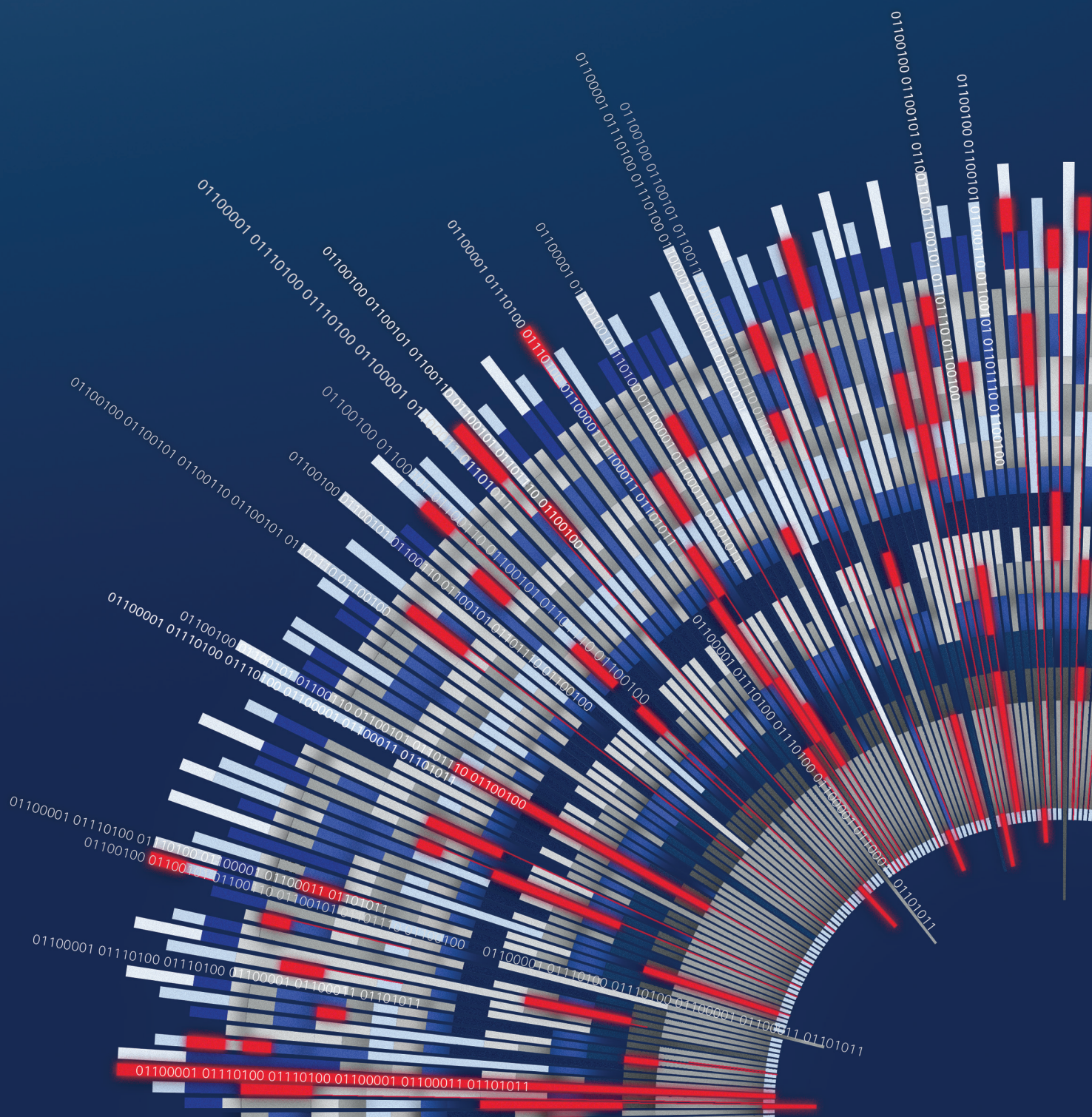
Cisco - 2015

Rapport semestriel sur la cybersécurité



Synthèse

Alors que les hackers développent et déploient toujours plus rapidement de nouveaux programmes malveillants qui peuvent ébranler les défenses du réseau et passer inaperçus, c'est tout le secteur de la cybersécurité qui lutte pour innover au même rythme.

Cette dynamique entraîne un problème de taille pour les entreprises qui investissent dans les produits et les services de sécurité : en choisissant comme souvent plusieurs solutions pour pallier les failles dans le système de sécurité, elles se retrouvent davantage exposées aux menaces.

Notre rapport semestriel sur la cybersécurité analyse ces problématiques croisées et fait le point sur certaines des menaces les plus sophistiquées. Basé sur les études menées par nos experts, il présente les principales menaces observées au premier semestre 2015. Il présente également les tendances qui vont sans doute se confirmer et donne des conseils aux entreprises de toute taille qui recherchent des solutions et des services de sécurité.

Le rapport s'articule en deux parties :

Panorama des menaces

Dans cette section, nous présentons les résultats des dernières études que nous avons menées. Vous y trouverez des informations sur :

- L'actualité des kits d'exploits tels que le kit Angler
- Les macros Microsoft Office, de plus en plus prisées des cybercriminels
- Les nouvelles tactiques des développeurs de malwares pour contourner les solutions de détection
- Le risque d'exposition aux programmes malveillants pour certains secteurs
- Les délais de détection des menaces
- L'actualité des spams, des alertes, des vulnérabilités Java et des publicités frauduleuses

Analyses et constats

Dans cette section, nous abordons la consolidation des solutions de cybersécurité et le concept émergent de protection intégrée. Nous parlerons également de l'importance de concevoir des produits fiables et sécurisés et de faire appel à des fournisseurs de services de sécurité dans un marché où les compétences en matière de cybersécurité se font rares. Enfin, nous verrons comment un cadre de cybergouvernance cohésif peut stimuler l'innovation dans les entreprises et la croissance économique à l'échelle mondiale.

Découvertes majeures

Les cybercriminels ne cessent d'innover et réussissent désormais à pénétrer dans les réseaux sans se faire repérer et en contournant les mesures de sécurité.

- L'exploitation des vulnérabilités Adobe Flash est en hausse. Ces exploits sont régulièrement intégrés à des kits d'exploitation populaires tels que les kits Angler et Nuclear.
- Le kit Angler reste à ce jour le kit d'exploitation le plus sophistiqué et efficace du marché.
- Les opérateurs de logiciels malveillants, tels que les logiciels rançonneurs, font appel à des développeurs professionnels pour s'assurer que leurs tactiques restent efficaces et rentables.
- Les cybercriminels se tournent vers le réseau anonyme Tor et le projet I2P (Invisible Internet Project) pour relayer des communications contrôle-commande sans être démasqués.
- Les cyberpirates utilisent à nouveau les macros Microsoft Office pour propager des programmes malveillants. Cette ancienne tactique qui avait été délaissée pendant un temps revient à la mode à mesure que les cyberpirates cherchent de nouveaux moyens de déjouer les solutions de protection.
- Certains développeurs de kit d'exploitation insèrent des extraits du célèbre roman *Raison et Sentiments* de Jane Austen dans les pages web qui hébergent leurs kits d'exploitation. Les antivirus et autres solutions de protection ont davantage tendance à faire confiance à ces pages après avoir « lu » ce type de texte.
- Les développeurs de programme malveillant utilisent de plus en plus de techniques telles que la détection en sandbox pour masquer leur présence sur les réseaux.
- Le nombre de spams est en augmentation aux États-Unis, en Chine et en Russie, mais est resté relativement stable dans les autres régions au cours des cinq premiers mois de l'année 2015.
- Les acteurs de la cybersécurité cherchent à réduire encore plus les vulnérabilités des solutions open source.
- On a assisté à une baisse du nombre d'exploits impliquant Java au cours du premier semestre 2015 comme le prévoyait le rapport annuel Cisco 2014 sur la cybersécurité.

Sommaire

Synthèse 2

Découvertes majeures 3

Introduction 5

Panorama des menaces 7

L'essor des exploits Adobe Flash au premier semestre 2015 8

L'exploitation Flash donne une nouvelle dimension au kit Angler 10

Angler : la face cachée de la cybercriminalité 11

Les données utiles chiffrées retardent la détection des exploits Angler 12

Les développeurs de kits d'exploitation maîtrisent l'art de dissimuler leurs pages web 13

La démocratisation des logiciels rançonneurs 13

Le réseau Tor plébiscité par les cybercriminels pour masquer leurs communications réseau 15

Les macros Microsoft Office à nouveau utilisées pour exploiter les vulnérabilités 15

Rombertik : un programme malveillant qui vole et détruit les données 18

Le nombre de spams reste stable 20

Menaces et vulnérabilités : les erreurs de programmation courantes, une véritable aubaine pour les exploits 21

Les vulnérabilités tierces 21

De moins en moins d'exploits impliquant Java 24

Les développeurs de programmes malveillants trouvent de nouveaux moyens d'échapper aux solutions de protection 25

Risque sectoriel d'exposition aux programmes malveillants : aucun secteur n'est à l'abri d'une attaque 26

Les activités de blocage : répartition géographique 27

Les types d'attaques en ligne 28

Les publicités frauduleuses : une menace web généralisée en pleine mutation pour contourner les solutions de protection et gagner en efficacité 29

Le point sur le délai de détection des menaces 30

Analyses et constats 31

Des solutions de cybersécurité toujours plus innovantes 32

Consolidation des offres de cybersécurité et protection intégrée contre les menaces 33

Des produits fiables 33

La valeur de l'expertise 34

Un cadre de cybergouvernance mondial pour promouvoir l'innovation 35

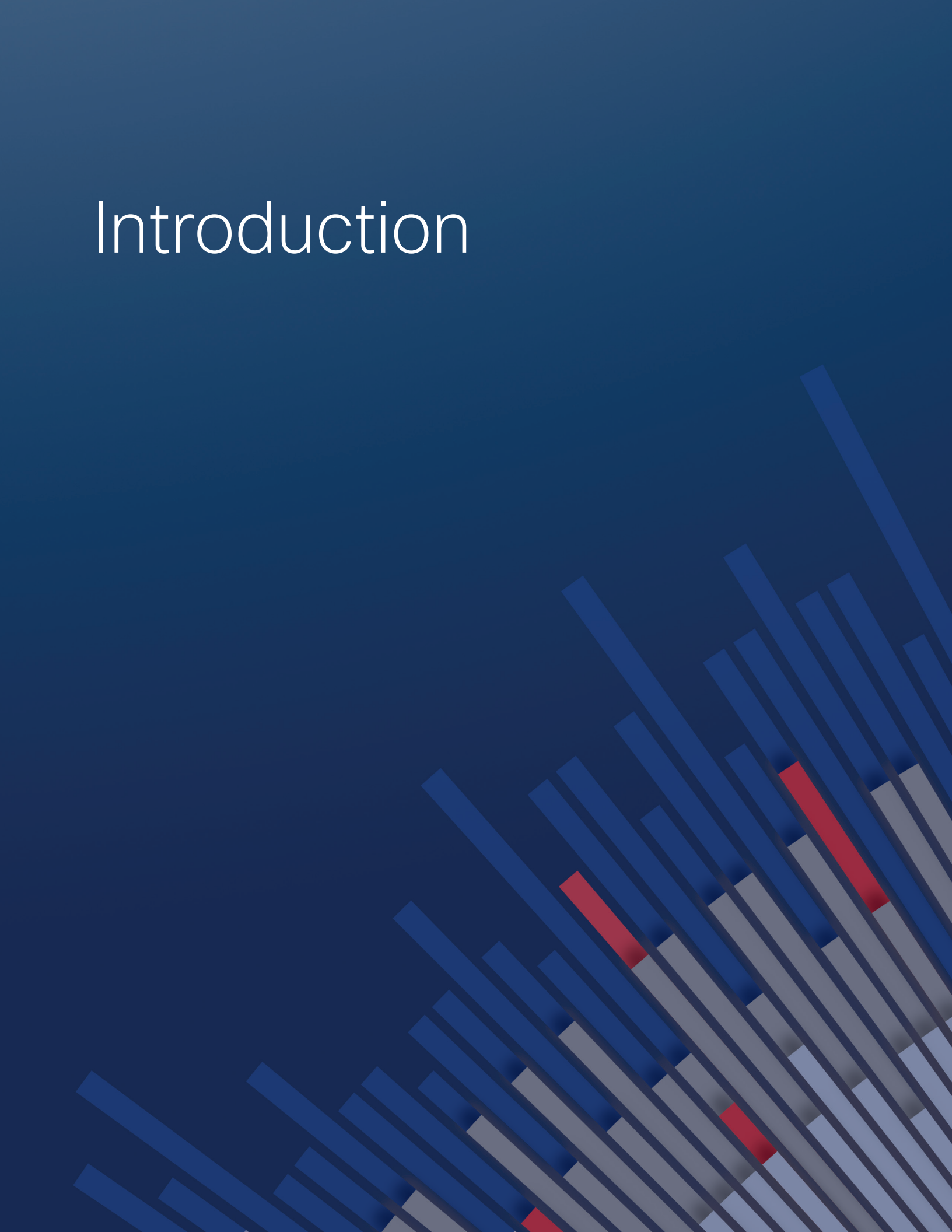
Une meilleure harmonisation des règles : une solution d'avenir ? 35

Conclusion 37

À propos de Cisco 39

Les acteurs du rapport semestriel 2015 Cisco sur la cybersécurité 40

Introduction



Introduction

Depuis plusieurs années, les développeurs de programmes malveillants et les cybercriminels utilisent des tactiques de plus en plus sophistiquées. Nos récents rapports sur la cybersécurité ont à de nombreuses reprises fait état de cette évolution dans l'économie parallèle et des efforts fournis par les professionnels de la sécurité pour contrer ces attaques.

Les cyberpirates démontrent une capacité toujours plus grande à innover rapidement et à trouver de nouveaux moyens pour compromettre les systèmes et déjouer les solutions de détection. Au cours du premier semestre 2015, on a avant tout constaté chez eux une volonté de mettre au point de nouveaux outils et stratégies ou d'adapter des techniques existantes afin de contourner les obstacles. Grâce à des tactiques telles que l'obfuscation, ils peuvent non seulement passer à travers les défenses du réseau, mais également mettre en œuvre leurs exploits pendant longtemps avant d'être repérés, si tant est qu'ils le soient.

