Rapport Cisco sur la cybersécurité
1er semestre 2016

Sommaire

Synthèse et principales conclusions

Les acteurs de la sécurité doivent réduire la fenêtre d'action des hackers. C'est là leur seul moyen de les mettre en difficulté.

Les hackers bénéficient actuellement d'une très large fenêtre d'action. Leurs campagnes, qui ciblent souvent les vulnérabilités connues qui auraient dû et pu être corrigées par les entreprises et les utilisateurs, peuvent rester actives et passer inaperçues pendant des jours, des mois et parfois même plus. De leur côté, les acteurs de la sécurité peinent à obtenir des informations précises sur les menaces et à réduire le délai de détection des menaces connues et nouvelles. S'ils font beaucoup de progrès, ils ont encore du chemin à parcourir pour empêcher leurs adversaires de poser les bases de leurs attaques et de frapper fort, là où ça fait mal.

Destiné aux professionnels de la sécurité, le rapport semestriel Cisco® 2016 sur la cybersécurité présente le travail, les conclusions et le point de vue des équipes de recherche sur la sécurité Cisco. Il décrit l'évolution des tendances identifiées dans notre précédent rapport sur la cybersécurité et analyse les tendances qui se dessinent pour la fin de l'année.

Les récents développements constatés au sein de l'économie parallèle confirment le fait que l'argent devient une motivation toujours plus forte pour les hackers. Les ransomwares (ou logiciels rançonneurs) se révèlent être un excellent outil pour gagner de l'argent et visent désormais un nombre toujours plus important d'entreprises.

Une grande partie des tendances en matière de sécurité décrites dans ce rapport sont liées aux ransomwares, des techniques utilisées pour lancer les campagnes d'attaque et dissimuler leur propagation, aux perspectives d'évolution de la nouvelle génération de ransomwares.

Ce rapport présente également les moyens d'action à la disposition des entreprises pour mieux se protéger contre ces attaques toujours plus efficaces. Voici quelques recommandations des chercheurs Cisco :

- Élaborer et tester un plan de gestion des incidents qui permet un rapide retour à la normale des activités de l'entreprise après une attaque par ransomware
- Se méfier des connexions HTTPS et des certificats SSL
- Corriger rapidement les vulnérabilités connues au niveau des systèmes et de la pile logicielle, y compris au niveau des routeurs et des commutateurs qui forment le socle de l'infrastructure Internet
- Informer les utilisateurs de la dangerosité des infections de navigateur
- Comprendre ce que sont réellement des informations exploitables sur les menaces

Ce rapport se divise en quatre thèmes principaux :

I. LES RANSOMWARES : UNE MENACE QUI PREND DE L'AMPLEUR

Les experts en sécurité de Cisco se sont intéressés aux ransomwares et ont cherché à comprendre les raisons de l'essor de ce nouveau type de malware. Ils analysent également les précédentes tendances en la matière pour évaluer les perspectives d'avenir des ransomwares. Enfin, ils expliquent comment les vulnérabilités au niveau des systèmes et des appareils obsolètes offrent une large fenêtre d'action aux hackers. Les entreprises sont devenues les nouvelles cibles des opérateurs de ransomware. Face à cette nouvelle menace, elles doivent stocker leurs données essentielles dans un endroit sécurisé et élaborer des plans d'action pour garantir un rapide retour à la normale de leurs activités après une attaque.

II. LA FENÊTRE D'ACTION DES HACKERS

Cette section analyse les vecteurs d'attaques côté client qui donnent aux hackers le temps et la possibilité de créer de nouvelles menaces et de mener à bien leurs campagnes. La multiplication des vulnérabilités liées à la cryptographie et aux autorisations d'accès est la preuve que les acteurs malveillants ciblent à présent les connexions sécurisées. Nos experts vous présentent les tendances actuelles en matière de kit d'exploit et de vecteur d'attaque, parmi lesquelles l'intérêt grandissant des hackers pour les exploits de serveurs qui leur donnent accès à de plus gros volumes de données. Ils nous parlent également de l'émergence de la « publicité malveillante en tant que service » (ou MaaS) et des nouvelles problématiques que cette dernière cause aux acteurs de la sécurité, notamment pour savoir qui doit protéger les utilisateurs du web.

III. LES DÉFIS EN MATIÈRE DE SÉCURITÉ

Dans cette section, les experts en sécurité de Cisco analysent l'inefficacité des solutions de sécurité actuelles face aux nouvelles attaques. Par exemple, si les fournisseurs ont réduit le délai entre l'identification des vulnérabilités publiques et la mise à disposition des correctifs correspondants, les utilisateurs mettent encore trop de temps à déployer ces correctifs. Ils nous parlent également des efforts réalisés par Cisco pour réduire le délai médian de détection et de l'impact de la « course à l'armement » qui oppose les cybercriminels et les acteurs de la sécurité. Il y est également question des protocoles HTTPS et TLS (Transport Layer Security) que les hackers utilisent de plus en plus pour mener à bien leurs campagnes et chiffrer leurs communications.

IV. PERSPECTIVE À L'ÉCHELLE MONDIALE ET RECOMMANDATIONS DE SÉCURITÉ

Cette section présente les tendances géopolitiques actuelles en matière de sécurité, notamment les défis auxquels font face les états pour suivre l'évolution de la technologie afin de mieux comprendre les menaces, mais aussi gérer et contrôler les données. Nos experts offrent un certain nombre de recommandations pour réduire la fenêtre d'action des hackers. Vous y apprendrez également que les indicateurs de compromission (IoC) n'offrent pas d'informations suffisantes sur les menaces, et pourquoi.

PRINCIPALES CONCLUSIONS

- Les ransomwares dominent actuellement le marché des malwares. Bien qu'ils existent depuis un certain temps, leur récente évolution les a érigés au rang des malwares les plus rentables de l'histoire de la cybercriminalité. Les entreprises sont également devenues une cible de choix pour certains opérateurs de ransomware. Au premier semestre 2016, on a assisté à un véritable essor de campagnes de ransomware toujours plus efficaces, aussi bien contre les particuliers que les entreprises. On craint désormais une propagation plus rapide et plus efficace de ces campagnes de ransomware qui risquent d'être encore plus dévastatrices et rentables.
- Les kits d'exploits, qui ont facilité la multiplication des ransomwares, continuent de tirer parti des vulnérabilités Adobe Flash. En analysant le célèbre kit d'exploit Nuclear, nos experts ont découvert qu'Adobe Flash était à l'origine de 80 % des tentatives d'exploitation réussies.
- Les vulnérabilités du logiciel d'applications professionnelles JBoss constituent un nouveau vecteur d'attaque pour des campagnes telles que les ransomwares. Une étude menée par Cisco révèle que les compromissions au niveau du logiciel JBoss avaient largement fragilisé les serveurs, les rendant ainsi plus vulnérables face aux attaques.
- Entre septembre 2015 et mars 2016, les experts Cisco ont constaté une multiplication par cinq du trafic HTTPS associé aux activités malveillantes. L'augmentation de ce type de trafic web s'explique en grande partie par l'essor des moteurs et des logiciels publicitaires malveillants. Les hackers utilisent de plus en plus le trafic chiffré HTTPS pour dissimuler leurs attaques sur le web et élargir leur fenêtre d'action.
- Si les principaux fournisseurs de logiciels proposent des correctifs presque immédiatement après la découverte d'une vulnérabilité, de nombreux utilisateurs tardent trop à télécharger et à installer ces correctifs. Ce décalage entre la mise à disposition et le déploiement de ces correctifs laisse aux hackers tout le temps nécessaire pour lancer leurs exploits.
- Pour attirer l'attention sur les risques qu'encourent les entreprises qui ne mettent pas à jour leur infrastructure vieillissante ou qui ne corrigent pas les vulnérabilités au niveau de leurs systèmes d'exploitation, les chercheurs Cisco ont analysé un échantillon d'appareils Cisco pour connaître « l'âge » des vulnérabilités connues qui touchent l'infrastructure sous-jacente des entreprises. Il apparaît ainsi que 23 % de ces appareils présentent des vulnérabilités datant de 2011 et 16 % des vulnérabilités connues depuis 2009.
- Un nombre faible mais croissant d'échantillons de malwares révèle que les hackers dissimulent leurs attaques à l'aide du protocole TLS (Transport Layer Security) habituellement utilisé pour chiffrer le trafic réseau. Cette nouvelle tendance complique le travail des professionnels de la sécurité car elle rend totalement inefficace l'inspection approfondie des paquets. Les techniques d'apprentissage automatique et les nouvelles vues de données offrent des informations beaucoup plus précises sur cette tendance.
- Entre décembre 2015 et avril 2016, Cisco a réduit son délai moyen de détection à environ 13 heures, ce qui est bien en dessous du délai actuel du secteur tout à fait inacceptable qui oscille entre 100 et 200 jours. Les fluctuations du délai de détection constatées au cours de cette période mettent en lumière une véritable course à l'armement entre les cybercriminels et les acteurs de la sécurité, dans laquelle les hackers ne cessent de lancer de nouvelles menaces que les fournisseurs de solutions de sécurité doivent rapidement identifier.

Introduction

Les systèmes ne sont actuellement pas assez bien protégés contre les nouveaux types d'attaques. Si les acteurs de la sécurité ont effectivement adapté leurs stratégies et leurs outils aux nouvelles techniques des hackers, ces derniers bénéficient encore d'une trop grande fenêtre d'action.

Le véritable problème est le manque de visibilité qui rend les utilisateurs vulnérables face aux attaques. Les solutions ponctuelles et l'approche de « tri » actuellement utilisées par les professionnels de la sécurité qui se contentent de stopper les attaques de manière sporadique au lieu d'adopter une approche plus globale de la sécurité, jouent largement en faveur des hackers.

Ces derniers disposent de tout le temps nécessaire pour identifier et exploiter les vulnérabilités au niveau des infrastructures, des systèmes et des appareils déployés depuis un certain temps mais jamais mis à jour. Ils peuvent donc s'introduire sur le réseau de l'entreprise et se déplacer latéralement jusqu'à leur cible. Ils lancent également des campagnes axées sur les serveurs qui agrandissent leur champ d'action et augmentent leurs retours sur investissement.

« En utilisant de manière plus efficace les outils à leur disposition, c'est-à-dire en réduisant le délai de correction des vulnérabilités et en mettant à niveau leur infrastructure, les acteurs de la sécurité peuvent identifier plus facilement les hackers et donc limiter, voire réduire à néant, le champ d'action de ces derniers. »

En dehors de cette large fenêtre d'action, les hackers restent limités dans la propagation de leurs attaques. Ils n'ont que peu de possibilités de pénétrer les réseaux. Ainsi, en utilisant de manière plus efficace les outils à leur disposition, c'est-à-dire en réduisant le délai de correction des vulnérabilités et en mettant à niveau leur infrastructure, les acteurs de la sécurité peuvent identifier plus facilement les hackers et donc limiter, voire réduire à néant, le champ d'action de ces derniers. Les acteurs de la sécurité peuvent également obtenir une visibilité complète sur les attaques, c'est-à-dire déceler la présence des hackers mais aussi savoir comment ils ont pénétré le réseau et quels systèmes ont réussi ou non à détecter la menace.

Malheureusement, face à tant de couches de réseau à sécuriser, les acteurs de la sécurité adoptent une approche de « tri ». Les hackers n'ont donc aucune difficulté à renforcer leurs attaques car ils bénéficient non seulement d'une grande fenêtre d'action, mais également de l'incapacité de leurs adversaires à éliminer les vecteurs d'attaques les plus basiques. Cela explique en grande partie l'essor des ransomwares, des menaces en perpétuelle évolution et de plus en plus difficiles à contrer (voir « Ransomwares : des attaques très rentables et difficiles à contrer », **page 7**).

Les ransomwares : une menace qui prend de l'ampleur

Les ransomwares : une menace qui prend de l'ampleur

Les ransomwares dominent actuellement le marché des malwares. Bien qu'ils existent depuis un certain temps, leur récente évolution les a érigés au rang des malwares les plus rentables de l'histoire de la cybercriminalité. Au premier semestre 2016, on a assisté à un véritable essor de campagnes de ransomware toujours plus efficaces, aussi bien contre les particuliers que les entreprises.

Le succès de récentes attaques de ransomware contre des entreprises, dont plusieurs établissements de santé, a très certainement encouragé d'autres hackers à mener des campagnes similaires. Les vulnérabilités au niveau des réseaux et des serveurs permettent aux hackers de poursuivre tranquillement leurs attaques qui peuvent affecter des secteurs entiers.

Ransomwares : des attaques très rentables et difficiles à contrer

Il existe de nombreux types de ransomware. Et si certains sont spécifiques à une langue, tous sont résilients. Les responsables de ces attaques, avec en première ligne les créateurs des célèbres ransomwares CryptoLocker et CryptoWall, ont considérablement amélioré l'efficacité de leurs malwares grâce au chiffrement cryptographique. Aujourd'hui, il est encore difficile de détecter les ransomwares connus, ce qui ne laisse que peu d'options aux victimes qui se retrouvent contraintes de verser la somme demandée.

Le paiement des rançons s'effectue généralement en bitcoins. L'anonymat dont bénéficient les utilisateurs de bitcoins est en partie responsable de l'essor des ransomwares. Pour ajouter encore un peu plus de complexité, la quasi-totalité des échanges de ransomware transite par le réseau d'anonymisation sur Internet, Tor. Les bitcoins peuvent également être fractionnés pour permettre aux hackers d'indemniser tous les membres de leur équipe avec un seul bitcoin, une méthode à la fois pratique et indétectable.

UN NOUVEAU VECTEUR POUR LES RANSOMWARES

Si l'e-mail et la publicité malveillante (ou malvertising) sont les principaux vecteurs des campagnes ransomware, certains auteurs de menaces exploitent aujourd'hui les faiblesses des réseaux et des serveurs.

Au début de l'année, une vaste campagne qui semblait cibler le secteur de la santé des États-Unis a propagé le ransomware Samas/Samsam/MSIL.B/C (« SamSam ») via des serveurs compromis. Les hackers ont utilisé les serveurs pour se déplacer latéralement au sein du réseau et compromettre d'autres machines, qu'ils ont ensuite prises en otage.

Ils ont utilisé JexBoss, un outil Open Source conçu pour tester et exploiter les serveurs d'applications JBoss, afin de s'infiltrer dans les réseaux des entreprises. Une fois qu'ils ont eu accès aux réseaux, ils ont commencé à chiffrer de nombreux systèmes Microsoft Windows au moyen des ransomwares SamSam.

« La prochaine vague de ransomwares devrait être encore plus invasive et résiliente. Les entreprises et les utilisateurs devraient se préparer dès à présent en enregistrant leurs données essentielles et en s'assurant que ces sauvegardes ne puissent pas être compromises. »

À bien des égards, l'attaque SamSam était inévitable : de nombreuses entreprises utilisaient des serveurs JBoss présentant des vulnérabilités non corrigées. (Lire « Plate-forme JBoss : des vulnérabilités au niveau de l'infrastructure élargissent la fenêtre d'action des cybercriminels », **page 18**.) Lors d'une enquête menée en avril 2016, Cisco a identifié pas moins de 2 100 serveurs JBoss déjà compromis et prêts à faire l'objet d'une attaque. Toutes les entreprises ont été informées qu'elles devaient mettre leurs serveurs hors ligne et procéder immédiatement à une mise à niveau.

La vulnérabilité des infrastructures Internet est un problème général et nous savons pertinemment que d'autres hackers l'exploiteront pour mener des campagnes malveillantes ciblant non seulement les entreprises, mais également des secteurs d'activité entiers. (Lire « Infrastructure vieillissante : des vulnérabilités de longue date à corriger d'urgence pour faire face à l'essor des ransomwares », **page 30**.)

AUTRE NOUVELLE PRÉOCCUPATION : L'INTÉGRITÉ DES DONNÉES

Les utilisateurs et les entreprises ciblées par les ransomwares se trouvent dans une situation peu enviable : ils sont contraints de faire confiance à leurs agresseurs. Si payer la rançon demandée peut sembler la solution la plus simple (et la seule), il est important que les utilisateurs pris en otage comprennent que leurs fichiers pourraient bien ne jamais être déchiffrés, voire être perdus. Des bugs présents dans les premières versions de certains ransomwares ont entraîné la perte de fichiers alors même que la rançon avait été payée.

Il existe par ailleurs un risque que les hackers falsifient intentionnellement les fichiers tant qu'ils en ont le contrôle. Selon les types de fichiers chiffrés – des dossiers médicaux ou des plans techniques, par exemple – la falsification des données peut avoir de graves conséquences.

Le risque de réinfection est une autre préoccupation, car il arrive qu'un ransomware s'attaque à deux reprises aux mêmes utilisateurs et à la même machine. Dans certains cas, le montant de la rançon était moins élevé lors de la deuxième attaque – une sorte de remise offerte à l'utilisateur concerné. À d'autres occasions, les hackers ont adopté la démarche inverse, demandant une rançon plus élevée quand les utilisateurs hésitaient à payer le montant initial.

Les ransomwares étant désormais extrêmement efficaces et rentables, il ne fait aucun doute que des hackers toujours plus nombreux chercheront à en faire une source de revenus facile. Pour les hackers, les entreprises offrent bien sûr l'opportunité d'exiger des montants qui dépassent largement ceux que pourrait payer un seul utilisateur. À l'évidence, les troubles et les coûts générés par les ransomwares qui ciblent une entreprise ou un secteur d'activité sont bien supérieurs.

La prochaine vague de ransomwares devrait être encore plus répandue et résiliente. (Lire « L'autopropagation des ransomwares », **page 9**.) Les entreprises et les utilisateurs devraient se préparer dès à présent en enregistrant leurs données essentielles et en s'assurant que ces sauvegardes ne puissent pas être compromises. Ils doivent également veiller à ce que les données sauvegardées puissent être restaurées rapidement après une attaque. Pour les entreprises, la restauration peut constituer une tâche considérable, c'est pourquoi elles doivent impérativement identifier les congestions potentielles de manière proactive. Elles doivent également s'assurer que les vulnérabilités de leurs systèmes et de leur infrastructure Internet ont été corrigées.

Pour en savoir plus sur la campagne SamSam et les vulnérabilités de JBoss, consultez les bulletins du blog Cisco Talos suivants :

« SamSam : The Doctor Will See You, After He Pays the Ransom »

« Widespread JBoss Backdoors a Major Threat »

L'autopropagation des ransomwares

L'attaque SamSam incarne une nouvelle approche : les hackers ne ciblent plus des utilisateurs mais corrompent désormais des réseaux entiers (voir **page 16**). Son mode de propagation est simple mais extrêmement efficace. Vu le succès de SamSam, les hackers ne devraient pas tarder à lancer des modes de propagation encore plus rapides et efficaces pour maximiser l'impact des attaques et augmenter leurs chances d'obtenir la rançon demandée.

En observant les tendances et l'évolution des malwares, les chercheurs Cisco estiment que les ransomwares autopropagés sont la prochaine étape vers laquelle se dirigent les hackers. Les utilisateurs sont donc encouragés à prendre les mesures qui s'imposent dès maintenant pour s'y préparer. En utilisant les portes dérobées de JBoss pour lancer des campagnes ransomware contre des établissements de santé, les hackers nous rappellent que, s'ils ont suffisamment de temps, ils trouveront de nouveaux moyens de compromettre les utilisateurs et les réseaux – et d'exploiter des faiblesses qui auraient dû être corrigées depuis longtemps.

Les malwares à autopropagation ne sont pas une nouveauté. Ils existent depuis plusieurs dizaines d'années sous la forme de vers et de botnets. Bon nombre de ces menaces restent répandues et toujours aussi efficaces. Les malwares à autopropagation peuvent présenter les caractéristiques suivantes :

- **Exploitation des faiblesses d'un produit déployé à grande échelle.** Les anciens vers les plus performants ont tiré parti des faiblesses de produits déployés sur Internet.
- **Réplication vers tous les lecteurs disponibles.** Certaines souches de malwares dénombrent les lecteurs locaux et distants, y compris les lecteurs réseau et les lecteurs USB, et se dupliquent sur ces lecteurs pour se propager ou persister. Ce mode opératoire rend possible l'infection des systèmes offline comme des systèmes inaccessibles via l'Internet public.
- **Corruption des fichiers** Les malwares corrompent les fichiers en s'attachant à la fin ou au début de leur contenu. Concrètement, ils s'ajoutent aux fichiers exécutables non protégés par Windows SFC ou SFP (System File Checker ou System File Protector). Certains vers s'attachent aux fichiers non exécutables, depuis lesquels ils se propagent ensuite.
- **Une action brutale mais limitée.** Peu de vers ont eu recours à cette méthode par le passé.
- **Des commandes et des contrôles résilients.** Certains vers tiennent compte des actions normalement effectuées pour perturber l'infrastructure de contrôle-commande et implémentent des mesures préventives pour contourner ces perturbations. De nombreux vers ne possèdent pas d'infrastructure de contrôle-commande. Ils se contentent d'effectuer une action par défaut simplifiée pour se propager aussi rapidement que possible.
- **Utilisation d'autres portes dérobées.** Certains auteurs de malwares, conscients du fait que d'autres infections ont pu laisser une trace dans un système, profitent de ces portes dérobées pour propager leurs programmes malveillants.

« En observant les tendances et l'évolution des malwares, les chercheurs Cisco estiment que les ransomwares autopropagés sont la prochaine étape vers laquelle se dirigent les hackers. Les utilisateurs sont donc encouragés à prendre les mesures qui s'imposent dès maintenant pour s'y préparer. »

LE SYSTÈME DE LA RANÇON DU ROI

D'après nos observations des techniques utilisées par les auteurs de ransomware, les hackers qui développent la nouvelle génération de ce type de virus vont probablement privilégier les logiciels de conception modulaire – une architecture commune à de nombreuses suites populaires de tests d'intrusion Open Source. Cette approche leur permet d'utiliser certaines fonctions selon leurs besoins. En plus d'accroître l'efficacité des attaques, elle offre aux pirates la possibilité de changer de stratégie si une technique est découverte ou s'avère inefficace.

Nous pensons que le système de demande de rançon nouvelle génération – que nous avons surnommé le système de la rançon du roi – inclura entre autres fonctionnalités centrales :

- Le chiffrement des emplacements standard des fichiers des utilisateurs et la possibilité de personnaliser les répertoires et les types de fichiers, pour une personnalisation ciblée
- Le balisage des systèmes et des fichiers qui ont déjà été chiffrés
- Des instructions pour le paiement de la rançon en bitcoins
- La possibilité pour le hacker de fixer le montant de la rançon en spécifiant deux échéances : le moment où ce montant sera augmenté et celui où la clé de chiffrage des données sera supprimée

Le système prendra également en charge différents modules afin que le hacker puisse personnaliser le ransomware en fonction de l'environnement ciblé et adopter des modes de propagation plus agressifs en cas d'opportunité. Parmi ces modules, citons les exemples suivants :

AUTORUN.INF / PROPAGATION PAR PROTOCOLE USB MASS STORAGE

Ce module chercherait des lecteurs mappés – locaux ou distants – au sein du système infecté. Il se dupliquerait ensuite à des emplacements spécifiques de ces lecteurs puis définirait les attributs des fichiers afin que ces copies soient plus difficiles à localiser et à supprimer. Pour finir, il exécuterait dans ces lecteurs un fichier « autorun.inf » associé à une requête : tous les ordinateurs auxquels ils seront connectés à l'avenir devront exécuter ces programmes infectés.

