le cas échéant, votre entreprise externalise-t-elle en tout ou partie auprès de tiers ?

Taille de l'entreprise	250-499	500-999	1 000-9 999	10 000+
Conseil	46 %	51 %	54 %	55 %
Surveillance	45 %	46 %	42 %	44 %
Audit	42 %	46 %	46 %	56 %
Traitement des incidents	39 %	44 %	44 %	40 %
Veille sur les menaces	35 %	37 %	42 %	41 %
Correction	33 %	38 %	36 %	36 %
Aucun	18 %	12 %	11 %	10 %

Pourquoi votre entreprise (PME de 250 à 499 employés) a-t-elle décidé d'externaliser ce/ces service(s) ?

Source : Enquête 2015 de Cisco sur l'efficacité des mesures de sécurité

PARTAGER

Enquête sur l'efficacité des mesures de sécurité de Cisco

Enquête sur l'efficacité des mesures de sécurité de Cisco

Pour savoir comment les professionnels de la sécurité perçoivent les mesures adoptées par leur entreprise en la matière, Cisco a interrogé des responsables de la sécurité et des responsables des opérations de sécurité d'entreprises de différentes tailles, dans plusieurs pays, pour savoir comment ils percevaient leurs ressources et procédures de sécurité. L'enquête 2015 de Cisco sur l'efficacité des mesures de sécurité fournit un aperçu du niveau de maturité des opérations et pratiques actuelles en matière de sécurité. Elle compare également les résultats avec ceux de la première enquête réalisée en 2014.

Confiance en berne malgré une forte mobilisation

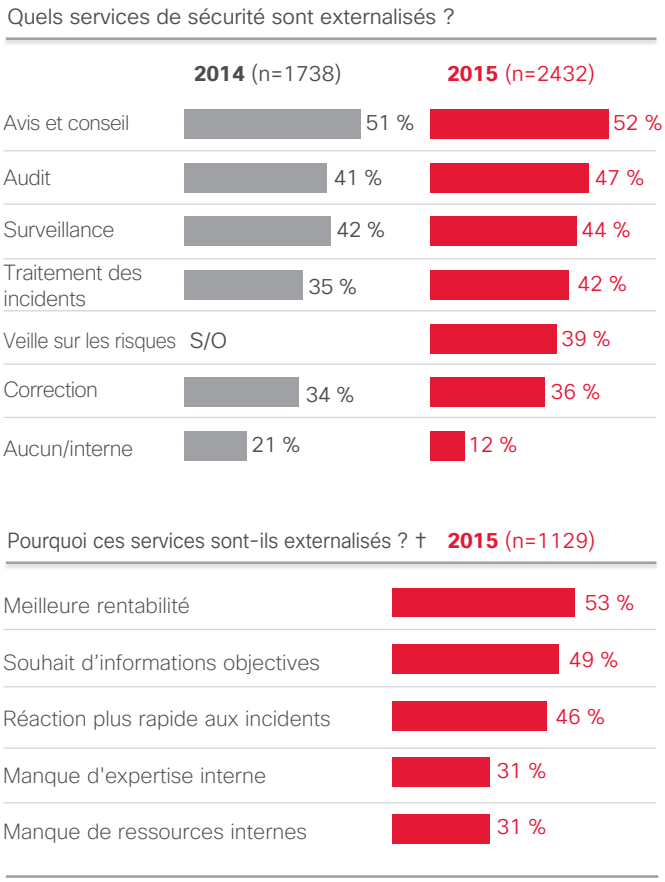
L'enquête de Cisco suggère que, face à des menaces de plus en plus sophistiquées, la confiance des professionnels de la sécurité est en berne. Parallèlement, les préoccupations croissantes en matière de sécurité modifient la manière dont ils protègent les réseaux. On remarque, par exemple, davantage de formations à la sécurité, une augmentation des politiques formelles écrites et l'externalisation d'un plus grand nombre de tâches telles que les audits de sécurité, le conseil et la gestion des incidents. En résumé, tout semble indiquer que les professionnels de la sécurité prennent des mesures pour combattre les menaces qui pèsent sur leurs réseaux.

La formation et l'externalisation constituent une évolution positive, mais le secteur de la sécurité ne peut pas s'arrêter là. Il doit intensifier son utilisation d'outils et de processus afin d'améliorer la détection, le confinement et l'élimination des menaces. Face aux problèmes de restrictions budgétaires et de compatibilité des solutions, le secteur doit également rechercher des systèmes intégrés efficaces de défense contre les menaces. Il doit par ailleurs mieux collaborer avec d'autres entreprises en cas de failles publiques (comme le botnet SSHPsychos ; voir **page 14**), car le partage de connaissances permet de prévenir les attaques futures.

RESSOURCES : LES ENTREPRISES SONT PLUS PORTÉES VERS L'EXTERNALISATION

Face aux nouvelles menaces, les professionnels de la sécurité sont susceptibles de rechercher des moyens d'améliorer leurs défenses, par exemple en externalisant les tâches de sécurité pouvant être plus efficacement gérées par des consultants ou des fournisseurs. En 2015, 47 % des entreprises interrogées externalisaient leurs audits de sécurité, contre 41 % en 2014. Par ailleurs, en 2015, 42 % des entreprises interrogées externalisaient leurs processus de résolution d'incidents, contre 35 % en 2014 (Figure 40).

Figure 40 : Vue d'ensemble des services externalisés



† Professionnels de la sécurité interrogés qui externalisent des services de sécurité (2015 ; n=2129)

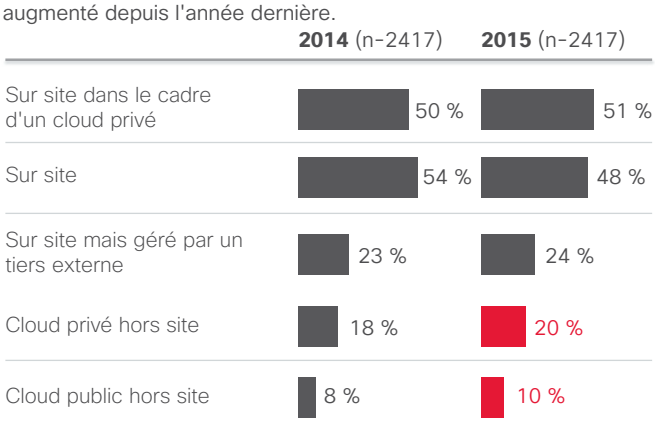
Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

De plus, un nombre accru de professionnels de la sécurité sous-traitent au moins une partie de leurs fonctions de sécurité. En 2014, 21 % des professionnels interrogés déclaraient ne sous-traiter aucun service de sécurité. En 2015, cette proportion a considérablement reculé. Elle est aujourd'hui de 12 %. 53 % des entreprises interrogées ont déclaré externaliser des services pour des questions de rentabilité, tandis que 49 % d'entre elles le font dans le but d'obtenir des informations objectives.

Les professionnels de la sécurité se sont dits ouverts au concept d'hébergement des réseaux hors site pour accroître la protection de leurs réseaux et données. Bien que l'hébergement sur site reste l'option privilégiée, le nombre de professionnels faisant appel à des solutions hors site a augmenté. En 2015, 20 % des professionnels utilisaient des solutions hors site de cloud privé, contre 18 % en 2014 (Figure 41).

Figure 41 : Hébergement hors site en augmentation

L'hébergement sur site des réseaux d'entreprise reste la solution la plus courante. Toutefois, la proportion d'hébergement hors site a augmenté depuis l'année dernière.



Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 42 : Les contraintes budgétaires représentent l'obstacle majeur aux mises à niveau de sécurité

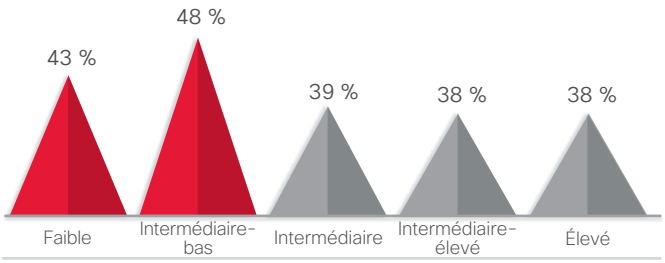
Principaux obstacles à l'adoption d'une sécurité avancée		Processus et technologies	**2015** (n=2432)
Contraintes budgétaires $	39 %	Manque de connaissances	23 %
Problèmes de compatibilité	32 %	Culture/attitude de l'entreprise	23 %
Conditions requises pour la certification	25 %	Manque de personnel qualifié	22 %
Priorités concurrentes	24 %	Réticence à l'achat avant que les produits aient fait leurs preuves sur le marché	22 %
Charge de travail trop importante	24 %	Achat de la haute direction	20 %

Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Bien que davantage tournées vers la protection efficace de leurs réseaux, les équipes de sécurité interrogées par Cisco peuvent être limitées dans leur capacité à concrétiser leurs projets. Pour les professionnels de la sécurité, les contraintes budgétaires (39 %) figurent en haut de la liste des motifs possibles de choix ou non de services et d'outils de sécurité, suivies des problèmes de compatibilité technologique (32 %) (voir Figure 42). Les contraintes budgétaires représentent davantage un problème pour les entreprises de faible ou moyenne maturité (voir Figure 43). Parmi les professionnels de la sécurité interrogés, 39 % citent les contraintes budgétaires comme un obstacle à l'adoption de processus de sécurité avancés. Ce chiffre englobe 43 % d'entreprises de faible maturité et 48 % d'entreprises de faible-moyenne maturité.

Figure 43 : Les contraintes budgétaires représentent un obstacle plus important pour les entreprises de faible maturité

Pourcentage des personnes interrogées qui considèrent les contraintes budgétaires comme le principal obstacle (n=2432)

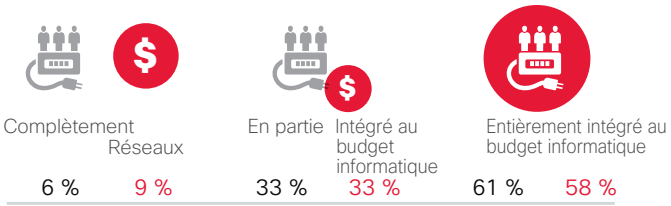


Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

La façon de structurer leur budget de sécurité témoigne du souci croissant qu'ont certaines entreprises de leurs ressources de sécurité. L'enquête montre une légère augmentation du nombre d'entreprises qui séparent leur budget sécurité de leur budget informatique global. En 2014, 6 % des professionnels déclaraient séparer totalement leurs budgets sécurité et informatique. En 2015, ce chiffre a atteint 9 % (voir Figure 44).

Figure 44 : Légère augmentation du nombre d'entreprises qui séparent leur budget de sécurité du budget informatique

Le budget dédié à la sécurité est-il intégré au budget informatique ?
2014 (n=1720) **2015** (n=2417)



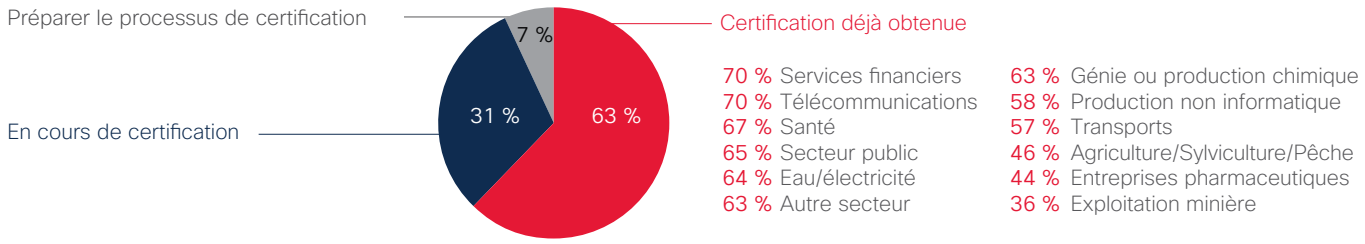
Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

PARTAGER

Les entreprises qui adoptent des politiques de sécurité normalisées ou qui se tournent vers la certification montrent leur souci d'améliorer la sécurité. Près des deux tiers des professionnels de la sécurité interrogés indique que leur entreprise a adopté des politiques ou pratiques de sécurité normalisées ou est en phase de certification (Figure 45). Cet autre signe positif montre que les entreprises trouvent important d'améliorer leurs connaissances en matière de sécurité et de réagir aux menaces.

Figure 45 : La plupart des entreprises sont certifiées ou en voie de certification

L'entreprise suit une pratique normalisée en matière de politique de sécurité de l'information (**2015** n=1265)



Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

En étudiant l'utilisation des protections de sécurité, nous avons constaté que les pare-feu sont les outils de sécurité les plus communément utilisés par les entreprises (65 %), suivis de la prévention des pertes de données (56 %) et des outils d'authentification (53 %) (voir Figure 46). En 2015, les entreprises ont été légèrement plus frileuses envers les outils orientés cloud. Malgré leur volonté manifeste d'externaliser les services de sécurité (voir **page 43**), les professionnels de la sécurité peuvent avoir plutôt tendance à déployer des outils en interne. (Voir la **page 71** pour la liste complète.)

Figure 46 : Les pare-feu et la prévention des pertes de données sont les outils de sécurité les plus courants

Mesures de protection utilisées par les entreprises	**2014** (n=1738)	**2015** (n=2432)	Défenses gérées par des services orientés cloud (professionnels sondés qui utilisent des défenses contre les menaces de sécurité) **2014** (n=1646)	**2015** (n=2268)
Pare-feu*	S/O	65 %		31 %
Prévention des pertes de données	55 %	56 %		
Authentification	52 %	53 %		
Chiffrement/confidentialité/protection des données	53 %	53 %		
Sécurité de la messagerie	56 %	52 %	37 %	34 %
Sécurité web	59 %	51 %	37 %	31 %
Sécurité réseau, pare-feu et prévention des intrusions*	60 %	S/O	35 %	

*Les pare-feu et la prévention des intrusions avaient pour mot d'ordre en 2014 : « Sécurité réseau, pare-feu et prévention des intrusions ».

Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

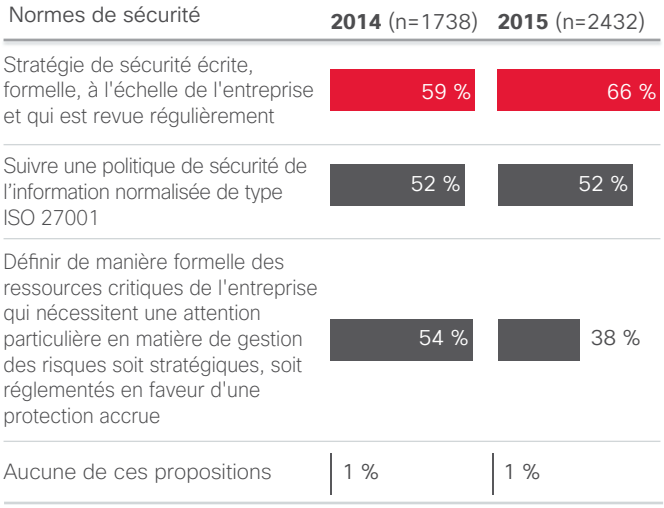
CAPACITÉS : LA CONFIANCE EN DÉCLIN

En 2015, les professionnels de la sécurité exprimaient moins de certitude quant à l'actualité de leur infrastructure de sécurité par rapport à 2014. Ce déclin de confiance est sans doute dû à la survenue régulière d'attaques importantes de grandes entreprises, au vol de données confidentielles qui en découle et aux excuses publiques d'entreprises dont les réseaux ont été atteints.

Ce déclin de confiance s'accompagne toutefois d'un intérêt croissant pour le développement de politiques plus robustes. Comme le montre la Figure 47, comparé à 2014 (59 %), davantage d'entreprises (66 %) possèdent en 2015 une stratégie de sécurité écrite et formelle.

Figure 47 : Davantage d'entreprises élaborent des politiques de sécurité formelles

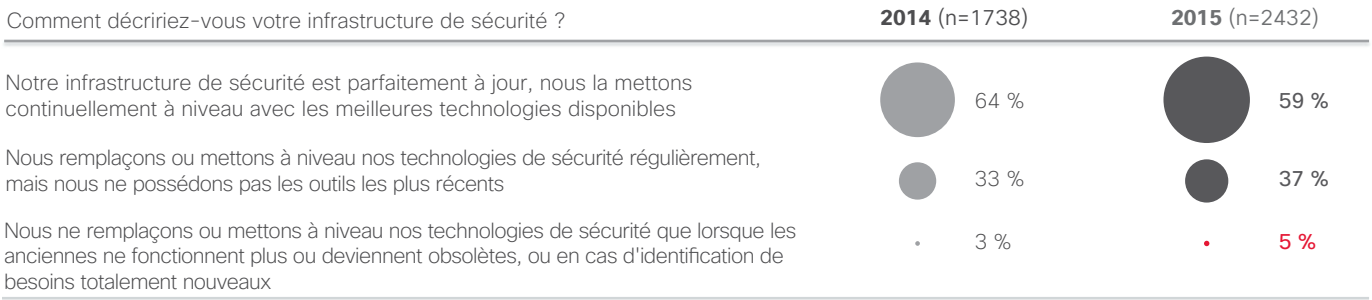
Près des deux tiers sont déjà certifiées selon une politique ou une pratique de sécurité normalisée.



Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

PARTAGER

Figure 48 : La confiance est en déclin en 2015

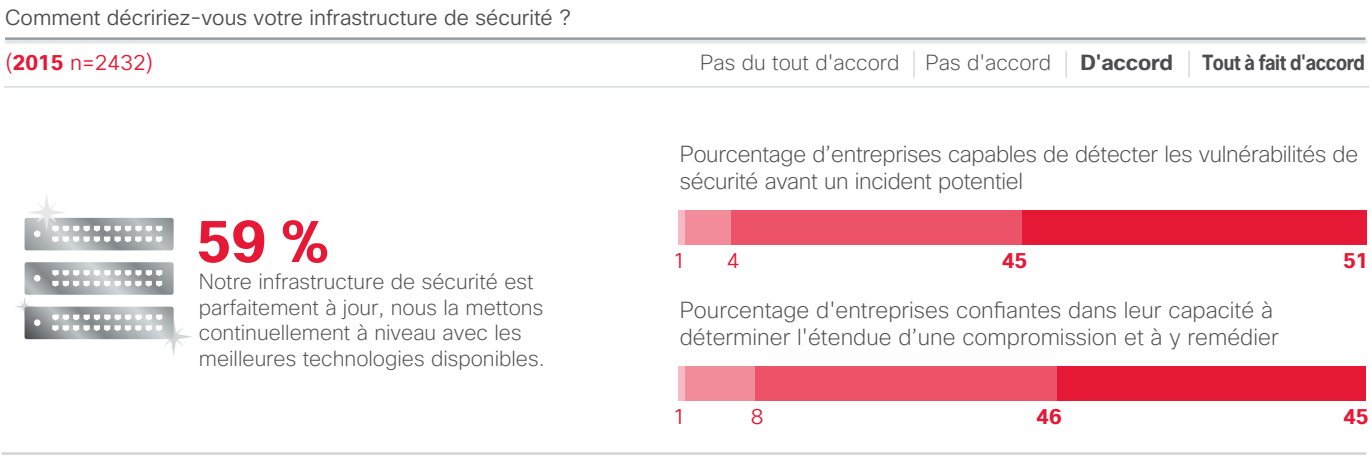


Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Les professionnels de la sécurité ont légèrement moins confiance dans leurs technologies, ce qui témoigne de ce déclin. En 2014, 64 % des entreprises interrogées ont in diqué que leur infrastructure de sécurité était à jour et mise à niveau en permanence. En 2015, ce chiffre a chuté à 59 % (voir Figure 48). En outre, en 2014, 33 % des sondés ont répondu que leur entreprise n'était pas été équipée des derniers outils de sécurité. Ce chiffre a atteint 37 % en 2015.

La confiance est quelque peu plus élevée chez les opérateurs de systèmes informatiques (CSO), plus optimistes que les responsables des opérations de sécurité (SecOp) : 65 % des CSO pensent que leur infrastructure de sécurité est à jour, contre 54 % chez les SecOp. La moindre confiance des responsables des opérations de sécurité est peut-être due au fait que ces derniers sont chargés de répondre aux incidents de sécurité quotidiens, ce qui leur donne une vision moins positive de leur préparation face aux menaces de sécurité.

Figure 49 : Niveaux de confiance variés en termes de capacité à repérer les compromissions

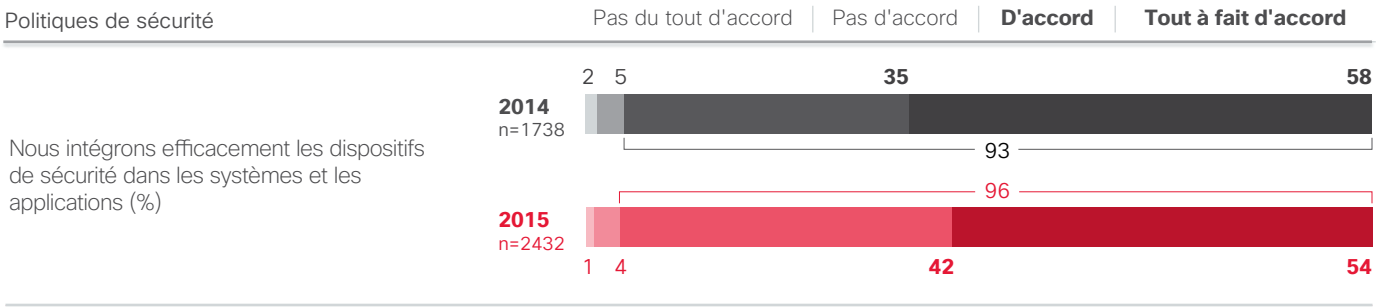


Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Par ailleurs, les professionnels de la sécurité sont partagés concernant leur capacité à contrecarrer les attaques. 51 % sont convaincus qu'ils sont capables de repérer les failles de sécurité avant qu'elles ne deviennent de véritables incidents, et seulement 45 % ont confiance dans leur capacité à déterminer l'étendue d'une compromission sur le réseau et à réparer les dommages (voir Figure 49).

Les professionnels de la sécurité expriment également une moindre confiance dans leur capacité à défendre leurs réseaux contre les attaques. Par exemple, en 2015, moins de professionnels sont convaincus qu'ils intègrent efficacement la sécurité dans leurs procédures d'acquisition, de développement et de gestion de systèmes (54 % en 2015, contre 58 % en 2014) (voir Figure 50). (Voir la **page 76** pour la liste complète.)

Figure 50 : Baisse de confiance dans la capacité à intégrer la sécurité dans les systèmes

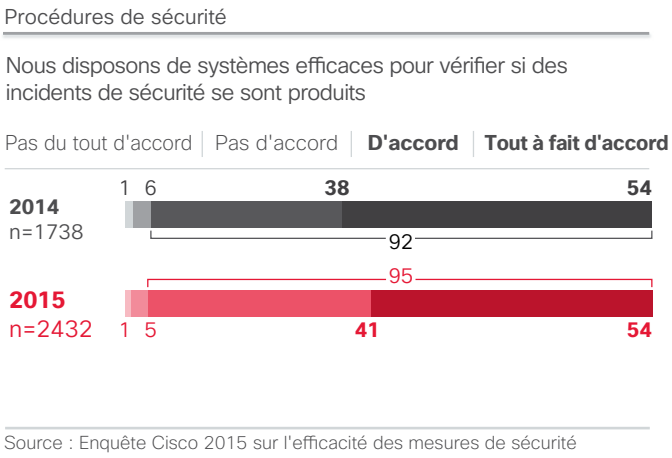


Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Dans certains domaines, la confiance dans les capacités de sécurité est assez faible. Par exemple, en 2015, seuls 54 % des professionnels interrogés pensaient disposer d'un système efficace pour confirmer la survenue d'incidents de sécurité (voir Figure 51). (Voir la **page 77** pour la liste complète.)

Les professionnels interrogés ne sont pas non plus certains que leurs systèmes soient capables d'évaluer et de confiner les compromissions. 56 % ont déclaré revoir et améliorer leurs pratiques de sécurité régulièrement, formellement et stratégiquement ; 52 % pensent que leurs technologies de sécurité sont bien intégrées et interagissent efficacement (voir Figure 52). (Voir la **page 79** pour la liste complète.)

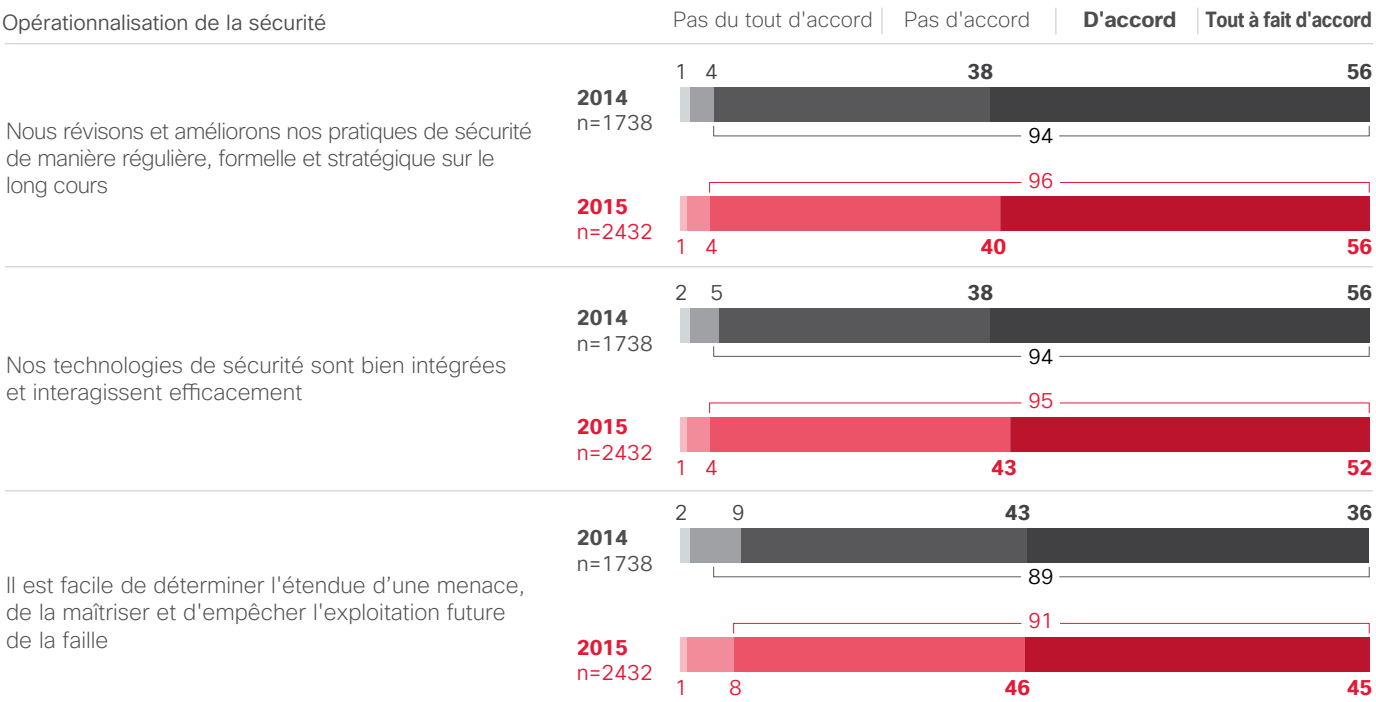
Figure 51 : Les entreprises pensent disposer de procédures de sécurité efficaces



Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

PARTAGER

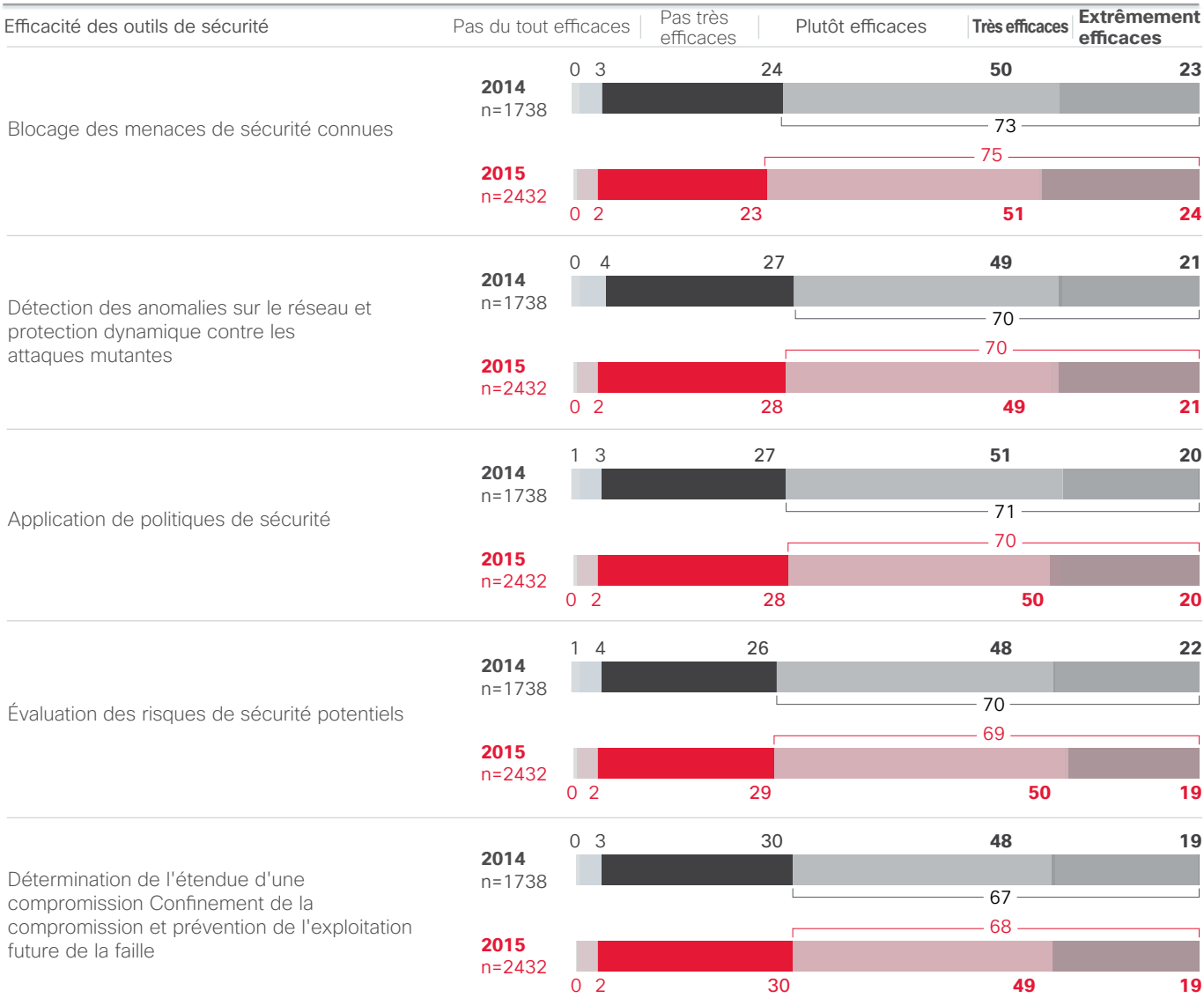
Figure 52 : Les entreprises expriment des niveaux de confiance variés en termes de capacité à confiner les compromissions



Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 53 : Un quart des entreprises estime que les outils de sécurité sont plutôt efficaces

Comme l'année dernière, plus d'un quart des professionnels interrogés perçoit ses outils de sécurité comme seulement « plutôt » efficaces (ni « très, » ni « extrêmement » efficaces).



Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

En 2014 comme en 2015, plus d'un quart des professionnels de la sécurité percevaient leurs outils de sécurité comme plutôt efficaces (Figure 53).

La survenue d'attaques de sécurité publiques tend à être décisive pour les entreprises. Après une attaque, elles semblent prendre davantage conscience de la nécessité d'empêcher de futures intrusions. Cependant, entre 2014 et 2015, moins de professionnels de la sécurité ont déclaré avoir dû faire face à des attaques de sécurité publiques, soit 53 % en 2014 et 48 % en 2015 (Figure 54).

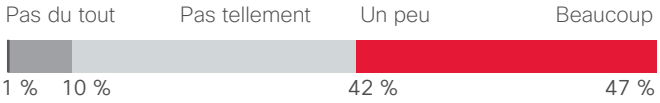
Les professionnels savent que les intrusions sont un signal d'alarme utile qui révèle l'importance du renforcement des processus de sécurité : pour 47 % des professionnels de la sécurité concernés par des attaques publiques, les intrusions ont donné lieu à de meilleures politiques et procédures. Par exemple, 43 % des professionnels interrogés ont déclaré avoir renforcé la formation sur la sécurité suite à une attaque publique, et 42 % ont déclaré avoir accru leurs investissements dans des technologies de défense.

Les entreprises qui ont subi une attaque de sécurité publiquee sont de plus en plus portées sur le renforcement de leurs processus de sécurité, ce qui est très positif. En 2015, 97 % des professionnels de la sécurité ont indiqué pratiquer de la formation sur la sécurité au moins une fois par an, soit une augmentation sensible comparé aux 82 % de 2014 (voir la Figure 90 à la **page 82**).

Figure 54 : Les attaques publiques peuvent améliorer la sécurité

Votre entreprise a-t-elle déjà dû faire face à la méfiance du public après la découverte d'une attaque ? (n=1701) (n=1347)

Dans quelle mesure l'attaque a-t-elle permis d'améliorer vos politiques, procédures ou technologies de défense contre les menaces de sécurité ? (n=1134)



Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 55 : Davantage d'entreprises pratiquent de la formation sur la sécurité

En 2015, 43 % des personnes interrogées ont indiqué avoir renforcé la formation sur la sécurité après une attaque publique.

Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

MATURITÉ : LES CONTRAINTES BUDGÉTAIRES ONT UNE GRANDE IMPORTANCE À TOUS LES NIVEAUX

Les entreprises déploient des pratiques et des politiques de sécurité plus évoluées. Dans ce contexte, la perception qu'elles ont de leur préparation en termes de sécurité peut varier. L'enquête Cisco 2015 sur l'efficacité des mesures de sécurité place les personnes interrogées et leur entreprise dans cinq catégories de maturité selon leurs réponses aux questions sur leurs processus de sécurité (Figure 56). L'enquête examine comment différentes caractéristiques, telles que les capacités, le secteur d'activité et le pays, peuvent impacter les niveaux de maturité.

Curieusement, les entreprises de niveaux de maturité différents semblent partager certains obstacles pour la mise en place de processus et d'outils de sécurité plus sophistiqués. Bien que les pourcentages exacts puissent varier, le défi des contraintes budgétaires arrive en haut de la liste à tous les niveaux de maturité (Figure 57).