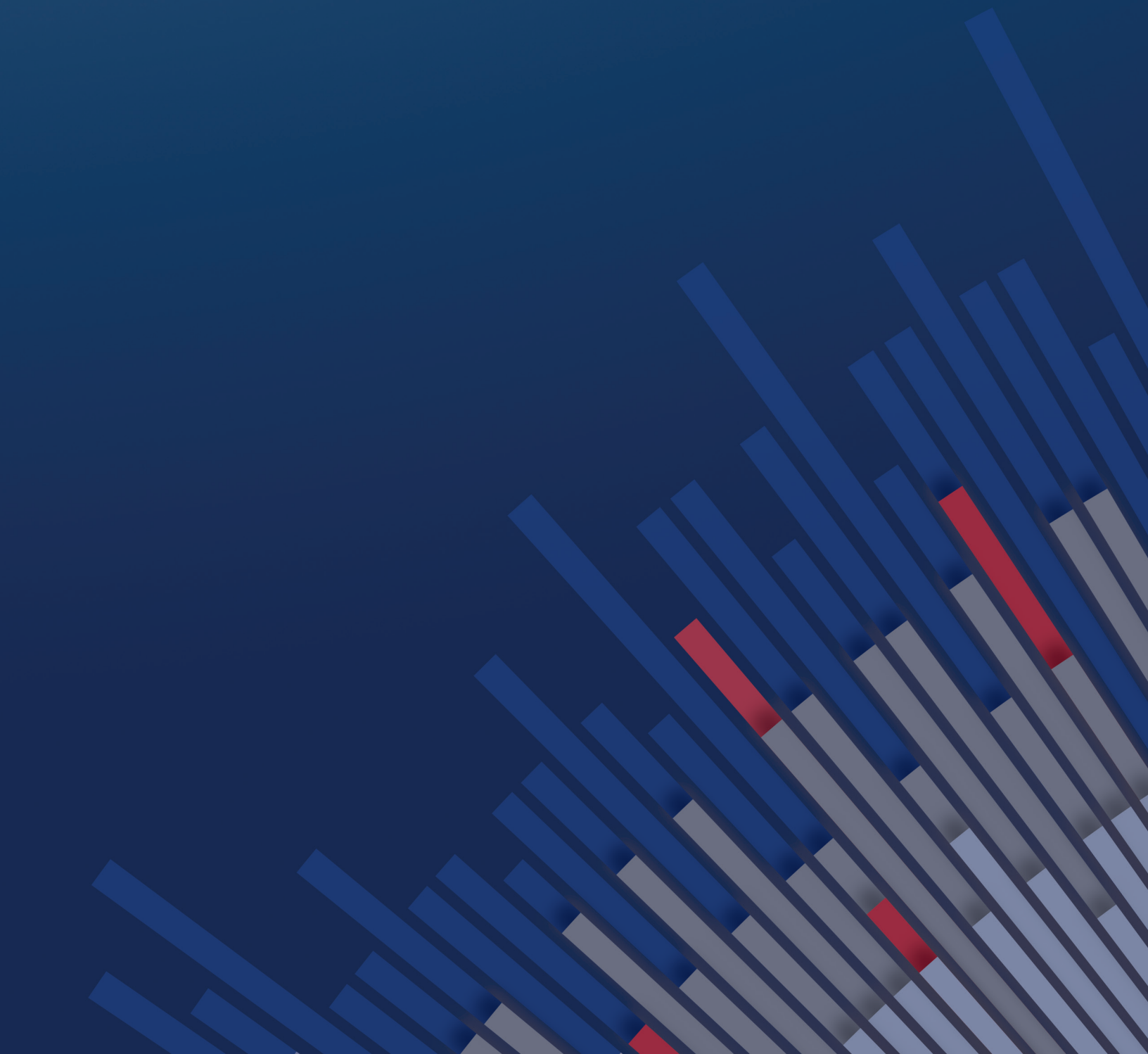
Pour contrer ces attaques, les fournisseurs de cybersécurité doivent également innover. Les analystes mettent à jour les solutions de protection afin qu'elles puissent analyser de nouveaux formats de fichiers, tels que .cab et .chm, qui sont utilisés par les nouvelles attaques. De leur côté, les équipementiers développent de nouveaux moteurs de détection et ne cessent d'évaluer et d'adapter les règles d'analyse heuristique.

Les fournisseurs de cybersécurité savent qu'ils doivent rester sur le qui-vive. Ils savent que s'ils baissent leur garde, même très brièvement, les cyberpirates sauront trouver la faille. Toutefois, l'innovation en matière de sécurité n'est pas aussi rapide qu'elle devrait l'être.

De nombreux fournisseurs proposent des solutions de protection partielles ou individuelles. Et les acheteurs, c'est-à-dire les entreprises qui leur achètent des outils de sécurité, s'orientent avant tout vers des solutions de dépannage plutôt que de mettre en place une véritable stratégie de protection. Et comme ils ne déploient pas les technologies et les processus à l'échelle de l'entreprise, ils peinent à gérer efficacement ces multiples outils de sécurité.

La consolidation des offres du marché de la cybersécurité et l'intégration étroite des meilleures technologies peuvent aider, à terme, à libérer les entreprises de cette approche si cloisonnée de leur défense (voir page 33). Parallèlement, une stratégie de défense approfondie et proactive, dont la technologie n'est qu'un composant, peut aider les entreprises de toute taille et leurs équipes chargées de la sécurité à prévenir la menace de l'innovation cybercriminelle dont fait état ce rapport.

Panorama des menaces



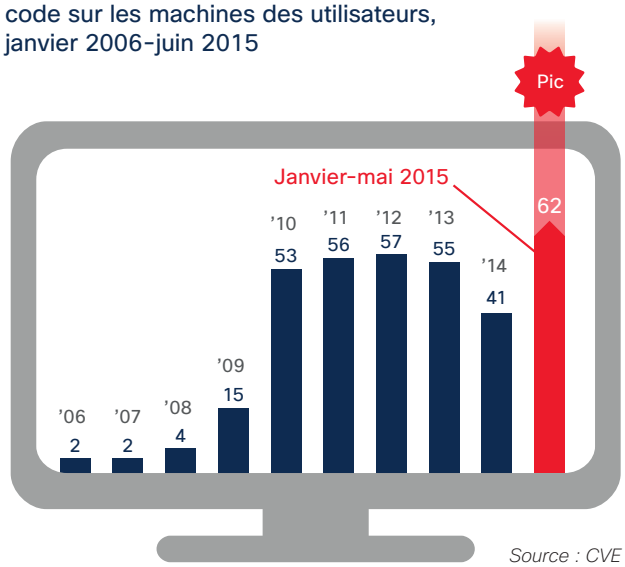
Panorama des menaces

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

L'essor des exploits Adobe Flash au premier semestre 2015

Pour les cinq premiers mois de l'année 2015, le dictionnaire CVE (Common Vulnerabilities and Exposures) a répertorié 62 vulnérabilités pour Adobe Flash Player entraînant l'exécution de code sur les machines des utilisateurs. Comme le montre la Figure 1, seules 41 de ces vulnérabilités avaient été identifiées en 2014. Le deuxième pic significatif a eu lieu a eu lieu en 2012 où 57 vulnérabilités Flash avaient été détectées. Si le même rythme d'identification de nouvelles vulnérabilités se poursuit au second semestre, 2015 serait l'année de tous les records avec plus de 100 exploits répertoriés.

Figure 1 : Nombre de vulnérabilités de Flash qui ont entraîné l'exécution de code sur les machines des utilisateurs, janvier 2006-juin 2015



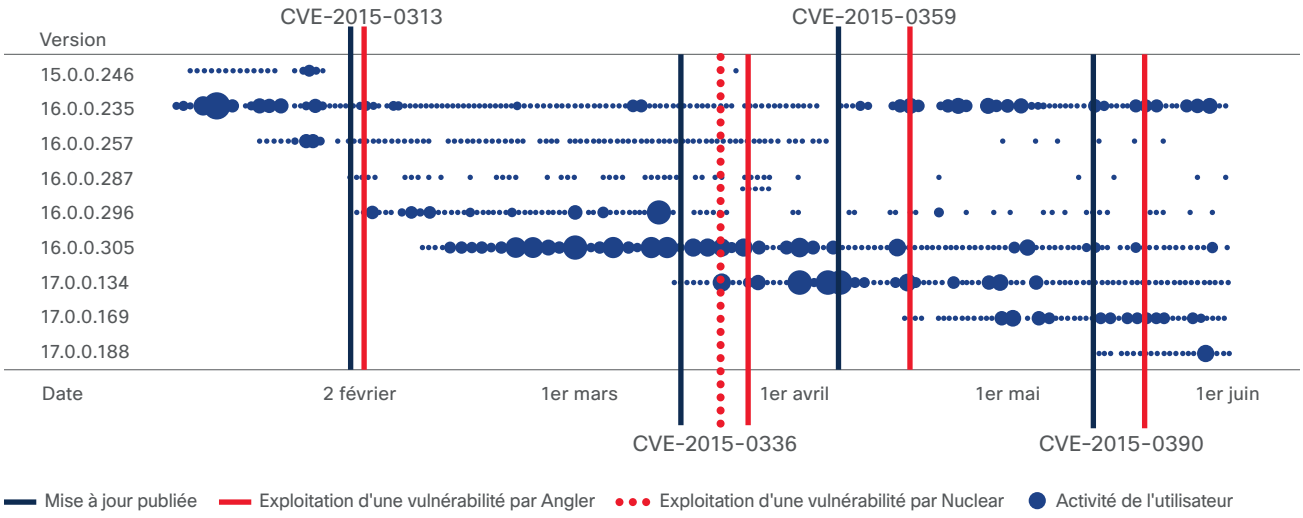
Source : CVE

La hausse récente de l'exploitation des vulnérabilités Flash a deux causes principales :

- **Les exploits Flash sont régulièrement intégrés aux dernières versions des kits d'exploitation tels que le kit Angler (voir page 9).**
- **Bien qu'Adobe mette fréquemment à jour son lecteur Flash Player, les utilisateurs attendent souvent trop longtemps avant d'appliquer ces mises à jour qui les protégeraient contre les attaques exploitant la vulnérabilité à l'origine du correctif.**

Il semblerait que de nombreux utilisateurs aient des difficultés à appliquer régulièrement les mises à jour Adobe Flash et qu'ils ignorent même jusqu'à l'existence de certaines mises à niveau. La Figure 2 montre que les développeurs du kit Angler profitent de cette « brèche de correction », c'est-à-dire le laps de temps entre la publication d'une mise à jour par Adobe et son installation par les utilisateurs. (La technologie Cisco permet aux analystes de vérifier les versions logicielles des utilisateurs à tout moment.)

Figure 2 : Requêtes effectuées par version de Flash, par date



Source : données Cisco AnyConnect

Par exemple, sur la période de février 2015 illustrée dans la Figure 2, on voit que de nombreux utilisateurs ont rapidement installé la dernière version de Flash (16.0.0.305). Cette mise à jour, publiée le 2 février 2015, visait à mettre fin à la vulnérabilité CVE-2015-0313. Cependant, alors que les utilisateurs passaient à la nouvelle version de Flash, le kit Angler a activement exploité la vulnérabilité connue de la précédente version.

La Figure 2 montre également que les créateurs du kit d'exploitation Angler ont rapidement su développer et mettre en place une attaque opérationnelle ciblant la vulnérabilité CVE-2015-0313. Nous avons constaté la même rapidité d'innovation avec d'autres exploits Flash au cours du premier semestre 2015. Par exemple, Nuclear, un autre kit d'exploitation sophistiqué et très actif, a rapidement su cibler les vulnérabilités CVE-2015-0336. Le kit Angler a commencé à exploiter la même vulnérabilité peu de temps après.

Cette lacune de correction explique en partie pourquoi les cyberpirates réussissent encore aujourd'hui à atteindre les utilisateurs Java (voir Figure 3).

Les attaques ciblant Flash et d'autres nouvelles vulnérabilités sont intégrées si rapidement aux kits d'exploitation tels qu'Angler et Nuclear que les équipes chargées de la sécurité ont de plus en plus de mal à suivre le rythme. Le délai de détection est également plus long car une analyse rétrospective est bien souvent nécessaire pour identifier ces menaces.

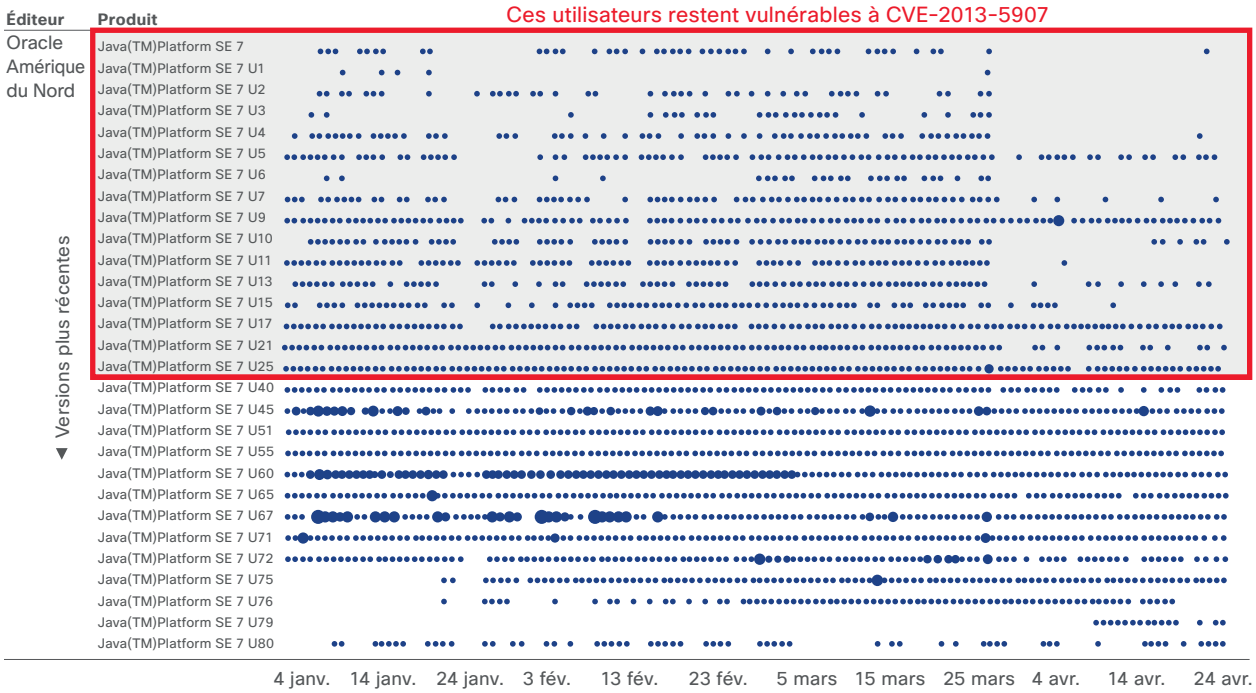
Aussi, pour les particuliers et les entreprises ne faisant appel qu'à un seul moteur de détection, le risque de compromission des données est très élevé. Et dans des environnements ne prenant pas en charge la fonctionnalité d'analyse rétrospective, les menaces liées à des attaques de type « zero-day » ou évasives peuvent longtemps passer inaperçues, voire ne jamais être identifiées.