EXPLOIT D'INFRASTRUCTURES D'AUTHENTIFICATION

Ce module tirerait parti des faiblesses connues des infrastructures d'authentification populaires utilisées par de nombreux réseaux d'entreprises. Il pourrait ensuite exploiter les informations d'identification pour donner l'accès à d'autres systèmes, parfois au niveau administrateur.

INFECTION DE L'INFRASTRUCTURE CONTRÔLE-COMMANDE (C&C) AVEC RAPPORT

Pour limiter le risque d'être découverts, les ransomwares nouvelle génération pourraient être configurés sans fonctionnalité contrôle-commande (C&C). Ce module transmettrait une balise avec identificateur global unique (GUID) à un domaine contrôle-commande (C&C) pour tenter de l'atteindre via des services et protocoles standard comme HTTP, HTTPS ou DNS et transmettre ainsi cette donnée. Le domaine pourrait alors collecter ces GUID pour obtenir des statistiques concernant le nombre de systèmes infectés et chiffrés au sein d'un réseau ciblé. Cette information permettrait aux hackers de déterminer l'efficacité de leur campagne.

LIMITEUR DE VITESSE DE TRANSMISSION

Ce module s'assurerait que le ransomware reste « poli » avec les ressources système afin que l'utilisateur soit moins susceptible de remarquer son exécution. Il garantirait une utilisation limitée du CPU et du réseau et veillerait à ce que le ransomware soit aussi discret que possible.

LIMITEUR AUX ADRESSES CIBLES RFC 1918

L'implant serait conçu pour attaquer et se greffer uniquement aux hôtes cibles possédant une adresse RFC 1918, ces adresses étant utilisées par les réseaux internes.

L'association d'une architecture soigneusement conçue et d'un système vigilant de gestion des mots de passe pourrait freiner le mouvement latéral des ransomwares à autopropagation de demain. Pour en savoir plus sur les solutions de défense contre les ransomwares nouvelle génération, veuillez consulter nos « Recommandations relatives à la sécurité », **page 52**.

Pour en savoir plus sur l'évolution des ransomwares et sur ce que les entreprises peuvent faire pour se préparer à faire face à ce type de menaces de nouvelle génération, consultez ce bulletin de blog Cisco Talos :

« Ransomware : Past, Present, and Future »

Vulnérabilités

Les vulnérabilités des systèmes font gagner du temps aux hackers, un avantage qu'ils utilisent pour lancer des campagnes avant que les acteurs de la sécurité aient pu corriger ces faiblesses. Par le biais de kits d'exploits, de ransomwares et de spams, les hackers exploitent les systèmes non corrigés et les équipements obsolètes pour atteindre leurs objectifs.

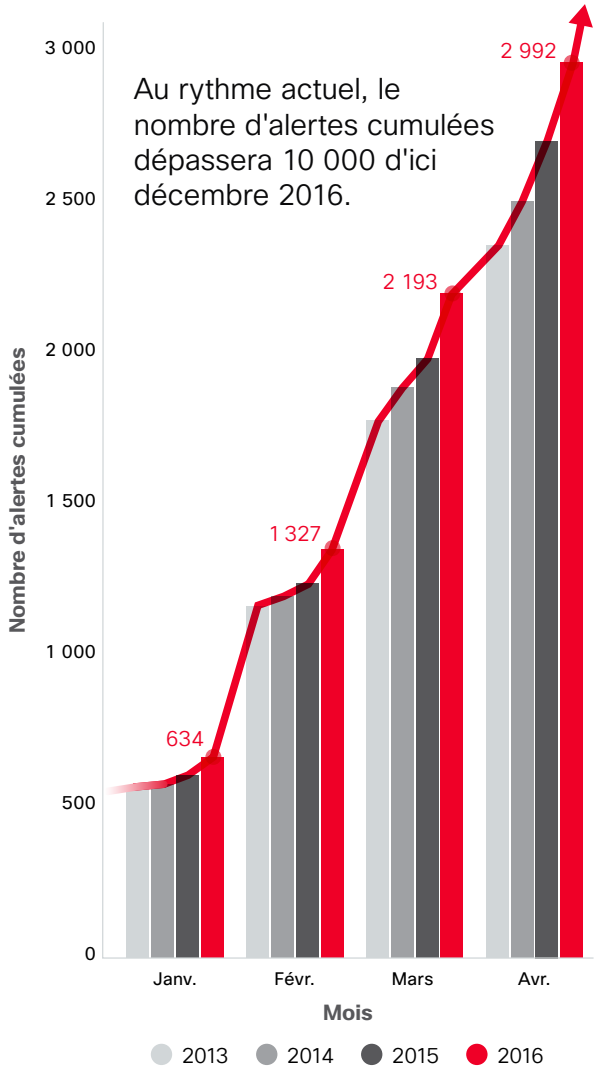
Les vulnérabilités dépendent des opportunités des hackers et de l'aptitude des défenseurs à protéger leur entreprise. Les défenseurs capables de fermer ces fenêtres d'opportunité en corrigeant les faiblesses de leurs systèmes sont en mesure de réduire la menace. Ceux qui ne font rien pour corriger ces faiblesses laissent aux hackers la liberté de les utiliser comme tremplins pour leurs campagnes.

Les prestataires accordent aujourd'hui plus d'attention à l'identification et la divulgation des vulnérabilités grâce à l'adoption de pratiques favorisant un cycle de vie de développement sécurisé (« secure development lifecycle » ou SDL). Mais comme expliqué à la **page 15**, les hackers portent également une attention particulière aux correctifs, les décomposant par rétroingénierie pour déterminer ce qui a été corrigé et développant de nouvelles approches basées sur ce qu'ils ont appris.

Les quatre premiers mois de l'année 2016 ont démontré une légère augmentation du nombre d'alertes annuelles cumulées par rapport au total des années précédentes sur la même période. Cette tendance s'explique probablement par les importantes mises à jour logicielles de fournisseurs comme Microsoft et Apple, le nombre accru de révisions du code, l'amélioration des outils de révision du code et l'adoption des pratiques SDL mentionnées plus haut (figure 1). Tous ces facteurs contribuent à l'identification accrue des vulnérabilités des produits.

Les acteurs de la sécurité perfectionnent et modernisent leurs processus pour combler les lacunes en divulguant et en corrigeant les vulnérabilités, mais les hackers rivalisent d'ingéniosité pour exploiter de nouveau ces lacunes et créer des attaques plus nombreuses et plus complexes qui entravent la capacité des professionnels de la sécurité à faire face. Les défenseurs doivent identifier et réduire à néant le champ d'action des hackers. Pour atteindre cet objectif, il est essentiel de corriger les vulnérabilités mises au jour et d'implémenter des systèmes de gestion des correctifs robustes.

Figure 1. Nombre total d'alertes annuelles cumulées



Source : Cisco Security Research

PARTAGER

« Les acteurs de la sécurité perfectionnent et modernisent leurs processus pour combler les lacunes en divulguant et en corrigeant les vulnérabilités, mais les hackers rivalisent d'ingéniosité pour exploiter de nouveau ces lacunes et créer des attaques plus nombreuses et plus complexes qui entravent la capacité des professionnels de la sécurité à faire face. »

DES CONNEXIONS SÉCURISÉES OFFRANT UNE FAUSSE IMPRESSION DE SÉCURITÉ

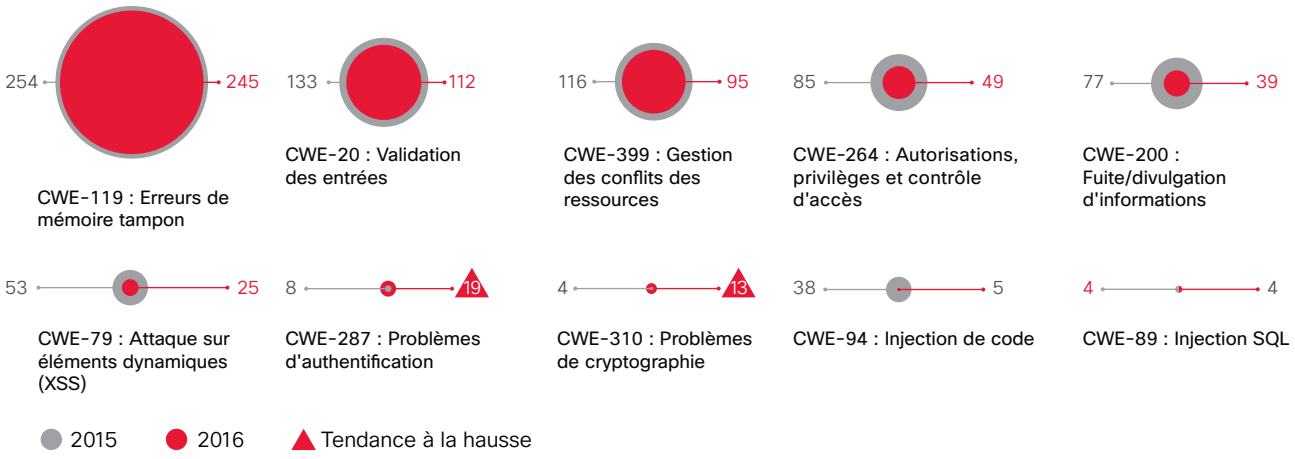
Les connexions sécurisées, comme celles créées par les connexions HTTPS et les certificats SSL, sont censées donner aux utilisateurs un sentiment de sécurité vis-à-vis de leurs activités en ligne. Pourtant, l'augmentation récente du nombre d'alertes liées au chiffrement et à l'authentification à de quoi inquiéter : elle laisse penser que les hackers sont en mesure de compromettre plus facilement les connexions sécurisées. Résultat : la sécurité des connexions est contestable.

Comme l'illustre ci-dessous (figure 2) le graphique listant les vulnérabilités fréquemment observées (CWE), les problèmes cryptographiques et d'authentification sont en augmentation depuis 2014 et 2015. Rien que sur la période décembre 2015-mars 2016, 19 problèmes d'authentification et 13 problèmes cryptographiques ont été identifiés, des chiffres proches du total des années précédentes.

L'utilisation croissante du chiffrement constitue une évolution positive car il contribue à protéger les informations des regards indiscrets. Il présente néanmoins d'un risque inhérent : en créant de la complexité, il génère de nouvelles vulnérabilités – tant au niveau des outils de chiffrement que de l'incapacité à satisfaire de manière certaine les attentes associées en matière de confidentialité. Si le chiffrement n'est pas effectué correctement, il n'offre aucune protection.

La mise en place de connexions sécurisées nécessite une chaîne complexe de processus et d'outils. Au-delà des certificats, cette chaîne est incertaine. Les appareils connectés à distance, via des passerelles VPN par exemple, ne sont pas forcément sécurisés. Par ailleurs, les sites web qui indiquent que les connexions sont sécurisées ont pu être compromis. Conclusion : les URL présentant l'icône de « verrouillage », que les observateurs peu attentifs considèrent comme l'assurance d'une activité sécurisée, ne doivent jamais être considérées comme sécurisées.

Figure 2 : Multiplication des problèmes cryptographiques et d'authentification, décembre-mars



Source : Cisco Security Research

La fenêtre d'action des hackers

La fenêtre d'action des hackers

L'augmentation des ransomwares et l'ampleur des campagnes récentes montrent à quel point les hackers profitent d'une fenêtre d'action illimitée. Ils ont le temps de préparer tranquillement leurs campagnes pour frapper quand ils sont prêts et parvenir à générer des revenus.

Pour cacher leur activité, ils utilisent les cryptomonnaies, le réseau ToR, le trafic HTTPS chiffré et le protocole TLS (Transport Layer Security). Parallèlement, les développeurs de kits d'exploits renforcent leur efficacité en décomposant les correctifs par rétroingénierie et en exploitant les vulnérabilités les plus difficiles à corriger. Enfin, avec les nouvelles formes de publicités malveillantes, les hackers disposent d'une méthode très performante et difficilement traçable pour augmenter le trafic vers les sites compromis, infecter les ordinateurs des utilisateurs et lancer des attaques de ransomwares.

Les vecteurs d'attaques côté client

Les cybercriminels ont toujours favorisé les attaques côté client car ils y trouvent davantage d'utilisateurs et que ces derniers sont toujours les plus faciles à pirater. En outre, les attaques côté client offrent aux cybercriminels de nombreuses opportunités d'élargir leur champ d'action. Les choix sont vastes.

Néanmoins, après plusieurs années de croissance, les attaques basées sur des vecteurs comme les fichiers PDF semblent s'être stabilisées. Dans le même temps, certains signes montrent que les hackers ont découvert de nouvelles opportunités côté serveur, où ils peuvent se déplacer d'un réseau à l'autre et gagner en force de frappe.

DES ATTAQUES PDF ET JAVA SUR LE DÉCLIN

La popularité des vecteurs d'attaque comme les PDF et Java continue à baisser. En janvier 2016, Oracle a annoncé l'interruption prochaine de son plug-in de navigateur Java, les fournisseurs de navigateurs prévoyant de mettre un terme à la prise en charge de ces plug-ins.[1] Oracle concentre désormais ses efforts sur sa technologie Java Web Start sans plugin.

Dans la mesure où le plug-in de navigateur Java va être abandonné, il sera de moins en moins utilisé comme vecteur d'attaque. Mais les experts en sécurité resteront attentifs et s'assureront que les cybercriminels ne font pas évoluer les anciennes menaces pour exploiter le nouvel outil Java. Les professionnels de la sécurité et les entreprises doivent envisager de bloquer Java, sauf lorsque les sites en ont absolument besoin.

[1] « Moving to a Plugin-Free Web », groupe responsable de la plate-forme Java, janvier 2016 : **https://blogs.oracle.com/java-platform-group/entry/moving_to_a_plugin_free**.

Quant aux attaques par PDF, même si elles diminuent également, elles sont toujours utilisées dans les e-mails. Elles consistent, par exemple, à convaincre les destinataires de cliquer sur des pièces jointes compromises. Les créateurs de spams utilisent la même tactique, en ajoutant un objet évoquant un sujet ou un événement d'actualité (reportez-vous à la **page 19** pour en savoir plus sur les spams).

Les développeurs de kits d'exploits utilisent toujours les technologies Flash, même si les contenus Flash sont de moins en moins utilisés en ligne. Cependant, un grand nombre d'applications en ligne, comme celles qui utilisent des contenus multimédias ou des publicités interactives, exploitent encore beaucoup les technologies Flash.

D'autres applications, telles que HTML5, commencent à être adoptées, mais la transition est progressive, d'où la poursuite de l'utilisation de Flash. Tant que les technologies Flash sont utilisées, elles restent un vecteur d'attaque.

LES VULNÉRABILITÉS FLASH, PRINCIPAL VECTEUR D'ATTAQUE DES KITS D'EXPLOITS

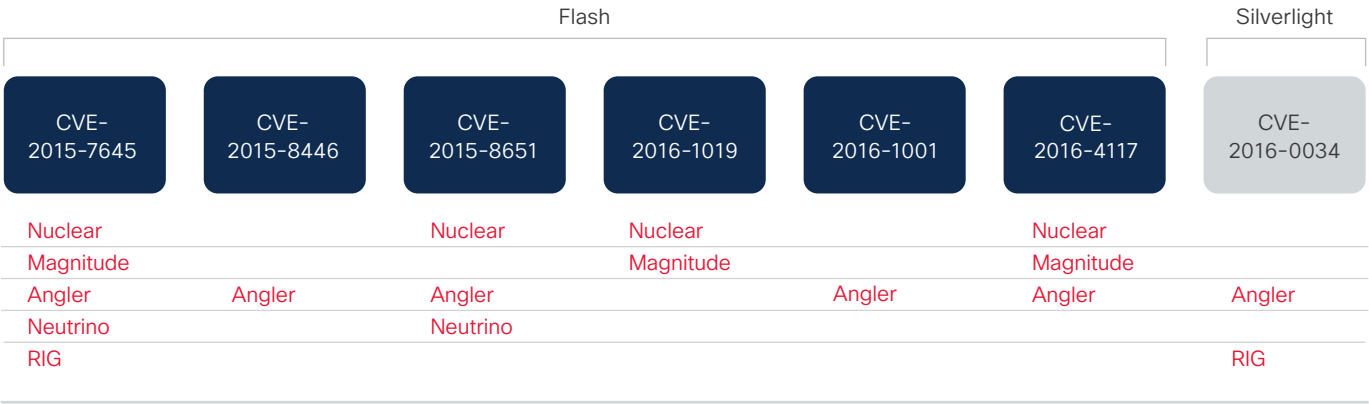
Les kits d'exploits, qui ont contribué à l'essor de la menace des ransomwares, continuent à exploiter les vulnérabilités d'Adobe Flash. Une étude récente menée par les experts de Cisco sur le kit d'exploit populaire Nuclear montre que la technologie Flash a été utilisée dans 80 % des tentatives d'attaque réussies.[2]

Même si Adobe répond à l'exposition fréquente des vulnérabilités par des correctifs, les cybercriminels sont aussi rapides à réagir. Dès qu'Adobe publie une mise à jour pour remédier à une vulnérabilité, les développeurs de kit d'exploit appliquent un outil de rétroingénierie au correctif pour découvrir ce qui a été corrigé. En une semaine au plus, les créateurs de l'exploit identifient et transforment les vulnérabilités du service Flash en armes qu'ils implémentent dans le code à distance.

Nous recommandons aux utilisateurs et aux administrateurs de désactiver ou de supprimer les plug-ins de navigateur inutiles pour réduire l'exposition aux menaces ou au moins de mettre leur logiciel Flash à niveau dès la publication des mises à jour.

La figure 3 souligne l'impact positif de l'installation des correctifs. Elle présente les différents kits d'exploits ayant incorporé les vulnérabilités du logiciel Flash et de Microsoft Silverlight. En installant les correctifs disponibles pour toutes ces vulnérabilités, les utilisateurs peuvent considérablement amortir l'impact des ransomwares propagés par les kits d'exploits.

Figure 3 : Les vulnérabilités utilisées par les kits d'exploits



Source : Cisco Security Research

PARTAGER

[2] « Threat Spotlight : Exploit Kit Goes International, Hits 150+ Countries », blog Cisco Talos, 20 avril 2016 : **http://blog.talosintel.com/2016/04/nuclear-exposed.html**.

Les kits d'exploits utilisent le réseau Tor pour masquer leurs communications

Les auteurs de kits d'exploits cherchent à contourner les systèmes de sécurité et font preuve d'une créativité débordante. À titre d'exemple, nous nous sommes récemment intéressés au kit d'exploit Nuclear. Ce kit, qui propage généralement des variantes de ransomware, a été observé en train de fournir une version de Tor, le logiciel utilisé pour les communications anonymes. Cette tactique semble rendre anonymes les éventuelles données utiles malveillantes, ce qui complique le suivi des activités pour les acteurs de la sécurité.

En général, lorsqu'un kit d'exploit diffuse un fichier malveillant, vous pouvez le détecter en surveillant le trafic de commande-contrôle en résultant, c'est-à-dire quand le programme malveillant « contacte sa base ». Cependant, nous avons remarqué que le kit d'exploit Nuclear a d'abord propagé un fichier exécutable Tor, puis a émis des demandes de communications via Tor. Tor étant un protocole de routage entièrement chiffré, les professionnels de la sécurité ne peuvent pas voir ce que le malware y fait.

Le ransomware fourni par des kits d'exploits est devenu une source de revenus considérable pour ses créateurs. (Reportez-vous à la section « Ransomwares : des attaques très rentables et difficiles à contrer », **page 7**.) Il est donc logique que les développeurs de ransomwares cherchent à les rendre encore plus efficaces et essaient de se démarquer des autres kits d'exploits. L'utilisation de Tor dans le kit d'exploit Nuclear est le signe d'une autre évolution intelligente proposée par les développeurs de malwares.

Consultez ce **bulletin du blog Cisco Talos** pour en savoir plus sur l'utilisation de Tor dans le kit d'exploit Nuclear.

L'ESSOR DES CAMPAGNES D'ATTAQUES AXÉES SUR LES SERVEURS

Les cybercriminels veulent tirer un maximum de profit de leurs campagnes. La propagation des malwares ou des kits d'exploits vers les clients ou les utilisateurs est efficace, mais ce type d'attaque a un impact limité. Les hackers ne peuvent pas amasser autant de bande passante et de fonctionnalités qu'ils le souhaitent en cas d'attaques côté client.

Ils ont compris qu'ils tireraient plus de profit de leurs efforts en étendant leurs campagnes aux attaques côté serveur. Ainsi, ils ont récemment utilisé la plate-forme applicative professionnelle JBoss pour accéder aux réseaux et distribuer SamSam, une variante de ransomware (voir **page 7**). Dans les cas étudiés par les experts de Cisco, les cybercriminels ont utilisé JexBoss, un outil open source, pour analyser et exploiter les serveurs d'applications JBoss, et s'introduire dans les réseaux des organismes de santé. Une fois entrés dans le réseau, ils ont pu chiffrer les fichiers Windows en utilisant SamSam.

En ciblant les vulnérabilités des serveurs pour propager les ransomwares, cette menace déjà pesante a pris une dimension supplémentaire. En analysant des ordinateurs en ligne, les experts de Cisco ont découvert que certains d'entre eux étaient déjà infectés et en attente d'exécution d'un ransomware. Cisco a en outre découvert l'installation de 2 000 portes dérobées sur 1 600 adresses IP. La plupart de ces portes dérobées avaient été installées dans les systèmes exploitant un outil de gestion commune des bibliothèques scolaires. Contacté par Cisco, le développeur de ce logiciel a agi rapidement et publié le correctif nécessaire.

En s'appuyant sur les vulnérabilités des systèmes côté serveur, les cybercriminels ont élargi leur terrain de jeu. Limiter les dégâts qu'ils causent nécessite désormais beaucoup plus de temps et d'efforts. Les applications côté client, par exemple les navigateurs web, sont de plus en plus souvent corrigées par des mises à jour automatiques, les rendant moins sujettes aux vulnérabilités.

D'un autre côté, les applications côté serveur sont souvent dépassées, dans la mesure où les correctifs et les mises à niveau peuvent être appliqués uniquement pendant les heures ouvrées de l'équipe informatique. Il est difficile de mettre à niveau ces systèmes sans aucun impact sur les opérations. En outre, la porosité du périmètre réseau permet aux cybercriminels d'accéder aux serveurs dont la sécurité reposait auparavant sur ce périmètre.