Figure 56 : Le modèle de maturité classe les entreprises par rapport aux processus de sécurité

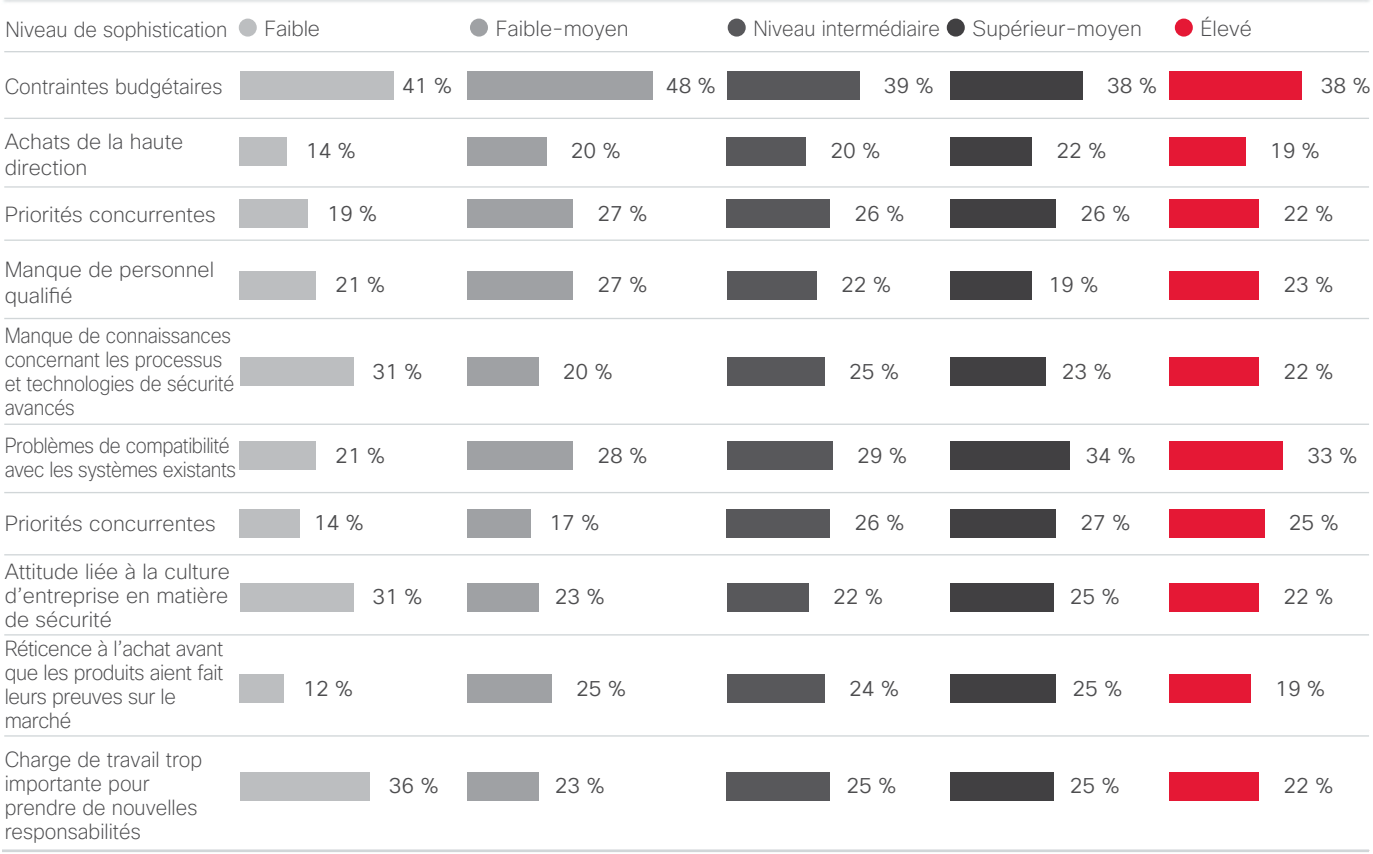
Cisco a exploré plusieurs possibilités avant de s'arrêter sur cinq niveaux déterminés à partir d'une série de questions relatives aux processus de sécurité. Cette solution correspond d'assez près au modèle CMMI (Capability Maturity Model Integration).

	Niveau		Solution basée sur cinq segments
Optimisation	1	Accent mis sur l'amélioration des processus	Élevé
Géré quantitativement	2	Processus quantitativement mesurés et contrôlés	Supérieur-moyen
Défini	3	Processus définis pour l'entreprise : souvent proactifs	Niveau intermédiaire
Reproductible	4	Processus définis pour des projets : souvent réactifs	Faible-moyen
Initial	5	Les processus sont ad hoc, imprévisibles	Faible

Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 57 : Le niveau de maturité n'a pas d'impact sur les obstacles à l'adoption d'une meilleure sécurité

Parmi les critères suivants, lesquels considérez-vous comme les obstacles majeurs à l'adoption de processus et technologies de sécurité avancés ?

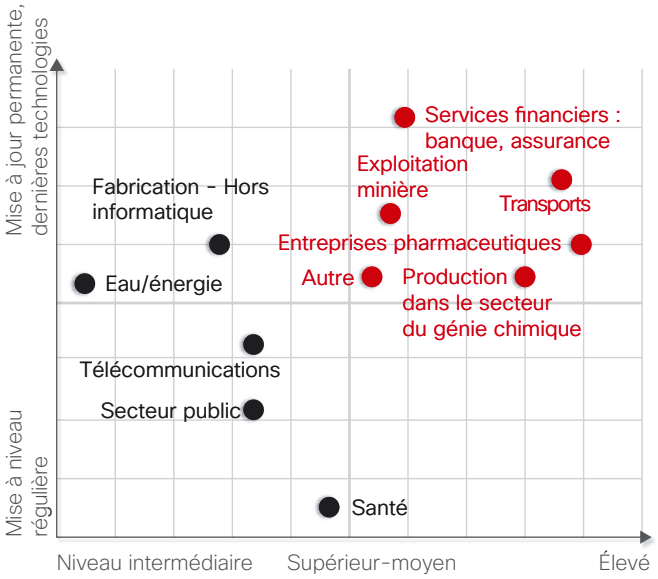


Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Les entreprises qui ont subi une attaque de sécurité Le graphique de droite établit une correspondance entre la qualité de l'infrastructure de sécurité et les niveaux de maturité de divers secteurs. Il se base sur la perception qu'ont les personnes interrogées de leurs processus de sécurité. Les secteurs en haut à droite présentent les niveaux les plus élevés de maturité et de qualité d'infrastructure.

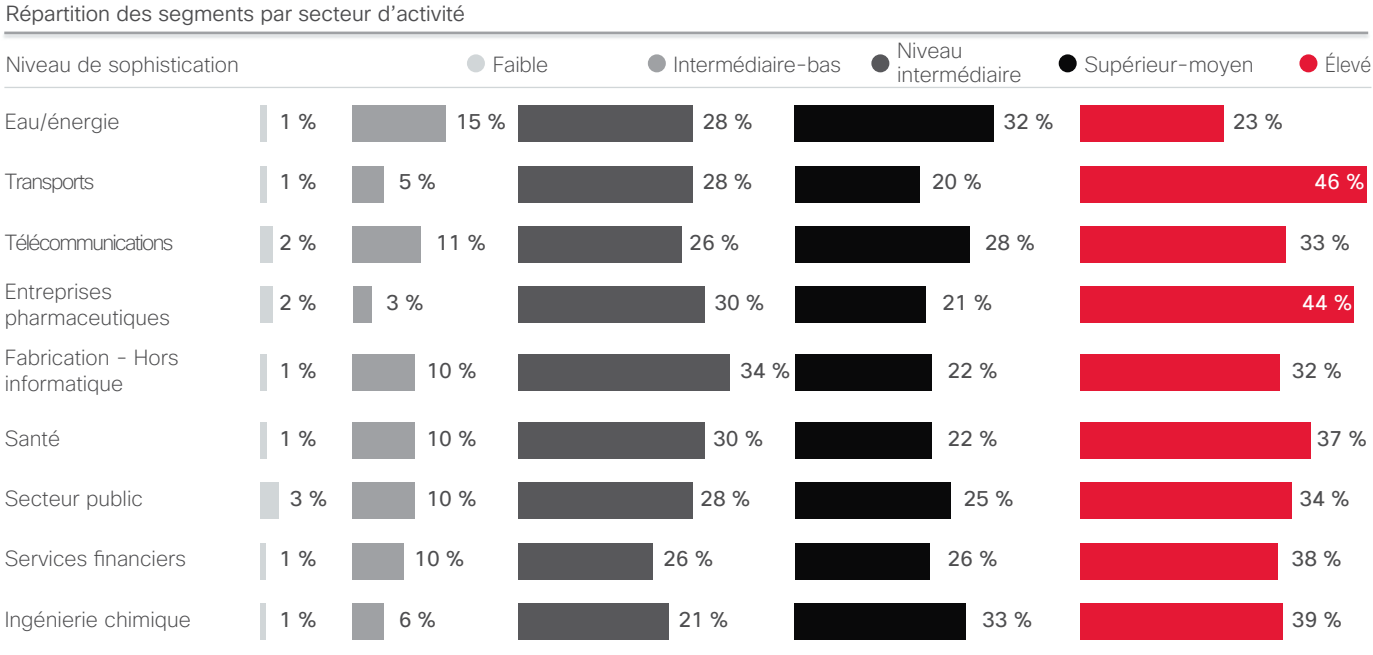
Le graphique ci-dessous illustre le placement dans les niveaux de maturité Cisco par secteur. En 2015, près de la moitié des entreprises sondées des secteurs des transports et pharmaceutique se situe dans le segment à forte maturité. Par rapport à 2014, les secteurs des télécommunications et des services de distribution d'eau et d'énergie sont moins susceptibles de figurer dans le segment à forte maturité en 2015. Les résultats sont basés sur la perception qu'ont les personnes interrogées de leurs processus de sécurité.

Figure 58 : Mesure de la maturité en matière de sécurité par infrastructure et par secteur



Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 59 : Niveaux de maturité par secteur

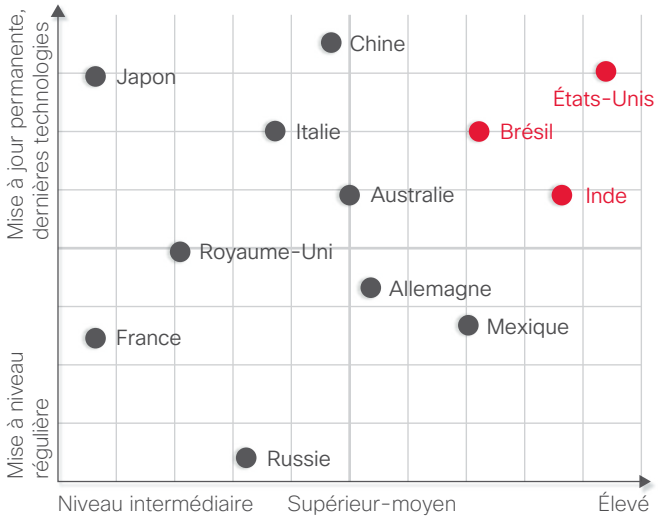


Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Le graphique de droite établit la correspondance entre la qualité de l'infrastructure de sécurité et les niveaux de maturité pour différents pays. Les pays en haut à droite présentent les plus hauts niveaux de maturité et de qualité d'infrastructure. Il est important de noter que ces résultats sont basés sur la perception qu'ont les professionnels de leur préparation en matière de sécurité.

Le graphique ci-après représente le placement dans les niveaux de maturité Cisco par pays. Les résultats sont basés sur la perception qu'ont les personnes interrogées de leurs processus de sécurité.

Figure 60 : Mesure de la maturité en matière de sécurité par infrastructure et par pays



Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 61 : Niveaux de maturité par pays

Répartition des segments par pays		**2014** (n=1637)			**2015** (n=2401)	
Niveau de sophistication	2014	Faible	Intermédiaire-bas	Intermédiaire	Supérieur-moyen	Élevé
États-Unis	3 % 2 %	10 % 4 %	27 % 22 %	16 % 27 %	44 % 45 %	
Brésil	2 % 1 %	5 % 9 %	24 % 24 %	35 % 26 %	34 % 40 %	
Allemagne	1 % 1 %	4 % 12 %	27 % 24 %	25 % 24 %	43 % 39 %	
Italie	1 % 4 %	23 % 3 %	13 % 36 %	25 % 23 %	38 % 34 %	
Royaume-Uni	8 % 0 %	8 % 14 %	25 % 32 %	18 % 22 %	41 % 32 %	
Australie	9 % 1 %	7 % 5 %	19 % 29 %	35 % 36 %	30 % 29 %	
Chine	0 % 0 %	3 % 6 %	32 % 37 %	29 % 25 %	36 % 32 %	
Inde	7 % 1 %	3 % 4 %	20 % 21 %	16 % 34 %	54 % 40 %	
Japon	7 % 2 %	15 % 16 %	14 % 34 %	40 % 16 %	32 % 32 %	
Mexique	6 %	8 %	20 %	16 %	50 %	
Russie	1 %	14 %	27 %	26 %	32 %	
France	1 %	15 %	35 %	20 %	29 %	

Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

RECOMMANDATIONS : FAIRE FACE À LA RÉALITÉ

Comme le montre notre enquête sur l'efficacité des mesures de sécurité, les professionnels de la sécurité doivent faire face à la réalité. Ils sont de moins en moins confiants dans leur préparation à bloquer les attaques. Toutefois, les prises de conscience issues d'exploits très médiatisés ont eu un effet positif sur le secteur, si l'on en juge par la légère hausse de la formation sur la sécurité et par le développement de politiques formelles. En outre, l'externalisation plus fréquente des audits et des services de résolution d'incidents indique que les défenseurs de la sécurité recherchent l'aide d'experts.

Les entreprises doivent continuer d'améliorer la connaissance qu'elles ont de leur état de préparation en matière de sécurité, et les professionnels de la sécurité doivent soutenir la croissance des dépenses budgétaires consacrées à la technologie et au personnel. Enfin, la confiance augmentera lorsque les professionnels de la sécurité déploieront des outils non seulement capables de détecter les menaces, mais aussi de maîtriser leur impact et d'améliorer la compréhension des moyens d'empêcher d'autres attaques.

Perspectives

Perspectives

Les experts géopolitiques de Cisco examinent l'évolution de l'environnement dans lequel s'inscrit la gouvernance de l'Internet, notamment les modifications apportées à la législation sur le transfert des données et les débats en cours sur l'utilisation du cryptage. Cette section présente également une sélection des résultats de deux études menées par Cisco. La première examine les préoccupations des dirigeants concernant la cybersécurité, quand la seconde met l'accent sur la perception des décideurs informatiques en matière de risque de sécurité et de fiabilité. Nous présentons également toute la valeur d'une architecture intégrée de protection contre les attaques et les dernières avancées de Cisco en matière de réduction du délai de détection.

Perspective géopolitique : l'incertitude de l'environnement associé à la gouvernance d'Internet

À l'ère post-Edward Snowden, l'environnement géopolitique dans lequel s'inscrit la gouvernance d'Internet s'est considérablement modifié. La libre circulation des informations entre pays n'est plus aussi évidente désormais. Les plaintes marquantes déposées par l'activiste autrichien Max Schrems, défenseur de la vie privée, contre le géant des réseaux sociaux Facebook ont probablement eu le plus gros impact, puisque la Cour de Justice de l'Union européenne (CJUE) a invalidé l'accord Safe Harbor des États-Unis dans son arrêt du 6 octobre 2015. [7]

Par conséquent, les entreprises se voient désormais contraintes de se fier à des mécanismes et des mesures de protection juridiques autres que le Safe Harbor lorsqu'elles transfèrent des données de l'Europe vers les États-Unis, ces mesures étant leur tour étroitement étudiées. Les entreprises de données tentent toujours d'évaluer les retombées de cette décision. Et tandis que les autorités de l'Union européenne et des États-Unis travaillent depuis deux ans à remplacer le Safe Harbor, le nouveau mécanisme prévu soulève bien des questions. Il pourrait même bien ne pas se concrétiser à la date butoir de janvier 2016, ou, plus vraisemblablement, ne pas permettre de restaurer la confiance des marchés s'il ne répond pas pleinement aux préoccupations soulevées par la CJUE, et être une fois de plus menacé d'invalidation. [8]

Car les experts en matière de protection des données s'attendent à ce que le Safe Harbor version 2.0 soit tout autant controversé que son prédécesseur. Il pourrait même suivre le même chemin, être attaqué en justice et déclaré non valide. [9]

Le chiffrement global, la façon dont il profite aux clients et aux entreprises, comme les défis qu'il génère pour l'application des lois lors des enquêtes sur l'activité criminelle et terroriste, est aussi un sujet qui risque de susciter cette année bien des débats entre les gouvernements et les industries. Dans le sillage des attaques terroristes de Paris, en novembre 2015, les décideurs insistent pour permettre aux officiers de police judiciaire d'accéder au contenu des communications cryptées.[10] Cela pourrait donner une impulsion supplémentaire au Safe Harbor 2.0, à l'heure où les questions de libertés civiles s'effacent face à la sécurité.

---

[7] « La décision de la Commission relative aux accords Safe Harbour est jugée invalide par la Cour de justice », CJUE, 6 octobre 2015 : **http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.**

[8] « Le cadre Safe Harbor 2.0 commence à chavirer à l'approche de la date butoir de janvier », par Glyn Moody, *Ars Technica*, 16 novembre 2015 : **http://arstechnica.com/tech-policy/2015/11/safe-harbour-2-0-framework-begins-to-capsize-as-january-deadline-nears/**.

[9] « Le cadre Safe Harbor 2.0 commence à chavirer à l'approche de la date butoir de janvier », par Glyn Moody, *Ars Technica*, 16 novembre 2015 : **http://arstechnica.com/tech-policy/2015/11/safe-harbour-2-0-framework-begins-to-capsize-as-january-deadline-nears/**.

[10] « Les attaques de Paris attisent les débats sur le cryptage », par Danny Yadron, Alistair Barr et Daisuke Wakabayashi, *The Wall Street Journal*, 19 novembre 2015 : **http://www.wsj.com/articles/paris-attacks-fan-encryption-debate-1447987407**.

Face à une telle incertitude, que doivent exiger les entreprises de leurs fournisseurs de données pour s'assurer que leur activité respecte les règlementations en matière de transfert de données ? Sur le court terme, il est clair qu'elles doivent rechercher des fournisseurs qui leur assurent, pour le transfert des données hors de l'UE, de respecter les clauses contractuelles types ou les règles d'entreprise contraignantes, et non pas le seul accord Safe Harbor.