Cependant, une seule mesure fondamentale, à savoir l'installation rapide et régulière des correctifs logiciels, permet de réduire de manière significative le risque de compromission par des menaces conçues pour exploiter les vulnérabilités connues dans Flash et Java.

Partager le rapport

Figure 3 : Nombre de requêtes effectuées par version de Java, par date

Partager le rapport



Source : données Cisco Cloud Web Security

L'exploitation Flash donne une nouvelle dimension au kit Angler

Partager le rapport

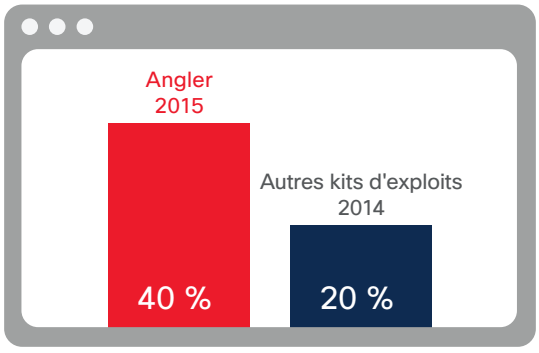
Plus tôt cette année,[1] Cisco a identifié le kit d'exploitation Angler comme LE kit à surveiller parmi tous les kits d'exploitation connus en raison de son utilisation inédite des vulnérabilités Flash, Java, Microsoft Internet Explorer et Silverlight. Jusqu'à présent, le kit Angler domine de loin ses concurrents en matière de sophistication et d'efficacité.

Tous les efforts récemment mis en œuvre par les développeurs du kit pour exploiter au mieux les vulnérabilités dans Adobe Flash illustrent parfaitement leur volonté d'innover.

Selon une étude Cisco, en moyenne 40 % des utilisateurs qui se retrouvent sur une page web du kit Angler sont victimes d'une attaque. (Voir Figure 4.) Cela signifie que le kit Angler est capable d'identifier une vulnérabilité Flash (ou autre) connue qu'il peut exploiter. Il télécharge ensuite les données utiles sur l'ordinateur de l'utilisateur.

En comparaison, en 2014, d'autres kits actifs intégrant différents types d'exploits présentaient un taux de réussite moyen de seulement 20 % selon notre étude.

Figure 4 : Taux de visiteurs avec exploitation de faille, décembre 2014-mai 2015



Source : Cisco Security Research

1 Rapport annuel 2015 de Cisco sur la sécurité, Cisco, janvier 2015 : http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html.

Angler : la face cachée de la cybercriminalité

Si le kit Angler démontre une telle efficacité à attaquer les utilisateurs en ligne, c'est en partie grâce à ses pages web à la fois simples et bien conçues. Les analystes Cisco pensent que les développeurs du kit d'exploitation s'appuient sur la science des données pour créer des pages web générées par ordinateur qui ressemblent à des pages web classiques et dupent facilement les utilisateurs. Les publicités frauduleuses (ou publicités malveillantes en ligne) constituent probablement la principale source du flux constant de trafic web vers ces pages. (Pour plus d'informations sur les publicités frauduleuses, voir la page 29.)

Le kit Angler est également très doué pour contourner les solutions de détection. Ses développeurs ont récemment utilisé la technique de « dissimulation de domaine ». Les développeurs du kit d'exploitation piratent le compte d'un utilisateur inscrit au nom de domaine, puis enregistrent un sous-domaine associé au domaine légitime de l'utilisateur compromis. Si les utilisateurs ne vérifient pas leurs informations de compte, ils n'ont aucun moyen de savoir que ces sous-domaines existent. Les sous-domaines mènent directement à des serveurs malveillants. Éphémères, aléatoires et contenant de très gros volumes de données, ils s'avèrent difficiles à bloquer.

La technique de dissimulation de domaine n'est pas nouvelle, mais son utilisation a augmenté depuis décembre 2014. Selon notre étude, plus de 75 % des activités connues de sous-domaine menées par les développeurs de kit d'exploitation peuvent depuis lors être attribuées à Angler. Le kit d'exploitation transmet diverses données utiles malveillantes, y compris le cheval de Troie rançonneur Cryptowall, via l'exploitation de fichiers.

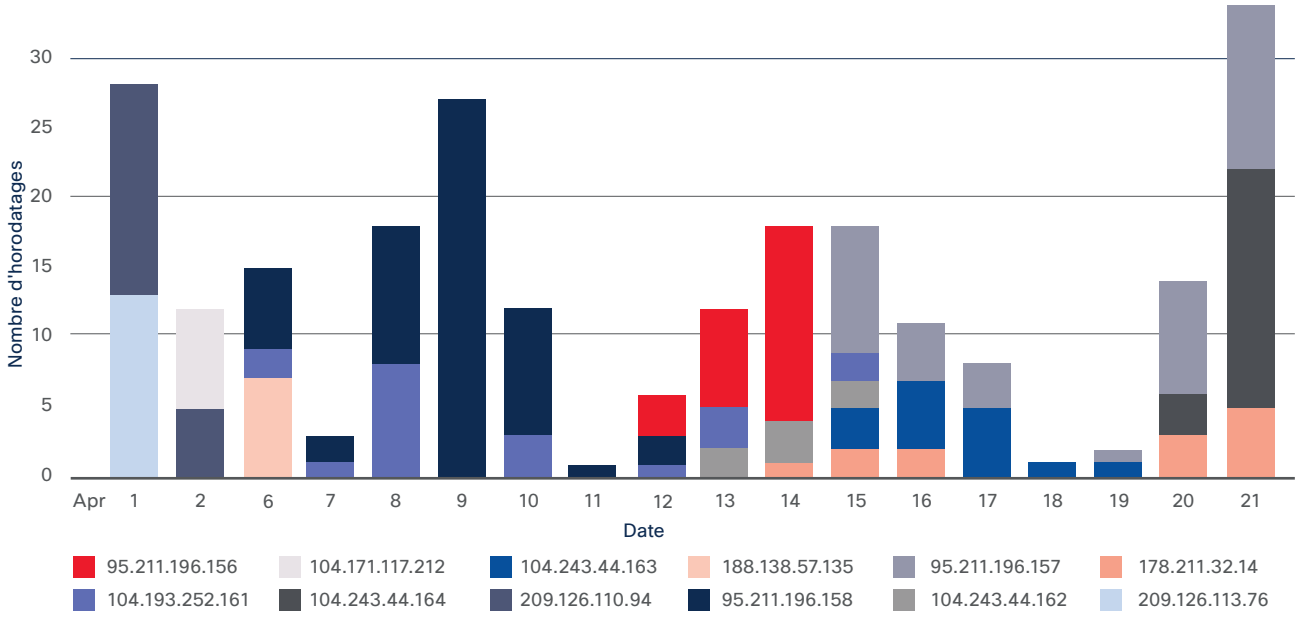
Outre la technique de dissimulation de domaine, le kit Angler utilise de multiples adresses IP pour rendre la détection encore plus difficile. L'exemple de la Figure 5 montre combien de fois et à quelle fréquence le kit Angler peut changer d'adresse IP en un seul jour. Le modèle semble aléatoire.

L'article « Threat Spotlight: Angler Lurking in the Domain Shadows », publié sur le blog du groupe de sécurité adaptative et de recherche Talos de Cisco, explique comment Angler crée des sous-domaines qui peuvent diffuser du contenu malveillant et pourquoi une approche de défense approfondie est essentielle dans la détection de ce type d'attaque.

Voir aussi **« Domain Shadowing Goes Nuclear: A Story in Failed Sophistication »**, une autre publication du blog Talos, qui examine une campagne Nuclear avec copie diissimulée de domaine. Ce travail encore en cours de développement sera probablement une plate-forme de kit d'exploit performante lorsqu'il sera terminé.

Figure 5 : Exploitations Flash réussies, avril 2015

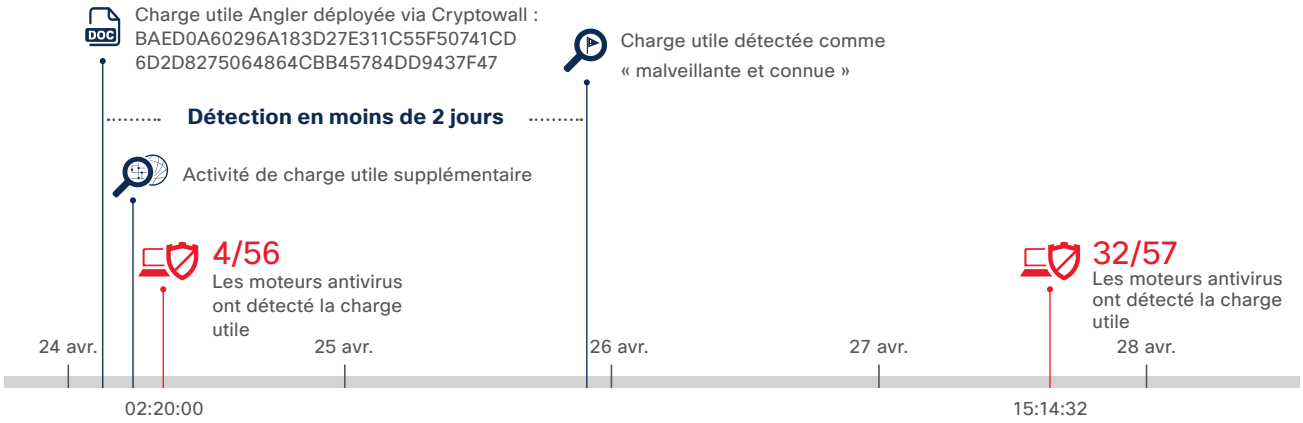
Partager le rapport



*Les couleurs représentent les plages d'adresses IP.

Source : Cisco Security Research

Figure 6 : Diminution du délai de détection pour les données utiles Angler le 24 avril 2015



Source : Cisco Security Research

Les données utiles chiffrées retardent la détection des exploits Angler

Le kit Angler transmet généralement des données utiles chiffrées, souvent sous la forme du cheval de Troie rançonneur Cryptowall. Si celui-ci n'est pas immédiatement bloqué, les données utiles ne peuvent être identifiées qu'à l'aide d'une analyse rétrospective et plusieurs jours peuvent s'écouler avant que la menace ne soit détectée.

Une fois les données utiles identifiées, les développeurs du kit d'exploitation, fidèles à leur réputation de maîtres en innovation, mettront rapidement au point une technique pour transmettre des éléments tels que Cryptowall et contourner les solutions antivirus.

La Figure 6 illustre le délai de détection des données utiles Angler Cryptowall lors de sa première découverte le 24 avril 2015 : BAED0A60296A183D27E311C55F50741 CD6D-2D8275064864CBB45784DD9437F47.

Le premier jour, seuls 4 des 56 moteurs antivirus déployés par VirusTotal ont identifié la nouvelle instance du programme malveillant. En revanche, le 27 avril, 32 des 57 moteurs antivirus avaient détecté la menace.

- 24/04/2015 02:20:00 **4/56** (4 des 56 moteurs antivirus déployés ont détecté les données utiles)
- 27/04/2015 15:14:32 **32/57** (32 des 57 moteurs antivirus déployés ont détecté les données utiles)

Cisco a identifié la menace comme « inconnue » le 24 avril, puis a analysé et rétrospectivement répertorié la menace comme « dangereuse et connue » moins de deux jours plus tard.

Voir « Le point sur le délai de détection des menaces » à la page 30 pour en savoir plus sur la manière dont nous définissons et calculons le délai de détection.

Partager le rapport

Les auteurs de kits d'exploit élèvent leur niveau intellectuel pour garder profil bas

Certains auteurs de kit d'exploit ont recours à la littérature de début du 19ème siècle pour masquer les attaques du 21ème siècle. Plus précisément, certains pirates intègrent des extraits de *Raison et sentiments* de Jane Austen aux pages web hébergeant leurs kits d'exploit.

L'ajout de passages de texte classique à une page web de kit d'exploit est une technique d'obscurcissement plus efficace que l'approche traditionnelle qui consiste à utiliser un texte aléatoire. L'utilisation de texte provenant d'œuvres plus contemporaines telles que des magazines et des blogs est une autre stratégie efficace. Un antivirus et d'autres solutions de sécurité sont plus susceptibles d'identifier la page web comme légitime après la « lecture » d'un tel texte.

Pour les utilisateurs, tomber sur des références inattendues à des personnages populaires d'Austen, tels qu'Elinor Dashwood et Mme Jennings, sur une page web peut être surprenant mais pas une source d'inquiétude. Mais leur manque de méfiance offre aux pirates davantage d'opportunités de lancer leurs exploits.

L'utilisation d'œuvres connues plutôt que de texte aléatoire est un exemple parmi tant d'autres de la manière dont les cybercriminels développent leurs modèles pour éviter toute détection.