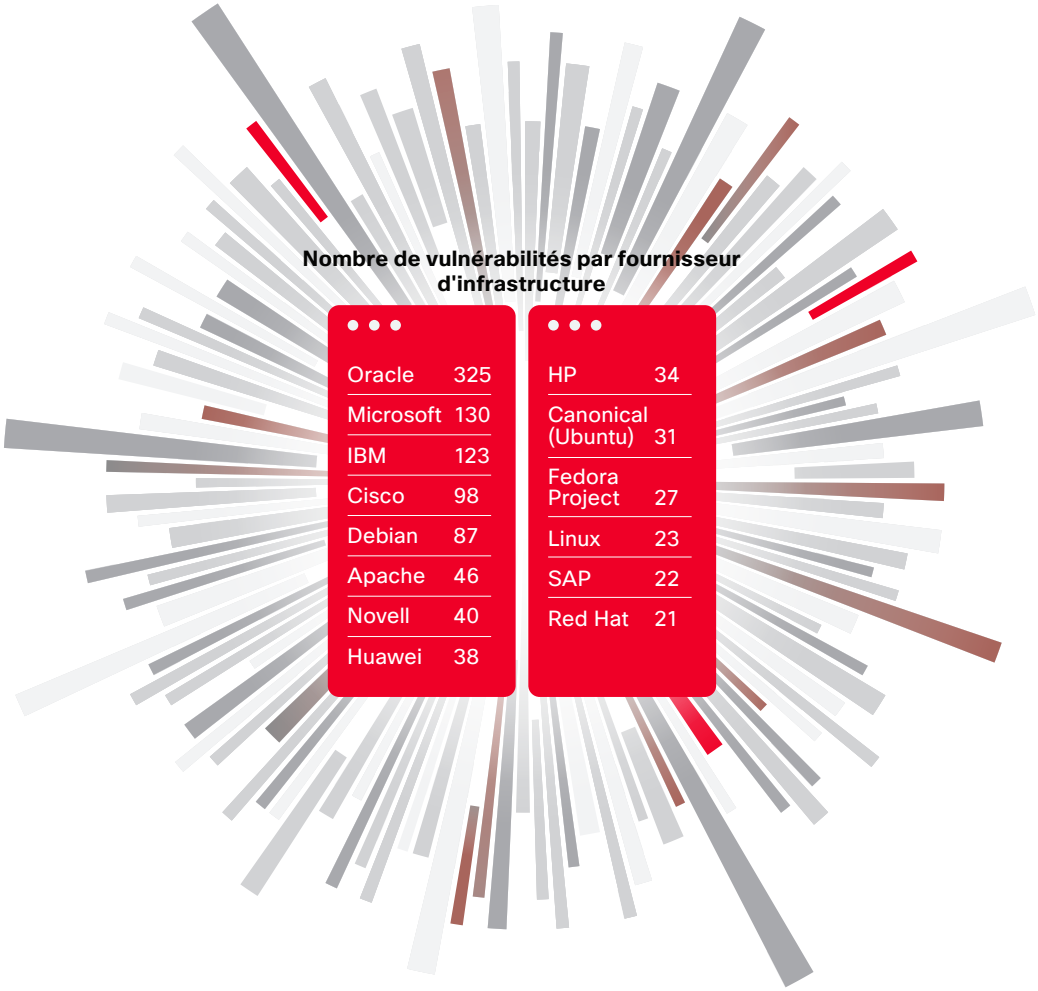
Comme le montre la figure 4, la majorité des produits des principaux fournisseurs d'infrastructure présente des vulnérabilités côté client et côté serveur.

Consultez ces bulletins du blog Cisco Talos pour en savoir plus sur les dangers des vulnérabilités dans les solutions de serveurs :

« Widespread JBoss Backdoors a Major Threat »

« SamSam : The Doctor Will See You, After He Pays the Ransom »

Figure 4 : Les vulnérabilités par fournisseur d'infrastructure, 1er janvier–30 mars 2016



Source : Cisco Security Research

PLATE-FORME JBOSS : DES VULNÉRABILITÉS AU NIVEAU DE L'INFRASTRUCTURE ÉLARGISSENT LA FENÊTRE D'ACTION DES CYBERCRIMINELS

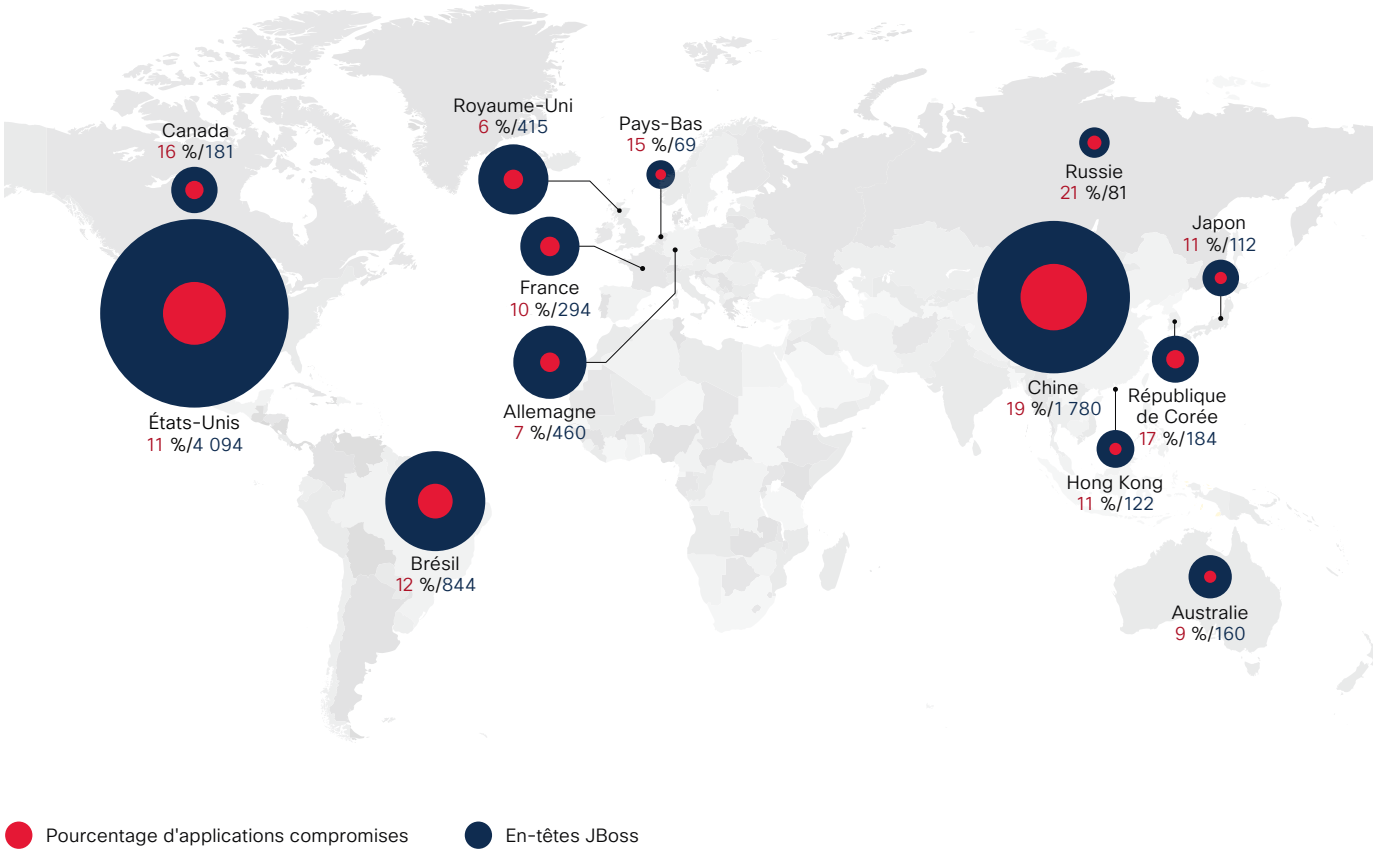
Les créateurs de ransomwares ont gagné un avantage dans leurs campagnes en utilisant le logiciel d'applications professionnelles JBoss. Comme nous l'avons constaté dans une campagne récente de ransomwares visant des organismes de santé (**page 7**), les vulnérabilités de JBoss permettent aux cybercriminels de s'introduire sur les réseaux et de gagner du temps pour collecter des données ou activer un malware. Les attaques activées via JBoss sont une preuve de plus que la maintenance des réseaux, si elle n'est pas faite correctement, offre un accès aux cybercriminels. Mais cet accès peut être bloqué.

Les experts de Cisco ont constaté que les attaques via JBoss ont ouvert des voies au sein des serveurs, les rendant vulnérables aux attaques. Lors de notre analyse d'Internet :

- Nous avons recherché des serveurs signalant l'installation de JBoss dans les en-têtes HTTP ou le contenu de la page.
- Nous avons ensuite recherché la présence de portes dérobées, de shells web ou d'autres attaques.jsp sur les hôtes.

La figure 5 montre le pourcentage des serveurs semblant avoir été compromis par rapport au nombre de serveurs signalant l'installation de JBoss. Aux États-Unis, par exemple, 11 % des shells web observés montrent des signes de corruption.

Figure 5 : La présence de shells web est signe d'une compromission des applications JBoss



Source : Cisco Security Research

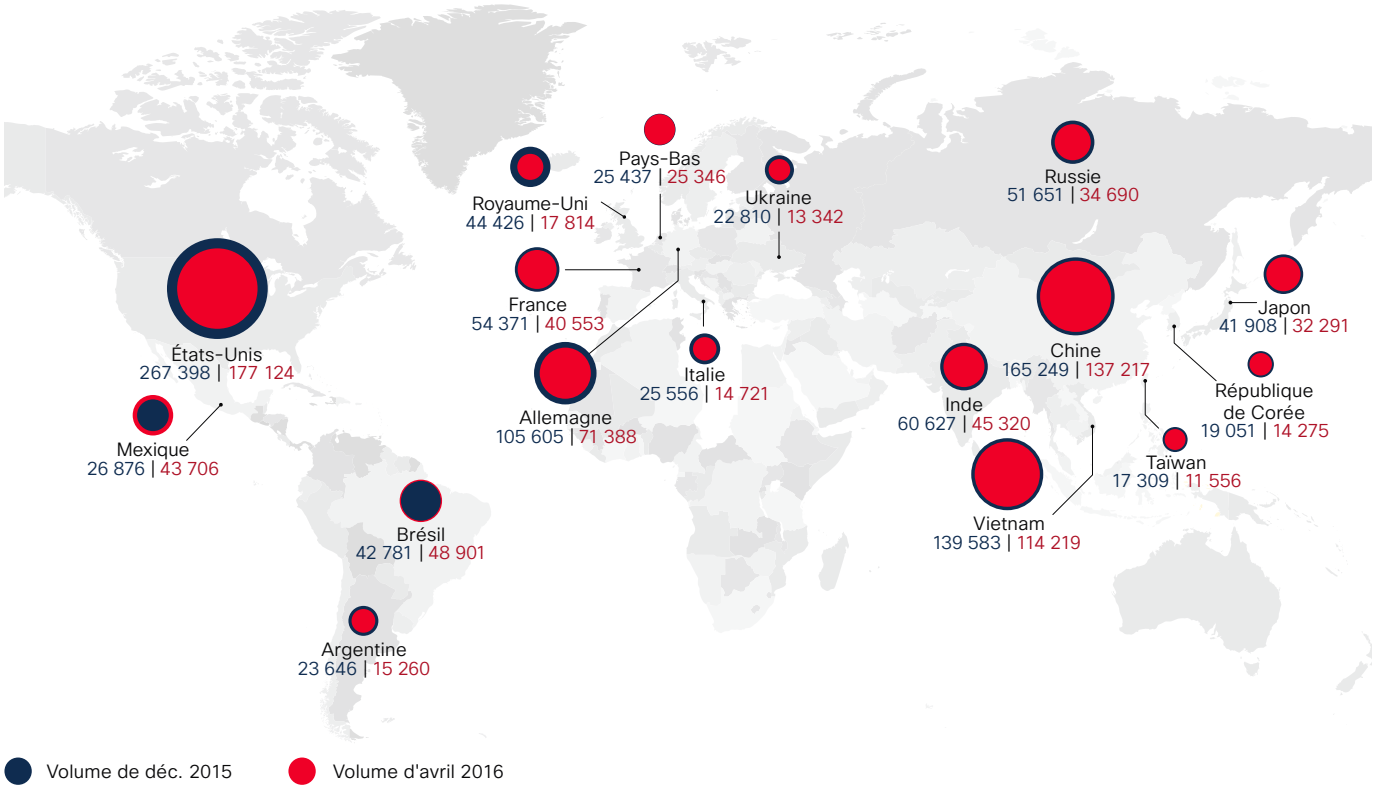
UN VOLUME DE SPAMS RELATIVEMENT STABLE À L'ÉCHELLE MONDIALE

Pour mesurer le trafic de spams dans le monde, Cisco collecte des exemples sur ses appliances de messagerie, en indiquant l'impact des décisions des règles codées dans les appliances de messagerie et les passerelles (par exemple, les e-mails bloqués ou marqués comme inconnus). Les spams sont souvent utilisés comme vecteurs d'attaque, en particulier pour les ransomwares.

D'après l'étude menée par Cisco sur le trafic des e-mails, le volume de spams est resté stable entre décembre 2015 et mai 2016 (figure 6). Au Brésil, le trafic de spams a atteint des pics en janvier et en mars 2016. Ces augmentations peuvent être dues à l'activité d'un botnet de spams à ces périodes.

Comme expliqué dans la section sur l'activité régionale de blocage de sites web (voir **page 47**), les cybercriminels changent souvent de pays et de fournisseur d'hôte, au gré des environnements accueillants trouvés pour lancer leurs attaques. Les spammeurs utilisent des ordinateurs botnets appartenant aux hôtes fiables au sein desquels ils sont regroupés. Ils les utilisent jusqu'à ce qu'ils soient repérés par les systèmes de détection, puis passent à un autre botnet.

Figure 6 : Le volume de courriers indésirables par pays, décembre 2015-mai 2016



Source : Cisco Security Research

PARTAGER

Figure 7 : Les sujets populaires des courriers indésirables qui utilisent le piratage psychologique

Nombre de versions	URL	Type de message	Langue	publication (heure GMT)
95	RuleID4626	Facture, paiement	Allemand, anglais	3.18.16
82	RuleID4400KVR	Bon de commande	Anglais	2.1.16
64	RuleID4626(cont)	Facture, paiement, confirmation d'expédition	Anglais, allemand, espagnol	1.28.16
62	RuleID4961KVR	Paiement, transfert, commande, expédition	Anglais	3.25.16
58	RuleID4961KVR	Demande de devis, commande de produit	Anglais, allemand et plusieurs autres langues	1.25.16
52	RuleID5118KVR	Commande de produit, paiement	Allemand, anglais	3.17.16
49	RuleID858KVR	Devis d'expédition, paiement	Anglais	3.14.16
47	RuleID4961	Transfert, expédition, facture	Anglais, allemand, espagnol	2.22.16
44	RuleID4627 et RuleID4627KVR	Billet d'avion électronique	Anglais	3.29.16
30	RuleID8337KVR	Commande, paiement, devis	Anglais	1.21.16

Source : Cisco Security Research

Grâce à des techniques intelligentes d'ingénierie sociale, les créateurs de spams parviennent toujours à convaincre certains utilisateurs de cliquer sur les pièces jointes (comme les PDF infectés par un malware, voir **page 15**) ou sur des liens dans les messages. Comme le montre la figure 7, les créateurs de spams créent des pièces jointes ou des liens contenant soi-disant des informations essentielles comme des factures, des modalités de voyage ou des devis. Les spammeurs créent également des versions de leurs messages dans d'autres langues pour piéger plus de victimes.

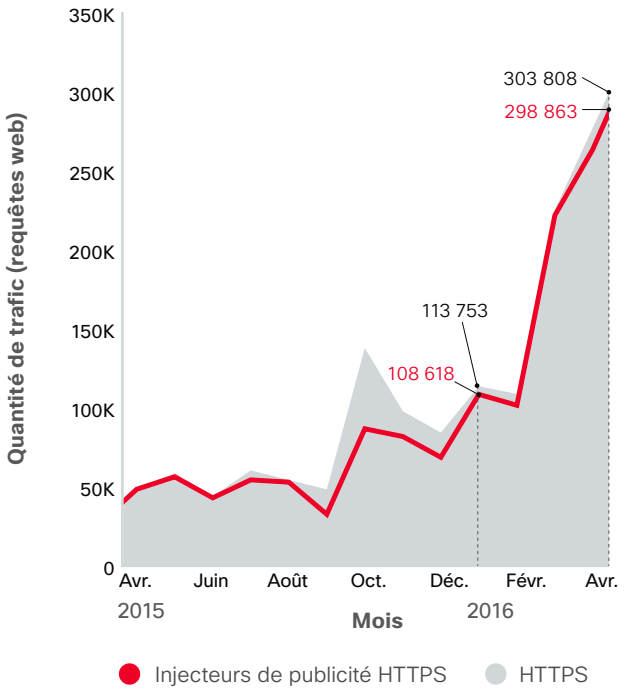
LE RETOUR DES LISTES NOIRES ? L'UTILISATION DU PROTOCOLE HTTPS PAR LES HACKERS COMPLIQUE LE TRAVAIL DES ACTEURS DE LA SÉCURITÉ

Lorsque les injecteurs de publicités propagent des publicités malveillantes en utilisant le trafic HTTPS chiffré, les utilisateurs et les équipes de sécurité ne peuvent pas se baser sur les informations envoyées via l'URL pour identifier la menace potentielle. Sachant cela, les hackers utilisent de plus en plus le trafic HTTPS chiffré pour masquer leur activité sur le web et élargir leur fenêtre d'action.

Entre septembre 2015 et mars 2016, les experts Cisco ont constaté une multiplication par cinq du trafic HTTPS associé aux activités malveillantes. Nous avons identifié cette tendance de l'utilisation du protocole HTTPS après avoir suivi 80 campagnes malveillantes réparties dans 8 catégories de menace sur une période de 16 mois. D'après notre étude, l'augmentation du trafic HTTPS peut être attribuée principalement aux injecteurs de publicités et aux logiciels publicitaires (figure 8).

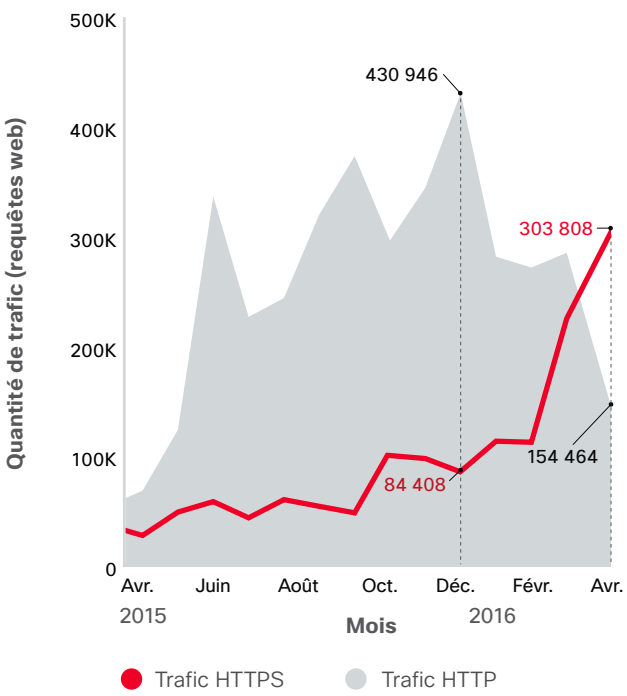
Nous avons également constaté que le trafic HTTPS associé aux injecteurs de publicités a augmenté de 300 % entre décembre 2015 et avril 2016 (figure 9).

Figure 8 : Les injecteurs de publicités expliquent la forte hausse de l'utilisation de HTTPS



Source : Cisco Security Research

Figure 9 : Le trafic HTTPS a augmenté de 300 % pour les injecteurs de publicités sur 4 mois



Source : Cisco Security Research

Les injecteurs de publicités malveillantes sont l'un des composants majeurs des infections par logiciels publicitaires (figure 10). Les cybercriminels s'appuient sur ces extensions de navigateur pour injecter des publicités frauduleuses sur les pages web, et présentent aux utilisateurs des publicités et des fenêtres contextuelles qui facilitent les campagnes de ransomwares et d'autres malwares. Les publicités malveillantes et les injecteurs de publicités malveillantes se trouvent dans une partie de l'écosystème de publicité où il est parfois difficile de distinguer un comportement normal d'une activité malveillante.

Les infections par injecteur de publicités et logiciels publicitaires ne doivent pas être ignorées. Cette année, les experts en sécurité de Cisco ont trouvé une nouvelle version du cheval de Troie DNSChanger propagée par un logiciel publicitaire. Ce développement augmente les risques associés aux infections par injecteurs de publicités et logiciels de publicités pour les utilisateurs et les entreprises.[3]

Nous avons également trouvé des preuves attestant que les hackers transmettent désormais les malwares via HTTPS. Cette évolution est moins rapide que celle observée pour les injecteurs de publicités. Cela est probablement dû au fait que les hackers cherchent à optimiser leurs revenus et n'apportent donc des modifications à l'infrastructure que lorsque cela est nécessaire.

Ironiquement, en repoussant ces mises à jour d'infrastructure, les cybercriminels reproduisent la même tendance que dans les entreprises légitimes. En effet, de nombreuses entreprises ont renoncé (souvent pendant plusieurs années) à appliquer les correctifs des vulnérabilités connues dans leur infrastructure Internet car elles craignaient une perte de revenus liée à la mise hors ligne des appareils et des logiciels lors des mises à niveau. (Voir « Infrastructure vieillissante : des vulnérabilités de longue date à corriger d'urgence pour faire face à l'essor des ransomwares », **page 30**). La difficulté d'appliquer des correctifs à un grand nombre d'hôtes infectés encourage sans aucun doute également les hackers à garder leur technologie existante opérationnelle.

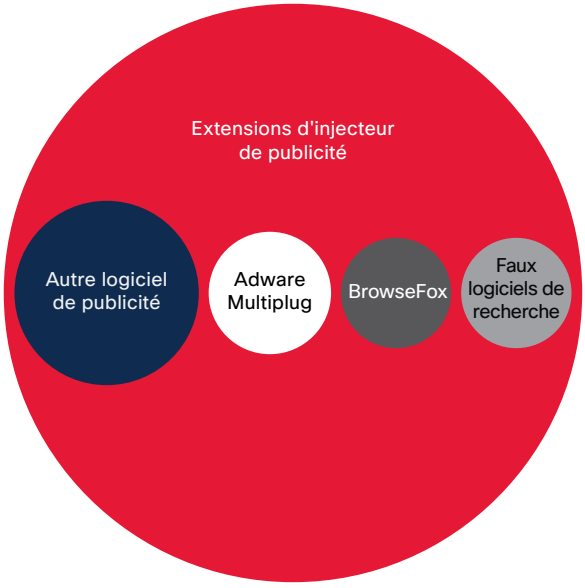
Au cours de nos 16 mois d'analyse, nous avons observé que les familles de malwares suivantes augmentaient leur utilisation du protocole HTTPS :

- Gamarue/Andromeda, un botnet polyvalent
- Necurs, un botnet volant des informations
- Miuref/Boaxxe, un botnet de fraude par clic
- Ramdo/Redyms, un botnet de fraude par clic
- Chevaux de Troie d'exfiltration des données

La croissance du trafic HTTPS chiffré lié à l'activité malveillante est préoccupante, dans la mesure où elle crée des défis importants pour les experts en sécurité qui suivent et étudient les campagnes de malwares. Les techniques utilisées par les acteurs de la sécurité pour identifier les menaces du trafic HTTP, telles que les systèmes de détection d'intrusion (IDS) par signatures reposant sur des modèles d'URL, ne peuvent pas être appliquées au trafic HTTPS sans ajouter des fonctionnalités d'inspection SSL. Dans de nombreux cas, les experts en sécurité ont seulement un nom de domaine ou une adresse IP comme point de départ pour leurs recherches.

La classification des menaces devient également difficile, dans la mesure où les menaces partagent souvent l'infrastructure. Pour remédier à cela, les acteurs de la sécurité utilisent parfois des listes noires (listes de tous les malwares connus), mais cette méthode est sujette à des erreurs et n'est pas suffisamment précise pour être efficace. Elle prend également beaucoup de temps, car les analystes recherchent et classent manuellement les menaces.