Une autre question géopolitique majeure à laquelle doivent veiller les entreprises concerne les vulnérabilités et les exploits. Certains gouvernements se montrent particulièrement préoccupés par l'émergence d'un marché des vulnérabilités non corrigées, ou « armes logicielles ». De tels outils sont essentiels à la communauté en charge de la recherche sur la sécurité, en quête de moyens pour protéger les réseaux du monde entier. Mais cette technologie, conçue pour la bonne cause, pourrait tout aussi bien entre de mauvaises mains, en particulier dans les mains de régimes répressifs, être exploitée à des fins de crimes financiers, de vol de secrets nationaux ou commerciaux, de répression des dissidents politiques, ou de perturbation d'infrastructures critiques.

Et comment restreindre l'accès aux vulnérabilités non corrigées sans entraver le travail de ceux qui mènent des recherches vitales ? C'est là un problème auquel les gouvernements vont devoir s'attaquer sérieusement dans les mois et les années à venir. Et quand ils tenteront de résoudre cet épineux problème, les gouvernements devront clairement évaluer l'impact de leurs décisions politiques sur la sécurité. Ainsi, l'incertitude à propos des lois qui régissent la transmission d'informations sur les vulnérabilités non publiées pourrait mettre à mal les avancées en matière de recherche sur les menaces de sécurité, ou encourager la publication de vulnérabilités avant même que les fournisseurs aient eu l'occasion de les corriger. Sans compter que toute approche visant à résoudre ces incertitudes devra être compatible à l'échelle du globe.

Les problèmes de cybersécurité préoccupent les dirigeants

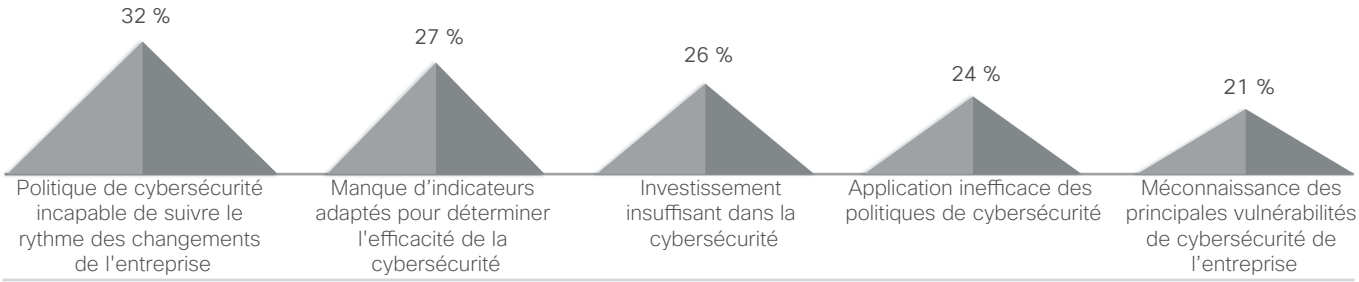
Il va de soi qu'une sécurité renforcée peut aider les entreprises à se protéger des violations et attaques désastreuses. Mais peut-elle contribuer à améliorer les chances de réussite d'une entreprise ? Selon une enquête réalisée par Cisco en octobre 2015 auprès des responsables des services financiers et commerciaux et portant sur le rôle de la cybersécurité dans la stratégie commerciale et du numérique, les dirigeant d'entreprise estiment que la protection de leurs activités contre les attaques peut dicter leur réussite ou leur échec. Dès que les entreprises renforcent leur part de numérique, leur croissance dépend de leur aptitude à protéger la plate-forme numérique.

Comme le révèle l'enquête, la cybersécurité est une préoccupation croissante des dirigeants : 48 % des personnes interrogées se disent très préoccupées par la violation de la cybersécurité, 39 % s'estimant modérément préoccupées. Et cette inquiétude grandit. 41 % indiquent que les violations de la sécurité les soucient beaucoup plus qu'il y a 3 ans, et 42 % affirment être un peu plus préoccupés que par le passé.

Les chefs d'entreprise s'attendent aussi à ce que les investisseurs et les organismes de contrôle leur posent des questions plus pointues sur les processus de sécurité, mais aussi sur d'autres fonctions opérationnelles. 92 % des personnes interrogées estiment que les organismes de contrôle et les investisseurs exigeront à l'avenir des entreprises davantage d'informations sur l'exposition au risque de cybersécurité.

Les entreprises semblent aussi avoir un sens aigu des défis associés à la cybersécurité. Le défi le plus couramment cité est l'incapacité des politiques de cybersécurité à suivre l'évolution de l'activité. Vient ensuite le manque d'indicateurs pour mesurer l'efficacité de la sécurité (Figure 62).

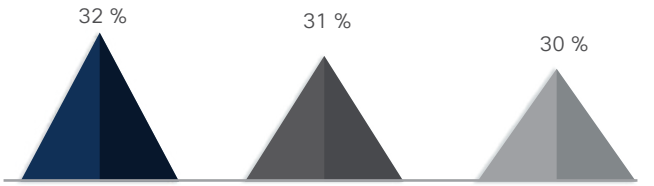
Figure 62 : Les entreprises confrontées à de vrais défis de cybersécurité



Source : Cisco Security Research

Environ un tiers des responsables s'inquiètent de leur capacité à protéger leurs données critiques. Quand on les interroge sur le type d'informations le plus difficile à protéger, ils répondent à 32 % les « informations financières confidentielles ». Ils nomment ensuite les « informations sur les clients » et les « informations commerciales confidentielles » (voir Figure 63).

Figure 63 : Les dirigeants préoccupés par la sécurisation des données sensibles



Source : Cisco Security Research

Enquête sur la fiabilité : expliquer les risques et les défis pour les entreprises

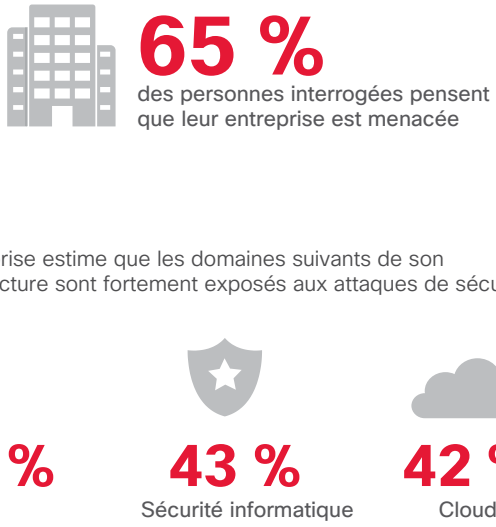
La multiplication des attaques nuisant à la sécurité des informations souligne la forte nécessité pour les entreprises de vouloir disposer de systèmes, données, partenaires commerciaux, clients et citoyens qui soient sûrs. La confiance en effet devient un facteur majeur de sélection d'une infrastructure IT et de réseau. En fait, nombreux sont ceux qui exigent désormais que sécurité et fiabilité soient intégrés sur tout le cycle de vie produit des solutions qui composent leur infrastructure.

En octobre 2015, Cisco a mené une enquête pour évaluer la perception qu'ont les décideurs informatiques des risques et défis associés à la sécurité, et déterminer le rôle joué par la fiabilité des fournisseurs IT dans les investissements IT de l'entreprise. Nous avons pour cela sondé, au sein d'entreprises de plusieurs pays, des décideurs chargés de la sécurité des informations et des décideurs n'ayant pas cette responsabilité. (Reportez-vous à **l'Annexe** pour plus de détails sur l'enquête portant sur le risque de sécurité et la fiabilité, notamment sa méthodologie.)

VOICI UNE SÉLECTION DES RÉSULTATS DE NOTRE ENQUÊTE :

65 % des personnes interrogées estiment que leur entreprise est confrontée à un risque de sécurité de niveau élevé, à savoir associé à l'utilisation de la mobilité, à la sécurité IT et aux solutions cloud dans l'entreprise (Figure 64).

Figure 64 : La perception du risque de sécurité



Source : Enquête Cisco sur les risques et la fiabilité de la sécurité

PARTAGER

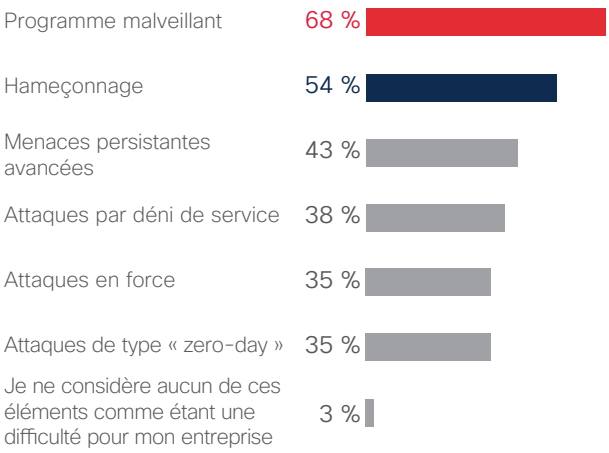
68 % des participants à notre enquête indiquent que les programmes malveillants sont le plus grand défi de sécurité externe auquel est confrontée leur entreprise. L'hameçonnage et les attaques complexes persistantes viennent compléter ce top trois, avec respectivement 54 % et 43 % des personnes interrogées (voir Figure 65).

Concernant les défis de sécurité interne (voir Figure 66), plus de la moitié (54 %) des personnes interrogées citent le téléchargement de logiciels malveillants comme représentant la principale menace, suivie des attaques internes par les employés (47 %), et des vulnérabilités logicielles et matérielles (46 %).

Nous avons également relevé que la plupart des entreprises (92 %) disposent en interne d'une équipe dédiée à la sécurité. 88 % des personnes affirment disposer d'une stratégie de sécurité formelle, à l'échelle de l'entreprise, qui est renouvelée régulièrement. Cependant, seuls 59 % des sondés disposent de politiques et procédures normalisées pour valider la fiabilité des fournisseurs IT (voir Figure 67).

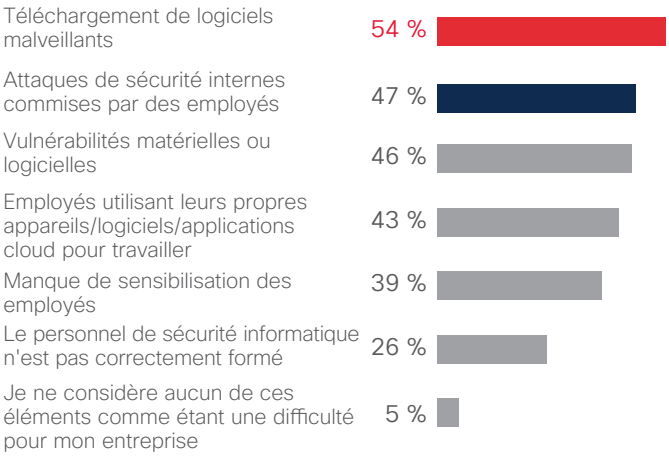
De plus, près de la moitié (49 %) des grandes entreprises tiennent à jour leur infrastructure de sécurité en utilisant les dernières technologies disponibles, et la plupart des autres mettent régulièrement à niveau leur infrastructure. D'après notre enquête, très peu attendent l'obsolescence de leur technologie pour procéder à une mise à niveau.

Figure 65 : Les défis de la sécurité externe (total des personnes interrogées)



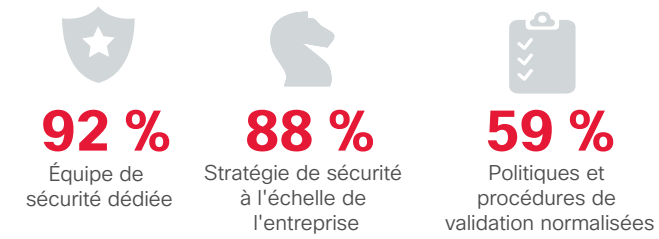
Source : Enquête Cisco sur les risques et la fiabilité de la sécurité

Figure 66 : Les défis de la sécurité interne (total des personnes interrogées)



Source : Enquête Cisco sur les risques et la fiabilité de la sécurité

Figure 67 : La plupart des grandes entreprises disposent d'une équipe de sécurité dédiée en interne



Source : enquête Cisco sur les risques et la fiabilité de la sécurité

Comment les fournisseurs peuvent prouver leur fiabilité

Dans l'environnement actuel axé sur les menaces, la confiance dans les processus, les politiques et les technologies des fournisseurs, mais aussi dans les personnes elles-mêmes, et la possibilité de vérifier leur fiabilité, est essentielle pour créer une relation de confiance durable entre fournisseurs et entreprises.

Les fournisseurs de technologie disposent des moyens suivants pour attester de leur fiabilité :

- Créer de la sécurité dans leurs solutions et la chaîne de valeur, et ce dès le début
- Mettre en place et respecter des politiques et processus de réduction du risque
- Créer une culture de sensibilisation à la sécurité
- Répondre aux attaques de façon transparente et rapide
- Garantir une élimination rapide et assurer une vigilance constante suite à un incident

Il va de soi que la mise à niveau d'une infrastructure constitue une bonne pratique. Les entreprises de toutes tailles se doivent de déployer une infrastructure sécurisée et fiable, dans laquelle la sécurité est envisagée à tous les niveaux du réseau. Cependant, ils peuvent aussi contribuer à réduire l'exposition aux attaques en favorisant une culture ouverte mais sensible à la sécurité.

Créer cette culture exige que les entreprises mettent en œuvre des politiques et des processus cohérents à l'échelle de l'entreprise, qui garantissent que la sécurité est intégrée dans chaque aspect de l'activité. Ils doivent ensuite s'attacher à étendre cet état d'esprit centré sur la sécurité à leur écosystème de partenaires et fournisseurs, et travailler en permanence à prouver leur transparence et leur responsabilité envers leurs clients, partenaires et autres parties prenantes.

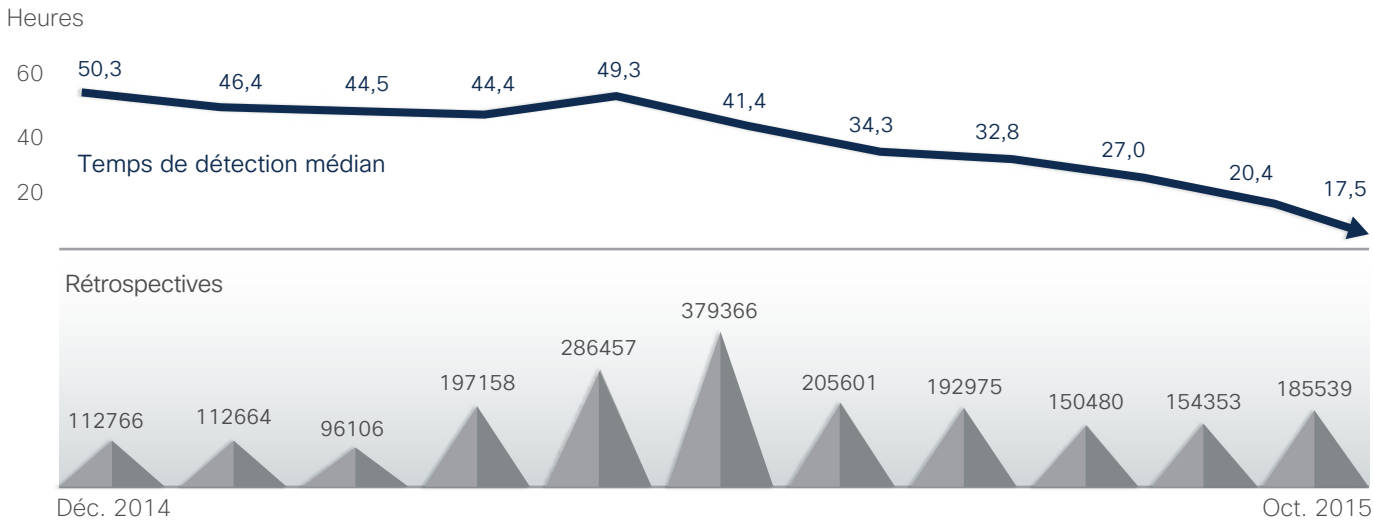
Le délai de détection : le réduire à tout prix

Le terme « Délai de détection » désigne le laps de temps entre la première observation d'un fichier inconnu et la détection d'une attaque. 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.

La catégorie « rétrospectives » de la figure 68 indique le nombre de fichiers que Cisco a initialement classés comme « inconnus » et qui ont été plus tard convertis en « dangereux connus ».

Comme le montre le Rapport Cisco sur la cybersécurité - 1er semestre 2015, le délai de détection médian était alors d'environ 2 jours (50 heures).

Figure 68 : Délai de détection, décembre 2014 - octobre 2015



Source : Cisco Security Research

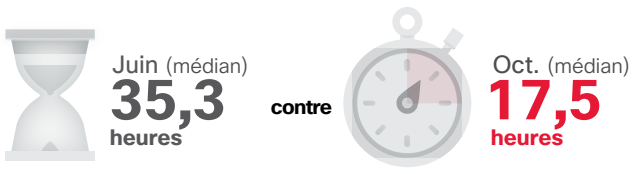
De janvier à mars, le délai de détection médian est resté plus ou moins le même, entre 44 et 46 heures, mais avec une légère tendance à la baisse. En avril, il a légèrement augmenté pour atteindre 49 heures. Cependant, fin mai, le délai de détection pour Cisco est redescendu à environ 41 heures.

Depuis cette date, le délai de détection médian décline rapidement. En octobre, Cisco avait réduit le délai de détection médian à environ 17 heures, soit moins d'une journée. Ce chiffre dépasse largement l'estimation actuelle faite par l'industrie du délai de détection (100 à 200 jours). Cette rapidité découle de l'inclusion de davantage de détails sur la façon dont les infections de courte durée sont atténuées.

L'industrialisation du piratage et la multiplication des malveillants courants ont largement contribué à réduire le délai de détection. Dès qu'une attaque s'industrialise en effet, elle se propage davantage et devient donc plus simple à détecter.

Cependant, nous sous-entendons également que la combinaison de mécanismes de défense contre les attaques complexes et de l'étroite collaboration entre chercheurs compétents en charge de la sécurité est probablement pour nous encore plus essentielle pour réduire de façon cohérente et significative le délai de détection médian en 2015.