Figure 7 : Exemple d'extrait de *Raison et sentiments utilisé* sur une page web de kit d'exploit

```
https://rt1.mtd.cisco-services.com/Ticket/
Display.html?
id=137668&results=ad470ba70bfbd94464c2a0e9deff943b

Sense and sensibility - jane austin
    <small>
      Mr. Ferrars comfortable as a continual flow of
tears would permit her. In the society of both. Why
they should both attend through
    </small>
     She looked down as a difference of the three, by
their presence; and it will be so easily settled. it
    <i>
     the cruel situation in which she had by that
which only could convince her, a better match for
your mother--will you allow him to give rise to
conjectures, which might make it rare; for his
sisters by the hand, and speaking in an audible
voice, and walking the
    </i>
```

Source : Cisco Security Research

La démocratisation des logiciels rançonneurs toujours plus innovants

Partager le rapport

Dans la nouvelle ère des programmes malveillants, les crypto-monnaies telles que le Bitcoin et les réseaux d'anonymisation tels que Tor (voir page 15) permettent aux cyberpirates de se lancer encore plus facilement sur le marché des programmes malveillants et de générer rapidement des revenus. Pour améliorer leur rentabilité tout en continuant à contourner les solutions de détection, les opérateurs de logiciels malveillants tels que les logiciels rançonneurs financent leurs propres équipes de développeurs professionnels dans le but de créer de nouvelles variantes et tactiques.

Les logiciels rançonneurs chiffrent les fichiers des utilisateurs, ciblant aussi bien les photos de famille que les données bancaires, et fournissent les clés de déchiffrage uniquement après que les utilisateurs aient payé une « rançon ». Les logiciels rançonneurs s'attaquent aussi bien aux grandes entreprises qu'aux écoles et aux particuliers.

Le programme malveillant est généralement transmis via un certain nombre de vecteurs, notamment les e-mails et les kits d'exploitation. Le kit d'exploitation Angler (voir page 11), par exemple, est connu pour transmettre les données utiles Cryptowall. Cryptowall est apparu après que son prédécesseur, Cryptolocker, ait été désactivé mi-2014 lors d'une opération policière de grande envergure.

La Figure 8 affiche un exemple de message que les utilisateurs peuvent recevoir lorsqu'ils sont attaqués par le logiciel rançonneur TeslaCrypt qui se présente comme un dérivé de Cryptolocker.

Figure 8 : Exemple de message sur l'écran du ransomware TeslaCrypt

Source : Cisco Security Research

La rançon demandée n'est pas exorbitante et est comprise en général entre 300 $ et 500 $. Pourquoi une rançon si peu élevée ? Les développeurs des logiciels rançonneurs ont réalisé une étude de marché pour déterminer le montant idéal des rançons. La rançon doit rester abordable pour la victime et ne pas l'inciter à aller voir la police. En réalité, la rançon est plutôt perçue comme une dépense collatérale. Et les utilisateurs paient.

Les experts Cisco ont constaté que presque toutes les transactions associées aux logiciels rançonneurs passent par le réseau web anonyme Tor (voir page 15). En utilisant des canaux comme le réseau Tor et le projet I2P (Invisible Internet Project), les cyberpirates s'assurent un faible risque de détection et une rentabilité élevée. I2P est une couche de réseau informatique qui permet aux applications de s'envoyer des messages entre elles sous pseudonymes et en toute sécurité. De nombreux logiciels rançonneurs font également appel à des équipes de cyberpirates chargées de détecter les nouvelles mises à jour publiées par les fournisseurs d'antivirus afin de prévenir les développeurs qu'une variante a été détectée et qu'il est donc temps de changer de techniques.

Le paiement des rançons s'effectue en bitcoins, ce qui complique le suivi des transactions pour les services de police. Et pour ne pas ternir leur réputation sur le marché, en apportant la preuve qu'ils permettent bien aux utilisateurs d'accéder à leurs fichiers chiffrés après le paiement de la rançon, plusieurs opérateurs de logiciels rançonneurs ont mis en place un service clients sophistiqué.

Nous avons récemment observé un certain nombre de campagnes personnalisées conçues pour compromettre des groupes d'utilisateurs spécifiques, tels que les joueurs en ligne. Certains développeurs de logiciels rançonneurs ont été jusqu'à créer des variantes dans des langues rares comme l'islandais pour être sûrs que les utilisateurs résidant dans ces zones comprennent bien le message.

Les utilisateurs peuvent se protéger contre les logiciels rançonneurs en sauvegardant leurs fichiers les plus précieux et en les conservant dans un endroit sûr ou en les isolant physiquement du reste du réseau. Les utilisateurs doivent également savoir que leur système continue à courir un risque même après qu'ils aient payé la rançon et déchiffré les fichiers. Presque tous les logiciels rançonneurs sont multivectoriels. Le programme malveillant peut avoir été propagé par une autre instance de programme malveillant, ce qui signifie que le vecteur d'infection initial doit être traité avant que le système puisse être considéré comme propre.

Pour en savoir plus sur les tendances en matière de faux logiciels de protection (ransomware), consultez les publications du blog du groupe Talos, **« Cryptowall 3.0: Back to Basics »** et **« Threat Spotlight: TeslaCrypt–Decrypt It Yourself »**.

ToR adopté par les cybercriminels pour masquer la communication réseau

Les auteurs de programmes malveillants tentent naturellement d'échapper à la détection et de dissimuler l'emplacement de leurs serveurs. Pour ce faire, beaucoup utilisent le réseau web anonyme ToR pour relayer des communications de contrôle-commande (C&C).

Nos chercheurs ont détecté plusieurs instances où les familles de programmes malveillants, en particulier les variantes de faux logiciels de protection, produisaient un trafic ToR. Bien que ToR soit généralement utilisé au sein des entreprises à des fins légitimes (par exemple, par des professionnels de la sécurité), sa présence peut indiquer un trafic malveillant sur un réseau. Certaines des fonctions qui attirent les utilisateurs légitimes vers le ToR sont également intéressantes pour les escrocs.

Si les professionnels de la sécurité détectent une activité ToR dans leurs réseaux, ils doivent corréler cette observation avec d'autres indicateurs possibles d'activités malveillantes, comme des téléchargements de fichiers exécutables inconnus ou des connexions à des serveurs de kit d'exploit, pour déterminer si le trafic ToR est légitime.

Comme le montre la Figure 9, les pirates déployant le faux logiciel de protection Cryptowall 2.0, ainsi que plusieurs gammes de programmes malveillants, sont des utilisateurs de ToR. (Voir « The Evolution of Ransomware: A Story of Innovation–and Lowering the Bar », page 13). Ces données proviennent de la surveillance des réseaux des clients par Cisco et montrent les incidents où ToR a été utilisé dans des familles de programmes malveillants entre octobre 2014 et mai 2015.

Figure 9 : Familles de programmes malveillants utilisant ToR pour les communications

Source : Cisco Security Research

Les macros Microsoft Office à nouveau utilisées pour exploiter les vulnérabilités

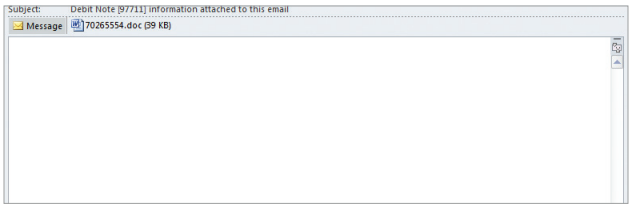
En constatant que les macros Microsoft Office étaient à nouveau utilisées pour lancer des chevaux de Troie bancaires, Cisco s'est rendu compte que non seulement les cybercriminels réutilisaient d'anciens outils ou vecteurs d'attaque, mais également qu'ils modifiaient les programmes si rapidement et si fréquemment qu'ils pouvaient lancer des attaques à répétition sans être détectés.

Les anciens outils utilisés par les créateurs de ces chevaux de Troie sont des macros que l'on retrouve dans les produits Microsoft Office tels que Microsoft Word. Très utilisées autrefois par les cyberpirates, ces macros avaient fini par être désactivées par défaut et avaient donc perdu tout leur intérêt. Toutefois, à l'aide de techniques de piratage psychologique, les cyberpirates réussissent désormais à convaincre les utilisateurs d'activer les macros, ajoutant ainsi une nouvelle tactique à leur actif.

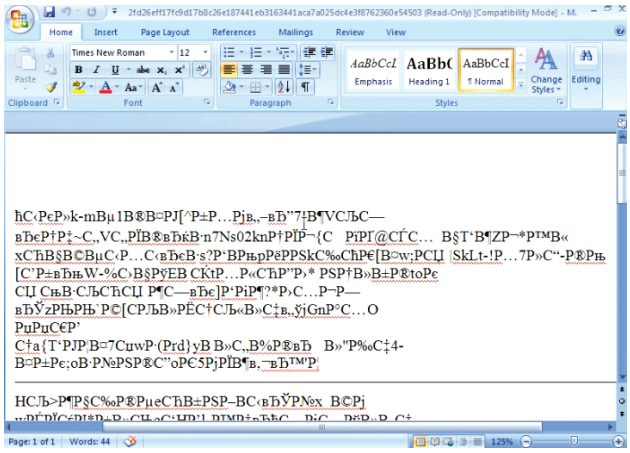
Nous avons étudié deux campagnes récentes dans lesquelles des chevaux de Troie Dridex étaient ajoutés en tant que pièces jointes à des e-mails envoyés à différents destinataires et censés contenir des factures ou d'autres documents importants. Depuis quelques mois, nous détectons chaque jour de nouvelles campagnes Dridex.

Dans la première campagne (Campagne 1), l'objet de l'e-mail avait pour objectif de duper les destinataires en leur faisant croire que les pièces jointes étaient des documents très importants alors que le corps des e-mails était parfois vide.

Dridex : Campagne 1



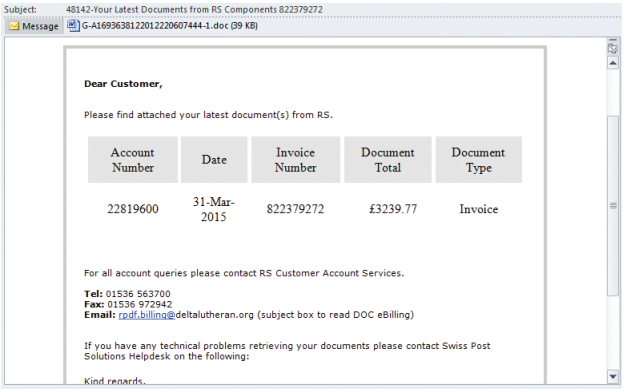
Lorsque les destinataires ouvraient les pièces jointes, un document Word s'affichait avec du texte n'ayant aucun sens.



Dans la deuxième campagne que nous avons étudiée (Campagne 2), le message contenu dans les e-mails semblait légitime car il faisait référence à des numéros de comptes et de factures spécifiques et prétendait que les documents joints étaient des factures. Mais lorsque les destinataires ouvraient le document Word en pièce jointe, le même type de texte incompréhensible téléchargé dans le cadre de la campagne 1 s'affichait.

Partager le rapport

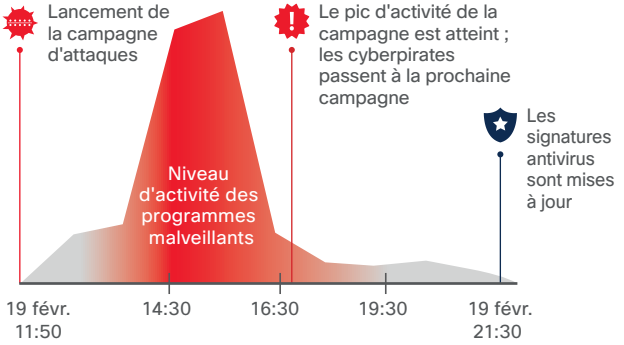
Dridex : Campagne 2



Dans les deux campagnes, les ennuis commençaient dès que le destinataire du message ouvrait le document Word. En arrière-plan, une macro utilisait les agents cmd.exe et PowerShell pour télécharger un fichier exécutable malveillant à partir d'une adresse IP codée. Certaines campagnes que nous avons observées comprenaient même des instructions expliquant à l'utilisateur comment activer les macros. Une fois les macros activées, Dridex pouvait ensuite essayer de voler les identifiants et les mots de passe des comptes bancaires des victimes.

Nos analystes ont constaté que les campagnes de spam transportant les données utiles de Dridex avaient une durée de vie très courte, peut-être de quelques heures seulement, et qu'elles mutaient très fréquemment pour ne pas être détectées. Bien que les solutions antivirus jouent un rôle essentiel dans la sécurité, elles ne sont pas en mesure de détecter des campagnes de spam aussi éphémères. Au moment où une campagne est détectée, les cyberpirates ont déjà modifié le contenu, les agents utilisateur, les pièces jointes et les liens des e-mails. Ils relancent ensuite la campagne que les systèmes antivirus doivent détecter à nouveau. Comme le montre la Figure 10 qui illustre une campagne du programme malveillant DyrezaC, les mises à jour de l'antivirus peuvent survenir à la fin d'une campagne.

Figure 10 : DyrezaC peut être plus rapide que les antivirus



Source : Cisco Security Research

Cette approche qui combine spam, macros Microsoft Office et Dridex a séduit de très nombreux cybercriminels au cours du premier semestre 2015. Nous avons étudié 850 échantillons uniques d'e-mails et de pièces jointes Microsoft Office transportant ce cheval de Troie, ce qui fait beaucoup pour une campagne de spam. Les créateurs de ces campagnes à mutation rapide savent parfaitement comment passer outre les mesures de sécurité. Ils connaissent le niveau de fiabilité de la détection antivirus pour ces menaces et adaptent leur tactique en fonction.

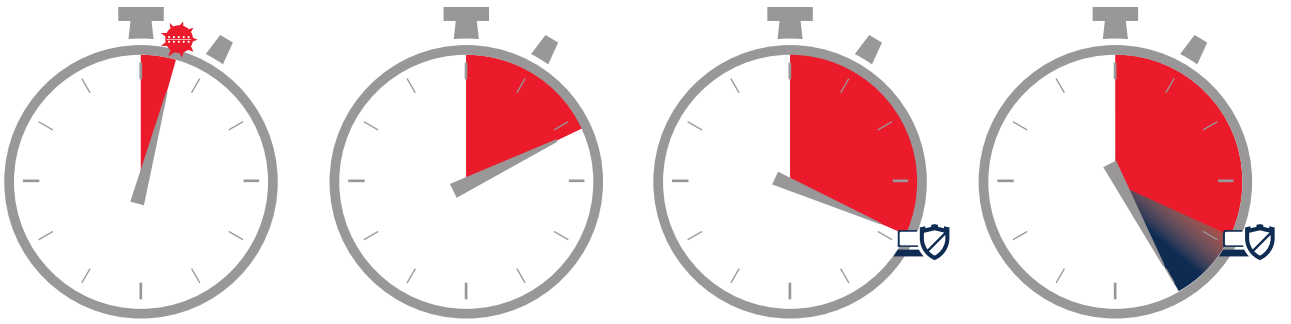
Dans l'exemple de la Figure 11, l'image montre que plusieurs heures s'étaient écoulées avant même que les moteurs antivirus ne commencent à détecter la menace Dridex. La campagne ayant duré environ cinq heures, les solutions antivirus ont protégé le système uniquement à la fin de la campagne.