Figure 10 : Les injecteurs de publicités sont fréquemment en cause dans les infections par logiciels publicitaires



Source : Cisco Security Research

[3] « DNSChanger Outbreak Linked to Adware Install Base », blog sur la sécurité Cisco, février 2016 : **http://blogs.cisco.com/security/dnschanger-outbreak-linked-to-adware-install-base**.

PUBLICITÉ MALVEILLANTE EN TANT QUE SERVICE : DES ATTAQUES ULTRAEFFICACES

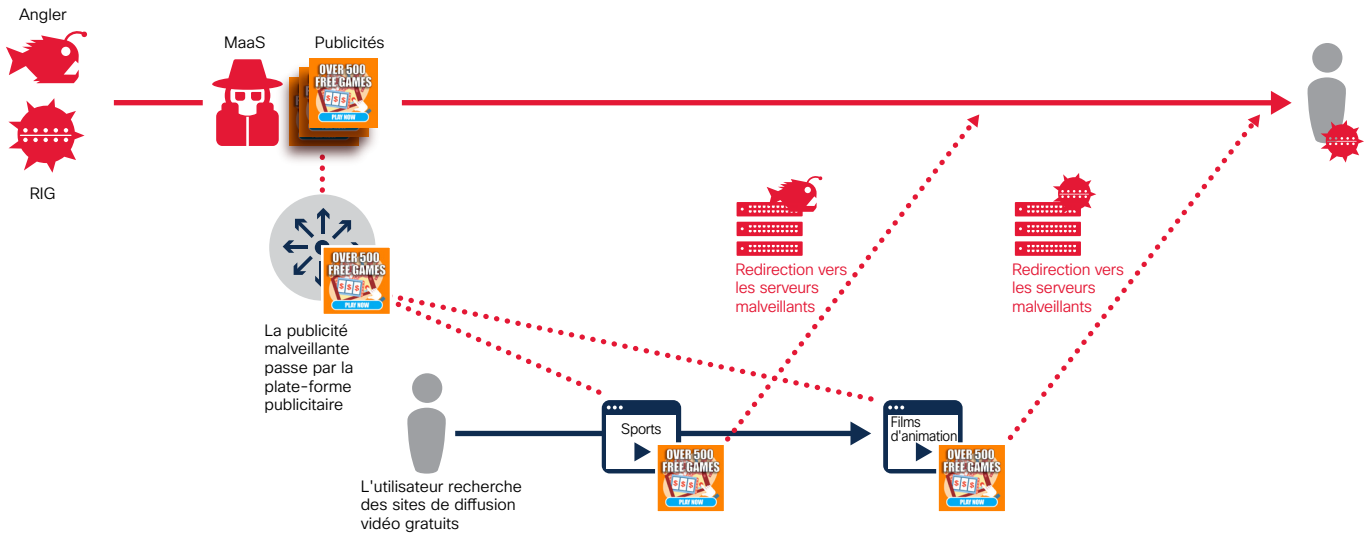
Les agences de publicité, sciemment ou non, favorisent les publicités malveillantes sur le web, notamment en permettant aux hackers d'adopter un nouveau modèle économique : les « publicités malveillantes en tant que service ». Les cybercriminels achètent des espaces publicitaires sur des sites web légitimes populaires pour transmettre les publicités malveillantes. Pour les acteurs de la sécurité, cela crée de nouveaux défis, en plus de soulever des questions concernant les personnes responsables de la protection des utilisateurs contre les publicités malveillantes.

En achetant des espaces publicitaires légitimes, les hackers peuvent facilement distribuer les menaces sur des sites non associés. Les publicités s'affichent seulement un court instant, laissant peu, voire pas de temps aux acteurs de la sécurité pour identifier la présence d'une menace. Dans la mesure où les agences de publicité utilisent des informations comme les types et les versions des navigateurs des utilisateurs, les hackers peuvent plus facilement et précisément cibler des groupes d'utilisateurs, y compris au niveau de la langue.

La tendance des publicités malveillantes en tant que service est similaire au squattage de domaine. Les squatteurs de domaine tirent profit de la vente ou de l'utilisation de noms de domaine que des utilisateurs souhaitent associer à des entreprises légitimes et à des marques connues. En redirigeant le trafic à partir de ces domaines, ils simplifient la distribution des malwares sans jouer un rôle direct dans la livraison des menaces.

L'activation des bloqueurs de publicité est une stratégie logique pour éviter l'exposition aux publicités malveillantes, en particulier la nouvelle variété que nous avons découverte. Celle-ci ne nécessite pas d'interaction de l'utilisateur pour infecter les machines et exécuter une charge. Toutefois, les principaux fournisseurs de contenus en ligne (dont les revenus reposent principalement sur les publicités numériques) exigent que les utilisateurs désactivent les bloqueurs de publicités pour afficher d'autres contenus sur le site. Cela crée bien évidemment un risque pour les utilisateurs, ainsi qu'un dilemme pour les équipes de sécurité, qui doivent décider de bloquer ou non les sites qui utilisent des publicités à partir d'une plate-forme de vente et d'achat d'espaces publicitaires.

Figure 11 : Le fonctionnement des publicités malveillantes en tant que service (MaaS)



Source : Cisco Security Research

Niveaux de redirection multiples

Les experts de Cisco ont observé que les cybercriminels achètent des espaces publicitaires pour propager des publicités malveillantes qui infectent directement les ordinateurs des utilisateurs ou redirigent ces derniers vers un autre emplacement pour exécuter la charge du malware. Généralement, les niveaux de redirection sont multiples. Mais parfois les utilisateurs n'ont même pas besoin d'interagir avec la publicité malveillante pour que leur ordinateur soit infecté. Tout se déroule en arrière-plan, complètement hors de leur vue.

Une campagne de publicités malveillantes en tant que service, apparue pour la première fois en octobre 2015, redirigeait les utilisateurs vers plusieurs kits d'exploits, notamment Angler et RIG, qui exécutaient différentes charges utiles. La plupart des charges utiles étaient des variantes de ransomwares comme TeslaCrypt et CryptoWall. Les utilisateurs étaient trompés par une publicité prétendant promouvoir un site de paris en ligne. Un lien vers JavaScript était dissimulé dans le code de la publicité. Ce lien dirigeait les utilisateurs vers une page web Angler, mais il y avait également d'autres redirections, y compris des iFrame.

L'émergence de cette nouvelle approche de la distribution de publicités malveillantes indique que l'économie parallèle est de plus en plus industrialisée. Les experts de Cisco s'attendent à ce que les publicités malveillantes en tant que service se développent, dans la mesure où les cybercriminels recherchent des moyens efficaces d'infecter un grand nombre d'utilisateurs web via des sites légitimes et d'échapper à la détection. Les publicités malveillantes jouent un rôle central. Elles aident les hackers à exécuter des campagnes de ransomwares, qui sont en train de devenir leur méthode d'attaque privilégiée en raison de leur forte rentabilité. (Reportez-vous à la section « Ransomwares : des attaques très rentables et difficiles à contrer », **page 7**.)

Pour en savoir plus sur la nouvelle tendance MaaS (publicités malveillantes en tant que service), consultez le bulletin du blog Cisco Talos suivant :

« Threat Spotlight : Spin to Win ... Malware »

« Les experts Cisco pensent que la tendance des publicités malveillantes en tant que service va continuer de se développer, ceci dans la mesure où les cybercriminels recherchent des moyens efficaces d'infecter un grand nombre d'utilisateurs web via des sites légitimes et d'échapper à la détection. »

MÉTHODES D'ATTAQUE WEB : DES RANSOMWARES EN PLEINE EXPANSION

Au premier semestre 2016, certaines tendances des méthodes d'attaque sur le web sont en rapport avec la croissance exponentielle des ransomwares. Par exemple, les binaires suspects Windows, qui se trouvent en haut de la liste dans la figure 12, sont utilisés par les hackers pour propager des menaces comme des logiciels espions et des logiciels publicitaires. Ces outils leur permettent de s'introduire dans l'infrastructure de réseau pour lancer des attaques telles que des ransomwares.

Les escroqueries via Facebook (ingénierie sociale), les chevaux de Troie et les iFrame restent des outils couramment utilisés pour obtenir l'accès initial aux ordinateurs des utilisateurs et aux réseaux des entreprises.

Les escroqueries via Facebook ont été la méthode d'attaque sur le web la plus populaire au 2e semestre 2015, comme indiqué dans notre dernier rapport sur la cybersécurité. Les fichiers binaires Windows sont en 4e position sur cette liste. Le malware JavaScript, qui occupait les trois premières places de notre classement précédent, n'apparaît même plus dans les 10 premières.

Cependant, il n'a pas du tout disparu. En fait, ce type de malware a joué un rôle essentiel dans de nombreuses campagnes de ransomwares cette année.

La liste de la figure 13 présente les malwares les moins fréquemment rencontrés et souvent les plus dissimulés dans la chaîne d'infection.

Dans la figure 13, la dernière partie du diagramme montre un exemple de présence de signatures de ransomwares, de chevaux de Troie et de droppers (injecteurs). En raison de l'utilisation croissante des ransomwares par les hackers, nous observons plus fréquemment des composants d'infrastructure pour ransomwares que des malwares volant des informations.

Figure 12 : Logiciels malveillants les plus couramment observés

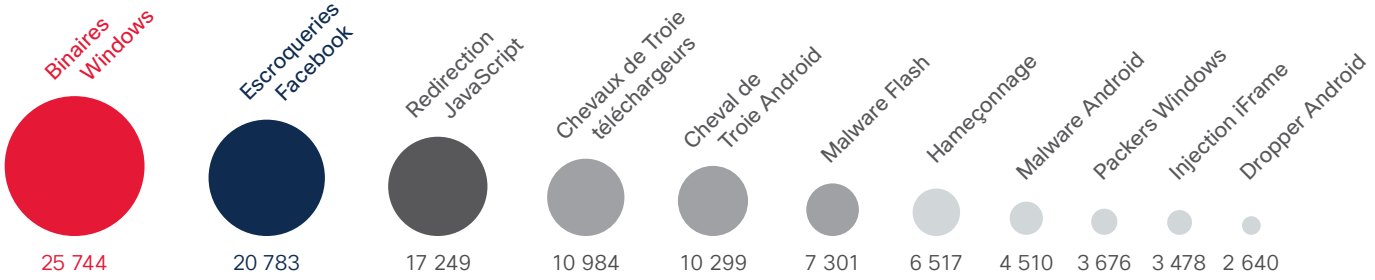
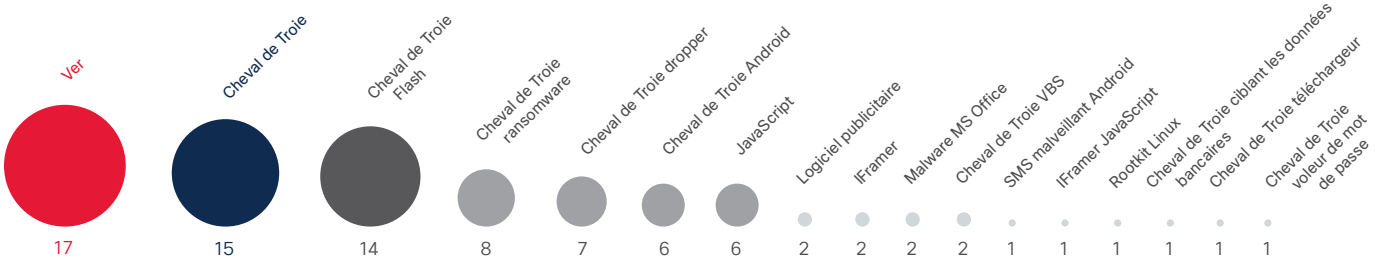


Figure 13 : Méthodes d'attaque de plus faible volume observées



Source : Cisco Security Research

Les défis en matière de sécurité

Les défis en matière de sécurité

Même si les acteurs de la sécurité innovent constamment, l'infrastructure sur laquelle repose l'économie numérique reste fragile. Elle est aussi dépendante de pratiques de sécurité inadéquates. Aujourd'hui, en raison de la variété de navigateurs web, d'applications et d'infrastructures présents dans la plupart des entreprises, il existe de nombreux points d'entrée pour les hackers.

Ces appareils et logiciels peu protégés offrent un champ d'action aux hackers que les professionnels doivent éliminer. La réduction du champ d'action des hackers et la détection de la présence de cybercriminels sont les principales tâches.

Correctifs : le décalage entre la mise à disposition et la mise en œuvre des correctifs et des mises à niveau multiplie les failles de sécurité

Ces dernières années, les principaux fournisseurs sont devenus plus proactifs, livrant les correctifs de plus en plus tôt après la révélation des vulnérabilités et des exploits. Ils coopèrent également avec les experts en sécurité qui ont identifié ces vulnérabilités. En fait, d'après une étude de Cisco portant sur l'examen de milliers de failles et vulnérabilités courantes (CVE), le délai médian entre la révélation publique des vulnérabilités et la disponibilité des correctifs est de moins d'un jour pour les principaux fournisseurs de logiciels de terminaux. En d'autres termes, lorsqu'une vulnérabilité est révélée publiquement, un correctif est également proposé. Les fournisseurs coordonnent donc ces révélations.

Cependant, toujours selon l'étude de Cisco, en dépit de la disponibilité rapide des correctifs, de nombreux utilisateurs ne les téléchargent pas et ne les installent pas en temps voulu. Le décalage entre la disponibilité et la mise en œuvre effective des correctifs offre aux cybercriminels l'opportunité de lancer des attaques, leur laissant une fenêtre d'action suffisante au sein du réseau alors que la simple application d'un correctif logiciel aurait pu les bloquer. Les hackers peuvent exploiter les vulnérabilités avant même qu'elles soient publiquement révélées. Par conséquent, pour une bonne protection, il est essentiel de ne laisser aucun délai entre la disponibilité des correctifs et l'installation.

Pour ce faire, les fournisseurs ont adopté différents types de fonctionnalités de mise à jour automatique de leurs produits. Il peut s'agir aussi bien de contrôles périodiques avec notifications à l'intention de l'utilisateur que de mises à jour en arrière-plan que l'utilisateur peut accepter ou refuser, mais qui sont de plus en plus difficiles à désactiver.

En fonction de la politique de mise à jour automatique en place, les utilisateurs peuvent choisir de différer cette mise à jour jusqu'à un moment plus pratique ou bien d'ignorer complètement la mise à jour. En étudiant les installations de logiciels de navigateurs sur les terminaux utilisés par les clients de Cisco, nous avons pu constater l'utilité des mises à jour automatiques. L'examen de l'installation du navigateur web Google Chrome, qui a mis en place une politique forte de désactivation, montre que la plupart des utilisateurs (60 à 85 % de la base d'utilisateurs à mesure que la politique de mise à jour automatique progresse) exécutent la dernière version du logiciel. Cela démontre l'intérêt des mises à jour automatiques.

75 à 80 % des utilisateurs utilisent au minimum la nouvelle version du navigateur ou la version précédente (figure 14). Google complique de plus en plus l'exécution des anciennes versions de son navigateur : pour désactiver les mises à jour automatiques, il faut disposer d'un accès administrateur. En outre, le fournisseur n'autorise pas le téléchargement des anciennes versions à partir de son site ou d'autres sites.

Les politiques de mise à jour automatique influencent considérablement la version exécutée par les utilisateurs, contrairement à la simple existence de mises à jour automatiques. Tous les logiciels examinés par Cisco utilisent un système pour les mises à jour automatiques, sauf si l'utilisateur a volontairement désactivé le processus. Il peut s'agir de fenêtres de notification pour l'utilisateur ou d'exécutions automatiques silencieuses, par exemple. Plus la politique est stricte, plus le comportement souhaité devient visible.

Figure 14 : Les installations Chrome par version (pour les 50 % d'utilisateurs les plus actifs)

Remarque : les graphiques relatifs au délai de correction dans cette section présentent les résultats des 50 % d'utilisateurs les plus actifs que nous avons étudiés. En nous intéressant à une majorité de la population, il est plus facile de savoir si les mises à jour atteignent l'objectif visé ou s'il reste d'autres obstacles à lever pour protéger les clients.

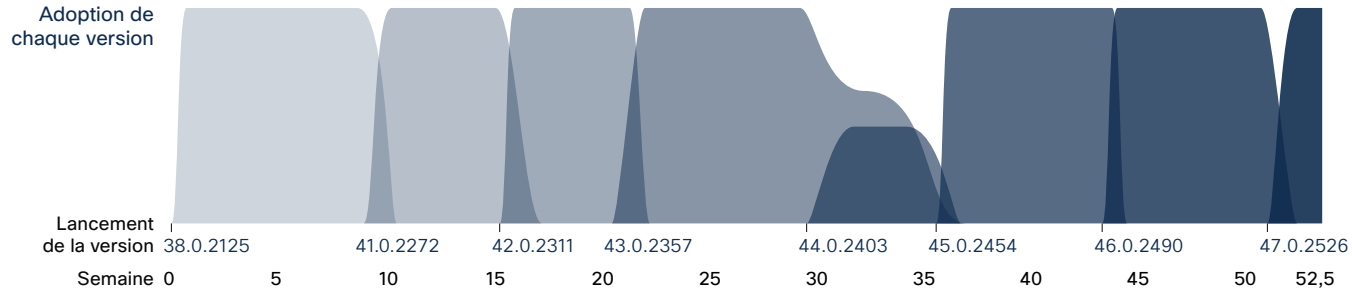


Figure 15 : Les installations Java par version (pour les 50 % d'utilisateurs les plus actifs)

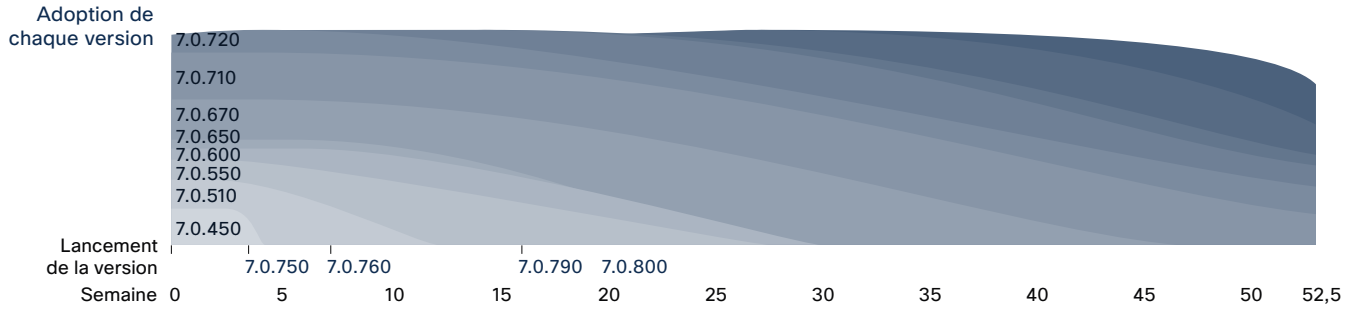
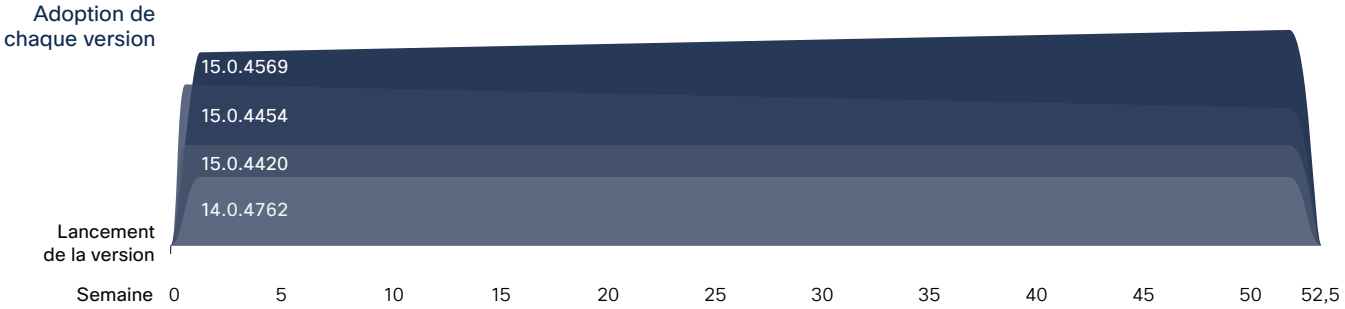


Figure 16 : Les installations de Microsoft Office par version (pour les 50 % d'utilisateurs les plus actifs)



Source : Cisco Security Research

En examinant les logiciels plutôt que les navigateurs, nous avons observé l'impact de l'absence de politique de mise à jour automatique. En étudiant les installations du logiciel Java sur les terminaux utilisés par les clients de Cisco (figure 15, page précédente), les experts de Cisco ont également relevé des indicateurs de compromission (IoC) : un tiers des systèmes examinés exécutent Java SE 6, qui est en cours de suppression par Oracle. La version actuelle est Java SE 10. (Les pourcentages réels étaient de 33 % au début de la période d'un an examinée et de 23 % à la fin de la période d'un an.)

En outre, beaucoup d'utilisateurs ayant installé les versions les plus récentes de Java disposent toujours des anciennes versions majeures sur leurs systèmes pour prendre en charge d'autres logiciels ou ne les ont tout simplement pas supprimées. cela signifie que les versions comportant des vulnérabilités connues sont toujours disponibles et dans un état exploitable. Les autres protections des utilisateurs, comme les systèmes de prévention des intrusions, offrent une certaine protection, mais celle-ci n'est pas garantie. Si les autres protections du terminal sont, par ailleurs, insuffisantes, le risque est encore plus important.

En examinant les installations de Microsoft Office (figure 16, page précédente), nous avons constaté les défis liés à la gestion de la suite. Bien qu'il y ait peu de mises à jour automatiques, la majeure partie de la population utilise une version définie et conserve cette version. D'autres facteurs peuvent contribuer à accroître les défis liés à l'application de correctifs, par exemple lorsque les mises à niveau entraînent des dépenses pour la licence ou l'assistance informatique, ou lorsque les utilisateurs craignent que les modifications changent le comportement d'un outil de productivité concerné par le même correctif.

Au cours de la période analysée, quatre versions majeures d'Office étaient disponibles, bien que la version la plus récente ait été peu adoptée. Parmi les trois versions majeures les plus adoptées, la répartition en pourcentage était d'environ 28-52-20, les migrations mineures augmentant au fil de l'année. Les changements de version majeure nécessitent un octroi de licence, tandis que les mises à jour de versions mineures font partie du cycle de vie normal de maintenance du logiciel. Nous nous attendions à ce que la majeure partie de la population utilisant une version majeure exécute la version la plus récente du Service Pack. Or, si l'on observe la version la plus récente (Office 2013/version 15x), les trois principaux moments de mise à jour de sécurité majeure auxquels nous faisons référence sont répartis quasiment de manière homogène.

Résultat : un grand nombre des principaux fournisseurs remplissent leurs obligations en matière de sécurité en publiant des notifications et des correctifs, et en distribuant ces correctifs rapidement. Mais cet intérêt pour l'application des correctifs ne se retrouve pas chez les utilisateurs, qui compromettent ainsi eux-mêmes leur sécurité et leurs entreprises.