Figure 69 : Comparaison des délais de détection, de décembre 2014 à octobre 2015



Source : Cisco Security Research

La comparaison des délais de détection donnée en Figure 69 montre que de nombreuses attaques ayant eu lieu en juin ont été bloquées en 35,3 heures environ. En septembre, le nombre d'attaques bloquées en quelques 17,5 heures était plus élevé. Une fois encore, cette réduction du délai de détection médian est imputable à une identification plus rapide des malveillants courants, tels que Cryptowall 3.0, Upatre et Dyre. L'intégration de nouvelles technologies, telles que celles de ThreatGRID, une société Cisco, est un autre facteur.

Cependant, malgré cette réduction du délai de détection, certaines attaques restent plus dures à détecter que d'autres. D'une façon générale, les programmes de téléchargement qui ciblent les utilisateurs de Microsoft Word sont les plus simples à détecter (< 20 heures). Les injections par logiciel publicitaire et navigateur comptent parmi les menaces les plus difficiles à détecter (< 200 heures).

Si cette détection est si délicate, c'est que ce type de menaces est souvent classé en priorité inférieure par les équipes chargées de la sécurité, et donc souvent ignoré dans la course pour déjouer les attaques de type « zero-day » (voir « Infections touchant les navigateurs : très répandues et source majeure de fuite de données », en **page 16**).

La Figure 70 présente les types de menaces généralement découvertes dans les 100 jours.

Figure 70 : Balises sur le cloud pendant 100 jours

Source : Cisco Security Research

PARTAGER

Les six principes de protection intégrée contre les attaques

Dans le Rapport Cisco sur la cybersécurité du 1er semestre 2015, les experts en sécurité Cisco affirment que la nécessité de solutions adaptatives intégrées générera dans les cinq prochaines années des modifications essentielles de l'industrie de la sécurité. On assistera au final à une restructuration de l'industrie et à un mouvement unifié vers une architecture de protection intégrée et évolutive contre les attaques. Une telle architecture offrira visibilité, contrôle, informations et contexte au sein de solutions diverses.

Ce cadre de « détection et réaction » permettra une réaction plus rapide tant aux attaques connues qu'émergentes. Au cœur de cette nouvelle architecture, une plate-forme de visibilité qui propose une totale prise en compte du contexte et est constamment mise à jour pour évaluer les attaques, corréler les informations locales et mondiales et optimiser les mécanismes de défense. Cette plate-forme a pour objectif de fournir une base sur laquelle tous les fournisseurs peuvent agir et à laquelle ils peuvent tous contribuer. La visibilité s'assortit d'un meilleur contrôle, ce qui se traduit par une meilleure protection sur davantage de vecteurs et la possibilité de contrer plus d'attaques.

Nous présentons par la suite six principes de protection intégrée visant à aider les entreprises et leurs fournisseurs de produits de sécurité, pour mieux comprendre les intentions et les atouts potentiels de cette architecture :

1. **Une architecture de réseau et de sécurité plus riche est indispensable pour gérer le volume et la complexité des attaques, en hausse constante.**

   Au cours des 25 années écoulées, le modèle de sécurité classique était « Si tu vois un problème, achète un kit. » Ces solutions pourtant, souvent composées de technologies issues de différents fournisseurs de sécurité, ne peuvent sérieusement communiquer entre elles. Elles génèrent des informations et renseignent sur les événements de sécurité, qui sont intégrés dans une plate-forme d'événements puis analysés par le personnel de sécurité.

   Une architecture intégrée de protection est un cadre de détection et de réaction qui offre davantage de possibilités et permet de répondre plus rapidement aux menaces en recueillant davantage d'informations depuis cette structure déployée, et ce de façon automatique et performante. Ce système permet donc d'observer plus intelligemment l'environnement de sécurité. Il ne se contente pas d'alerter les équipes de sécurité sur des événements suspects et des violations de politiques, mais donne une image précise du réseau et de ce qui s'y passe. Ces informations supplémentaires permettent de prendre de meilleures décisions en matière de sécurité.

2. **Mais la meilleure technologie ne peut à elle seule gérer les attaques actuelles ou à venir. Elle ne fait qu'ajouter de la complexité à cet environnement en réseau.**

   Les entreprises investissent en effet dans les meilleures technologies de leur secteur. Mais comment savoir si ces solutions fonctionnent réellement ? Le grand nombre de manchettes de journaux portant ces dernières années sur des attaques est bien la preuve que nombre de technologies ne sont pas assez performantes. Et lorsqu'elles échouent, elles échouent réellement.

   La multiplication des fournisseurs de sécurité proposant les meilleures solutions ne risque pas d'améliorer cet environnement de sécurité, sauf si ces fournisseurs proposent des solutions radicalement différentes de celles de leurs concurrents, et non de pâles copies légèrement modifiées. Car aujourd'hui, dans la plupart des domaines de la sécurité, il est bien difficile de trouver de réelles différences entre les nombreuses offres des grands fournisseurs.

3. **Un trafic plus crypté exigera une protection intégrée, capable de converger sur une activité malveillance cryptée, face à laquelle les produits isolés s'avèrent inefficaces.**

   Comme nous l'avons déjà relevé dans ce rapport, le trafic Web crypté se développe. Il existe naturellement de bonnes raisons pour opter pour le cryptage. Mais pour les équipes en charge de la sécurité, le cryptage est synonyme de difficultés supplémentaires pour suivre les attaques.

   Le « problème » du cryptage peut être résolu par une meilleure visibilité de ce qui se passe sur les appareils et les réseaux. C'est là que peuvent intervenir les plateformes de sécurité intégrées.

4. **Les API ouvertes sont une composante essentielle d'une architecture de protection intégrée.**

   Dans des environnements multifournisseurs, une plate-forme commune est indispensable pour améliorer la visibilité, le contexte et le contrôle. L'élaboration d'une plate-forme d'intégration frontale peut soutenir une meilleure automatisation et permettre de mieux comprendre les produits de sécurité à proprement parler.

5. **Une architecture de protection intégrée réduit le nombre des équipements et des logiciels à installer et gérer.**

   Les fournisseurs de sécurité devraient donc s'efforcer de proposer des plates-formes comptant autant de fonctionnalités étendues que possible sur une plate-forme unique. Ces produits permettront de réduire la complexité et la fragmentation de l'environnement de sécurité, cette dernière représentant pour les hackers autant d'opportunités d'accès simple et de dissimulation.

6. **Dans un système de défense intégrée, l'automatisation et la coordination contribuent à réduire le délai de détection et favorisent maîtrise et élimination.**

   La réduction des faux positifs permet aux équipes de sécurité de se concentrer sur l'essentiel. La contextualisation appuie une analyse des événements de première ligne en cours, aide les équipes à évaluer si ces événements nécessitent une attention immédiate, et peut enfin générer des réponses automatiques et des analyses plus approfondies.

La performance en chiffres : la valeur de la collaboration industrielle

La collaboration industrielle est essentielle non seulement pour développer une future architecture de protection autorisant des réactions plus rapides face aux menaces, mais aussi dès aujourd'hui pour tenir la cadence d'une communauté mondiale d'effrontés auteurs malveillants, novateurs et obstinés, qui ne cesse de s'étoffer. Les hackers en effet sont passés maîtres dans l'art de déployer des campagnes très rentables et difficiles à détecter. Nombreux sont ceux qui utilisent désormais des actifs légitimes au sein de l'infrastructure pour soutenir leurs campagnes... Et ce avec un franc succès.

Dans cet environnement, rien d'étonnant à ce que les spécialistes de la sécurité interrogés dans notre Enquête 2015 sur l'efficacité des mesures de sécurité de Cisco aient moins confiance dans leurs aptitudes à contribuer à la sécurité de leur entreprise. Nous leur suggérons d'examiner le puissant impact que peut avoir une collaboration industrielle dynamique continue pour mettre au jour l'activité cybercriminelle, casser la capacité qu'ont les hackers à générer des revenus et réduire l'opportunité de futures attaques.

Comme nous l'avons abordé plus en détail précédemment (voir « Témoignages », en **page 10**), la collaboration entre un contributeur partenaire de Cisco et notre écosystème Cisco CSI, mais aussi la coopération avec les fournisseurs de services, ont largement contribué à offrir à Cisco la capacité de découvrir, vérifier, et écarter les opérations mondiales impliquant le kit d'exploit Angler, et d'affaiblir l'un des botnets DDoS les plus grands jamais observés par nos chercheurs, à savoir SSHPsychos.

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 collecte d'informations sur les menaces, regroupent l'ensemble des informations sur les risques issues des données télémétriques émanant des nombreux appareils et capteurs, des flux publics et privés, et de la communauté open source Cisco. 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, Internet, data centers, terminaux, appareils mobiles, systèmes virtuels, e-mails et cloud. L'analyse de ces données nous permet de renforcer en temps réel la sécurité des produits et des services que nos clients utilisent dans le monde entier.

Pour en savoir plus sur notre approche de la sécurité axée sur les attaques, consultez la page **www.cisco.com/go/security**.

Contributeurs du rapport annuel Cisco 2016 sur la sécurité.

GROUPE DE SÉCURITÉ ADAPTATIVE ET DE RECHERCHE TALOS

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

ÉQUIPE DE TRANSFORMATION ET D'OPTIMISATION DES SERVICES AVANCÉS CLOUD ET IT

Cette équipe propose des recommandations et optimise les réseaux, les data centers et les solutions cloud pour les plus grands fournisseurs de services et entreprises du monde entier. Cette offre de conseil est axée sur l'optimisation de la disponibilité, de la performance et de la sécurité des solutions critiques des clients. Le service d'optimisation est fourni à plus de 75 % des entreprises figurant au classement du Fortune 500.

ÉQUIPE ACTIVE THREAT ANALYTICS

L'équipe d'analyse des attaques actives (Active Threat Analytics, ATA) de Cisco aide les entreprises à se défendre contre les intrusions connues, les attaques jour zéro et les attaques persistantes avancées en tirant parti de technologies avancées de big data. Ce service entièrement géré est fourni par nos experts en sécurité et notre réseau mondial de centres d'opérations de sécurité. Il offre une surveillance constante et des analyses à la demande, 24 heures sur 24, sept jours sur sept.

DÉPARTEMENT CISCO THOUGHT LEADERSHIP

Le département Cisco de leadership éclairé (Thought Leadership) met en avant les opportunités mondiales, les transitions du marché et les solutions clés transformant les entreprises, les industries et les expériences. Il propose une vision perspicace et intuitive de ce que les entreprises sont en droit d'attendre dans un monde en perpétuelle évolution, et explique comment elles peuvent lutter au mieux. Le leadership éclairé consiste essentiellement à aider les entreprises à passer au numérique en faisant le lien entre environnements physiques et virtuels de façon sûre et transparente, afin d'accélérer l'innovation et d'atteindre les objectifs commerciaux souhaités.

COGNITIVE THREAT ANALYTICS

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

GLOBAL GOVERNMENT AFFAIRS

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

ÉQUIPE INTELLISHIELD

L'équipe du service IntelliShield effectue des recherches sur les attaques et la vulnérabilité, l'analyse, l'intégration et la corrélation des données et informations émanant des opérations et de la recherche sur la sécurité Cisco ainsi que de sources externes pour générer le service IntelliShield Security Intelligence, qui supporte plusieurs produits et services Cisco.

LANCOPE

Lancope, une société Cisco, est un des principaux fournisseurs de solutions de visibilité sur le réseau et d'informations de veille visant à protéger les entreprises contre les principales attaques actuelles. Par une analyse de NetFlow, IPFIX, et d'autres types de données de télémétrie réseau, le système Lancope StealthWatch® fournit des analyses de sécurité contextuelles permettant de détecter rapidement un large éventail d'attaques, qui vont des menaces persistantes avancées et des DDoS aux attaques de type « zero-day » et aux menaces internes. En combinant une surveillance continue sur l'ensemble des réseaux d'entreprise et des informations sur les utilisateurs, les appareils et les applications, Lancope accélèrent la résolution des incidents, améliorent les analyses et réduisent le risque pour l'entreprise.

OPENDNS

OpenDNS, une société Cisco, est la plus grande plate-forme de sécurité cloud au monde. Elle dessert au quotidien plus de 65 millions d'utilisateurs de plus de 160 pays. Le laboratoire OpenDNS est l'équipe de recherche sur la sécurité chargée de gérer la plate-forme de sécurité. Pour plus d'informations, consultez les pages **www.opendns.com** ou **https://labs.opendns.com**.

DÉPARTEMENT SECURITY AND TRUST

Le département Security and Trust de Cisco souligne l'implication de Cisco pour répondre à deux des enjeux les plus critiques, et qui constituent une priorité pour les dirigeants et leaders du monde entier. Le département a pour principales tâches la protection des clients publics et privés de Cisco, l'établissement d'un cycle de développement sécurisé et de systèmes fiables sur toute la gamme de produits et services Cisco, ainsi que la protection de l'entreprise Cisco contre les cyberattaques, 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 une excellence opérationnelle dans tous les domaines : InfoSec, fiabilité de l'ingénierie, protection et la confidentialité des données, sécurité du cloud, transparence et validation, recherche sur la sécurité avancée et gouvernement. Pour plus d'informations, consultez la page **http://trust.cisco.com.**

SECURITY RESEARCH AND OPERATIONS (SR&O)

Le département Security Research & Operations (SR&O) est responsable de la gestion des attaques et des vulnérabilités pour tous les produits et services Cisco, y compris pour l'équipe PSIRT, leader du secteur, en charge des incidents liés à la sécurité des produits. Le département SR&O aide les clients à comprendre ces attaques 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 de l'industrie. Le département SR&O innove également pour proposer de nouveaux services, par exemple le service Cisco d'informations de veille personnalisées (Custom Threat Intelligence), qui permet d'identifier des indicateurs de compromission non encore détectés ou atténués par les infrastructures de sécurité existantes.

Contributeur partenaire Cisco

LE LABORATOIRE DE RECHERCHE SUR LES MENACES LEVEL 3

Level 3 Communications compte parmi les principaux fournisseurs mondiaux de communications. La société a son siège à Broomfield, Colorado, et propose des services de communication aux entreprises, au gouvernement et aux opérateurs. Soutenue par des réseaux fibre étendus sur trois continents, connectés par des installations sous-marines, notre plate-forme mondiale de services intègre des ressources avancées permettant de couvrir plus de 500 marchés dans plus de 60 pays. Le réseau de Level 3 offre une vue exhaustive de l'environnement mondial des menaces.

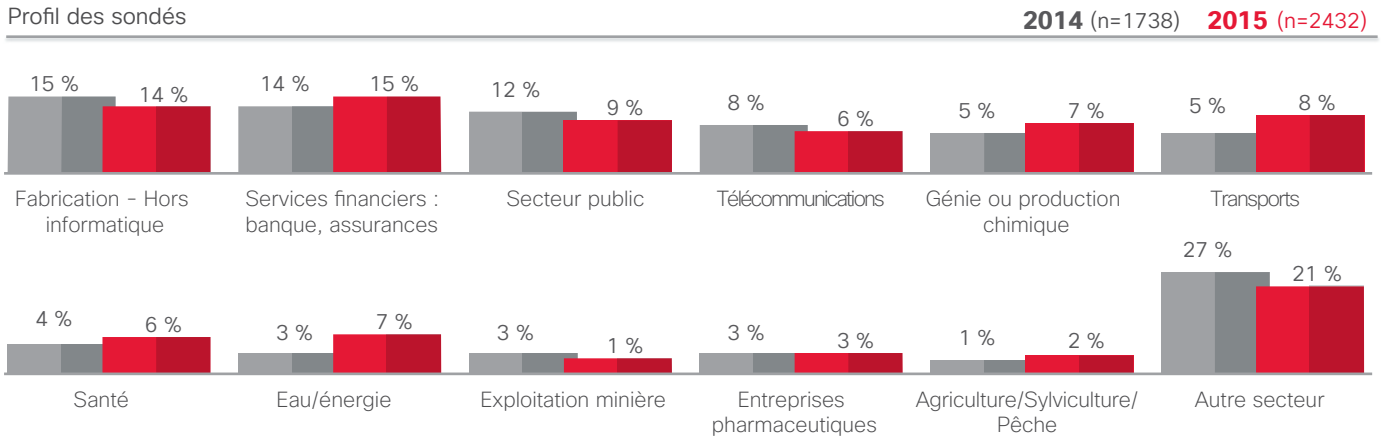
Le laboratoire de recherche sur les menaces de Level 3 est le groupe de sécurité qui analyse dynamiquement les menaces mondiales et recoupe ses informations issues de sources internes et externes pour aider à protéger les clients Level 3, leur réseau et l'Internet public. Le groupe tisse régulièrement des partenariats avec les leaders de l'industrie, tels que Cisco Talos, pour favoriser la recherche et atténuer les attaques.