S'ils considèrent l'exploitation de macros comme une tactique obsolète, les professionnels de la sécurité ne pourront pas protéger leurs réseaux de ces menaces. La meilleure protection repose sur une stratégie de défense complète qui associe plusieurs solutions de sécurité à l'antivirus. Les filtres contre les attaques de virus, par exemple, peuvent mettre en quarantaine les messages suspects pendant une période maximale de 12 heures pour permettre à l'antivirus de détecter les nouvelles menaces.

Pour plus d'informations sur les macros Microsoft Office et le cheval de Troie Dridex, consultez la publication du blog du groupe Talos, **« Threat Spotlight: Spam Served With a Side of Dridex »**.

Figure 11 : Graphique de détection pour Dridex, mars-avril 2015

Partager le rapport



Source : Cisco Security Research

Rombertik : un programme malveillant qui vole et détruit les données

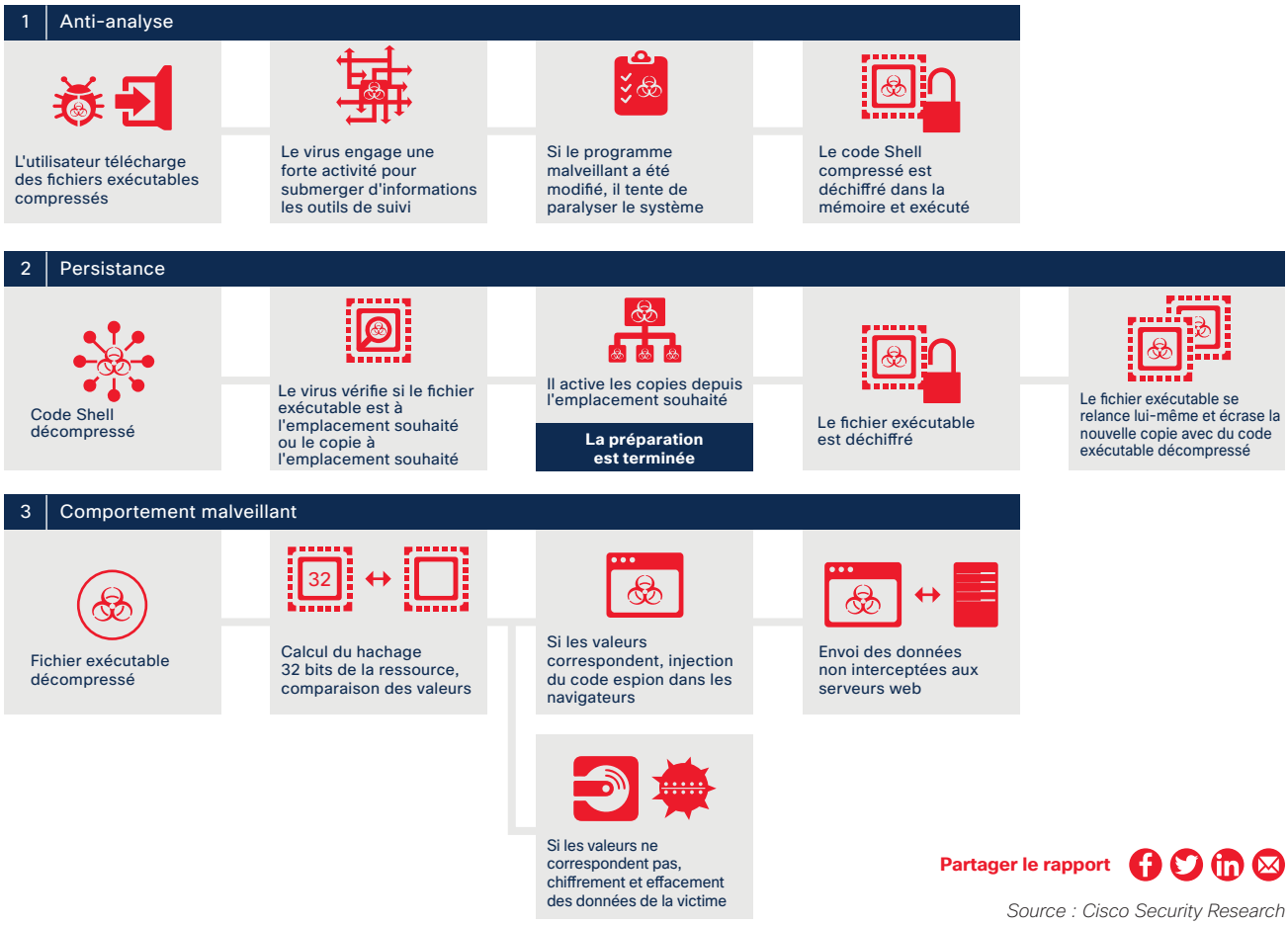
Lorsqu'ils mettent au point un programme malveillant sophistiqué, les développeurs le configurent pour qu'il s'arrête de fonctionner lorsqu'il est analysé par les systèmes de sécurité afin qu'il ne soit pas bloqué ou détruit. Parallèlement, les experts en sécurité recherchent constamment de nouveaux outils d'analyse statiques, dynamiques et automatisés qui permettraient de détecter plus facilement les cyberpirates.

À cette fin, Cisco a récemment effectué de l'ingénierie inverse sur le programme malveillant complexe Rombertik qui est en mesure de détecter toute tentative de modification de son système binaire, à l'instar de ce qui se passe en ingénierie inverse. Le programme Rombertik tente de détruire le MBR (Master Boot Record) de son ordinateur hôte. Lorsque cela n'est pas possible, il tente de détruire les fichiers du répertoire personnel de l'utilisateur.

Contrairement aux autres programmes malveillants qui tentent de passer inaperçus, Rombertik semble avoir été conçu pour se faire remarquer. L'ingénierie inverse est une technique essentielle utilisée par Cisco et d'autres spécialistes des menaces pour comprendre le fonctionnement d'un programme malveillant, et notamment comment il échappe aux solutions de détection.

L'objectif de Rombertik consiste à s'introduire dans le navigateur web d'un utilisateur afin d'en extraire des données sensibles et de les transmettre à un serveur géré par des cyberpirates. Sur le principe, Rombertik est similaire au programme malveillant connu sous le nom de Dyre.[2] Cependant, Dyre a pour but de voler des identifiants bancaires, tandis que Rombertik semble collecter aléatoirement toutes sortes de données utilisateur.

Figure 12 : La combinaison unique d'anti-analyse et de comportements malveillants de Rombertik



Partager le rapport

Source : Cisco Security Research

Rombertik s'introduit dans les systèmes des utilisateurs via des spams ou des messages d'hameçonnage qui utilisent le piratage psychologique pour convaincre les destinataires de télécharger et de décompresser les pièces jointes contenant le programme malveillant. Lorsqu'un utilisateur décompresse le fichier, celui-ci ressemble à un PDF alors qu'il s'agit en réalité d'un fichier exécutable d'écran de veille qui commence à endommager le système. Comme le montre la Figure 12, si Rombertik se rend compte qu'on est en train de le modifier, il tente de détruire le MBR du système et redémarre l'ordinateur qui sera ensuite inutilisable.

Les outils d'anti-analyse avancés des programmes malveillants d'aujourd'hui

Il est possible que Rombertik soit le pionnier de la nouvelle ère des programmes malveillants, car les développeurs de programmes malveillants adoptent rapidement les meilleures tactiques de leurs pairs. Comme nos analystes ont pu s'en rendre compte, Rombertik associe plusieurs fonctionnalités d'obfuscation et de destruction. Par exemple, Rombertik inclut du code excessif ou « poubelle » qui oblige les analystes de sécurité à passer plus de temps à vérifier et à analyser le programme malveillant afin que, surchargés de travail, ils n'aient plus le temps d'en analyser chaque fonction.

Pour contourner les solutions de détection et forcer l'expiration du délai d'analyse en sandbox avant la prise en charge des données utiles malveillantes, Rombertik adopte une approche unique. En général, lorsqu'il se trouve dans un sandbox, le programme malveillant se met en veille jusqu'à expiration du délai. Les outils d'analyse de sécurité devenant de plus en plus efficaces dans la détection du processus de mise en veille, les développeurs du programme malveillant ont dû adapter leur stratégie.

Dans le cas de Rombertik, le programme malveillant écrit 960 millions de fois un octet de données aléatoires dans la mémoire. Cela peut affecter à la fois les sandboxes et les outils de suivi des applications. Ainsi, l'application peut gagner du temps sans que les sandboxes ne s'en rendent compte car celle-ci ne dort pas vraiment. En outre, consigner les 960 millions de demandes d'écriture prend beaucoup de temps et complique l'analyse pour les deux types d'outils.

Rombertik dispose de plusieurs techniques d'obfuscation de ce type lorsqu'il est en cours d'analyse ou d'ingénierie inverse, mais sa technique antimodification finale peut causer de sérieux dégâts. Si le programme malveillant détecte qu'il a été modifié en vue d'une analyse, il tente de remplacer le MBR de la machine. S'il ne peut pas le faire, il détruit tous les fichiers du répertoire personnel de l'utilisateur. Lorsque la machine redémarre, elle est inutilisable.

Si Rombertik passe toutes ces étapes antimodification avec succès, il peut enfin commencer sa principale activité : voler toutes les données que les utilisateurs saisissent dans leur navigateur pour les transmettre à son serveur.

Rombertik : un défi de taille pour les spécialistes de la sécurité

Ce qui pose le plus problème avec Rombertik, ce sont ses techniques avancées pour échapper aux analyses et sa capacité à endommager le système d'exploitation des machines sur lesquelles il s'exécute. Cette approche représente un défi de taille pour les spécialistes de la sécurité qui devront encore faire face à de nombreux programmes malveillants de cette envergure à l'avenir. Il y a fort à parier que les autres développeurs de programmes malveillants ne se contenteront pas seulement d'adopter les tactiques de Rombertik mais qu'ils les rendront encore plus agressives.

Les bonnes pratiques en matière de sécurité peuvent protéger les utilisateurs, tout comme le simple fait de leur déconseiller d'ouvrir les pièces jointes provenant d'expéditeurs inconnus. Toutefois, face à des programmes malveillants aussi sophistiqués et dangereux que Rombertik, il est primordial de mettre en place une stratégie de protection complète qui agit tout au long du processus d'attaque.

Consultez la publication du blog du groupe Talos, **« Threat Spotlight: Rombertik - Gazing Past the Smoke, Mirrors, and Trapdoors »**, pour une analyse approfondie du programme malveillant Rombertik.

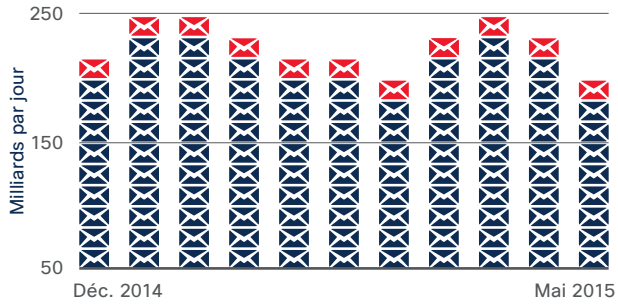
2 « Threat Spotlight: Dyre/Dyreza: An Analysis to Discover the DGA », blog sur la sécurité Cisco, 30 mars 2015, http://blogs.cisco.com/security/talos/threat-spotlight-dyre.

Le nombre de spams reste stable

Même si les cybercriminels développent des méthodes de plus en plus sophistiquées pour passer à travers les défenses du réseau, les spams et les e-mails d'hameçonnage continuent de jouer un rôle majeur dans ces attaques. Le volume de spams à l'échelle mondiale est resté relativement stable, comme le montre la Figure 13.

Dans la Figure 14, une analyse pays par pays révèle que le nombre de spams est en augmentation aux États-Unis, en Chine et en Russie, mais qu'il est resté relativement stable dans les autres régions du monde. Cette évolution s'explique par les fluctuations de l'activité au sein des réseaux sous-jacents de spammeurs.

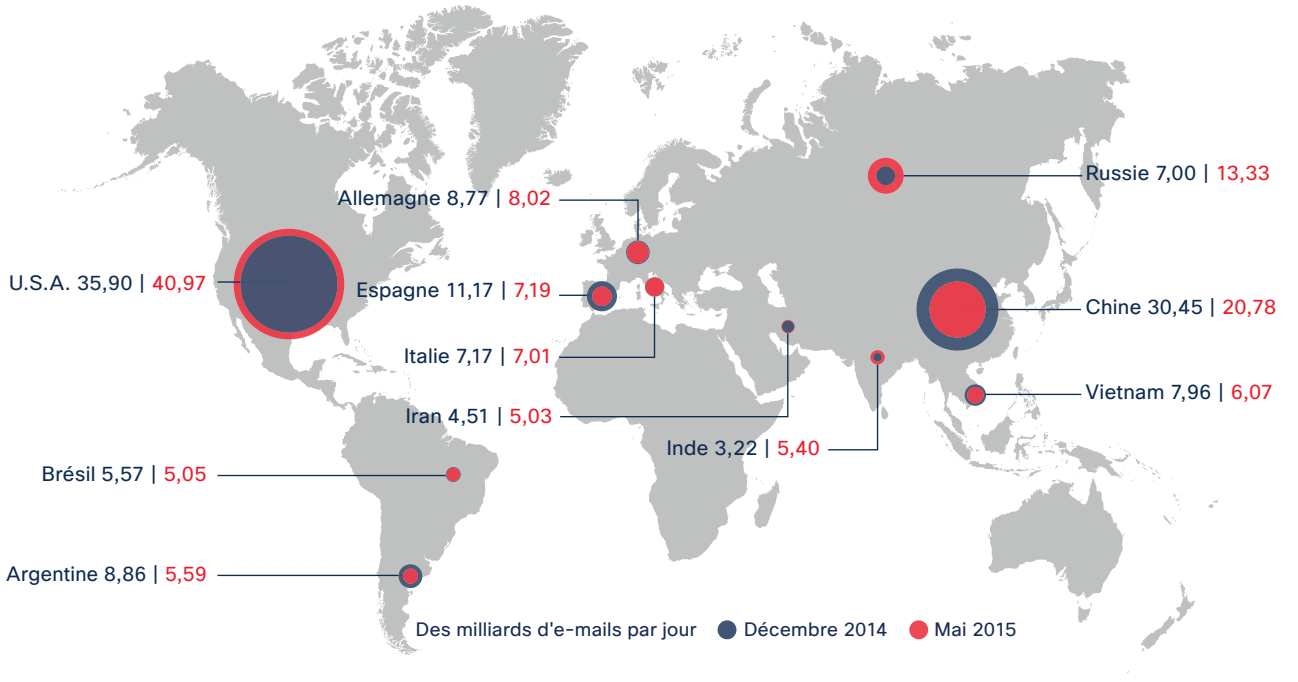
Figure 13 : Le volume de spam est stable



Source : Cisco Security Research

Figure 14 : Volume de spams par pays

Partager le rapport



Source : Cisco Security Research

Menaces et vulnérabilités : les erreurs de programmation courantes, une véritable aubaine pour les exploits

En analysant les vulnérabilités les plus courantes au premier semestre 2015, nous trouvons les mêmes types d'erreurs que chaque année. Par exemple, comme le montre la Figure 15, les erreurs de mémoire tampon arrivent à nouveau en tête de la liste des catégories CWE (Common Weakness Enumeration) établie par la National Vulnerability Database (https://nvd.nist.gov/cwe.cfm).