En plus de tirer parti des publications rapides de correctifs, les professionnels de la sécurité doivent envisager l'utilisation des fonctionnalités de mise à jour automatique comme un outil utile pour appliquer rapidement des correctifs. Bien sûr, il est plus facile d'appliquer les mises à jour automatiques sur certains systèmes que sur d'autres. Par exemple, les mises à jour de navigateur sont les plus légères pour les terminaux, tandis que les mises à jour des applications professionnelles et de l'infrastructure côté serveur sont plus difficiles et peuvent entraîner des problèmes de continuité des activités. Leur correction a donc généralement lieu moins souvent. Les professionnels de la sécurité doivent hiérarchiser les mises à jour et les correctifs pour être en mesure de sécuriser les réseaux contre les menaces connues et évidentes.

Les versions de sécurité sont souvent associées aux versions de fonctionnalités, ce qui ajoute aux difficultés car les utilisateurs évitent parfois d'appliquer une mise à jour qui risque de changer la fonctionnalité qu'ils utilisent. La combinaison des versions augmente la charge d'assistance et la complexité pour le fournisseur.

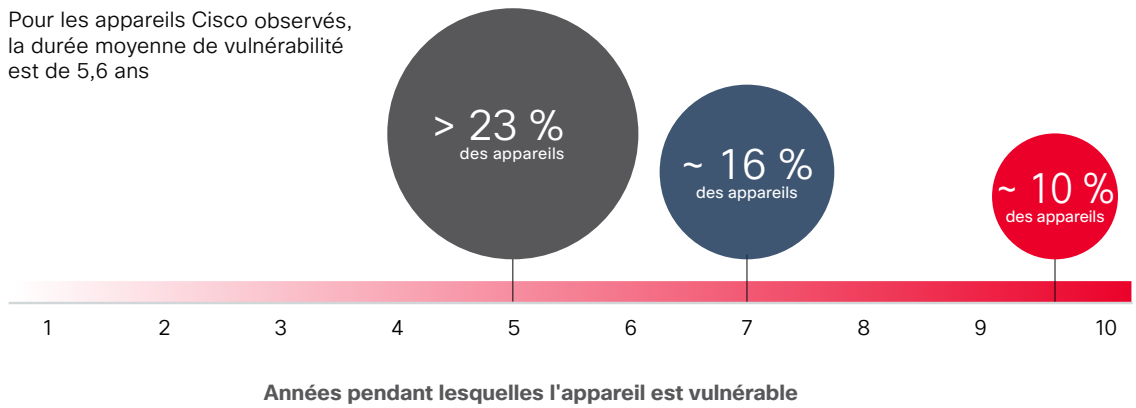
Infrastructure vieillissante : des vulnérabilités de longue date à corriger d'urgence pour faire face à l'essor des ransomwares

En 2015, Cisco a analysé 115 000 appareils Cisco sur Internet et sur les environnements des clients pour attirer l'attention sur les risques liés aux entreprises qui n'assurent pas correctement la maintenance d'une infrastructure vieillissante ou qui corrigent des systèmes d'exploitation vulnérables.[4] Nous avons constaté que 106 000 des 115 000 appareils Cisco (soit 92 %) exécutent des logiciels comportant des vulnérabilités connues.

Pour ce rapport, nous souhaitions examiner un échantillon d'appareils Cisco pour déterminer l'ancienneté des vulnérabilités connues s'exécutant sur l'infrastructure de base (routeurs et commutateurs). Notre échantillon se composait de 103 121 appareils Cisco sur Internet (installations observables avec CVE connues datées de 2002 à 2016). Chaque appareil exécutait, en moyenne, 28 vulnérabilités connues.

Les appareils de cet échantillon exécutaient des vulnérabilités depuis 5,6 ans en moyenne. Plus de 23 % de ces appareils comportaient des vulnérabilités remontant à 2011. Près de 16 % comportaient des vulnérabilités qui avaient été publiées pour la première fois en 2009. Enfin, près de 10 % comportaient des vulnérabilités connues ayant plus de 10 ans (figure 17).

Figure 17 : Le pourcentage d'appareils exécutant des vulnérabilités connues par âge

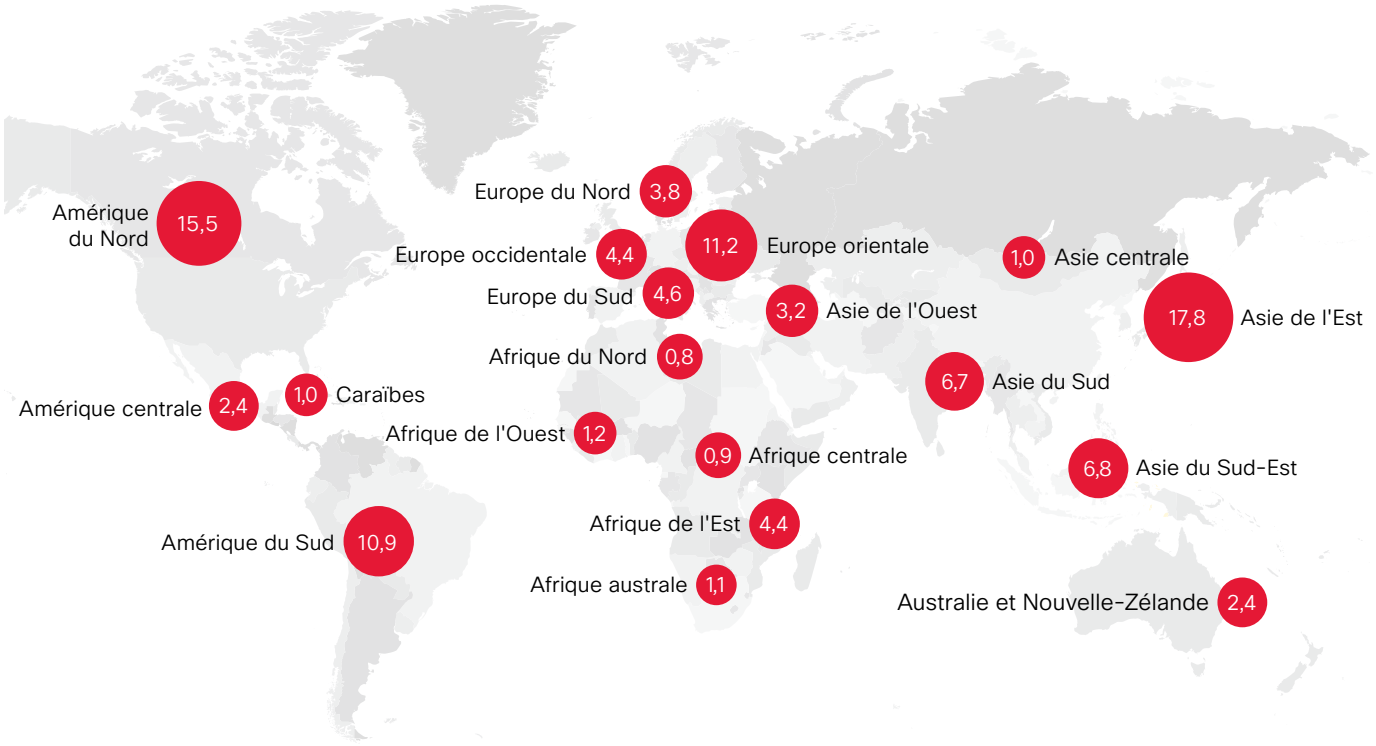


Source : Cisco Security Research

PARTAGER

[4] 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'entreprise d'un point de vue extérieur (en partant d'Internet vers l'entreprise). Pour en savoir plus sur les modalités de l'analyse, consultez le rapport semestriel 2016 de Cisco sur la cybersécurité, disponible ici : **cisco.com/go/msr2015**.

Figure 18 : Le pourcentage d'appareils Cisco vulnérables par zone géographique



Source : Cisco Security Research

Selon nos experts Cisco, les pourcentages les plus élevés d'appareils Cisco vulnérables se trouvent en Asie de l'Est (17,8 %) et en Amérique du Nord (15,5 %). (Voir Illustration 18.)

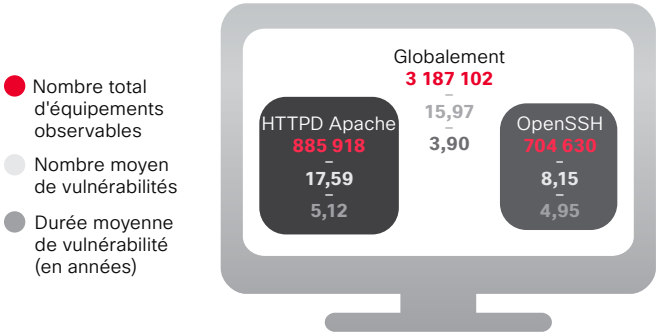
Point de comparaison : infrastructure logicielle vulnérable

Les experts de Cisco ont examiné les vulnérabilités d'une infrastructure logicielle courante pour déterminer si les entreprises étaient plus consciencieuses concernant l'application de correctifs de vulnérabilités connues dans ces produits (figure 19). Notre échantillon de plus de 3 millions d'installations observables comportant des vulnérabilités incluait un large éventail de produits, mais la plupart étaient des produits Apache httpd (885 918) ou OpenSSH (704 630). Le nombre moyen de vulnérabilités connues pour ces produits logiciels était proche de 16.

Selon notre étude, les entreprises utilisant des logiciels de serveur web ont exécuté des vulnérabilités connues pendant 3,9 ans, en moyenne.

Concernant les résultats régionaux, nous avons observé le nombre le plus élevé d'installations logicielles vulnérables en Amérique du Nord, en Europe occidentale et en Europe orientale (figure 20).

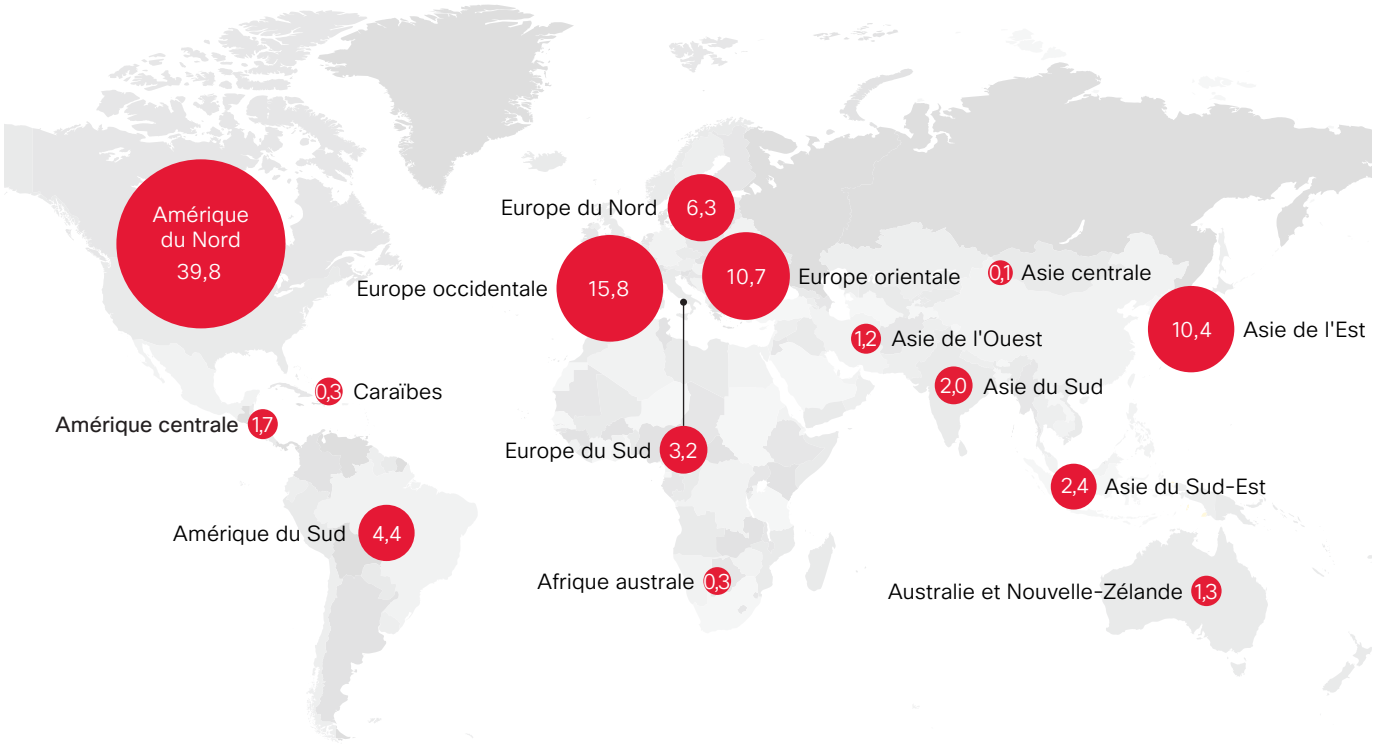
Figure 19 : Le pourcentage d'installations logicielles vulnérables par produit



Source : Cisco Security Research

PARTAGER

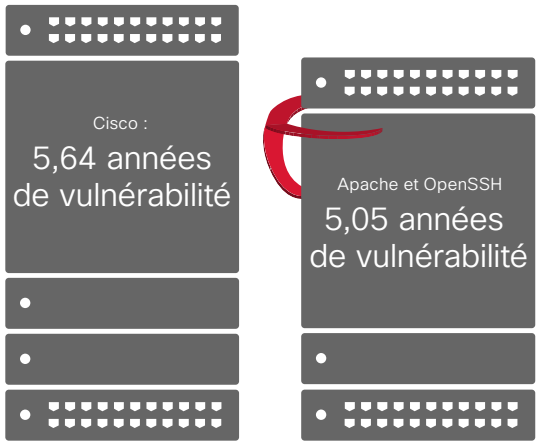
Figure 20 : Le pourcentage d'installations logicielles vulnérables par zone géographique



Source : Cisco Security Research

Notre analyse des produits Cisco, Apache et OpenSSH a déterminé que les entreprises ne sont pas assidues en ce qui concerne la correction des vulnérabilités dans les groupes de produits, quels qu'ils soient (figure 21). Certaines attendent de remplacer leur infrastructure plutôt que de faire l'effort d'appliquer des mises à niveau. D'autres ont attendu si longtemps qu'elles pensent ne plus pouvoir mettre à niveau leurs produits, lesquels ne sont plus pris en charge. Dans tous les cas, nous avons constaté que les produits sont exécutés avec des vulnérabilités connues pendant environ 5 ans, en moyenne.

Figure 21 : Présentation des logiciels : comparaison de Cisco avec Apache et OpenSSH



Source : Cisco Security Research

Ne reportez plus : c'est le moment d'agir

Bien que la mise à niveau de leur infrastructure de réseau soit parfois longue et coûteuse, les entreprises qui n'effectuent pas les mises à jour nécessaires offrent d'excellentes opportunités aux cybercriminels. La campagne de ransomwares SamSam (voir **page 7**) est la preuve que les hackers peuvent tirer parti de vulnérabilités connues de longue date dans l'infrastructure Internet pour lancer des attaques ultraciblées paralysantes et coûteuses pour les entreprises qui ne prennent pas de précautions suffisantes. (Voir « Plate-forme JBoss : des vulnérabilités au niveau de l'infrastructure élargissent la fenêtre d'action des cybercriminels », **page 18**.)

Les entreprises doivent bien garder à l'esprit que toutes les installations de produits incluses dans notre analyse peuvent être observées par des agents extérieurs disposant des outils et de l'expertise adéquats. Les hackers en font partie.

Il est impératif que les entreprises du monde entier donnent la priorité à la résolution du problème de l'infrastructure et des systèmes vieillissants. Il ne s'agit pas simplement de corriger les anciennes vulnérabilités trop longtemps négligées, mais également d'évaluer la résistance globale et la cyberrésilience de l'infrastructure et des systèmes déployés. Pour de nombreuses entreprises, le moment est venu de réaliser qu'elles doivent renoncer aux produits qui ne sont plus pris en charge et ne peuvent plus être mis à niveau pour relever les défis actuels de la sécurité.

Certains indicateurs montrent que les pays en voie de développement ont pris du retard dans ces démarches, comme illustré dans les figures 22 et 23.

Figure 22 : Le nombre médian d'années pendant lesquelles les appareils Cisco étaient vulnérables par zone géographique

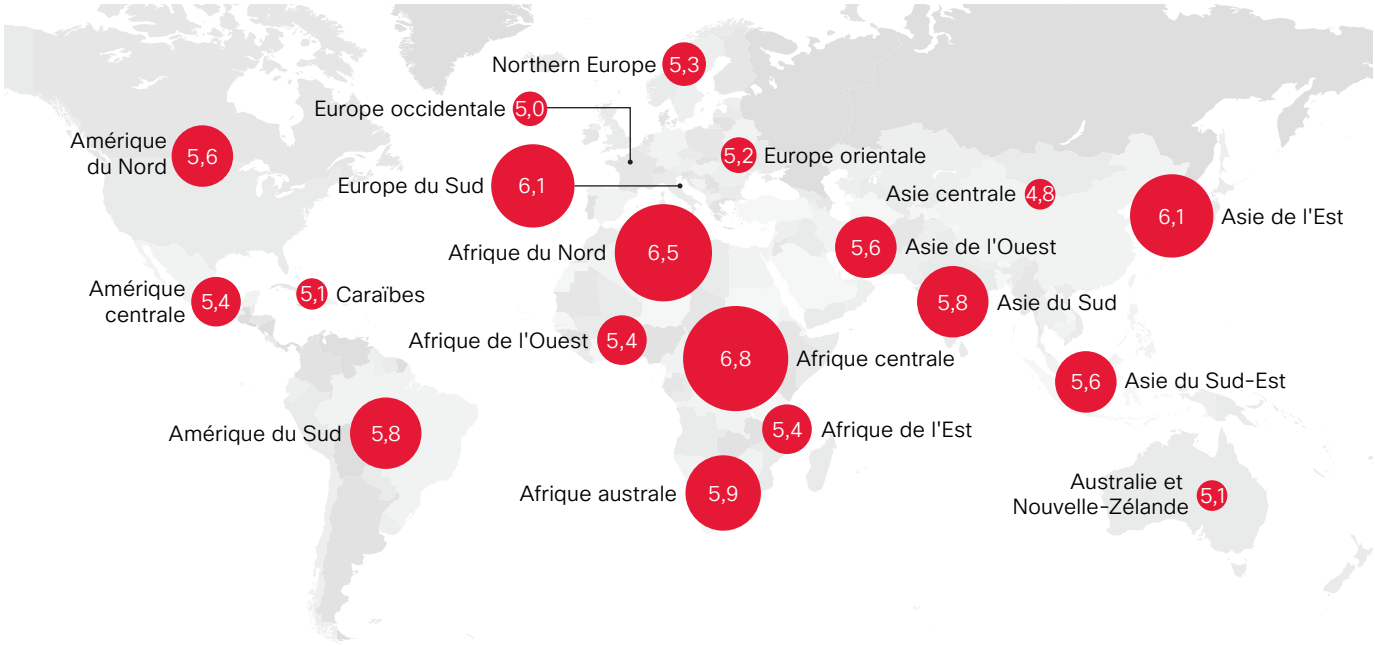
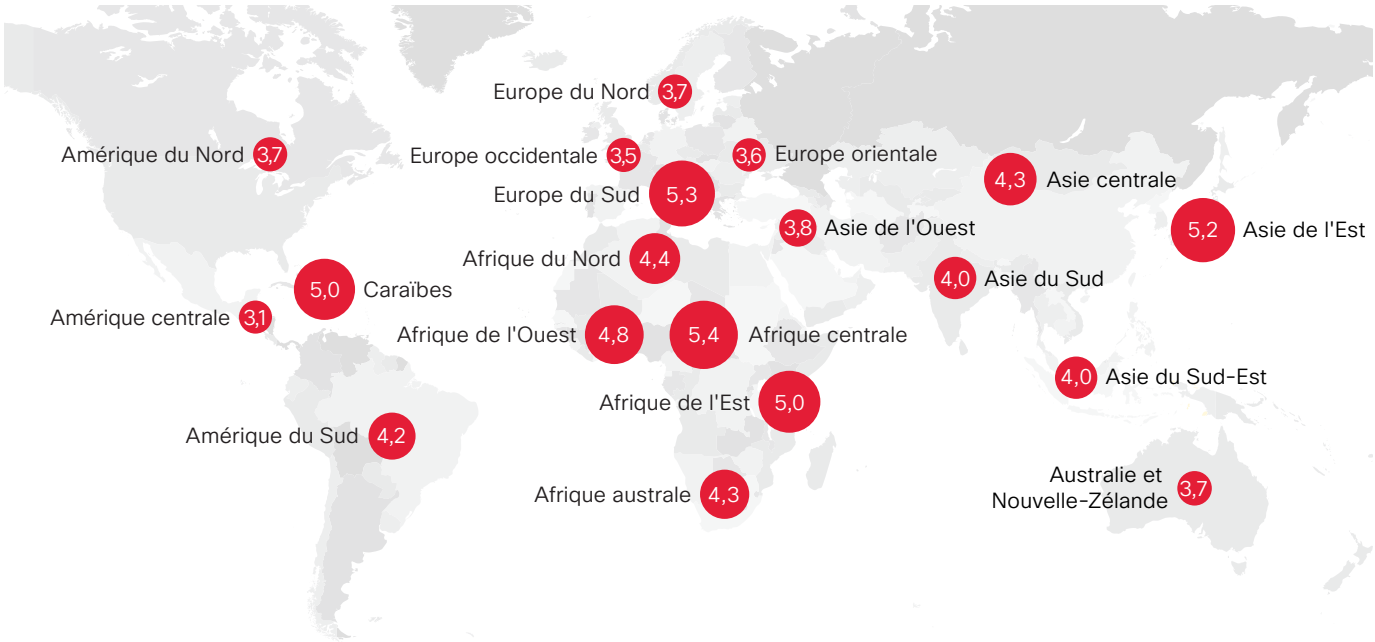


Figure 23 : Le nombre médian d'années pendant lesquelles les divers types de logiciels de serveurs étaient vulnérables par zone géographique



Source : Cisco Security Research

Une infrastructure fragile non sécurisée ne peut pas prendre en charge l'économie numérique de nouvelle génération qui émerge. Pour tirer pleinement parti des bénéfices de la numérisation et de l'Internet des objets, les entreprises doivent résoudre les problèmes de sécurité de la première vague numérique.

Ces problèmes sont dus en partie au fait que l'entreprise manque de clairvoyance concernant la nécessité d'intégrer la sécurité dans l'infrastructure Internet. Au tout début d'Internet, personne ne se doutait que l'infrastructure deviendrait une cible pour les cybercriminels. Ceci dit, les problèmes de sécurité des infrastructures vieillissantes peuvent aussi être attribués à la procrastination des entreprises, qui sont pourtant bien informées de l'existence des correctifs de vulnérabilités connues. Au lieu de se confronter à un risque calculé en mettant temporairement hors ligne leur infrastructure critique pour procéder à une mise à niveau, elles préfèrent parier sur le peu de chance que les cybercriminels les épargneront.