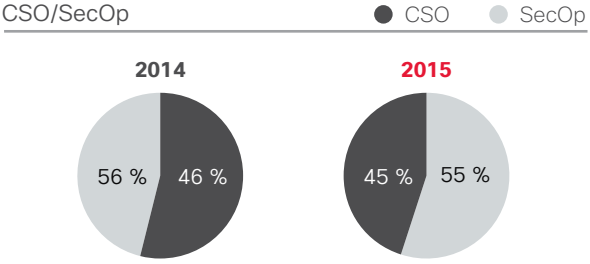
Annexe

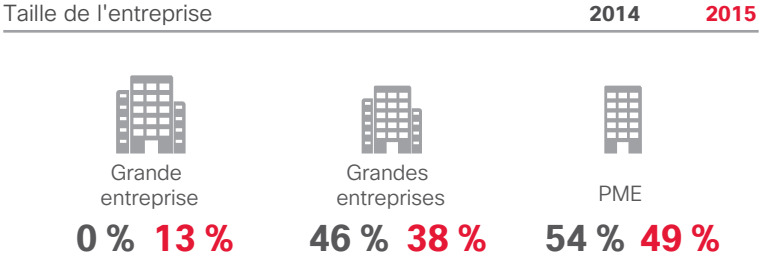
Annexe

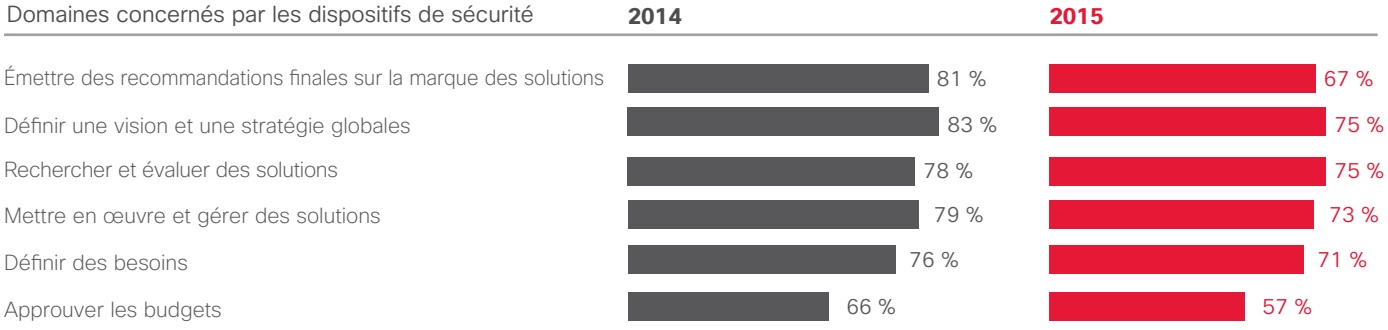
Enquête 2015 sur l'efficacité des mesures de sécurité de Cisco : profil des personnes interrogées et ressources

Figure 71 : Profil des personnes interrogées





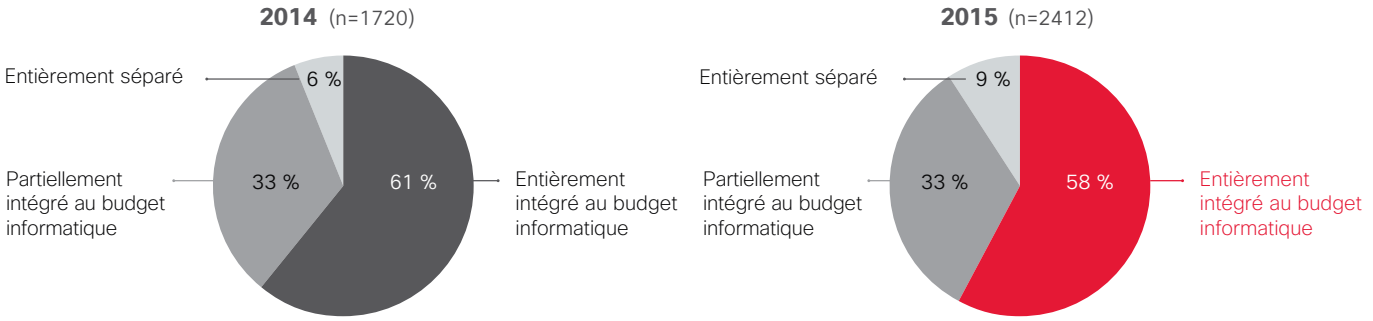




Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 72 : Si seuls 9 % disposent d'un budget sécurité séparé du budget IT, ce chiffre a considérablement augmenté depuis 2014

Le budget dédié à la sécurité est-il intégré au budget informatique ? (Membres du service informatique)

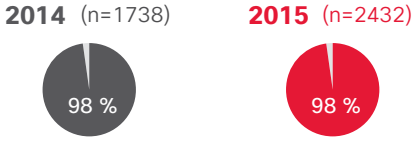


Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

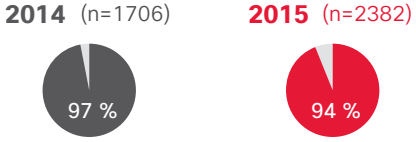
Figure 73 : Fonctions : les personnes interrogées et leur responsable

Membres du service informatique

Service ou équipe dédiés à la sécurité



Membres d'une équipe de sécurité



Fonction		Intitulé de poste du responsable	
Responsable de la sécurité	22 %	Directeur général	34 %
Responsable technologique	18 %	Président/Propriétaire	18 %
Directeur ou responsable de service IT	16 %	Responsable de la sécurité	6 %
Directeur informatique	13 %	Directeur informatique	6 %
Directeur des opérations de sécurité	7 %	Responsable technologique	6 %
Vice-président de la sécurité informatique	5 %	Directeur ou responsable informatique	4 %
Directeur de la conformité et de la gestion des risques	4 %	Vice-président de la sécurité informatique	4 %
Responsable des opérations de sécurité	4 %	Vice-président informatique	2 %
Architecte sécurité	4 %	Conseil de direction	2 %
Vice-président informatique	3 %	Directeur opérationnel	1 %
Directeur opérationnel	3 %	Directeur financier	1 %
Autre intitulé	2 %	Autre intitulé	0 %

Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 74 : Le pare-feu est le principal outil de protection contre les menaces de sécurité ; par rapport à 2014, moins de mécanismes de protection contre les menaces de sécurité sont gérés par des services cloud en 2015

Mesures de protection utilisées par les entreprises	**2014** (n=1738)	**2015** (n=2432)	Mesures de protection gérées par des services orientés cloud (professionnels sondés qui utilisent des mesures de protection contre les menaces de sécurité) **2014** (n=1646)	**2015** (n=2268)
Pare-feu*	S/O	65 %		31 %
Prévention des pertes de données	55 %	56 %		
Authentification	52 %	53 %		
Chiffrement/confidentialité/protection des données	53 %	53 %		
Sécurité de la messagerie	56 %	52 %	37 %	34 %
Sécurité web	59 %	51 %	37 %	31 %
Protection des terminaux/Logiciels contre les programmes malveillants	49 %	49 %	25 %	25 %
Autorisation/contrôle d'accès	53 %	48 %		
Administration des identités/Provisionnement des utilisateurs	45 %	45 %		
Prévention des intrusions*	S/O	44 %		20 %
Sécurité de la mobilité	51 %	44 %	28 %	24 %
Réseau sans fil sécurisé	50 %	41 %	26 %	19 %
Analyse des vulnérabilités	48 %	41 %	25 %	21 %
VPN	48 %	40 %	26 %	21 %
Informations sur la sécurité et gestion des événements	43 %	38 %		
Protection contre les attaques par déni de service (DDoS)	36 %	37 %		
Tests de pénétration	38 %	34 %	20 %	17 %
Application de correctifs et configuration	39 %	32 %		
Analyse des réseaux	42 %	31 %		
Analyse des terminaux	31 %	26 %		
Sécurité réseau, pare-feu et prévention des intrusions*	60 %	S/O	35 %	
Aucune de ces propositions	1 %	1 %	13 %	11 %

*Les pare-feu et la prévention des intrusions avaient pour mot d'ordre en 2014 « Sécurité réseau, pare-feu et prévention des intrusions. »

Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

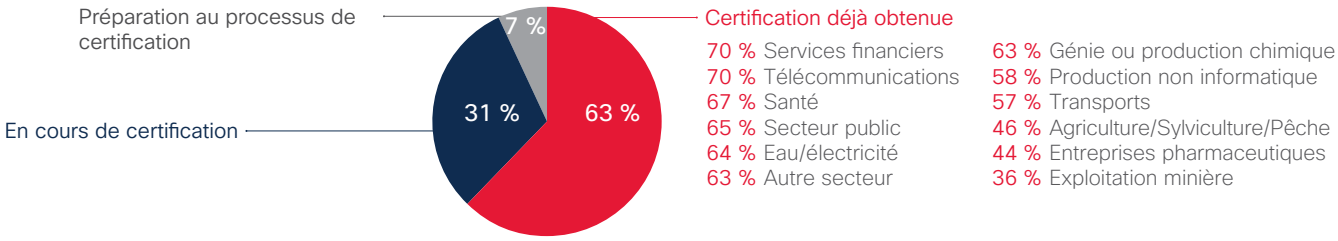
Externalisation

Figure 75 : Le conseil reste le principal service de sécurité externalisé

Augmentation significative constatée de l'externalisation de l'audit et de la réponse aux incidents. L'externalisation est considérée comme étant plus rentable.

La moitié (52 %) suit une pratique de sécurité normalisée de type ISO 27001 (identique à l'année dernière). Parmi ces entreprises, la grande majorité est déjà certifiée ou en voie de certification.

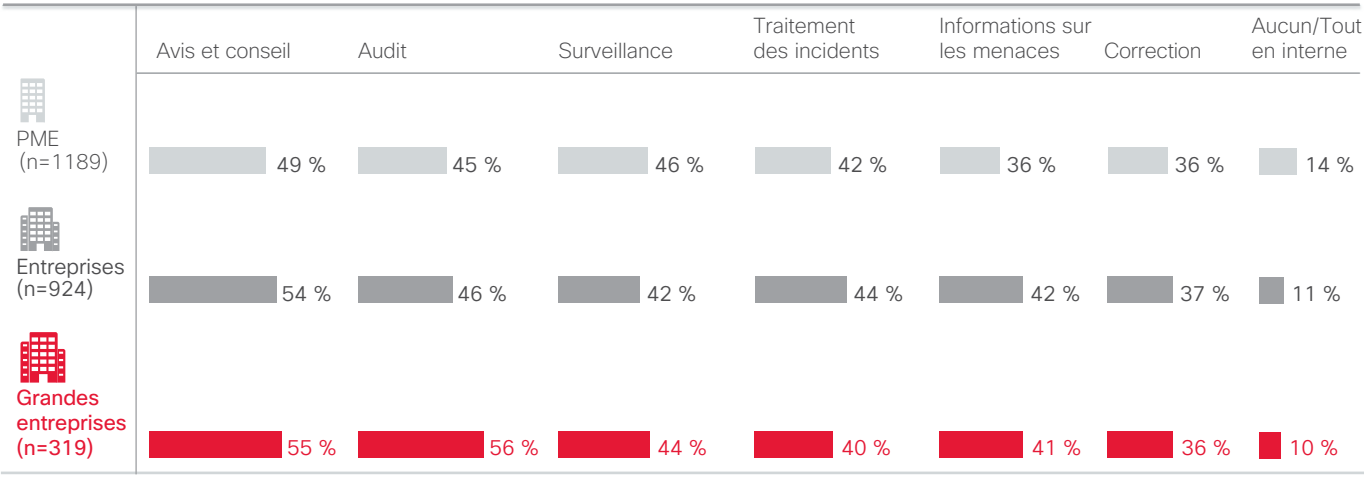
Pratique de sécurité normalisée
L'entreprise suit une pratique de sécurité de l'information normalisée (**2015** : n=1265)



Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 76 : L'externalisation selon les sociétés : les grandes entreprises sont plus susceptibles d'externaliser les audits et le conseil

Quels services de sécurité sont externalisés ?



Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

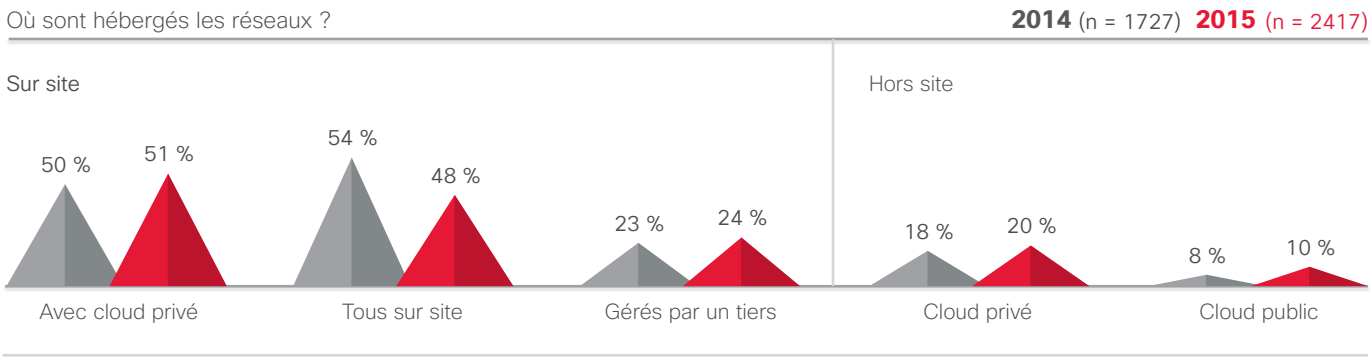
Figure 77 : L'externalisation selon les pays : le Japon est beaucoup plus susceptible d'externaliser le conseil

Quels services de sécurité sont externalisés ?

	TOTAL	États-Unis	Brésil	Allemagne	Italie	Royaume-Uni	Australie	Chine	Inde	Japon	Mexique	Russie	France
Avis et conseil	52 %	52 %	51 %	19 %	51 %	44 %	54 %	52 %	54 %	64 %	58 %	41 %	55 %
Audit	47 %	50 %	55 %	38 %	48 %	50 %	36 %	33 %	51 %	41 %	63 %	40 %	59 %
Surveillance	44 %	48 %	49 %	32 %	39 %	41 %	52 %	31 %	51 %	51 %	49 %	37 %	50 %
Traitement des incidents	42 %	46 %	39 %	32 %	38 %	43 %	53 %	34 %	49 %	53 %	45 %	27 %	54 %
Informations sur les menaces	39 %	42 %	40 %	37 %	46 %	36 %	16 %	36 %	48 %	47 %	44 %	42 %	39 %
Correction	36 %	34 %	32 %	38 %	34 %	31 %	47 %	37 %	41 %	40 %	21 %	41 %	41 %
Aucun/Tout en interne	12 %	18 %	9 %	18 %	13 %	19 %	4 %	19 %	12 %	10 %	3 %	16 %	4 %

Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 78 : L'hébergement sur site des réseaux reste l'hébergement le plus courant. L'hébergement hors site a cependant augmenté depuis l'an dernier



Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Atteintes à la sécurité publique

Figure 79 : Le nombre d'entreprises rapportant en 2015 avoir dû faire face à la méfiance du public après la découverte d'une faille a baissé

Les attaques incitent fortement à améliorer la sécurité :

Par rapport à **2014**, le nombre d'entreprises rapportant en **2015** avoir dû faire face à la méfiance du public après la découverte d'une faille a baissé

2014 **53 %** VS 2015 **48 %**

Les attaques vous incitent-elles vraiment à améliorer vos politiques, procédures ou technologies de protection ? (n = 1134)

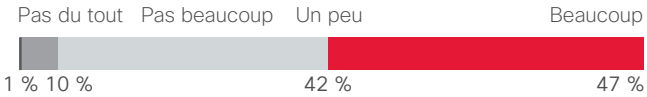
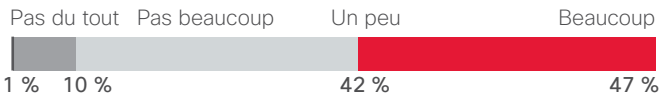


Figure 80 : Les attaques publiques peuvent améliorer la sécurité

Les attaques incitent fortement à améliorer la sécurité :
Personnes interrogées en charge de la sécurité
2014 (n = 1701) **2015** (n = 1347)

2014 **53 %** **Oui** VS 2015 **48 %** **Oui**

Les attaques vous incitent-elles vraiment à améliorer vos politiques, procédures ou technologies de protection ? (n = 1134)



Les responsables de la sécurité mentionnent plus d'améliorations suite à une attaque que ne le font les responsables des équipes chargées de la sécurité.

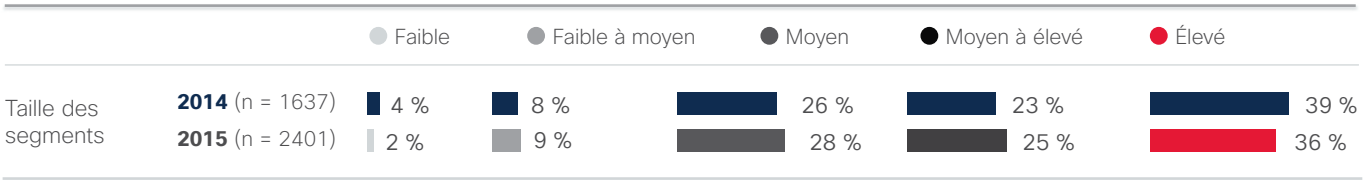
Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Leadership et maturité

Figure 81 : Le modèle à 5 segments correspond d'assez près au modèle CMMI (Capability Maturity Model Integration).