Les erreurs de mémoire tampon, de validation d'entrée et de gestion des ressources, les trois catégories de points faibles les plus courants illustrées dans la Figure 15, comptent encore et toujours parmi les cinq erreurs de programmation les plus courantes exploitées par les cybercriminels. Si les fournisseurs ont accès à la liste CWE, comment de telles erreurs peuvent encore se produire à une telle fréquence ?

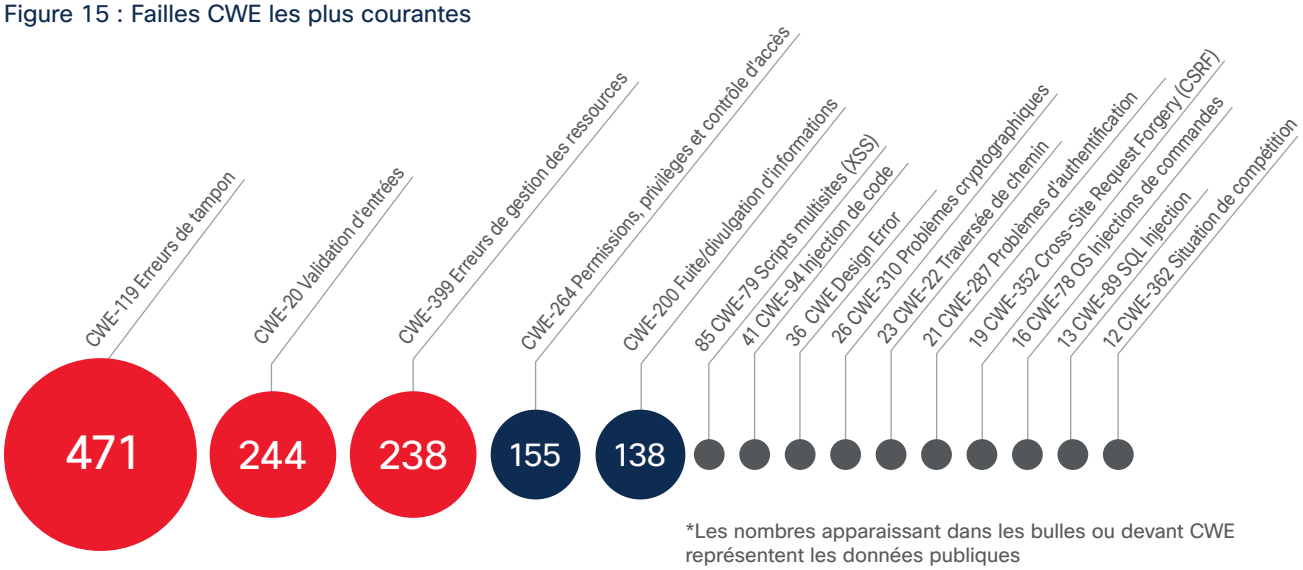
C'est parce que la question de la sécurité n'est pas abordée assez tôt dans le cycle de développement d'un produit. Les mesures de sécurité et les tests de vulnérabilité doivent être intégrés au produit au moment de sa conception. Au lieu de cela, les fournisseurs attendent que le produit soit commercialisé pour évaluer ses vulnérabilités.

Les fournisseurs doivent davantage mettre l'accent sur la sécurité à l'étape du développement. S'ils ne le font pas, ils continueront à perdre du temps et de l'argent à essayer de combler les failles. De plus, les fournisseurs de sécurité doivent tout mettre en œuvre pour offrir à leurs clients des solutions fiables et sécurisées, en intégrant notamment des tests de vulnérabilité à l'étape de développement du produit.

Les vulnérabilités tierces

Depuis la découverte en avril 2014 de la faille Heartbleed touchant le protocole TLS (Transport Layer Security), les vulnérabilités de logiciels tiers sont devenues plus que jamais un point sensible pour les entreprises luttant contre la cybercriminalité. L'apparition de la faille Heartbleed a marqué le lancement d'analyses plus approfondies des vulnérabilités de logiciels tiers, notamment avec la démocratisation des solutions open source.

Figure 15 : Failles CWE les plus courantes

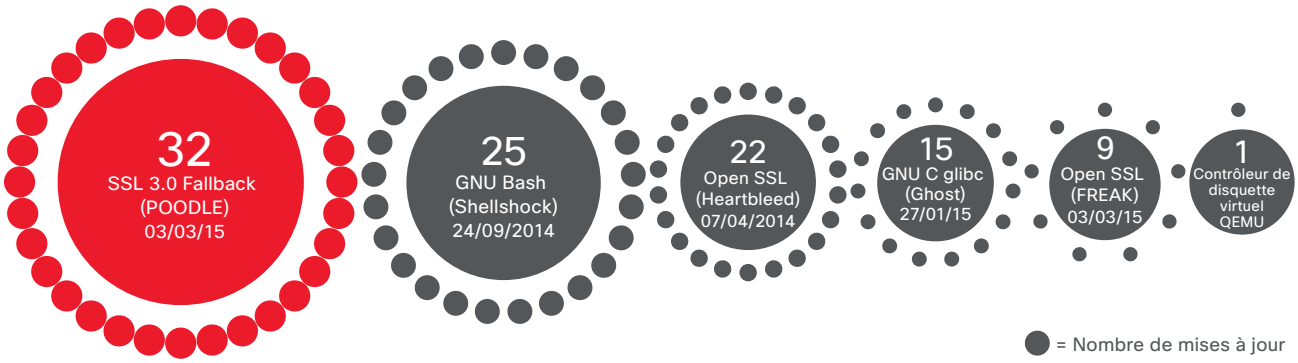


*Les nombres apparaissant dans les bulles ou devant CWE représentent les données publiques

Source : Cisco Security Research

Partager le rapport

Figure 16 : Failles open source



Source : Cisco Security Research

La Figure 16 présente six des vulnérabilités open source les plus courantes que nous avons suivies au cours du premier semestre 2015. (Pour en savoir plus sur les délais de réponse des fournisseurs, cliquez sur les vulnérabilités ci-dessus, puis faites défiler l'écran vers le bas jusqu'à Historique d'alertes.)

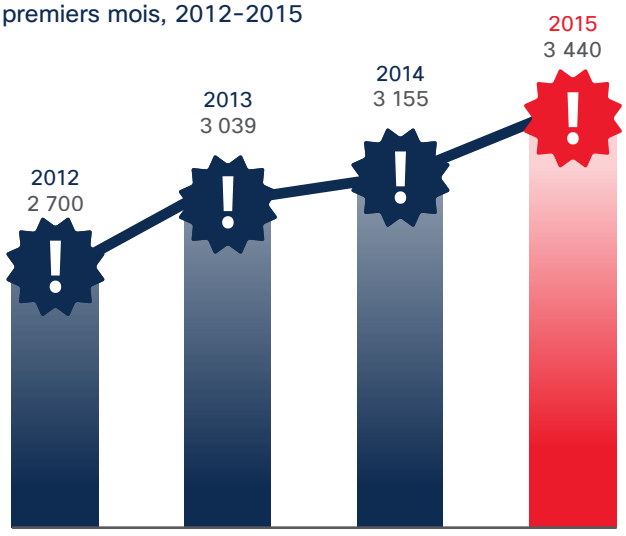
Les vulnérabilités open source posent un problème de taille : la résolution d'une vulnérabilité nécessite une intervention coordonnée de la part de multiples fournisseurs. La communauté de développeurs qui gère les solutions open source peut rapidement fournir un correctif, mais celui-ci doit ensuite être intégré dans toutes les versions du produit.

La bonne nouvelle : plus la communauté de sécurité en apprend sur les vulnérabilités open source, plus elle est en mesure d'y remédier rapidement. Par exemple, lorsque la vulnérabilité VENOM (Virtualized Environment Neglected Operations Manipulation), qui affecte le code open source des systèmes de virtualisation, a été découverte pour la première fois, les équipementiers ont publié des correctifs avant même que la vulnérabilité n'ait été annoncée publiquement.

Les investissements récents dans OpenSSL par plusieurs entreprises leaders en technologie, dont Cisco, permettent d'améliorer l'infrastructure OpenSSL. Ces investissements prennent la forme de dons à la Fondation Linux. Ils permettent aux analystes en sécurité de réaliser des analyses de codes visant à trouver des correctifs pour les solutions open source. [3]

Avec la démocratisation des logiciels open source dans les entreprises, les professionnels de la sécurité doivent savoir où et comment sont utilisés ces logiciels dans leur entreprise et si leurs bibliothèques ou leurs modules open source sont à jour. Par conséquent, la gestion de la chaîne d'approvisionnement logiciel devient plus stratégique que jamais.

Figure 17 : Totaux cumulés d'alertes annuelles, cinq premiers mois, 2012-2015



Source : Cisco Security Research

Partager le rapport

3 « Cisco, Linux Foundation, and OpenSSL », blog sur la sécurité Cisco, 25 avril 2014 : http://blogs.cisco.com/security/cisco-linux-foundation-and-openssl.

Le nombre annuel total d'alertes IntelliShield cumulées pour les cinq premiers mois de 2015 a légèrement augmenté par rapport à la même période en 2014 (Tableau 1). Comme dit précédemment, l'augmentation continue du nombre total d'alertes s'explique probablement par le fait que les fournisseurs multiplient les tests de sécurité et cherchent davantage à identifier et à corriger leurs propres vulnérabilités.

Tableau 1. Niveaux d'activités d'alerte

	Mises à jour	Nouvelles	Total
Janvier	211	359	570
Février	255	379	634
Mars	285	471	756
Avril	321	450	771
Mai	237	472	709
	1309	**2131**	**3440**
Jan – Mai 2014		**Total alertes : 3155**	

Source : Cisco Security Research

Le Tableau 1 montre l'activité associée aux alertes enregistrées ainsi qu'aux alertes mises à jour. Nous avons constaté une hausse de 9 % du nombre total d'alertes en mai 2015 par rapport au mois de mai 2014. Les fournisseurs et analystes de sécurité identifient toujours plus de nouvelles alertes, tandis que le nombre d'alertes mises à jour a baissé. Les entreprises doivent donc se concentrer davantage sur la gestion des correctifs.

Le Tableau 2 répertorie certaines des vulnérabilités les plus souvent exploitées, selon le Système d'évaluation standardisé de la criticité des vulnérabilités (CVSS). La base de données NVD (National Vulnerability Database) du NIST (National Institute of Standards and Technology), une agence gouvernementale américaine, a permis de formaliser la façon de communiquer les caractéristiques et l'impact des vulnérabilités et alimente le CVSS.

Dans la classification CVSS, le score « Urgence » indique que ces vulnérabilités sont activement exploitées. Les entreprises peuvent également identifier dans la liste des produits attaqués ceux qu'elles utilisent afin de les surveiller et de les corriger.

Partager le rapport

Tableau 2. Failles les plus souvent exploitées

ID de l'alerte	Titre	Urgence	Crédibilité	Gravité	CVSS de base	CVSS temporaire
35845	Gestion de la chaîne de valeurs de la variable d'environnement GNU Bash	●●●●○	●●●●●	●●●●○	10,0	9,0
35816	Vulnérabilité au niveau de l'injection de commande de la variable d'environnement GNU Bash	●●●●○	●●●●●	●●●●○	10,0	8,6
37181	Vulnérabilité de type Buffer Overflow détectée par la fonction GNU Glibc Gethost	●●○○○	●●●●●	●●●●○	10,0	7,8
37318	Vulnérabilité du code d'exécution distant d'Adobe Flash Player	●●○○○	●●●●●	●●●●○	9,3	7,7
37848	Contournement de l'environnement sandbox par le moteur de script Elasticsearch Groovy	●●○○○	●●●●●	●●●●○	9,3	7,7
37123	Utilisation d'Adobe Flash Player après exécution libre de code arbitraire	●●○○○	●●●●●	●●●●○	9,3	7,7
36849	Vulnérabilité de type Buffer Overflow au niveau de la pile NTP Daemon	●●○○○	●●●●●	●●●○○	7,5	5,5
37181	Vulnérabilité de type Buffer Overflow détectée par la fonction GNU Glibc Gethost	●●○○○	●●●●●	●●●●○	10,0	7,8
36956	Vulnérabilité au niveau de la clé cryptographique temporaire en cas de rétrogradation de version de OpenSSL RSA (FREAK)	●●○○○	●●●●●	●●○○○	5,0	4,1

Source : Cisco Security Research

De moins en moins d'exploits impliquant Java

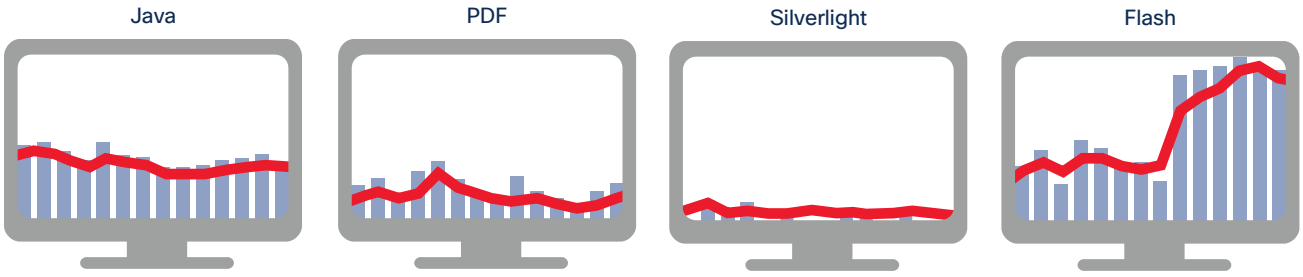
On a assisté à une baisse du nombre d'exploits impliquant Java au cours du premier semestre 2015 comme le prévoyait le rapport annuel Cisco 2014 sur la cybersécurité[4]. Java était auparavant un vecteur d'attaque largement plébiscité par les cybercriminels, mais des améliorations de sécurité et la publication de correctifs avancés les ont contraints à s'en détourner. Aucune attaque de type « zero-day » n'a été identifiée pour Java depuis 2013.