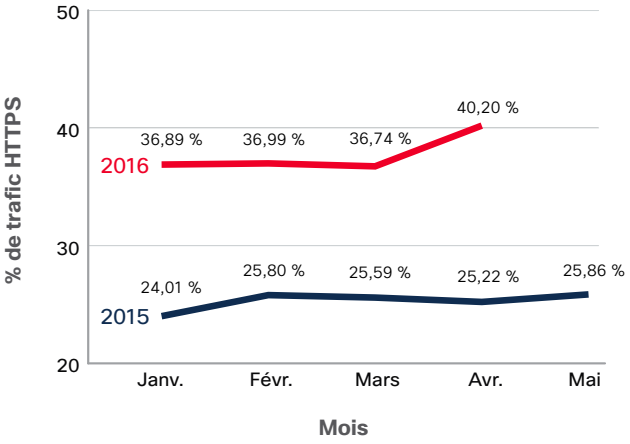
« Une infrastructure fragile non sécurisée ne peut pas prendre en charge l'économie numérique de nouvelle génération qui émerge. Pour tirer pleinement parti des bénéfices de la numérisation et de l'Internet des objets, les entreprises doivent résoudre les problèmes de sécurité de la première vague numérique. »

Chiffrement : un trafic HTTPS stable au premier semestre 2016... une tendance à suivre

Comme nous l'avons expliqué dans notre dernier rapport sur la sécurité, le chiffrement est devenu un outil privilégié pour les entreprises qui veulent protéger leurs données sensibles et la confidentialité de leurs clients. De janvier à avril 2016, le volume de requêtes HTTPS est resté relativement stable, après avoir progressé de manière importante tout au long de l'année 2015.

L'utilisation du chiffrement ayant augmenté en 2015, les experts en sécurité pensent que cette tendance se confirmera en 2016, même si le trafic n'a que peu augmenté cette année pour le moment (figure 24).

Figure 24 : Le trafic HTTPS chiffré est relativement stable en 2016

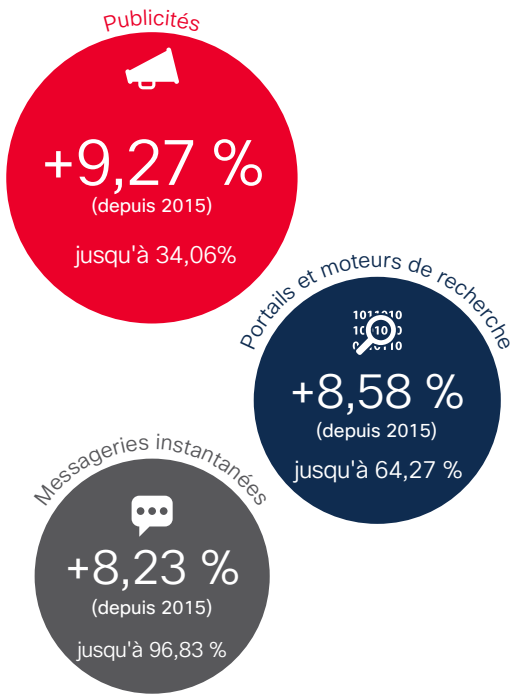


Source : Cisco Security Research

Concernant les publicités, nous avons observé une augmentation du trafic HTTPS au cours des quatre premiers mois de 2016 (voir figure 25). Cette augmentation est probablement due à la volonté du secteur de protéger la confidentialité des utilisateurs et de perturber les campagnes malveillantes. Toutefois, elle reflète peut-être également la hausse d'utilisation du HTTPS par les développeurs de campagnes malveillantes : les injecteurs de publicités, qui sont le principal composant des infections par logiciels malveillants, sont devenus la principale source d'augmentation du nombre de campagnes malveillantes utilisant HTTPS.

Comme le montre la figure 26, les trois principales applications utilisant HTTPS sont la messagerie d'entreprise, la messagerie instantanée et la messagerie hébergée sur Internet.

Figure 25 : L'augmentation du trafic HTTPS des programmes malveillants, janvier 2015-avril 2016



Source : Cisco Security Research

Si l'utilisation régulière du chiffrement par les entreprises légitimes est une bonne nouvelle pour les utilisateurs, elle l'est beaucoup moins pour les professionnels de la sécurité. Les cybercriminels ont également compris l'intérêt du chiffrement qui leur permet de cacher leurs activités aux acteurs de la sécurité puisqu'ils disposent de plus de temps pour poursuivre leurs activités sans être interrompus (pour plus d'informations sur l'utilisation du HTTPS par les développeurs de malwares, voir **page 22**). En l'absence de visibilité sur les indicateurs de compromission (IoC) cachés par le trafic chiffré, l'efficacité des solutions ponctuelles est réduite et les acteurs de la sécurité ont plus de difficulté à identifier les activités malveillantes avant qu'elles provoquent des dégâts durables.

Figure 26 : Les principales applications qui utilisent HTTPS

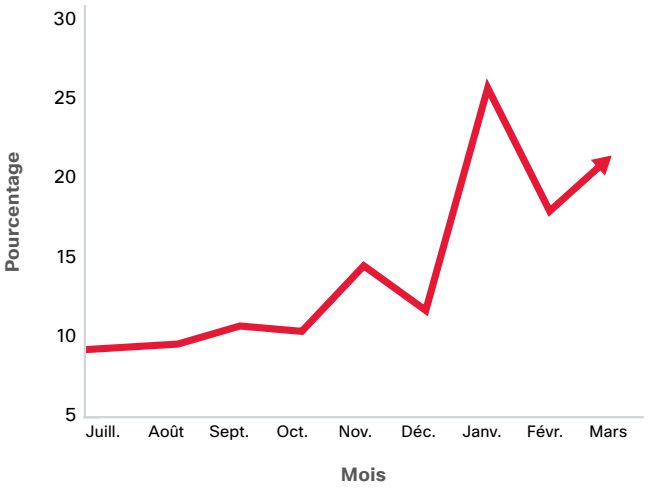
Catégorie (janvier-avril)	% moyen HTTPS
E-mail d'entreprise	97,88 %
Messagerie instantanée	96,83 %
Messagerie hébergée sur Internet	96,31 %
Stockage et sauvegarde en ligne	95,70 %
Téléphonie sur Internet	95,07 %
Portails professionnels	90,78 %
Réseaux sociaux	81,15 %
Services de transfert de fichiers	67,63 %
Vidéo en ligne	64,71 %
Moteurs de recherche et portails	64,27 %
Recherche de photos/images	61,90 %
Traduction de pages web	54,60 %
SaaS et B2B	54,36 %

Source : Cisco Security Research

Le protocole TLS chiffre les données utiles mais n'empêche pas les comportements malveillants

Les créateurs et les utilisateurs de malwares cherchent continuellement les moyens d'agir plus longtemps sans se faire repérer. Ils choisissent souvent pour cela des outils technologiques généralement utilisés à des fins légitimes. Le protocole TLS (Transport Layer Security), qui est le plus utilisé pour assurer le chiffrement du trafic réseau, est la nouvelle méthode privilégiée par les cybercriminels. En observant les en-têtes TLS non chiffrés, les experts de Cisco ont constaté qu'un nombre réduit mais croissant d'échantillons de malwares utilise le protocole TLS pour les communications protégées. C'est une difficulté pour les professionnels de la sécurité, car l'inspection approfondie des paquets n'est par conséquent plus une solution efficace.

Figure 27 : Le pourcentage d'échantillons de programmes malveillants qui utilisent TLS



Source : Cisco Security Research

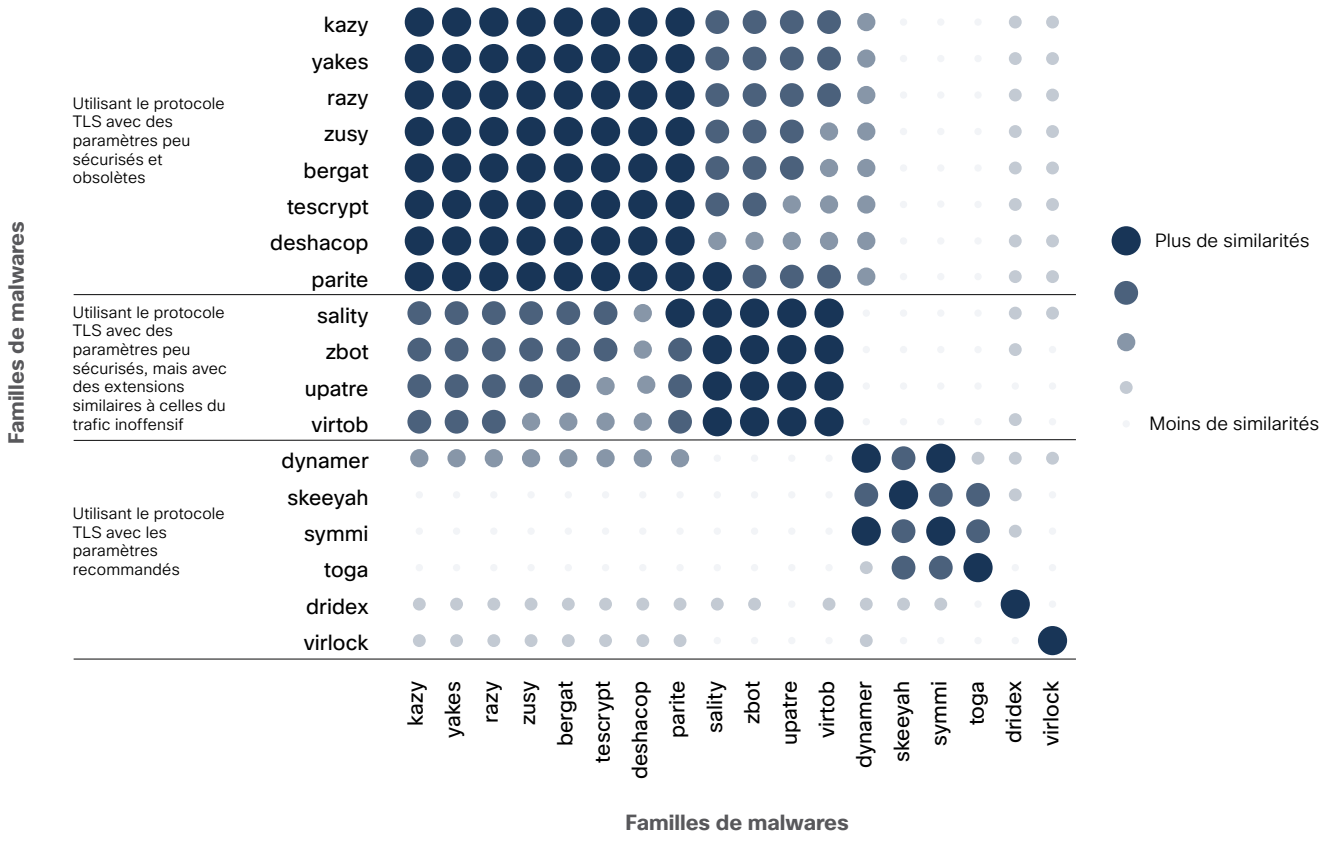
Selon nos experts, pas moins de 60 % de l'ensemble du trafic réseau utilise le protocole TLS pour le chiffrement. Dans les échantillons de malwares analysés par les experts, environ 10 % des malwares utilisaient le protocole TLS. Ce pourcentage peut paraître faible, mais les experts estiment qu'il va augmenter dans la mesure où l'utilisation globale du chiffrement dans le trafic inoffensif augmente. Ils ont observé une hausse du trafic malveillant chiffré entre juillet 2015 et mars 2016 (figure 27).

Sachant que les hackers risquent d'accélérer leur utilisation du protocole TLS, comment les professionnels de la sécurité peuvent-ils utiliser ces connaissances pour améliorer la détection des malwares qui utilisent cette tactique ? Les malwares ne font pas le même usage du protocole TLS que le trafic inoffensif. Cette constatation permet de classer avec précision les modèles de trafic malveillant de la plupart des familles de malwares.

Nos experts ont découvert que les créateurs de malwares utilisent généralement des paramètres cryptographiques plus anciens que ceux utilisés dans le trafic réseau inoffensif. Ainsi, les anciennes suites de chiffrement utilisées par les malwares peuvent être un indicateur de trafic malveillant. Les applications inoffensives utilisent plus souvent les bonnes pratiques TLS actuelles, car leurs créateurs veulent différencier leurs produits en offrant plus de sécurité.

D'un autre côté, les utilisateurs de malwares choisissent des bibliothèques cryptographiques plus anciennes car elles sont réputées pour s'adapter à de nombreux environnements d'exploitation et ne pas provoquer d'erreurs. En effet, le chiffrement des malwares peut être perturbé si, par exemple, les bibliothèques que l'exécutable du malware s'attend à trouver sur l'hôte ne sont pas présentes. Dans ce cas, il y a une erreur et l'exécutable ne peut pas s'exécuter.

Figure 28 : Les paramètres TLS similaires des diverses familles de malwares



Source : Cisco Security Research

Nos experts ont examiné 18 familles de malwares, des milliers d'échantillons de malwares uniques et des dizaines de milliers de flux réseau chiffrés pour identifier les modèles d'utilisation du protocole TLS par les familles de malwares. Ils ont identifié les familles de malwares suivantes :

- Celles qui utilisent TLS avec des paramètres recommandés, comme le malware Skeeyah
- Celles qui utilisent TLS avec des paramètres peu sécurisés, mais avec des extensions similaires à celles du trafic inoffensif, tel que Sality
- Celles qui utilisent des paramètres faibles et obsolètes, tels que tescrypt

Comme le montre la figure 28, nos experts ont pu démontrer que certaines familles de malwares présentent des similitudes dans la façon dont elles utilisent le chiffrement TLS.

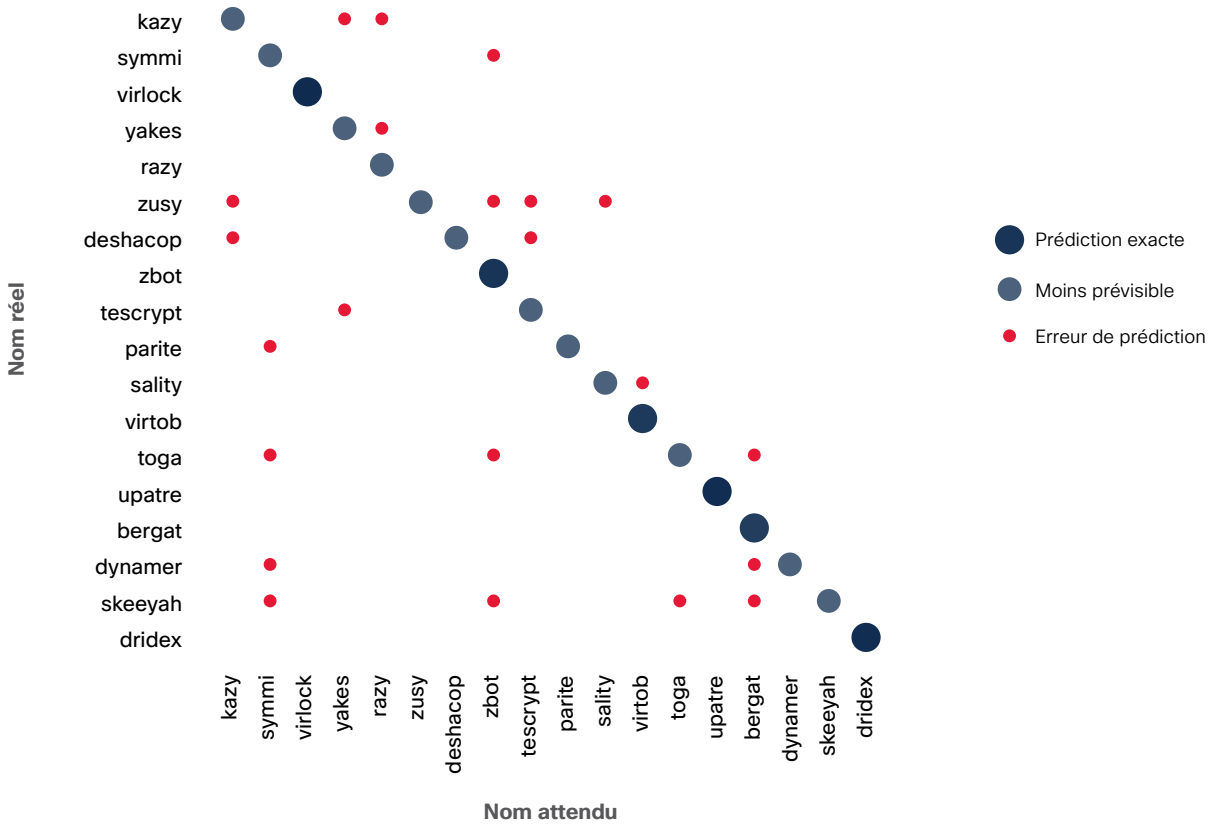
La matrice de confusion (figure 29) montre combien il est facile de faire la différence entre les familles de malwares. L'étiquette de prévision est susceptible de correspondre à l'étiquette réelle (indiquée par un grand cercle). Les prévisions incorrectes (indiquées par un petit cercle) sont beaucoup moins probables.

Sans surprise, les familles de malwares qui développent activement l'utilisation du protocole TLS sont plus difficiles à classer. Toutefois, nos experts ont constaté qu'en appliquant des connaissances spécifiques au domaine au trafic examiné (par exemple, en vérifiant si le certificat TLS a été autosigné), ils pouvaient identifier des modèles avec une plus grande précision. Par exemple, ils ont pu attribuer des communications réseau à une famille donnée de malwares avec une précision de 86,8 %, même lorsque ces communications étaient réduites à un simple flux chiffré.

Cela confirme la nécessité et l'avantage d'utiliser une protection intégrée contre les menaces, notamment les techniques d'apprentissage automatique qui complètent les classifications naïves. La combinaison de méthodes d'apprentissage automatique et de différentes vues des données fournit des informations de meilleure qualité aux professionnels de la sécurité.

Pour eux, la capacité d'attribuer précisément des échantillons de malwares à une famille de malwares connue peut s'avérer précieuse. Elle indique aux intervenants quel type de menace ils doivent gérer avant de commencer le processus de rétroingénierie des échantillons de malwares. En outre, l'examen des flux de trafic chiffré aide les équipes d'intervention à mieux définir l'ordre des priorités (par exemple, attribuer plus de ressources aux infections de malwares les plus graves).

Figure 29 : Matrice de confusion : distinguer les diverses familles de programmes malveillants



Source : Cisco Security Research

Délais de détection : une véritable course à l'armement

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

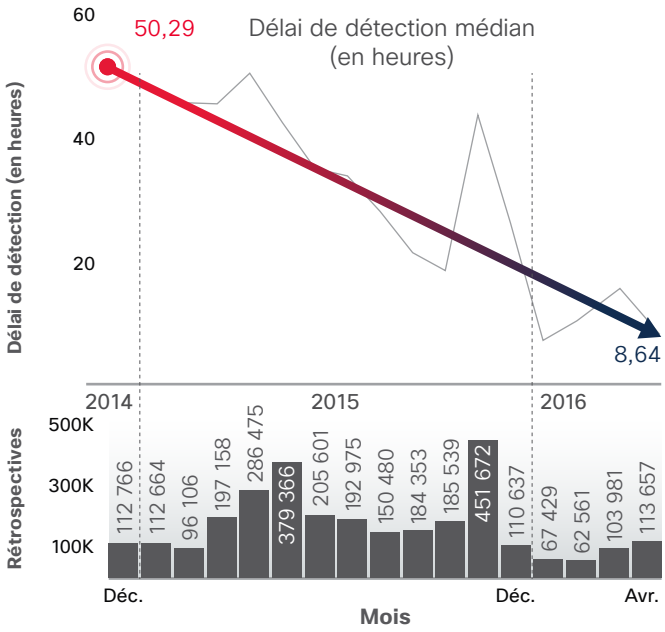
Depuis la fin de l'année 2014, nous avons suivi les progrès effectués pour réduire notre délai de détection. Il y a un an, nous avons indiqué que le délai de détection médian était d'environ deux jours (50 heures).[5]Avant octobre 2015, Cisco avait réduit son délai de détection médian à environ 17 heures.

Pendant la période de décembre 2015 à avril 2016, le délai de détection médian a encore baissé pour passer à environ 13 heures. Ce chiffre correspond à la moyenne pondérée de cinq valeurs médianes au cours de la période observée.

Notre délai de détection médian est bien inférieur à celui estimé pour le secteur, qui est de 100 à 200 jours. Nous continuons à accélérer notre capacité de détection des menaces, aussi nombreuses soient-elles. La figure 30 illustre la diminution globale du délai de détection de Cisco entre décembre 2014 et avril 2016.

La tendance régulière à la baisse du délai de détection médian est parfaitement visible dans la figure 30. La courbe de la période est également marquée de nombreux pics et creux. Ce sont des indicateurs de la « course à l'armement » entre les hackers et les acteurs de la sécurité.

Figure 30 : Le délai de détection médian par mois, décembre 2014-avril 2016



Source : Cisco Security Research

PARTAGER

« Notre délai de détection médian est bien inférieur à celui estimé pour le secteur, qui est de 100 à 200 jours. Nous continuons à accélérer notre capacité de détection des menaces, aussi nombreuses soient-elles. »

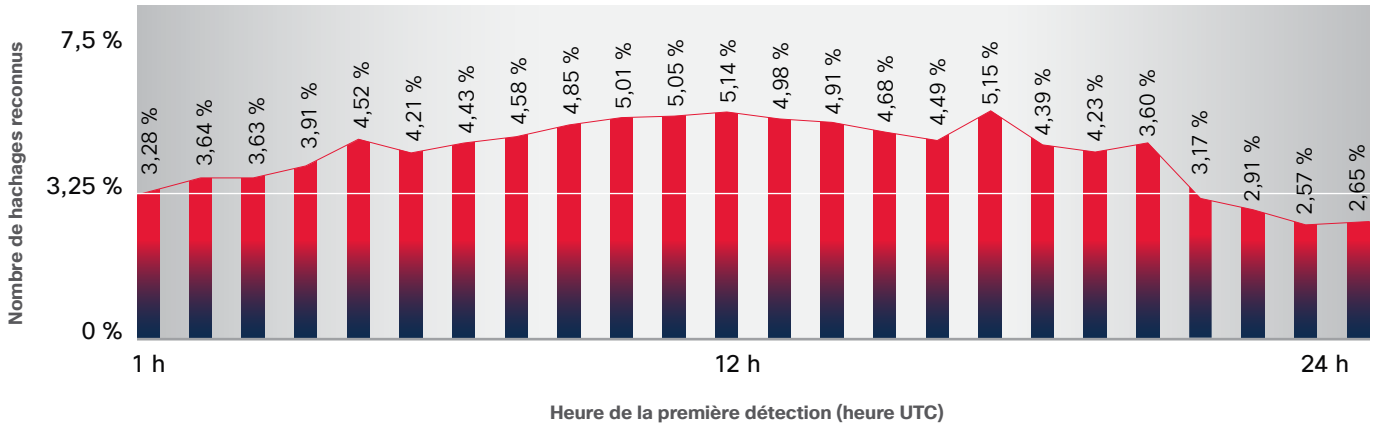
[5] Rapport semestriel 2015 de Cisco sur la cybersécurité, disponible ici : **cisco.com/go/msr2015**.

Les hackers créent en permanence des techniques furtives pour éviter toute détection. Les fournisseurs de solutions de sécurité contrent ces efforts en améliorant l'intégration et la détection des menaces. Ils intègrent ensuite les indicateurs de compromission qu'ils identifient dans les technologies de détection automatisées et ajoutent du contexte à ces données pour en faire des informations exploitables par les clients. (Voir « Les indicateurs de compromission n'offrent pas d'informations suffisantes sur les menaces », **page 53**.)