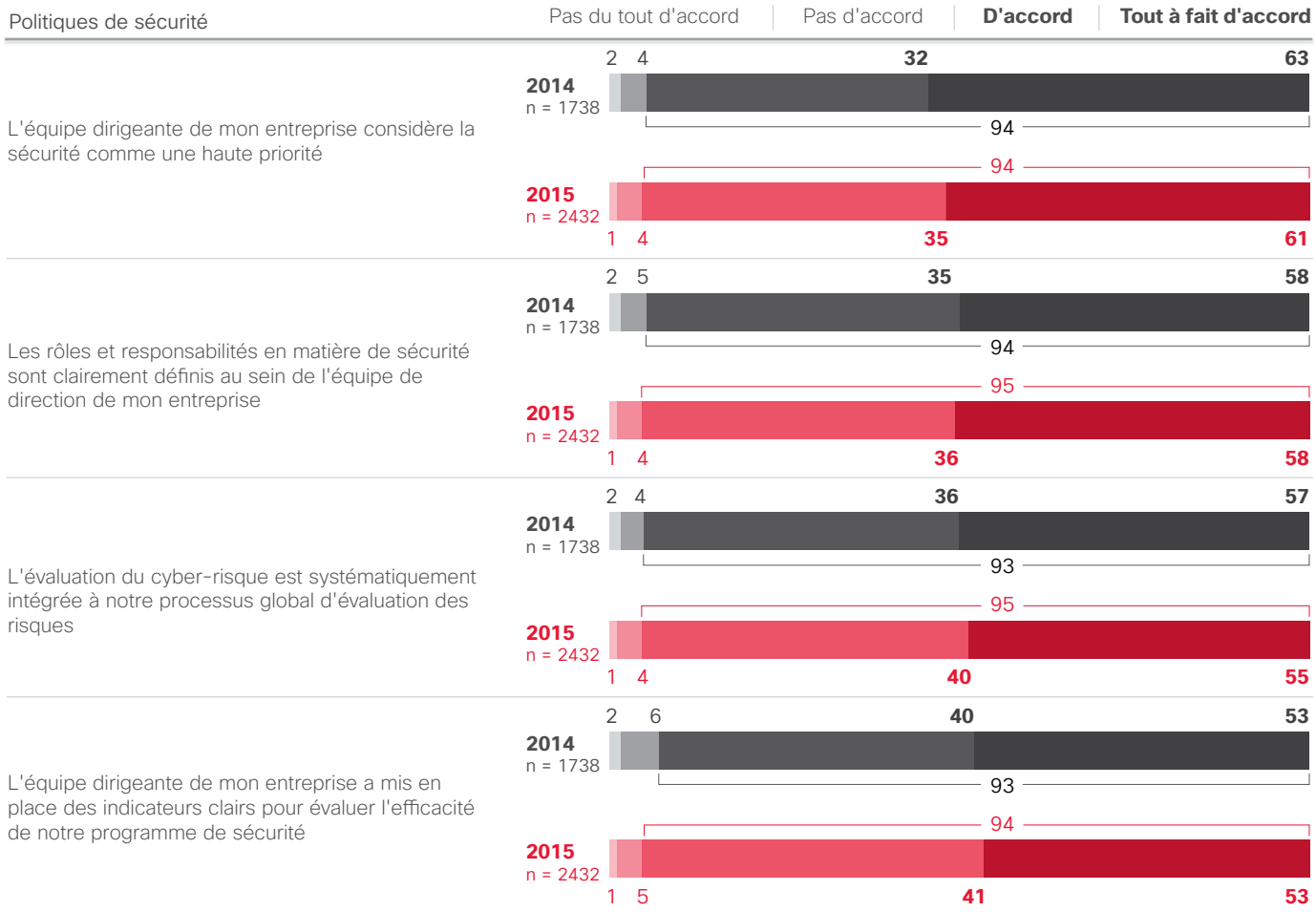
Les segments reflètent un modèle similaire à celui de l'an passé pour ce qui est de la maturité associée à la priorité de la sécurité et de la façon dont celle-ci se traduit en processus et procédures.

60 % ou plus affichent des profils plus conscients de la sécurité. C'est vrai pour la plupart dans les différents pays et les différents secteurs.



Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 82 : Comme en 2014, presque tous sont d'accord ou tout à fait d'accord pour dire que les dirigeants d'entreprise considèrent la sécurité comme une haute priorité



Parmi les personnes interrogées, les membres du secteur pharmaceutique tout à fait d'accord avec l'assertion « l'équipe de direction de mon entreprise a mis en place des indicateurs clairs pour évaluer l'efficacité de notre programme de sécurité » sont plus nombreux que les professionnels de la plupart des autres industries.

Il y a beaucoup plus de responsables de la sécurité à être d'accord avec toutes les assertions relatives à l'engagement de la direction que d'opérateurs de sécurité.

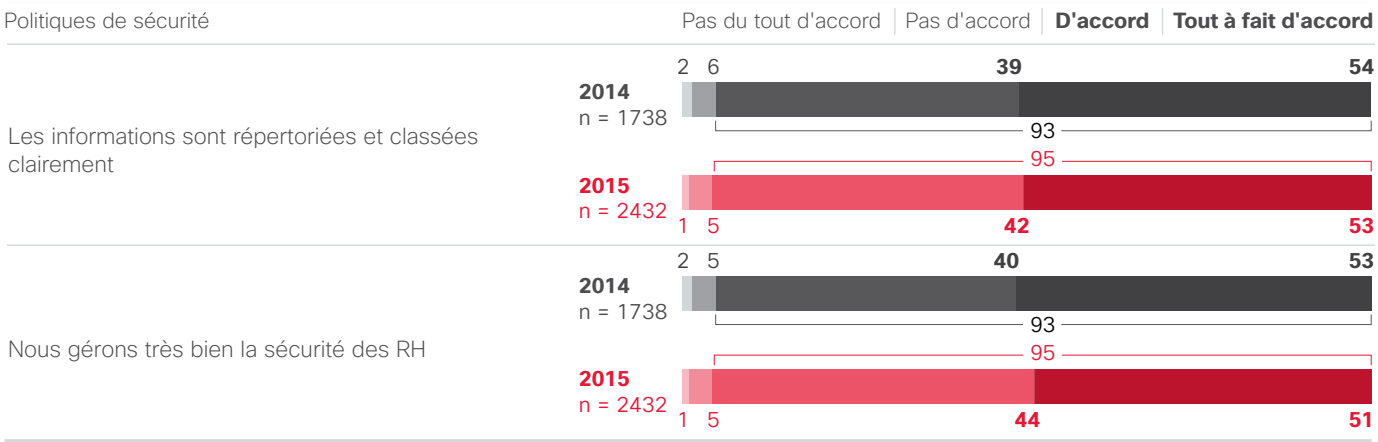
Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Processus

Figure 83 : Une confiance mitigée dans l'aptitude à créer de la sécurité au sein des systèmes

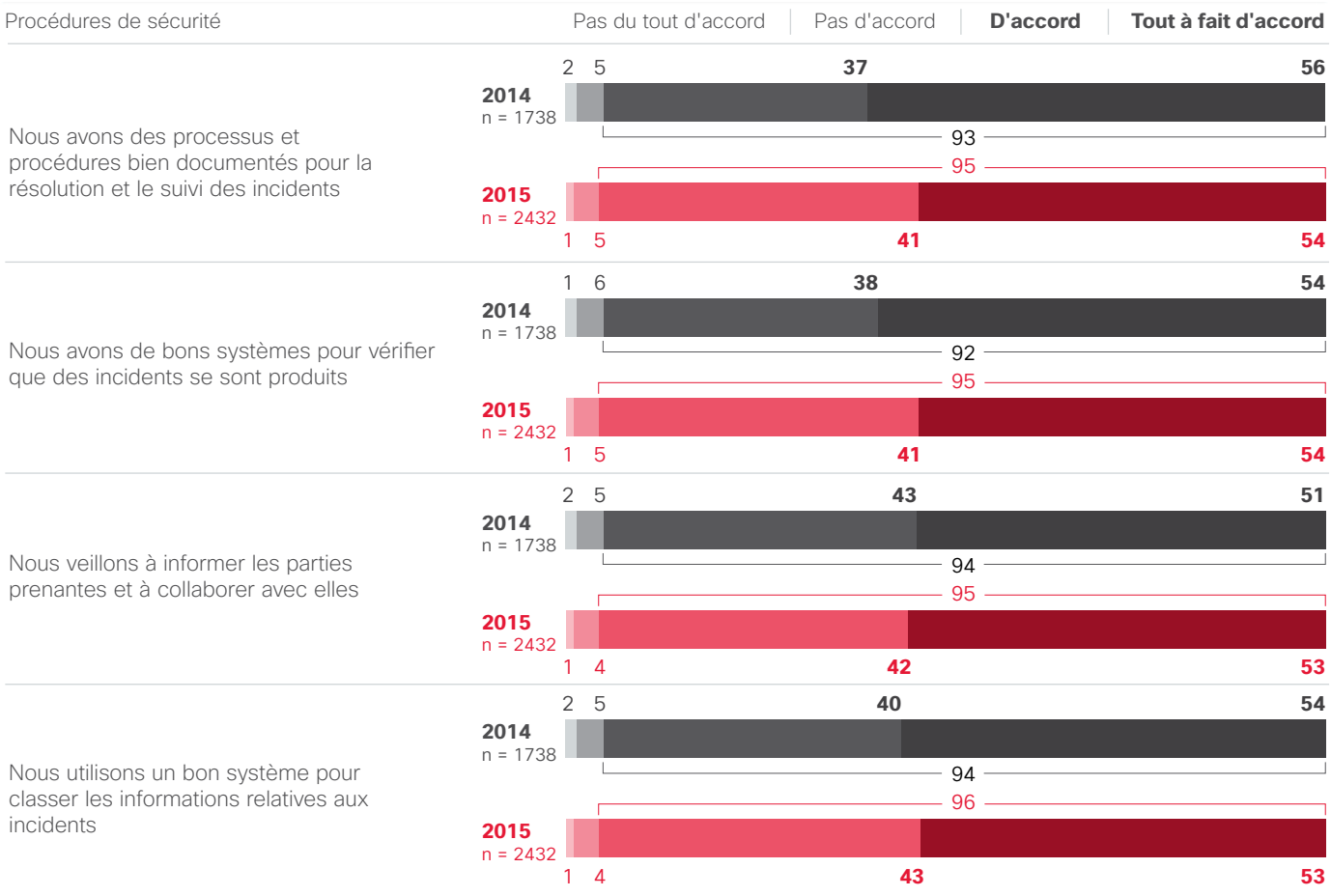
Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 83 : Une confiance mitigée dans l'aptitude à créer de la sécurité au sein des systèmes (suite)



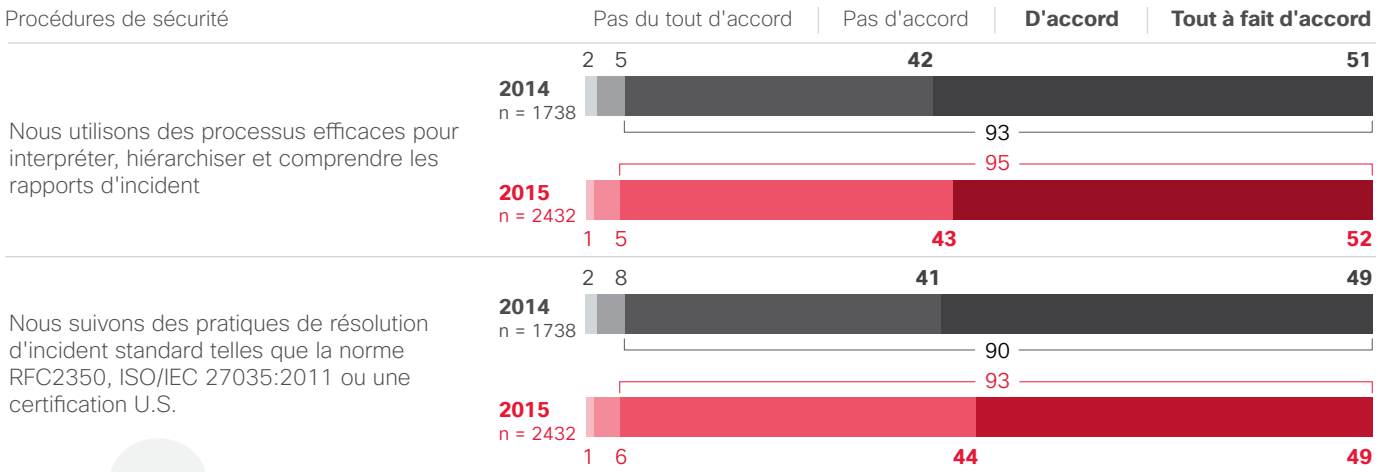
Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 84 : Les entreprises estiment qu'elles disposent de bons contrôles de sécurité



Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 84 : Les entreprises estiment qu'elles disposent de bons contrôles de sécurité (suite)



Les collaborateurs des services financiers interrogés sont plus susceptibles d'être tout à fait d'accord avec l'assertion « Nous utilisons un bon système pour classer les informations relatives aux incidents » que les professionnels des autres secteurs.

À l'exception de l'assertion « Nous veillons à informer les parties prenantes et à collaborer avec elles », les responsables de la sécurité sont plus positifs sur les attributs associés aux contrôles de sécurité que les responsables des opérateurs de sécurité.

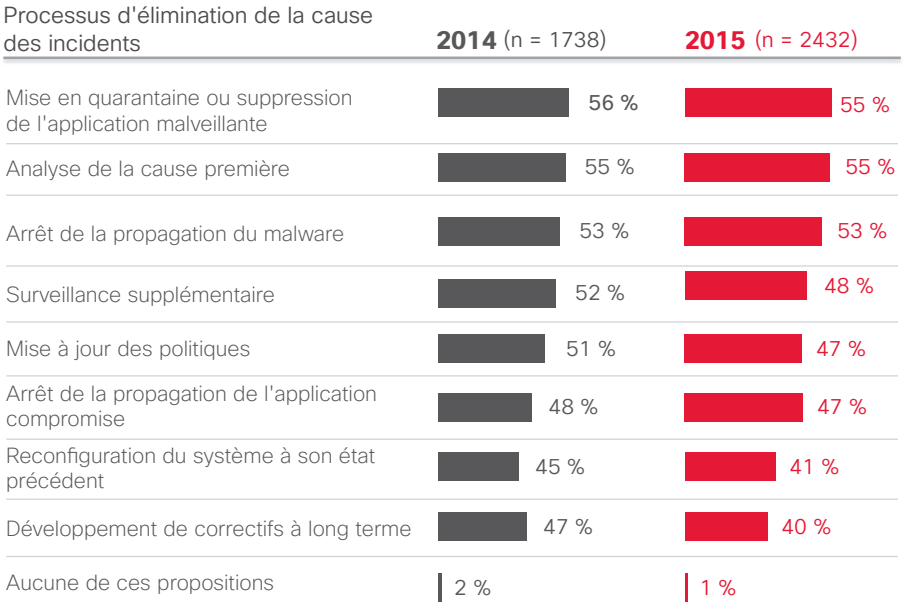
Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 85 : La mise en quarantaine/le retrait des applications malveillantes et l'analyse des causes premières continuent d'être les principaux processus utilisés

Par rapport aux personnes interrogées de la plupart des pays, les Étasuniens sont beaucoup plus nombreux à répondre « Aucune de ces propositions » lorsqu'on les interroge sur les processus permettant d'éliminer la cause d'un incident lié à la sécurité.

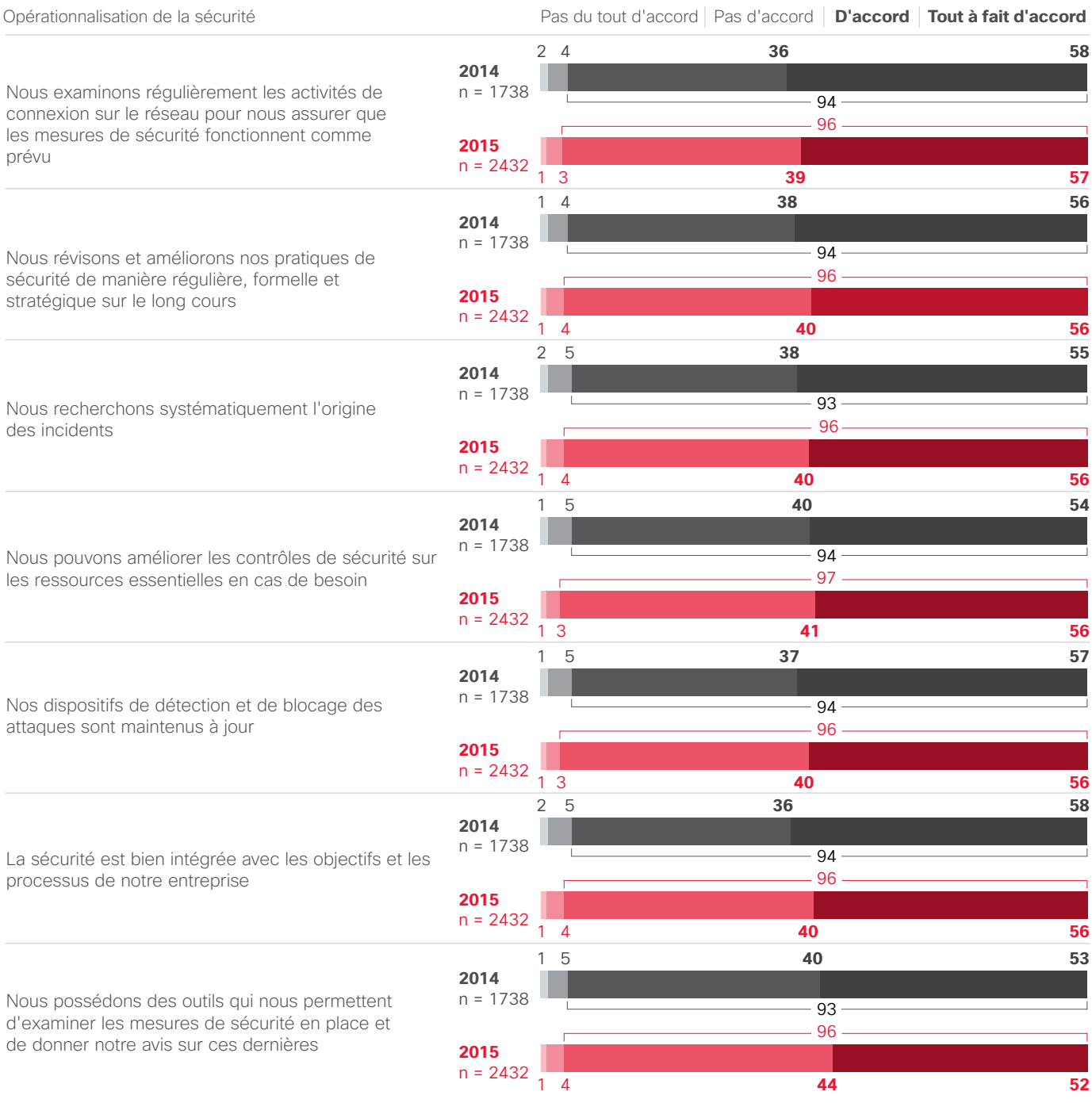
États-Unis

Incidents liés à la sécurité



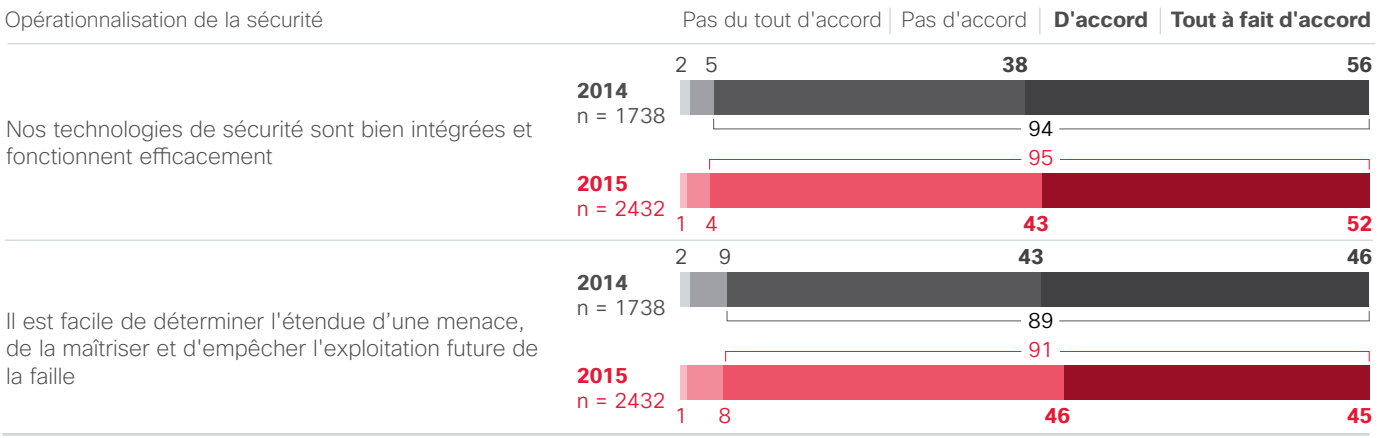
Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 86 : Les entreprises affichent une confiance mitigée dans l'aptitude à contenir les compromissions



Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

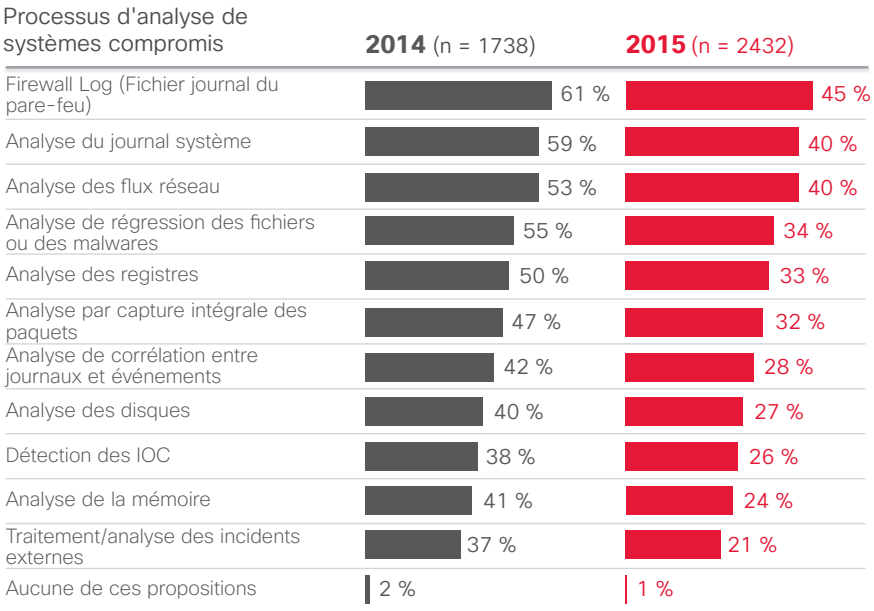
Figure 86 : Les entreprises affichent une confiance mitigée dans l'aptitude à contenir les compromissions (suite)



Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 87 : L'analyse des journaux de pare-feu et des journaux système continue d'être le processus le plus couramment utilisé pour analyser les systèmes compromis

Les entreprises et les grandes entreprises ont tendance à utiliser davantage de processus d'analyse des systèmes compromis que les entreprises de taille moyenne.



Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 88 : La restauration à partir d'une sauvegarde pré-incident est en 2015 le processus le plus répandu pour restaurer les systèmes affectés

Les personnes interrogées en Chine indiquent qu'elles corrigent et mettent à jour les applications jugées vulnérables plus fréquemment que les personnes interrogées dans d'autres pays.

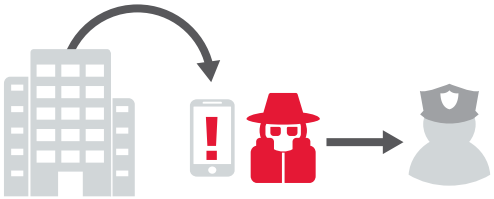
Processus de restauration des systèmes affectés	**2014** (n = 1738)	**2015** (n = 2432)
Restauration à partir d'une sauvegarde pré-incident	57 %	59 %
Mise en œuvre de nouveaux contrôles et dispositifs de détection, en fonction des vulnérabilités identifiées après un incident	60 %	56 %
Application de correctifs et mise à jour des applications jugées vulnérables	60 %	55 %
Restauration différentielle (élimination des modifications générées par un incident)	56 %	51 %
Restauration de l'image de référence	35 %	35 %
Aucune de ces propositions	2 %	1 %

Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 89 : Le PDG ou le Président est le plus susceptible d'être informé des incidents liés à la sécurité. Viennent ensuite le département Opérations et le département Finance

La notification à des autorités externes en cas d'incident est beaucoup plus fréquente dans les grandes entreprises que dans les PME.

Grande entreprise



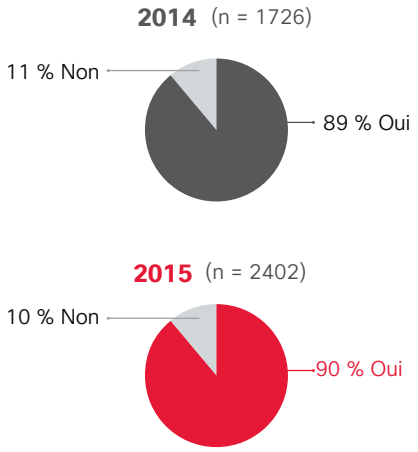
Groupes notifiés en cas d'incident	**2014** (n = 1738)	**2015** (n = 2432)
Directeur général	S/O	45 %
Opérations	46 %	40 %
Finances	S/O	40 %
Partenaires technologiques	45 %	34 %
Engineering	38 %	33 %
Ressources humaines	36 %	32 %
Les services juridiques	36 %	28 %
Fabrication	33 %	27 %
Tous les employés	35 %	26 %
Relations publiques	28 %	24 %
Partenaires commerciaux	32 %	21 %
Autorités externes	22 %	18 %
Compagnies d'assurance	S/O	15 %

Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

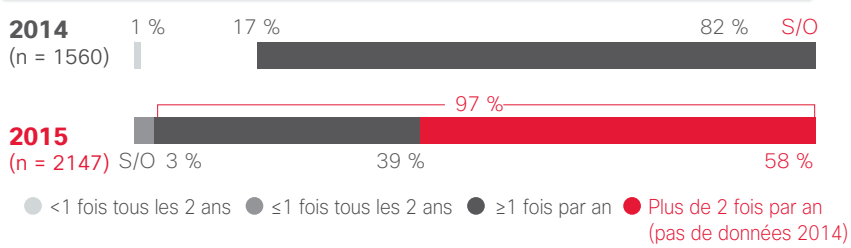
Formation

Figure 90 : Quasiment toutes les entreprises (97 %) dispensent au moins une fois par an une formation à la sécurité

Le personnel chargé de la sécurité connaît-il le contexte et/ou suit-il des programmes de formation à la sécurité régulièrement ? (Personnes interrogées dédiées à la sécurité)



À quelle fréquence une formation à la sécurité est-elle dispensée ?
(Personnes interrogées dont les équipes de sécurité reçoivent une formation)



Les entreprises qui ont régulièrement subi une attaque réalisent davantage des programmes de sensibilisation et/ou de formation à la sécurité (96 %) que celles qui n'en ont pas connu (83%).

Ont **96 %** vs N'ont pas **83 %**

Par rapport aux entreprises moyennes (88 %) et aux petites entreprises (89 %), plus de grandes entreprises indiquent qu'elles disposent de programmes de sensibilisation et/ou de formation à la sécurité (93 %).

Grande entreprise **93 %** PME **88 %** Petites entreprises **89 %**

Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 91 : La fréquence de la formation de sensibilisation à la sécurité et l'impact des politiques de sécurité formelles augmentent depuis 2014 – preuve d'action

(les 5 mentions les plus citées) Personnes interrogées affectées par une attaque (2015 n = 1109)

Formation de sensibilisation à la sécurité avancée pour les employés

En 2015, 43 % des personnes interrogées affirment avoir renforcé leur formation à la sécurité suite à une atteinte à la sécurité publique.

43 %

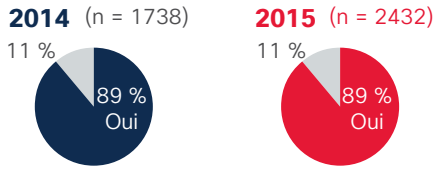
En 2015, 41 % des personnes interrogées indiquent avoir mis en place un ensemble de politiques et procédures de sécurité.

41 %

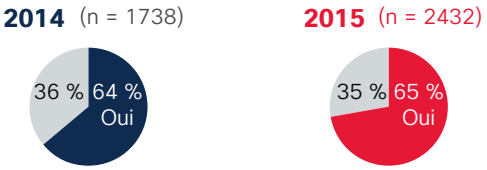
Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Figure 92 : Comme en 2014, près de 90 % des personnes interrogées affirment que leur personnel en charge de la sécurité assiste à des conférences ou des formations axées sur la sécurité

Le personnel dédié à la sécurité assiste-t-il à des conférences et/ou à des formations externes pour améliorer et entretenir ses compétences ?
(Personnes interrogées dédiées à la sécurité)



Les employés participent-ils à des conseils ou comités sur la sécurité ?
(Personnes interrogées dédiées à la sécurité)



Source : Enquête Cisco 2015 sur l'efficacité des mesures de sécurité

Enquête sur le risque de sécurité et la fiabilité

Figure 93 : Contexte et méthodologie

Cisco tient à mieux comprendre la perception des décideurs IT des entreprises et des fournisseurs de services concernant les risques et défis de sécurité, et le rôle joué par la fiabilité du fournisseur IT dans l'achat d'une solution IT.

On compte parmi les objectifs spécifiques :

- Mesurer le niveau de risque des attaques et vulnérabilités externes et internes
- Comprendre les stratégies, politiques et solutions mises en œuvre pour atténuer les risques de sécurité
- Identifier le processus d'achat de solutions informatiques et le rôle de la fiabilité des fournisseurs IT dans ce processus
- Estimer l'intérêt associé à la réception de communications portant sur des moyens de validation de la fiabilité d'un fournisseur IT
- Déterminer s'il existe des différences entre les visions et approches du risque de sécurité d'une industrie à l'autre et d'un public à l'autre

Méthodologie : Approche qualitative et quantitative

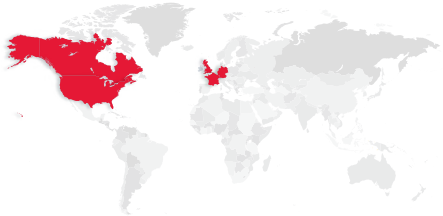
Deux méthodologies ont été utilisées pour examiner chacun de ces objectifs de recherche :

(Toutes les personnes interrogées impliquées dans la prise d'une décision d'achat IT)

Étude Web quantitative réalisée sur
1 050 entreprises (fabricants de technologies et équipements intégrés)
(402 États-Unis, 282 RU, 197 Allemagne, 169 France)

Entretiens qualitatifs approfondis avec
20 fournisseurs de service
(7 États-Unis., 3 Canada, 3 RU, 4 Allemagne, 3 France)

L'étude a été menée aux États-Unis, au Royaume-Uni, en France, en Allemagne et au Canada (IDI uniquement)



La collecte de données a eu lieu d'août à septembre 2015

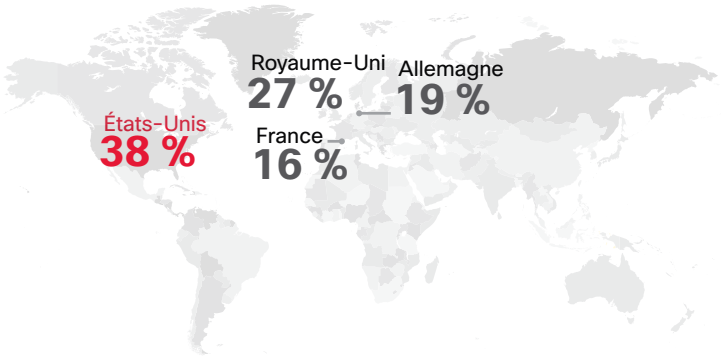
20
Sondage rapide réalisé en ligne

45
Entretiens rapides approfondis

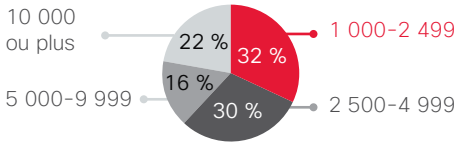
Source : Étude sur le risque de sécurité et la fiabilité, Cisco

Figure 94 : Profil quantitatif des entreprises interrogées

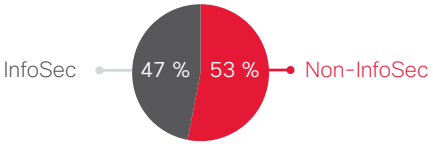
Pays



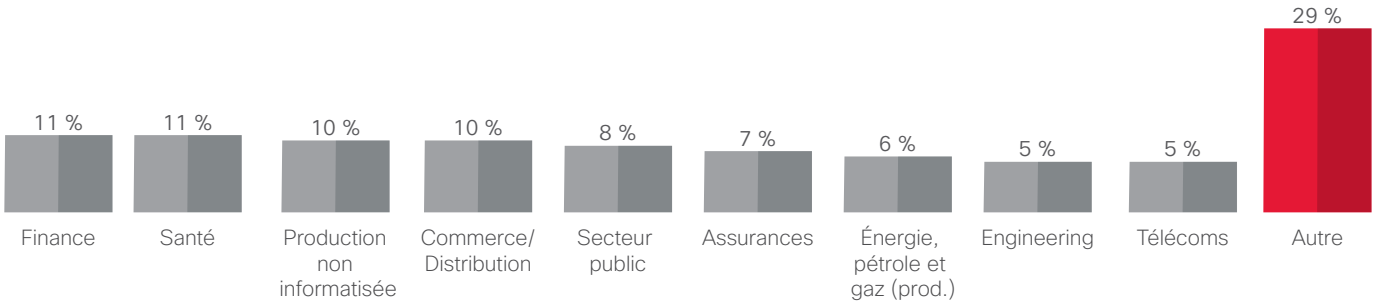
Taille de l'entreprise



Classification PoE



Secteur (plus de 5 % enregistrés)



Fonction

Niveau C (DSI, responsable de la sécurité, Directeur des technologies, etc.).	25 %
Vice-président	9 %
Directeur	30 %
Ingénieur principal/Architecte	6 %
Ingénieur	3 %
Responsable hiérarchique	26 %
Les services juridiques	2 %

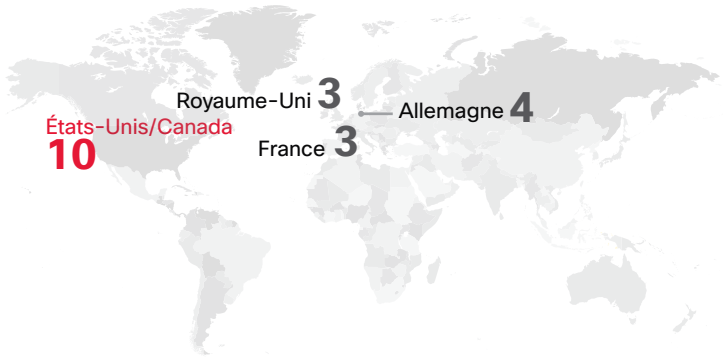
Implication d'achat

Définir la vision/stratégie	69 %
Garantir la conformité aux normes en vigueur	71 %
Approuver les principaux achats	69 %
Rechercher/évaluer les solutions	77 %
Fournir des données ou prendre des décisions en matière de marque	80 %
Mettre en œuvre/gérer les solutions	77 %
Autoriser le financement/approuver le budget	53 %

Source : Étude sur le risque de sécurité et la fiabilité, Cisco

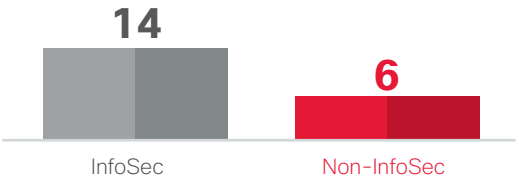
Figure 95 : Profil qualitatif des fournisseurs de services interrogés

Pays



Taille de l'entreprise

Classification InfoSec



Type de fournisseur de services

Services d'applications	11 %
Services techniques	11 %
Télécommunications mobiles	6 %
Services multimédias	4 %
Télécommunications câblées	3 %

Fonction

DSI/directeur des technologies/responsable de la sécurité	7 %
Vice-président informatique	1 %
Directeur informatique	8 %
Responsable senior	1 %
Ingénieur principal/ Architecte	2 %
Responsable hiérarchique	1 %

Implication d'achat

Définir la vision/stratégie	80 %
Garantir la conformité aux normes en vigueur	100 %
Approuver les principaux achats	70 %
Rechercher/évaluer les solutions	95 %
Prendre des décisions finales en matière de marque	85 %
Mettre en œuvre/gérer les solutions	75 %
Autoriser/approuver le financement	60 %

Source : Étude sur le risque de sécurité et la fiabilité, Cisco

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

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

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

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

Publication janvier 2016