Oracle a pris plusieurs mesures pour améliorer la sécurité de Java, notamment en éliminant progressivement les applets non signés. La dernière version Java 8 est également dotée de contrôles plus performants que les versions précédentes. Cette version est également plus difficile à attaquer, car elle nécessite désormais une intervention humaine, comme par exemple l'activation de Java via une boîte de dialogue.

Le groupe Oracle a annoncé en avril 2015 qu'il n'offrirait plus aucune assistance pour Java 7[5] Malheureusement, lorsqu'un fournisseur décide de ne plus prendre en charge une version donnée d'un produit, les entreprises n'adoptent pas toujours la nouvelle version immédiatement. Ce décalage offre aux cybercriminels une fenêtre d'opportunité pour exploiter les vulnérabilités de la version qui n'est désormais plus prise en charge. Il est possible que nous constations une légère hausse du nombre d'exploits Java au second semestre en raison de la migration des entreprises de Java 7 à Java 8.

Figure 18 : Vecteurs de programmes malveillants les plus courants

Partager le rapport



Source : Cisco Security Research

La Figure 18 illustre le volume du journal d'exploitations de failles Java, PDF ou Flash au cours du premier semestre 2015. Les attaques PDF varient d'un mois à l'autre, mais ne sont généralement pas aussi fréquentes que les attaques Flash. Flash est un outil particulièrement prisé par les développeurs de kits d'exploit, donc sa présence dans le tableau du volume de journal ci-dessus peut être connectée directement à des propagations d'activités criminelles impliquant des kits d'exploit tels que Angler (voir page 10). En outre, le volume d'exploitations de failles Silverlight est très limité comparé au nombre d'attaques basées sur Flash, PDF,et Java.

4 Rapport de sécurité annuel Cisco 2015, Cisco, janvier 2015 : http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html.

5 « Oracle to End Publicly Available Security Fixes for Java 7 This Month », Paul Krill, *InfoWorld*, 15 avril 2015 : http://www.infoworld.com/article/2909685/application-development/oracle-cutting-publicly-available-security-fixes-for-java-7-this-month.

Les auteurs de programmes malveillants adoptent des techniques de détection et d'évitement

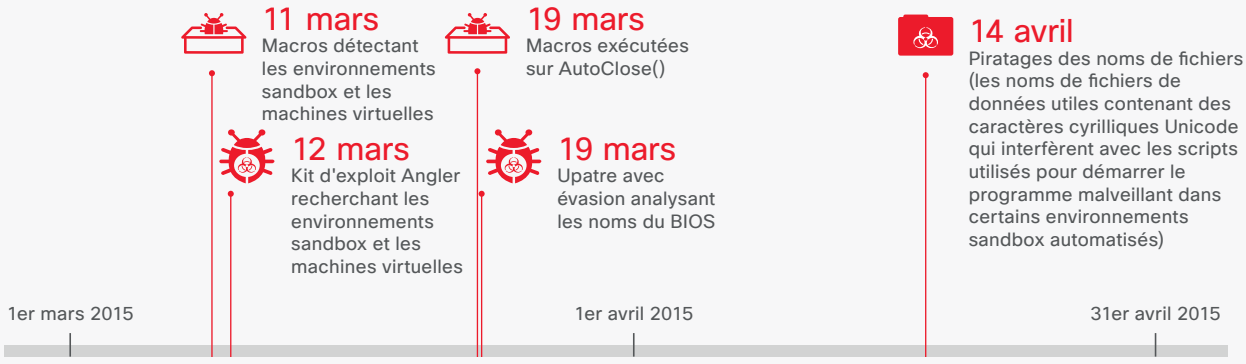
Les cybercriminels sont devenus des experts pour cacher leurs activités, aux dépens des chercheurs et des solutions technologiques de sécurité. Par exemple, ils savent créer un programme malveillant qui tente de contourner les contrôles traditionnels, tels que les sandboxes, que les analystes utilisent pour activer le programme malveillant et enregistrer son activité.

Dans les cas que nous avons examinés, ce type de programme malveillant ne s'est pas déclenché s'il détectait l'activité de sandbox. Cette tactique a été observée dans une variante du kit d'exploit Angler, certaines variantes du programme malveillant Upatre, et des documents malveillants Microsoft Office.

Pour lutter contre les programmes malveillants utilisant cette tactique d'évitement, les entreprises doivent adopter une approche de défense en profondeur qui comprend si possible la capacité d'analyser et d'identifier les programmes malveillants rétrospectivement, après qu'ils ont glissé entre les lignes de défense initiales.

Détection récente de sandbox

La détection de sandbox n'est pas une nouvelle tactique de la part des auteurs de programmes malveillants, mais elle est de plus en plus courante, selon nos chercheurs, qui ont trouvé les incidents suivants entre mars et avril 2015 :



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

Cisco a revu et simplifié sa méthodologie de suivi des secteurs présentant un risque élevé d'exposition aux attaques de programmes malveillants afin d'obtenir des résultats plus précis. Nos analystes ne comparent plus le taux de fréquence moyen pour toutes les entreprises qui passent par le service Cisco® Cloud Web Security au taux de fréquence médian pour toutes les entreprises d'un secteur donné qui passent par le service. Ils comparent désormais les volumes associés au trafic d'attaques (« taux de blocage ») à ceux du trafic «normal » ou prévu.

La Figure 19 présente 25 secteurs importants et la part de leur activité de blocage respective sur le 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.

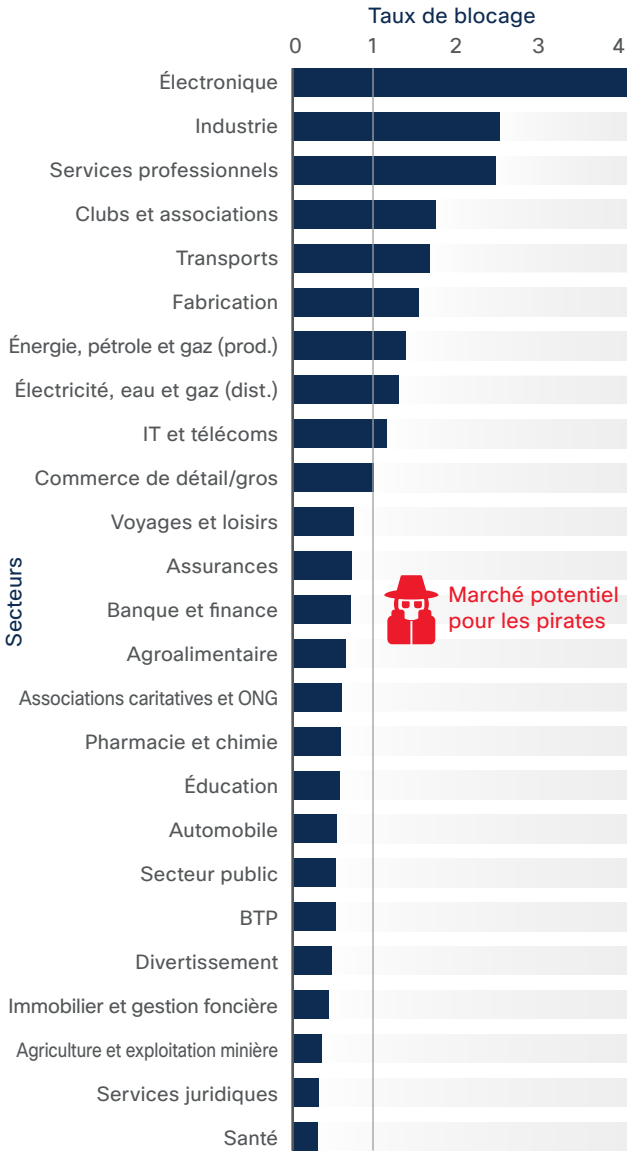
Par exemple, les taux de blocage pour le secteur du commerce/de la vente en gros sont proportionnels au volume du trafic observé dans ce secteur.

En analysant les taux de blocage des clients Cisco, nous avons constaté que le secteur de l'électronique présentait le plus grand nombre d'attaques bloquées parmi les 25 secteurs étudiés. D'après nous, cela s'explique par une propagation de logiciels espions Android.

Comme le montre la Figure 19, la plupart des secteurs présentent un ratio « normal » (ligne 1) d'attaques par rapport au trafic réseau normal. Toutefois, il serait inexact de considérer les secteurs ayant un ratio supérieur à 1 comme beaucoup plus vulnérables aux attaques, surtout si l'on tient compte du fait que l'analyse ne couvre que le premier semestre 2015.

En outre, aucun secteur ne devrait se sentir « plus à l'abri » qu'un autre en termes de cybersécurité. Chaque entreprise, quel que soit le secteur, doit penser qu'elle est vulnérable, que des attaques vont se produire et qu'il est donc de son devoir de mettre en place une stratégie de défense complète.

Figure 19 : Taux de blocage par activité/secteur comparativement au volume de trafic observé



Source : Cisco Security Research

Partager le rapport

Les activités de blocage : répartition géographique

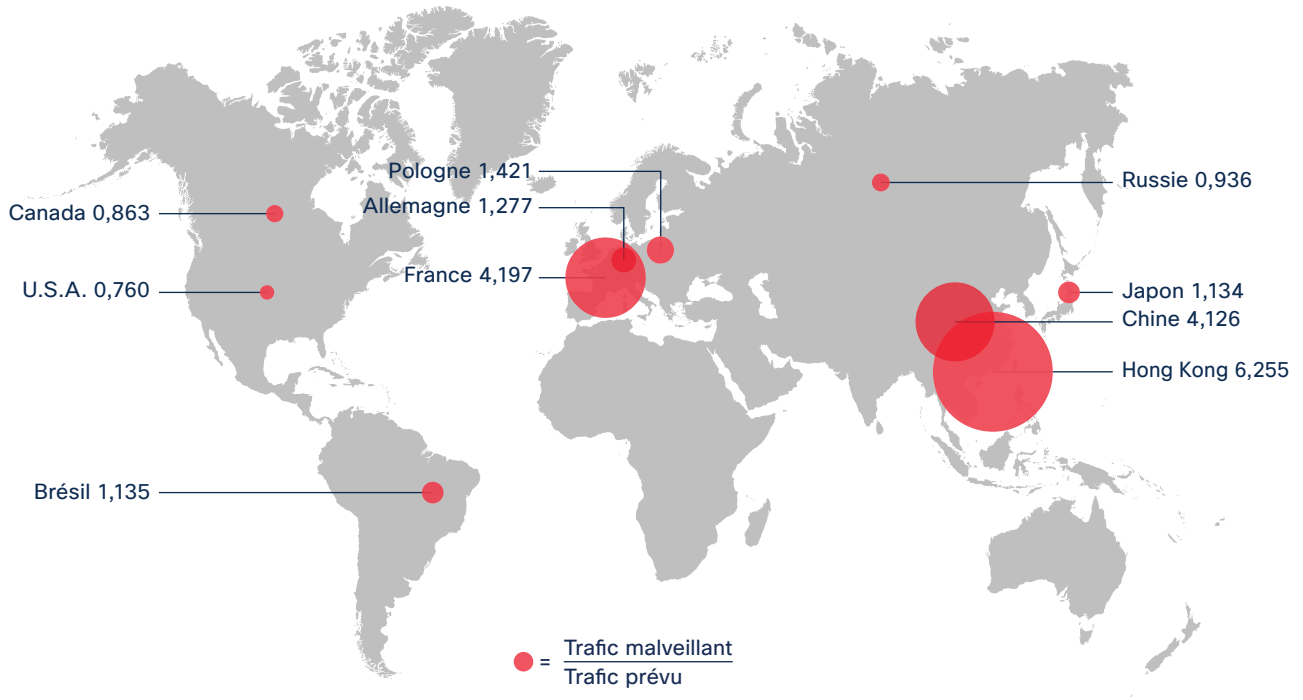
Nos chercheurs se sont également intéressés aux pays et aux régions d'où proviennent les activités de blocage basées sur des programmes malveillants, comme le montre la Figure 20. Les pays ont été sélectionnés pour l'enquête en fonction du volume de trafic Internet. Un taux de blocage de 1 indique que le nombre de blocages observés est proportionnel à la taille du réseau.

Les programmes malveillants réussissent à s'introduire sur les appareils vulnérables. Les pays et régions où les activités de blocage sont supérieures au taux normal ont probablement de nombreux hôtes et serveurs web présentant des failles sur leurs réseaux. Une présence dans des réseaux de grande taille commercialement viables qui traitent un grand volume de trafic Internet est un autre facteur d'activités de blocage élevées.

La Figure 20 présente les zones géographiques où les serveurs sont hébergés. Ce graphique n'attribue pas de modèles d'activités web malveillantes aux pays ou aux zones représentés. Hong Kong, en première position dans la liste, est un exemple de zone où on observe un pourcentage élevé de serveurs web vulnérables. Un petit nombre de réseaux hébergés en France ont subi une attaque au cours de la période couverte par le rapport, ce qui a placé son profil plus haut que prévu.