Les diminutions importantes des délais de détection correspondent aux périodes pendant lesquelles Cisco a pris de l'avance sur les hackers, en détectant les menaces plus rapidement qu'ils ne pouvaient développer et exécuter de nouvelles techniques. Les pics indiquent les périodes auxquelles les hackers ont riposté avec des innovations qui, pour être détectées, nécessitaient beaucoup de travail des analystes ou d'autres sources d'information, augmentant à nouveau le délai de détection médian.

La course à l'armement entre les cybercriminels et les acteurs de la sécurité est incessante. Les hackers libèrent un flot constant de nouvelles menaces qui obligent les fournisseurs de solutions de sécurité à agir rapidement pour les identifier. La figure 31 montre le nombre de hachages (fichiers) reconnus au cours d'une journée typique pendant la période observée (de décembre 2015 à avril 2016). Globalement, le taux de reconnaissance est relativement homogène au cours de la journée.

Figure 31 : Les hachages reconnus par heure de la journée



Source : Cisco Security Research

PARTAGER

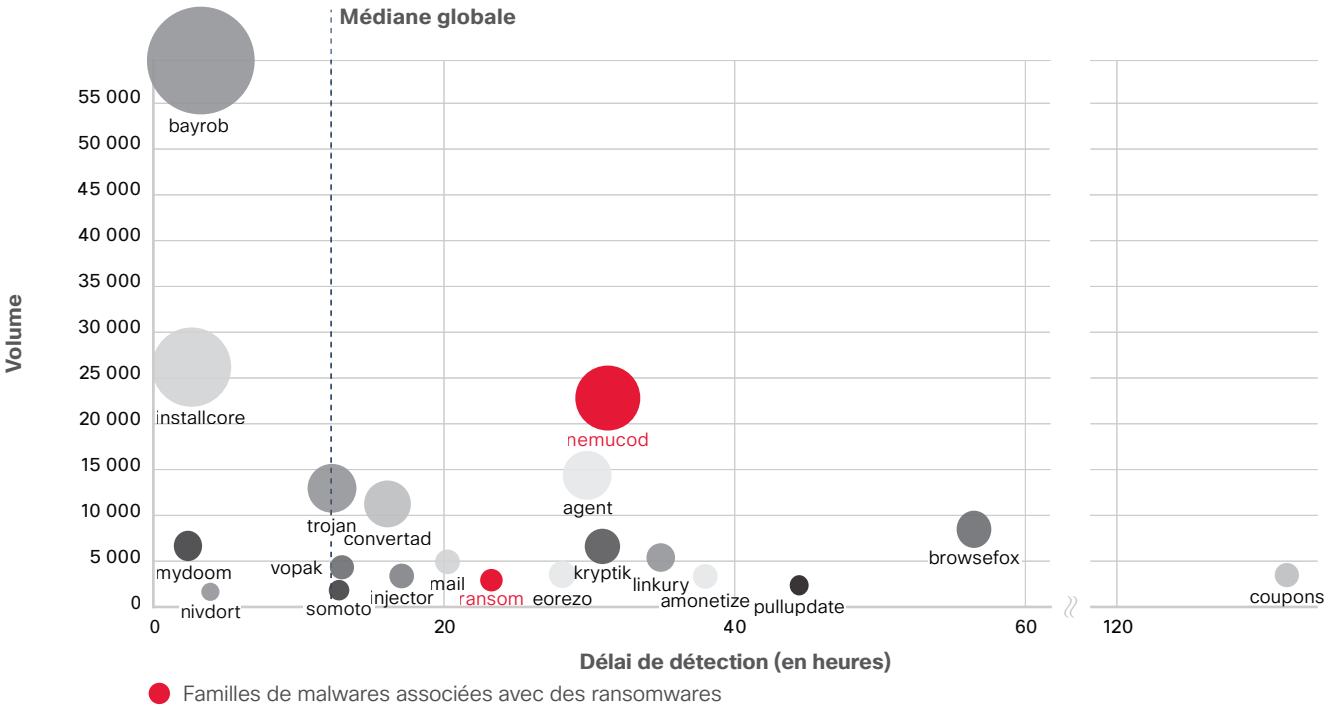
« Les fortes diminutions des délais de détection correspondent aux périodes auxquelles Cisco a pris de l'avance sur les hackers, en détectant les menaces plus rapidement qu'ils ne pouvaient développer et exécuter de nouvelles techniques. »

L'explosion des ransomwares : un facteur des fluctuations récentes du délai de détection médian

Comme nous l'avons remarqué dans notre dernier rapport sur la cybersécurité, l'industrialisation de l'économie parallèle et l'augmentation de l'utilisation des malwares courants ont été des facteurs importants. Depuis 2014, ils nous ont permis de réduire le délai de détection régulièrement et de façon importante. Les menaces industrialisées se propagent rapidement, les rendant plus faciles à détecter.

Au cours des cinq premiers mois de l'année 2016, les familles de malwares détectées par Cisco pendant le délai de détection médian (environ 13 heures) étaient des menaces anciennes, qui restent répandues. Il s'agissait par exemple de Bayrob, un malware botnet présent depuis 2007 ayant connu un regain il y a quelques mois et de Mydoom, un virus informatique propagé par e-mail observé pour la première fois en 2004 affectant Microsoft Windows. InstallCore, le logiciel malveillant bien connu, était également fréquent, probablement en raison de son rôle dans la distribution des ransomwares (figure 32).

Figure 32 : Les délais de détection médians des principales familles de malwares (les 20 familles comptant le plus de détections)



Source : Cisco Security Research

PARTAGER

L'explosion des ransomwares au cours de l'année passée a été un facteur d'augmentation de l'utilisation de certaines familles de malwares (et donc de leur détection).

Pour certaines familles de malwares associées au ransomware, le délai de détection a été globalement plus élevé car il a fallu plus de temps aux analystes pour analyser ces menaces. Les techniques automatisées telles que l'analyse heuristique et le sandboxing n'ont pas permis de les détecter plus tôt.

La figure 33 présente les tendances mois par mois des principales familles de malwares que Cisco a détectées entre janvier et avril 2016. Les noms mis en évidence sont des exemples de familles de malwares associées aux ransomwares. La croissance ou la baisse de l'utilisation de certaines familles de malwares par les hackers sont à l'origine des fluctuations du délai de détection médian. Les menaces ne pouvant être détectées qu'après examen des analystes de Cisco ont été à l'origine de l'augmentation du délai de détection médian au-delà de 14 heures en mars 2016, contre seulement 9 heures en février.

La figure 34 montre qu'il est difficile pour les acteurs de la sécurité de réduire le délai de détection, mais aussi que les entreprises doivent utiliser une protection intégrée contre les menaces. Les menaces qui peuvent être détectées avant le délai de détection médian sont identifiées par le biais de techniques automatisées, comme le sandboxing. Les menaces émergentes plus avancées nécessitent une analyse et des informations internes ou tierces, ce qui rend leur détection plus longue.

Les campagnes de malwares vont et viennent, mais une chose ne change pas : la relation antagoniste entre les cybercriminels et les acteurs de la sécurité. Les hackers cherchent constamment des menaces capables d'échapper à la détection pour augmenter leur délai d'action. Les acteurs de la sécurité, quant à eux, contrent ces efforts en traquant inlassablement les malwares nouveaux et émergents. Pour cela, ils intègrent les indicateurs de compromission de leurs technologies de détection automatisées et transforment ces données en informations réelles sur les menaces.

Cisco s'engage à réduire son délai de détection médian au cours des prochains mois. Nous recommandons aux entreprises de mesurer leur propre délai de détection médian afin d'entamer un processus d'amélioration et de réduire le délai actuel inacceptable de 100 à 200 jours estimé pour le secteur.

L'amélioration des pratiques en matière de délai de détection et de délai de correction ainsi que l'utilisation du chiffrement et la résolution proactive du problème de l'infrastructure vieillissante contribuent à réduire le champ d'action illimité des hackers. Le délai de détection et le délai de correction, par exemple, sont des indicateurs clés de performance. Ils permettent aux acteurs de la sécurité de se concentrer sur le moment et les moyens d'améliorer leur capacité de détection de la présence d'un hacker. Ils limitent par ailleurs la capacité d'un cybercriminel à changer de tactique et à échapper à l'identification.

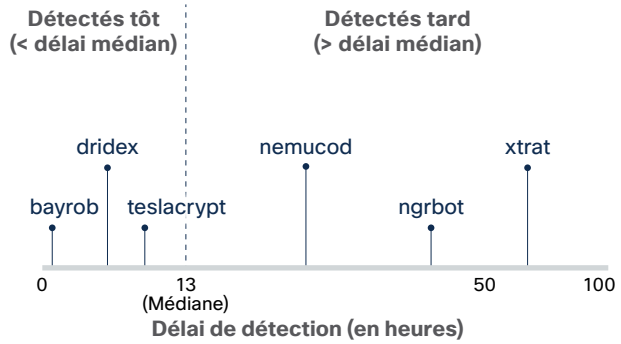
Figure 33 : Les 10 familles de malwares les plus détectées chaque mois

	Janvier	Février	Mars	Avril
1.	bayrob	downloader	downloader	bayrob
2.	downloader	installcore	nemucod	downloader
3.	installcore	convertad	agent	installcore
4.	agent	msil	installcore	nemucod
5.	convertad	browsefox	convertad	agent
6.	ransom	linkury	mydoom	convertad
7.	linkury	nemucod	msil	fareit
8.	kryptik	agent	browsefox	msil
9.	browsefox	kryptik	kryptik	trojan
10.	msil	mydoom	vilsel	heur

● Familles de malwares associées avec des ransomwares

Source : Cisco Security Research

Figure 34 : Des exemples de détection précoce et tardive de familles de malwares, par rapport au délai de détection médian de 13 heures



Source : Cisco Security Research

Gestion des incidents : des pratiques qui affectent la sécurité de l'entreprise

Les failles des réseaux, les attaques de ransomwares et les malwares malicieux font la une des médias dédiés à la sécurité. L'impact de ces incidents est également très commenté, qu'il s'agisse de l'interruption des activités d'une entreprise ou de l'atteinte à la réputation d'une marque. Cependant, la probabilité de telles attaques surprend toujours les entreprises qui pensent disposer de systèmes robustes de détection des menaces et d'intervention en cas d'incident, ces derniers étant en réalité relativement perméables.

Ces entreprises ont souvent recours à des technologies et des pratiques de sécurité qui ont dix ans de retard sur les offres actuelles. Ainsi, lorsqu'une attaque se produit, les professionnels de la sécurité qui adoptent une approche généraliste sont rapidement dépassés par des besoins nécessitant les compétences de spécialistes.

Cisco joue le rôle de consultant auprès d'entreprises de toutes tailles pour évaluer leur stratégie de sécurité. Nous constatons régulièrement l'absence de bonnes pratiques qui pourraient pourtant contribuer à renforcer la sécurité. L'équipe constate également que les hackers identifient ces faiblesses et les utilisent comme opportunités d'accès aux réseaux.

Par exemple, les entreprises qui entament une opération de fusion/acquisition n'effectuent pas toujours toutes les vérifications préalables requises pour contrôler le niveau de tolérance au risque de l'entreprise partenaire. Il arrive qu'elles ne réalisent les défaillances des entreprises récemment regroupées qu'une fois l'opération terminée, lorsqu'il est trop tard pour résoudre les problèmes ou lorsqu'il est plus difficile de le faire car les réseaux sont désormais interdépendants. Les responsables de la sécurité des systèmes d'information (RSSI) doivent évaluer attentivement toutes les solutions de protection de la sécurité avant d'entamer une opération de fusion/acquisition. Ils doivent au minimum s'assurer au préalable qu'il n'y a pas de trace d'activité suspecte sur les réseaux respectifs.

Les réseaux mal évalués offrent aux hackers un délai d'action supplémentaire, de même que les mauvaises pratiques comme les mots de passe faibles ou l'utilisation fréquente des droits d'administrateur. L'absence de prise en compte des événements ayant affecté leurs réseaux par le passé est un autre indicateur du manque de préparation des entreprises pour combattre les menaces avancées. Une entreprise qui déclare n'avoir jamais subi de faille de sécurité sur leur réseau n'a pas une visibilité réelle sur l'activité de son réseau. Toutes les entreprises qui existent depuis un certain temps ont forcément été exposées à des malwares courants et à des tentatives de franchissement des systèmes de protection.

Cisco constate également que les entreprises n'ont pas conscience de l'attrait qu'elles présentent pour les cybercriminels. Ces dernières années, les secteurs comme celui de la santé sont devenus plus attrayants pour les hackers, en combinant des données précieuses et une sécurité traditionnellement plus faible (voir **page 45**). En outre, Cisco a remarqué que les cybercriminels s'intéressent désormais aux institutions vulnérables telles que les établissements scolaires car ils savent que leurs protections sont en général minimes. Pour connaître les bonnes pratiques de mise en œuvre d'une intervention efficace en cas d'incident, voir les « Recommandations relatives à la sécurité », **page 52**.

« Une entreprise qui déclare n'avoir jamais subi de faille n'a pas une visibilité réelle sur l'activité de son réseau. Toutes les entreprises qui existent depuis un certain temps ont forcément été exposées à des malwares courants et à des tentatives de franchissement des systèmes de protection. »

Attaques par ransomware dans le secteur de la santé : une leçon pour toutes les entreprises

Le secteur de la santé a fait face à plusieurs attaques par ransomware cette année. En nous intéressant de plus près à nos clients dans ce secteur qui ont subi des attaques par ransomware, nous avons identifié un certain nombre de vulnérabilités qui ont favorisé les infections dans ces entreprises. Elles incluent :

- Des mots de passe partagés et des comptes disposant de trop de privilèges
- Un enregistrement de sécurité insuffisant pour détecter les mots de passe compromis
- Des applications en ligne avec les 10 principales vulnérabilités **OWASP**
- Des systèmes d'exploitation et des applications présentant des failles

Les chercheurs Cisco ont également découvert que tous les PC d'un hôpital exécutent souvent les mêmes versions vulnérables de logiciels comme Windows XP, le lecteur Adobe Flash ou Java. Il convient aussi de noter que la plupart des toutes dernières infections par ransomware que nous avons analysées peuvent s'expliquer par le fait que le personnel des cliniques a effectué des recherches sur Internet depuis une station de travail dénuée des correctifs du lecteur Flash.

Le manque de processus formels visant à installer rapidement des correctifs est également récurrent chez nos clients du secteur de la santé.

En outre, la plupart des fournisseurs médicaux ciblés par un ransomware ne disposaient pas de plans de riposte. Ils ont donc eu beaucoup plus de mal à répondre efficacement aux attaques.

Par ailleurs, les organismes de santé sont très peu nombreux à posséder des équipes de sécurité dédiées. La maintenance des ressources informatiques est généralement assurée par un ou plusieurs informaticiens généralistes qui manquent de savoir-faire dans le domaine de la sécurité.

Nous recommandons aux entreprises confrontées à de tels challenges de prendre au moins les mesures suivantes pour améliorer leur niveau de sécurité global :[6]

- Renforcer les systèmes pour résister aux programmes malveillants et aux piratages
- Évaluer l'environnement IT de l'entreprise : quels appareils sont connectés sur le réseau et combien sont-ils ? Où se trouvent ces terminaux ?
- Informer les utilisateurs sur les menaces et les former aux bonnes pratiques
- Développer un plan de riposte en cas d'incident
- Surveiller activement le réseau à la recherche de preuves de compromissions

Il est fondamental de traiter les vulnérabilités connues. Des vulnérabilités de longue date au niveau des serveurs JBoss ont permis aux cybercriminels à l'origine de la récente campagne SamSam de se déplacer latéralement dans l'infrastructure Internet pour cibler les réseaux du secteur de la santé (voir **page 7**). Les chercheurs Cisco estiment que les hackers cibleront de plus en plus ces infrastructures pour lancer des campagnes d'attaques par ransomware, vu les très nombreux appareils et logiciels vulnérables présents sur Internet. (Pour en savoir plus, reportez-vous à la section « Infrastructure vieillissante : des vulnérabilités de longue date à corriger d'urgence pour faire face à l'essor des ransomware », **page 30**.)

Les entreprises, tous secteurs confondus, peuvent s'inspirer du secteur de la santé très touché par les attaques par ransomware. Elles doivent envisager de prendre des mesures pour s'assurer que le personnel technologique chargé de gérer la sécurité dispose des outils, des ressources et des politiques pour agir efficacement.

[6] Remarque : lorsqu'elles renforcent la sécurité, les entreprises doivent prendre en compte les exigences en matière de respect de la réglementation ou d'autres directives propres au secteur auxquelles elles doivent se conformer. En effet, ces exigences peuvent affecter la manière dont elles approchent certains aspects de sécurité, tels que la protection et la confidentialité des données.

Perspective à l'échelle mondiale et recommandations de sécurité

Perspective à l'échelle mondiale et recommandations de sécurité

Les programmes malveillants trouvent leur origine dans le monde entier et les cybercriminels sont capables de déplacer rapidement leur base opérationnelle d'une zone géographique à une autre en cas de besoin. Une chose est sûre pour les entreprises qui pensent être à l'abri des hackers : aucun secteur n'est épargné. Les entreprises qui cherchent à mieux détecter les menaces et à y répondre grâce aux indicateurs de compromission (IoC) et non aux informations collectés sur les menaces ne font en fait pas grand-chose pour renforcer leur sécurité.

Parallèlement, les entreprises doivent également faire face à une autre incertitude en présence de menaces de plus en plus sophistiquées : le gouvernement, dans sa volonté de contrôler les données, crée des signaux, des lois et des exigences contradictoires. Cette situation peut au final limiter et contrecarrer le commerce international, la technologie sécurisée et les partenariats publics-privés fiables.

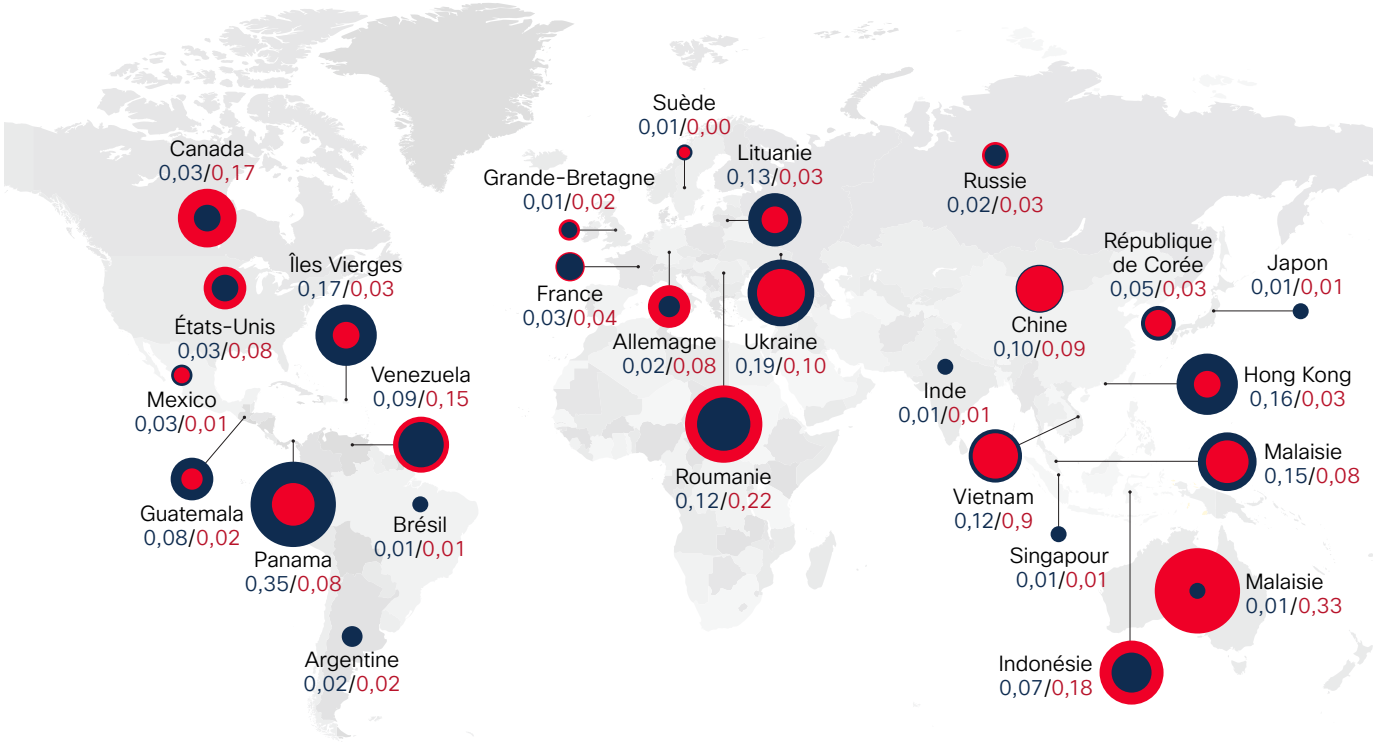
Blocage du trafic web par zone géographique

En examinant le volume du trafic Internet mondial et l'activité de blocage, les chercheurs Cisco peuvent fournir des informations sur la provenance du programme malveillant. En Amérique, le Canada semble être la source la plus importante de trafic bloqué en dehors des États-Unis.

En Europe, au Moyen-Orient et en Afrique, l'Ukraine et la Roumanie sont les principales sources de trafic bloqué par rapport au trafic mondial. Tandis qu'en Asie-Pacifique, l'Australie arrive en tête (voir la figure 35 à la page suivante).

Pour diverses raisons telles que la disponibilité des serveurs facilement piratés, les cybercriminels déplaceront leur base opérationnelle d'une zone géographique à l'autre.

Figure 35. Blocages de sites web par pays



Source : Cisco Security Research

PARTAGER

En examinant les secteurs d'activité (**page 49**), on découvre qu'aucun pays ni aucune zone géographique n'est à l'abri du trafic malveillant. Les programmes malveillants représentent un fléau mondial. Quelques zones géographiques et pays peuvent enregistrer une activité de blocage proportionnellement plus élevée parce que les cybercriminels ont trouvé les points faibles des infrastructures. En outre, un pic d'activité malveillante, observé en Australie en décembre 2015 et en janvier 2016, entraînera des changements notables au niveau du classement des pays et de leur trafic bloqué.

Risque d'exposition aux programmes malveillants : aucun secteur n'est à l'abri d'une attaque

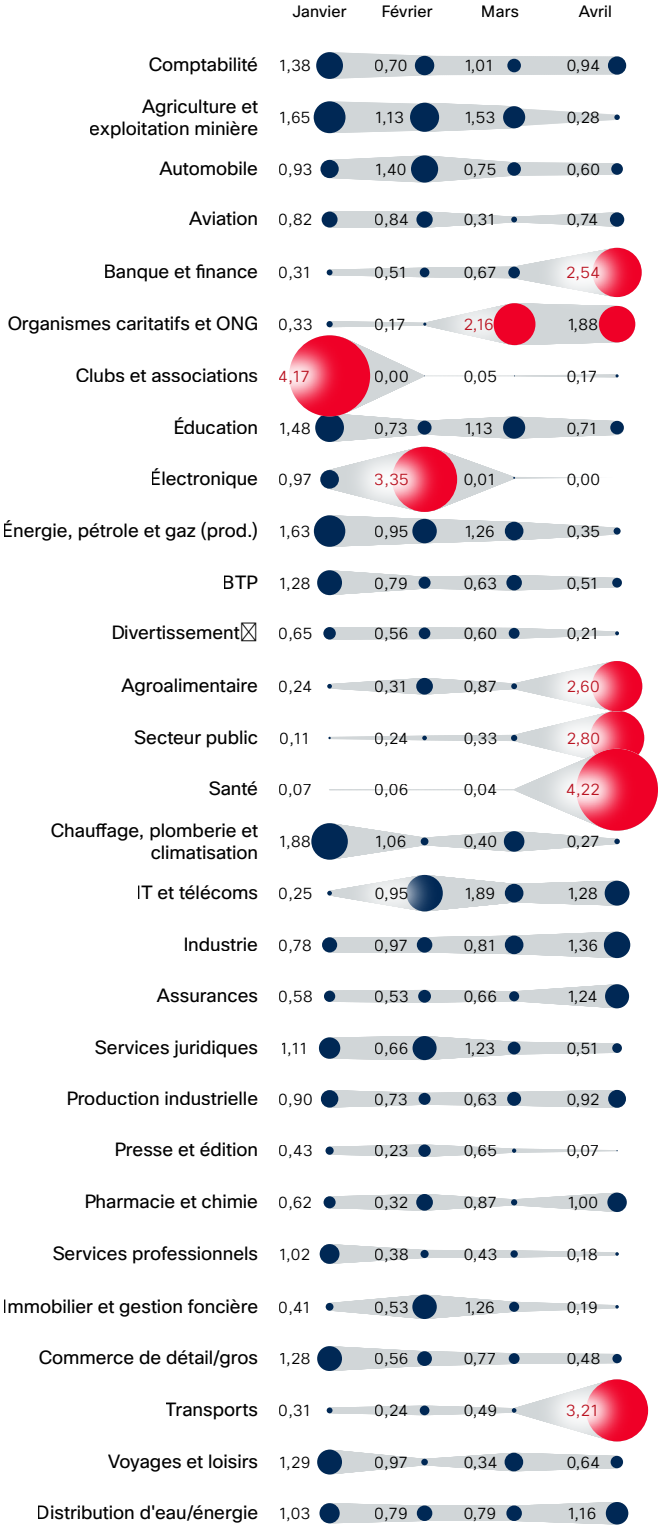
Nous avons un message pour les professionnels de la sécurité qui pensent que leur secteur n'est pas visé par les cyberpirates : ne soyez pas si confiants. En comparant régulièrement les volumes associés au trafic d'attaques (« taux de blocage ») à ceux du trafic « normal » ou prévu, il est évident qu'aucun secteur n'est protégé face aux programmes malveillants. Tout le monde peut être victime de cybercriminels à la recherche d'un moment et d'espace pour lancer leurs campagnes.

Même si le secteur de la santé a été dépeint dans les médias comme un secteur très apprécié des hackers (voir **page 7**), nos données prouvent que, pendant les premiers mois de l'année 2016, d'autres secteurs ont eu affaire à des volumes de malwares tout aussi importants. Par exemple, les clubs et les associations, les organismes caritatifs, les ONG et les entreprises spécialisées dans les produits électroniques ont tous connus des taux de blocage très élevés.

Après examen de ces taux de blocage, il ressort que chaque secteur court des risques. Même si les données mettent en avant des pics de trafic dans certains secteurs, il est évident que les cybercriminels s'intéressent à divers secteurs dès qu'ils entrevoient une occasion de compromettre des réseaux. Dès qu'ils ont atteint leur but, ils jettent leur dévolu sur le secteur qui offre le meilleur retour sur investissement. Leurs campagnes sont motivées par les opportunités, le secteur n'a que peu d'importance.

La Figure 36 présente 29 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 36 : Taux de blocage mensuels par secteur, janvier-avril 2016



Source : Cisco Security Research

Point sur la situation géopolitique : le secteur public et les entreprises face au dilemme de la protection des données

D'un point de vue géopolitique, les fournisseurs technologiques, les opérateurs télécoms et d'autres entreprises internationales sont toujours confrontés à un environnement réglementaire complexe et souvent contradictoire en matière de cybersécurité. Cette situation oppose des éléments contraires : le secteur public et les entreprises d'une part et la confidentialité et la sécurité de l'autre.

La sécurité des données est devenue la priorité absolue des états, qu'il s'agisse de protéger les données personnelles des individus ou l'intégrité d'une infrastructure physique, comme les systèmes nationaux d'alimentation en eau ou en électricité. Toutefois, les états veulent pouvoir accéder aux données quand ils en ont besoin via une interception légale par exemple.

Ils se rendent compte qu'ils ont perdu le contrôle sur la technologie et l'accès aux données et veulent le récupérer, en partie du moins. Les attaques terroristes et la croissance économique mondiale médiocre les obligent également à prouver qu'ils protègent bien leurs citoyens et les entreprises commerciales :

- Suite aux révélations d'Edward Snowden, le débat qui oppose les droits des individus aux droits de l'État a conduit au remaniement d'accords comme le Safe Harbor. Le nouveau bouclier de protection de la confidentialité américano-européen oblige les entreprises américaines à mieux protéger les données personnelles des citoyens européens contre les tentatives d'accès par les états.
- La crise migratoire dans l'Union européenne (UE) et les récentes attaques terroristes à Paris, à Bruxelles, en Turquie, aux États-Unis et ailleurs ont lancé un débat sur un accès des autorités répressives aux communications privées chiffrées. Le monde entier se sent concerné par ce problème, ce qui explique l'intérêt poussé pour le face-à-face qui oppose le FBI américain à Apple Inc. portant sur le déverrouillage d'un iPhone utilisé par un terroriste.
- Les gouvernements et les entreprises de sécurité privées veulent également prendre plus de mesures pour répondre à l'espionnage et au vol cautionné par les états. Les attaques perpétrées contre des banques via le réseau financier international SWIFT (Society for Worldwide Interbank Financial Telecommunication) sont attribuées à la Corée du Nord. Le gouvernement allemand a récemment attribué une attaque contre son parlement, le Bundestag, à Moscou.

Les états du monde entier envisagent de prendre des mesures qui leur permettront de bénéficier d'un contrôle plus poussé sur la technologie afin de combattre les menaces comme le terrorisme et la cybercriminalité. Ils prennent le risque de découvrir de nouvelles vulnérabilités et, dans certains cas, se réservent le droit de les exploiter. Ils ne partagent pas nécessairement toutes ces informations avec les fournisseurs technologiques, ce qui conduit inévitablement à la question suivante : qui est responsable des vulnérabilités détectées ? Les entreprises commerciales sont en première ligne si on tient compte de la réaction du grand public face à une intrusion plus importante de l'État.

Malgré la mondialisation rapide, aucune réponse internationale unifiée n'a été trouvée à la question de la cybersécurité ou à d'autres problèmes liés, comme la transparence, la responsabilité, la protection des données et le chiffrement. Les efforts se poursuivent pour établir des « règles de conduite » qui s'appliqueraient à Internet à l'échelle mondiale, mais vu les divergences de priorités, les entreprises continuent de travailler dans un environnement largement politisé et risqué sur un plan juridique.

« Malgré la mondialisation rapide, aucune réponse internationale unifiée n'a été trouvée à la question de la cybersécurité ou à d'autres problèmes liés, comme la transparence, la responsabilité, la protection des données et le chiffrement. »

Un environnement réglementaire en pleine évolution

Les opérateurs télécoms et les fournisseurs technologiques internationaux doivent s'adapter aux législations de chaque pays, en respectant les règles de chaque nation souveraine tout en se conformant au cadre légal et aux attentes du public de leur propre pays. Ce chemin est rempli d'embûches, vu les nombreux types de lois potentielles promulguées par les différents pays.

Au Royaume-Uni par exemple, un projet de loi du gouvernement, le Investigatory Powers Bill, essaie de regrouper tous les pouvoirs de surveillance des services de sécurité dans une seule loi d'ici la fin de cette année. Elle est actuellement débattue au parlement britannique. Des politiciens, des entreprises et des groupes de défense des droits humains critiquent les nombreuses mesures controversées de ce projet de loi, notamment la clause de « décryptage à la demande » qui oblige les fournisseurs technologiques et les opérateurs télécoms à lever le chiffrement des données à la demande des services de sécurité britanniques.

D'autres pays vont plus loin et cherchent à accélérer de telles mesures. Par exemple :

- La directive européenne « Network and information security » devrait être finalisée cet été.
- En France, une loi antiterrorisme est actuellement à l'ordre du jour du parlement. Elle prévoit d'infliger des amendes importantes aux entreprises et recommande des peines de prison pour les dirigeants qui refusent de coopérer dans le cadre d'enquêtes antiterroristes. Les auteurs de cette loi espèrent qu'elle sera adoptée avant la fin de l'état d'urgence prolongé, déclaré suite aux attaques qui ont touché Paris en novembre.
- Le gouvernement hongrois discute d'une loi qui rendrait les logiciels de chiffrement illégaux.
- Très inquiètes face au terrorisme, la Russie et la Chine veulent prendre des mesures visant à renforcer leur contrôle sur les réseaux technologiques nationaux.

L'ensemble de ces mesures préoccupe les opérateurs télécoms et les fournisseurs technologiques au vu des exigences strictes et des ramifications légales potentielles.

La complexité diminue le niveau de sécurité

Cet environnement réglementaire toujours plus complexe pose de véritables challenges aux entreprises. Au final, la complexité diminue le niveau de sécurité et les cybercriminels profitent de ces divergences.

- Les États-Unis occupaient une position unique, parce que jusqu'à présent, la plupart des données utiles aux gouvernements étaient stockées sur des serveurs américains. Mais ce n'est plus le cas. Des pays, comme l'Allemagne, la Russie et la Chine développent des plates-formes réglementaires et des lois relatives à la localisation des données.
- Les États-Unis réfléchissent également à une loi qui irait encore plus loin que le projet de loi du Royaume-Uni évoqué précédemment. Elle imposerait à toutes les entreprises qui produisent des logiciels ou du matériel (ou qui gèrent un app store) de fournir au gouvernement des données dans un format lisible et de proposer une technologie de « rétroingénierie » qui les transformerait en informations exploitables.

En l'absence d'initiatives globales, il est impératif d'améliorer la communication et la compréhension entre les secteurs public et privé en matière de cybersécurité. Pour atteindre cet objectif, il est judicieux de commencer par des systèmes plus efficaces d'échange des demandes de données. Il est aussi fondamental que le secteur public et les entreprises partagent des informations, même s'il reste des mésententes à régler.

Par exemple, les entreprises avancent qu'obliger les fournisseurs technologiques à proposer une « porte dérobée » vers les données peut offrir des bénéfices à court terme, mais peut au final briser la confiance des utilisateurs. Cette situation pourrait ensuite faire du mal aux entreprises qui forment l'épine dorsale de l'économie.

La protection des données est un dilemme commun aux secteurs privé et public. Des accords, comme le bouclier de confidentialité américano-européen, sont conçus pour faciliter le flux international des données afin de permettre un traitement analytique et de prouver aux clients qu'eux et leurs données ne courent aucun risque. Reste à voir si les utilisateurs adopteront de telles mesures.

« En l'absence d'initiatives globales, il est impératif d'améliorer la communication et la compréhension entre les secteurs public et privé en matière de cybersécurité. »

Recommandations relatives à la sécurité

À mesure que la nouvelle génération de ransomware évolue, les entreprises doivent bâtir une « première ligne de défense » qui retardera les déplacements latéraux et la propagation, et qui réduira la fenêtre d'action des hackers. Outre les bonnes pratiques de base comme la mise à jour des systèmes et des infrastructures Internet vulnérables (voir **page 22** et **page 29**) et l'amélioration de la gestion des mots de passe (**page 44**), la première ligne de défense englobe la segmentation du réseau.

Celle-ci permet aux entreprises de stopper ou de ralentir le déplacement latéral des menaces qui se propagent automatiquement, mais aussi de les contenir. Elles doivent envisager d'implémenter plusieurs composants pour segmenter leur réseau, notamment :

- Des VLAN et des sous-réseaux pour séparer logiquement l'accès aux données, surtout au niveau de la station de travail
- Un pare-feu dédié et la segmentation de la passerelle
- Des pare-feu basés sur l'hôte qui filtrent les entrées et les sorties
- Des listes noires et blanches d'applications
- Des autorisations de partage réseau basées sur le rôle (moindre privilège)
- Une gestion appropriée des informations d'identification

LA DERNIÈRE LIGNE DE DÉFENSE : LA RESTAURATION DES SAUVEGARDES

La restauration des sauvegardes constitue la dernière ligne de défense pour les entreprises qui cherchent à éviter, aujourd'hui et à l'avenir, de payer une importante rançon aux cybercriminels qui ont chiffré leurs données à l'aide d'un ransomware (**page 10**). Toutefois, restaurer un environnement suite à l'attaque d'un ransomware en minimisant les pertes de données et les interruptions de service dépendra des sauvegardes de systèmes et des sites de reprise après sinistre touchés.

Si le ransomware a effacé, supprimé ou bloqué les sauvegardes locales, les sauvegardes hors site restent souvent le seul espoir de rétablir le service sans payer de rançon. La fréquence d'envoi des sauvegardes hors site détermine donc le volume de données inaccessibles ou perdues.

N'IGNOREZ PAS LA MENACE QUE REPRÉSENTENT LES INFECTIONS DE NAVIGATEUR

Lorsque des publicités malveillantes sont insérées via le trafic chiffré HTTPS, les acteurs de la sécurité ne peuvent pas identifier instantanément la menace (voir **page 21**). En outre, les hackers utilisent de plus en plus le protocole HTTPS pour masquer leur activité, les équipes de sécurité doivent donc plus que jamais arrêter de considérer les infections de navigateur comme une menace de faible ampleur pour l'entreprise et ses utilisateurs.

Une infection de navigateur qui semble bénigne peut vite devenir un problème grave. Il est prouvé que les injecteurs de publicités malveillantes jouent un rôle primordial en permettant aux hackers de poser les bases d'attaques plus risquées.

En surveillant de plus près les infections de navigateur, les entreprises pourront mieux les identifier et les corriger. Les outils d'analyses du comportement et les informations collaboratives sur les menaces sont des ressources essentielles pour les acteurs de la sécurité qui cherchent à remédier à ce type de problème. Il est également fondamental de former les utilisateurs de sorte qu'ils préviennent les équipes de sécurité en cas d'augmentation du nombre de fenêtres publicitaires intempestives ou autres publicités non sollicitées.

PRÉVOIR L'INSTALLATION RÉGULIÈRE DE CORRECTIFS

Les entreprises de toutes tailles, tous secteurs confondus, doivent aller au-delà des exigences réglementaires qui ne suffisent plus face aux menaces modernes. Une approche qui donne la priorité à la sécurité nécessite une défense intégrée contre les menaces, en plus d'un engagement financier.

Par exemple, les professionnels de la sécurité doivent régulièrement vérifier la présence de comptes système ou administrateur non prévus à l'aide des outils à leur disposition. Ils doivent aussi consigner et analyser l'ensemble des communications sur le réseau à la recherche de trafic malveillant, mais aussi examiner ce trafic suspect pour y trouver des indicateurs de compromission. De leur côté, les dirigeants doivent fournir les outils nécessaires pour réaliser de telles investigations en profondeur.

En outre, ils doivent s'assurer que l'environnement est à jour en installant régulièrement les tout derniers correctifs des systèmes d'exploitation et des logiciels couramment utilisés pour éviter que les hackers ne trouvent et n'exploitent leurs faiblesses.

Les indicateurs de compromission n'offrent pas d'informations suffisantes sur les menaces

Les indicateurs de compromission (IoC) constituent le langage des informations sur les menaces. Cependant, aussi précieuses que peuvent être ces données pour les acteurs de la sécurité chargés de mener des investigations, les IoC n'offrent pas d'informations suffisantes.

Les entreprises peuvent dépenser des millions de dollars pour obtenir des listes d'IoC qui sont commercialisées comme étant des informations sur les menaces. Mais il incombe ensuite à leurs équipes de sécurité d'analyser ces données pour découvrir dans quelle mesure elles s'avèrent intéressantes pour l'entreprise. Ce processus qui mobilise énormément de ressources peut éloigner les experts de la sécurité des activités prioritaires. Dans certains cas, à trop faire confiance aux IoC, l'entreprise peut penser à tort qu'elle est protégée des cybercriminels qui s'intéressent davantage au système de sécurité d'une autre entreprise.

Mais alors, qu'est-ce que la collecte d'informations sur les menaces ? Il s'agit de récolter des données qui sont converties en informations exploitables en fonction du contexte dans lequel elles ont été générées. Les informations sur les menaces incluent la marche à suivre en fonction de ce que disent les données. Sans cette application professionnelle, les données ne sont pas analysables.

Pour s'assurer qu'elles investissent dans de véritables informations sur les menaces et en tirent effectivement parti, les entreprises doivent trouver des fournisseurs de solutions de sécurité qui associent les indicateurs de compromission, le contexte avec l'impact sur l'entreprise et des instructions. Elles doivent prendre soin d'ajouter un élément humain dans le processus et d'intégrer ces données dans leurs outils afin d'automatiser les informations sur les menaces pour les équipes de sécurité.

Il est important de distinguer les IoC des informations sur les menaces. Ces dernières aident les acteurs de la sécurité à cerner l'attaque dans son ensemble et à améliorer les délais de détection et la gestion des incidents.

« Il est important de distinguer les IoC des informations sur les menaces. Ces dernières aident les acteurs de la sécurité à cerner l'attaque dans son ensemble et à améliorer les délais de détection et la gestion des incidents. »

Conclusion

Les acteurs de la sécurité ont bien des difficultés à faire face aux attaques d'aujourd'hui. Tant que les cybercriminels ont le champ libre pour mener à bien leurs activités et développer de nouvelles techniques, ils sont inarrêtables. Par contre, si une entreprise peut réduire le champ d'action des hackers et les empêcher de préparer et d'exécuter leur attaque, ces derniers devront prendre des décisions sous la pression. Ils courent donc plus de risques d'être démasqués et arrêtés.

Prendre le dessus sur les hackers en les obligeant à modifier leurs techniques en permanence permet de réduire leur champ d'action. Plus ils doivent s'adapter, plus ils risquent de laisser une piste qui pourrait permettre de les identifier, peu importe le nombre de voies empruntées pour éviter d'être détectés et couvrir leurs traces.

C'est pourquoi c'est une stratégie importante. Si les acteurs de la sécurité ne connaissent pas leurs capacités à détecter les menaces, ils ne peuvent pas se perfectionner. Les délais de détection et de correction doivent être considérés comme des indicateurs clés de performance. Ainsi, les équipes de sécurité pourront se concentrer sur les techniques qui permettent de restreindre les cybercriminels et de les obliger à changer de stratégie.

Comme toujours, les entreprises et les utilisateurs jouent un rôle prépondérant en contribuant à réduire le champ d'action des hackers. Pour les entreprises, c'est sûrement le moment ou jamais de renforcer la sécurité.

Mettre à niveau les systèmes et une infrastructure vieillissante, et corriger les vulnérabilités empêcheront les cybercriminels d'utiliser ces ressources pour mettre en œuvre leurs campagnes. Les hackers responsables d'attaques par ransomware SamSam ont déjà prévenu l'économie parallèle qu'il était possible d'exploiter d'anciennes vulnérabilités afin de compromettre des utilisateurs et de bénéficier d'une meilleure rentabilité. (Reportez-vous à la section « Ransomwares : des attaques très rentables et difficiles à contrer », **page 7**.)

De nombreuses entreprises ont atteint un seuil critique avec leur infrastructure Internet. Elles veulent simplifier et mettre à jour leurs appareils et leurs logiciels afin de réduire les coûts et de poser les bases d'un environnement IT fort qui contribuera à leur réussite à l'heure de l'économie numérique de nouvelle génération. C'est le moment de renforcer leur sécurité et leur visibilité sur tout le réseau et ainsi de réduire la fenêtre d'action dont profitent actuellement les hackers.

« De nombreuses entreprises ont atteint un seuil critique avec leur infrastructure Internet... C'est le moment de renforcer leur sécurité et leur visibilité sur tout le réseau et de réduire ainsi la fenêtre d'action dont profitent actuellement les hackers. »

À propos de Cisco

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

Les chercheurs de Cisco CSI, notre écosystème de sécurité adaptative collective, regroupent l'ensemble des informations sur les menaces déduites 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 axée sur les menaces, rendez-vous sur **www.cisco.com/go/security**.

Les participants au rapport semestriel 2016 Cisco sur la cybersécurité

GROUPE D'INFORMATIONS DE SÉCURITÉ ADAPTATIVE ET DE RECHERCHE TALOS

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

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 l'excellence opérationnelle dans tous les domaines : InfoSec, fiabilité de l'ingénierie, protection et confidentialité des données, sécurité du cloud, transparence et validation, recherche sur la sécurité avancée et organismes publics. Pour en savoir plus, visitez **http://trust.cisco.com**.

GLOBAL GOVERNMENT AFFAIRS

Cisco est impliqué à différents niveaux auprès des états pour les aider à façonner des politiques publiques et des réglementations qui soutiennent le secteur technologique et aident les pays 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 se compose d'anciens élus, parlementaires, membres d'organismes de réglementation, représentants du gouvernement américain ainsi que de personnes travaillant dans des organismes publics qui soutiennent Cisco dans la promotion et la protection des technologies dans le monde entier.

COGNITIVE THREAT ANALYTICS

Cognitive Threat Analytics (CTA) de Cisco est un service cloud qui détecte les failles, les programmes malveillants opérant à l'intérieur des réseaux protégés et d'autres menaces, au moyen d'analyses statistiques des données du trafic réseau. En procédant à une analyse de comportement et à une détection des anomalies, la solution identifie les symptômes d'une infection par programme malveillant ou d'une violation des données, et comble les failles des défenses 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.

ÉQUIPE INTELLISHIELD

L'équipe du service IntelliShield effectue des recherches sur les menaces et la vulnérabilité, l'analyse, l'intégration et la corrélation des données et des 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 prend en charge plusieurs produits et services Cisco.

LANCOPE

Lancope, une société de Cisco, est l'un des principaux fournisseurs de solutions pour la visibilité sur le réseau et la sécurité adaptative visant à protéger les entreprises contre les principales attaques. Par une analyse de NetFlow, IPFIX et d'autres types de données de télémétrie de 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 zero-day et aux menaces internes. En combinant une surveillance continue sur l'ensemble des réseaux de l'entreprise et des informations sur les utilisateurs, les appareils et les applications, Lancope accélère la résolution des incidents, améliore les analyses et réduit le risque pour l'entreprise.

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 zero-day et les menaces 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, 7 jours sur 7.

SECURITY RESEARCH AND OPERATIONS (SR&O)

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

ADVANCED SECURITY RESEARCH AND GOVERNMENT (ASRG)

Le groupe Advanced Security Research and Government (ASRG) offre des conseils et des recommandations pour une vision à long terme de la sécurité. Pour atteindre cet objectif, le groupe ASRG effectue des recherches internes dans des domaines de sécurité clés, comme la cryptographie avancée et les analyses de sécurité. Il finance et s'associe également avec des chercheurs universitaires qui l'aideront à résoudre les problèmes à long terme.

SERVICES DE TRAITEMENT DES INCIDENTS DE SÉCURITÉ DE CISCO (CSIRS)

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

Télécharger les graphiques

Vous pouvez télécharger tous les graphiques de ce rapport à cette adresse : **www.cisco.com/go/mcr2016graphics.com**

Mises à jour et corrections

Pour consulter les mises à jour de ce rapport et connaître les corrections apportées aux informations, visitez : **www.cisco.com/go/mcr2016errata.com**

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

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

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

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

Publié en juillet 2016