Figure 20 : Blocages web par pays ou région

Partager le rapport



Source : Cisco Security Research

Les types d'attaques en ligne

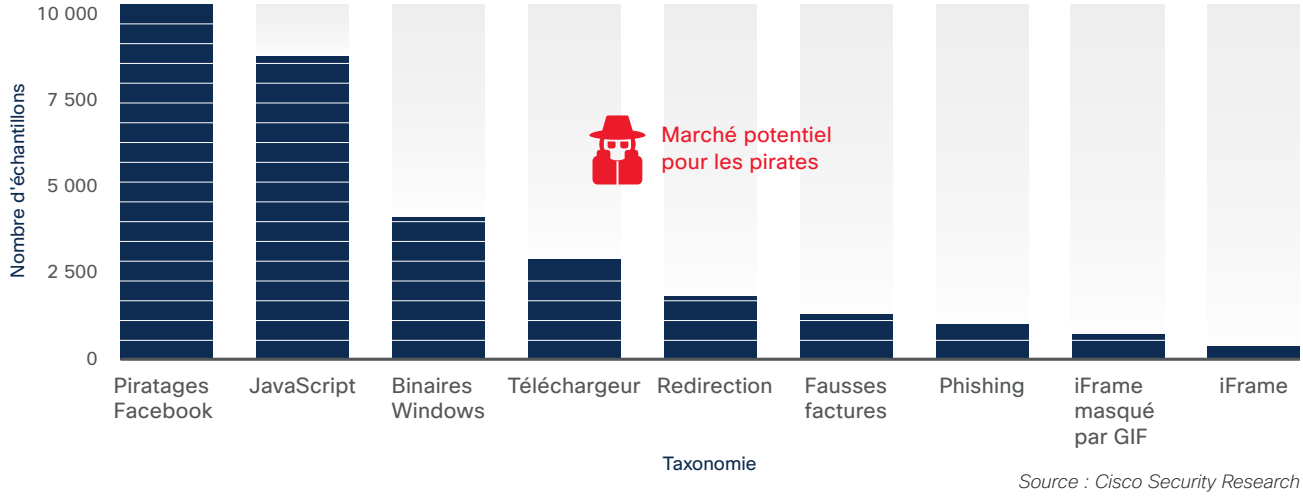
Les Figures 21 et 22 illustrent les divers types de techniques que les pirates utilisent pour accéder aux réseaux des entreprises. La Figure 21 illustre les méthodes observées le plus souvent, y compris les escroqueries Facebook et les redirections malveillantes.

La Figure 22 présente les méthodes d'attaque de plus faible volume observées dans l'échantillon aveugle que nous avons étudié. Notez qu'un « volume plus faible » ne signifie pas « moins efficace. » Les méthodes d'attaque de plus faible volume et les programmes malveillants associés peuvent représenter de nouvelles attaques ou des campagnes extrêmement ciblées.

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

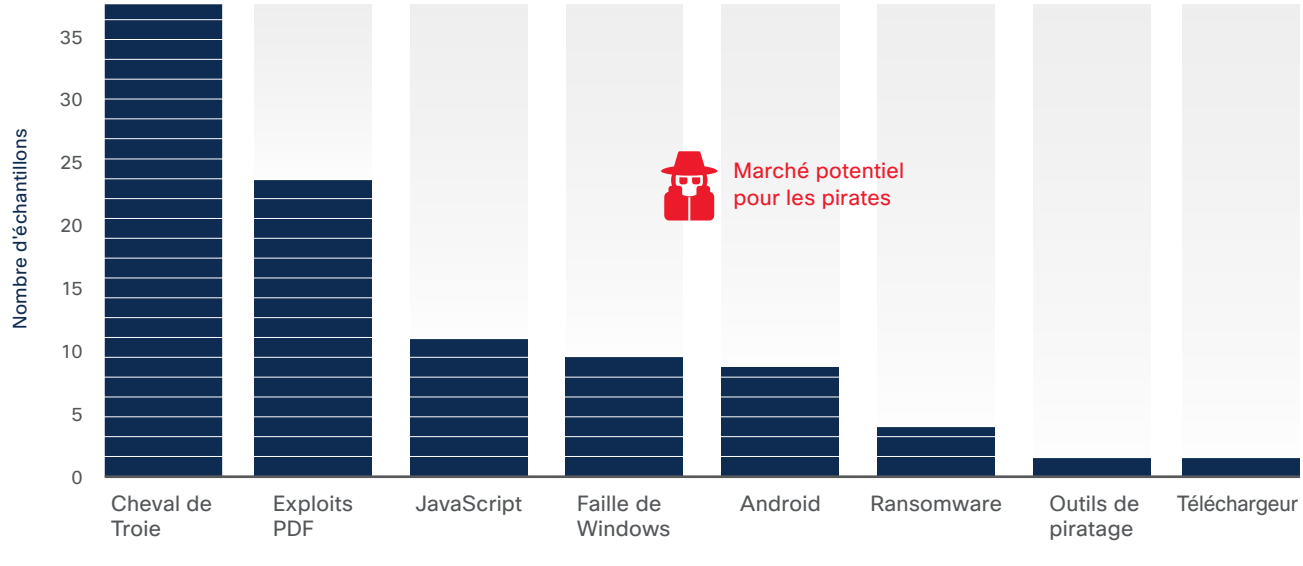
Figure 21 : Méthodes les plus couramment observées

Partager le rapport



Source : Cisco Security Research

Figure 22 : Exemple de méthodes de plus faible volume observées



Source : Cisco Security Research

Les publicités frauduleuses : une menace web généralisée en pleine mutation pour contourner les solutions de protection et gagner en efficacité

Comme indiqué dans notre rapport annuel Cisco 2015 sur la sécurité,[6] nous avons effectué en 2014 une analyse approfondie des attaques web très sophistiquées de type botnet, qui utilisent les publicités frauduleuses des modules complémentaires des navigateurs web comme support de distribution des logiciels malveillants et des applications indésirables. Cette famille de programmes malveillants porte une signature claire : le logiciel publicitaire MultiPlug. Les extensions de navigateur sont intégrées à d'autres applications qui semblent utiles mais sont indésirables, telles que des outils PDF et des lecteurs vidéo.

La sécurité des utilisateurs est compromise lorsqu'ils installent ces applications indésirables et le logiciel intégré. Dans de nombreux cas, ce sont des modules complémentaires de navigateur, auxquels ils font une confiance totale ou qu'ils considèrent comme inoffensifs. Les informations de l'utilisateur, en particulier la page web interne ou externe que l'utilisateur visite (et non ses informations de connexion), sont extraites par ces extensions de navigateur lorsqu'elles sont installées.

Cette diffusion de programmes malveillants repose sur un modèle de monétisation basé sur le principe du paiement à l'installation, selon lequel le créateur d'un programme malveillant est payé pour chaque installation de ce programme inclus avec l'application demandée. Cela explique l'augmentation du nombre de programmes malveillants délibérément conçus pour avoir un impact minimal sur l'hôte infecté, mais optimisés pour garantir des gains à long terme sur le plus grand nombre d'hôtes possible.

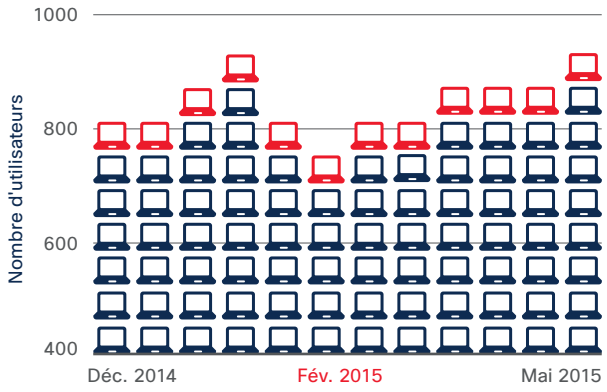
Masqués dans le trafic web courant

Cisco surveille cette attaque depuis plus d'un an. Nous avons observé que les attaques évoluent en permanence afin d'éviter toute détection. Le délai moyen pendant lequel l'attaque utilise un nom de domaine est de trois mois et les noms des modules complémentaires évoluent constamment. Comme indiqué dans notre rapport annuel Cisco 2015 sur la sécurité, nous avons jusqu'ici découvert plus de 4 000 noms de modules complémentaires différents et plus de 500 domaines associés à cette attaque.

En janvier 2015, les chercheurs ont commencé à remarquer que l'attaque connaissait une mutation. En particulier, elle a abandonné son modèle de codage d'URL lui permettant d'éviter la détection pour pouvoir se dissimuler dans le trafic web courant. Ce changement de tactique semble augmenter l'efficacité des attaques contre les utilisateurs.

Nous avons daté l'apparition du trafic associé à ce nouveau modèle à août 2014, mais il n'a commencé à être remarqué que pendant la période décembre 2014-janvier 2015 en raison du volume de trafic. Comme le montre la Figure 23, le nombre d'utilisateurs associés à cette attaque a augmenté depuis février.

Figure 23 : Nombre d'utilisateurs affectés, par mois, décembre 2014-mai 2015



Source : Cisco Security Research

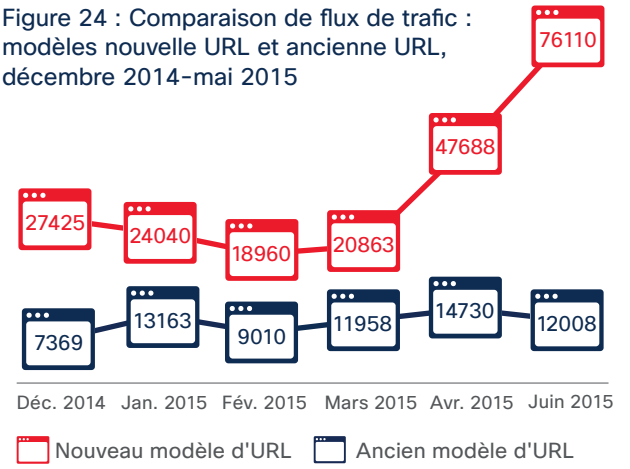
Pour plus d'informations sur cette étude, consultez la publication du blog du groupe Talos, **« Bad Browser Plug-Ins Gone Wild: Malvertising, Data Exfiltration, and Malware, Oh My! »**.

Partager le rapport

6 Rapport annuel 2015 de Cisco sur la sécurité, Cisco, janvier 2015 : http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html.

La Figure 24 indique que le nombre de flux de trafic associés au nouveau modèle d'URL a considérablement dépassé celui de l'ancien modèle, notamment depuis mars 2015.

Figure 24 : Comparaison de flux de trafic : modèles nouvelle URL et ancienne URL, décembre 2014-mai 2015



Source : Cisco Security Research

Le point sur le délai de détection des menaces

Le terme « Délai de détection » désigne le laps de temps entre la première observation d'un fichier et la détection d'une attaque. Nous déterminons cette fenêtre à l'aide des données télémétriques de sécurité collectées sur une base volontaire à partir des produits de sécurité Cisco déployés dans le monde entier.

La catégorie « rétrospectives » de la Figure 25 indique le nombre de fichiers que Cisco a initialement classés comme « inconnus » et qui ont été plus tard convertis en « dangereux connus ».

Le nombre de rétrospectives n'a cessé d'augmenter depuis décembre 2014. Cette tendance est encore un indicateur que les concepteurs de programmes malveillants innovent rapidement pour conserver une longueur d'avance sur les fournisseurs de solutions de sécurité. Cependant, dans le même temps, le délai de détection médian des attaques par Cisco a diminué.

En décembre 2014, le délai de détection médian, avant qu'une analyse ne révèle qu'un fichier inconnu représentait une attaque, était d'environ deux jours (50 heures). Le standard du secteur actuel pour le délai de détection est de 100 à 200 jours, un niveau inacceptable étant donné la vitesse à laquelle les auteurs de programmes malveillants sont capables d'innover.

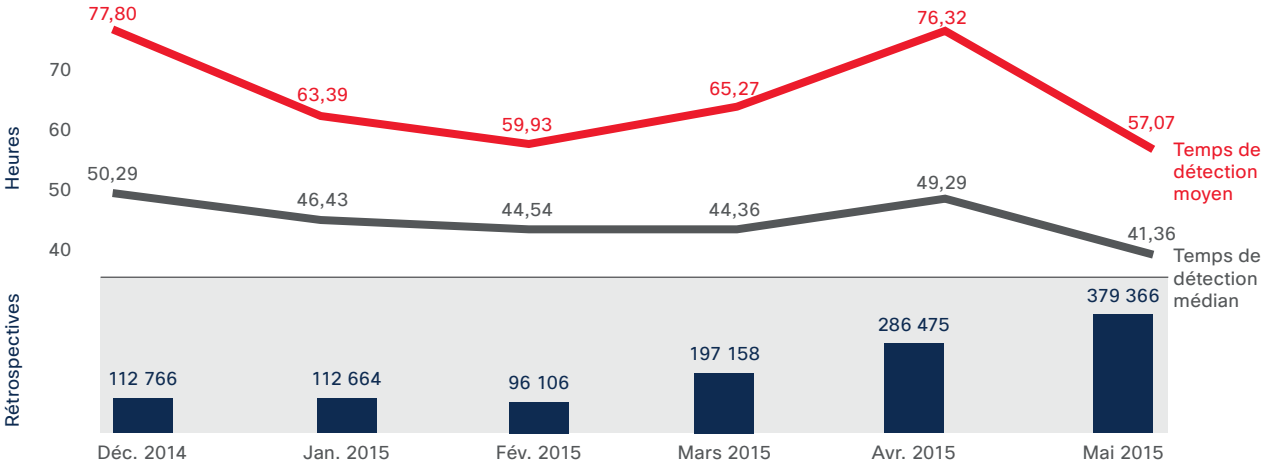
Nous attribuons cette tendance à la hausse des rétrospectives à une augmentation des activités d'évitement (voir « Malware Authors Adopt Detection and Evasion Tactics », page 25) et au déploiement réussi des données utiles des nouvelles exploitations de failles Flash par le biais des kits d'exploit Angler et Nuclear (voir page 9).

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

Cependant, avant la fin mai, le délai de détection pour Cisco a diminué pour descendre à environ 41 heures. Cette amélioration est due en partie à la capacité de Cisco à identifier rapidement les programmes malveillants courants tels que Cryptowall, qui sont évasifs mais ne sont pas nouveaux.

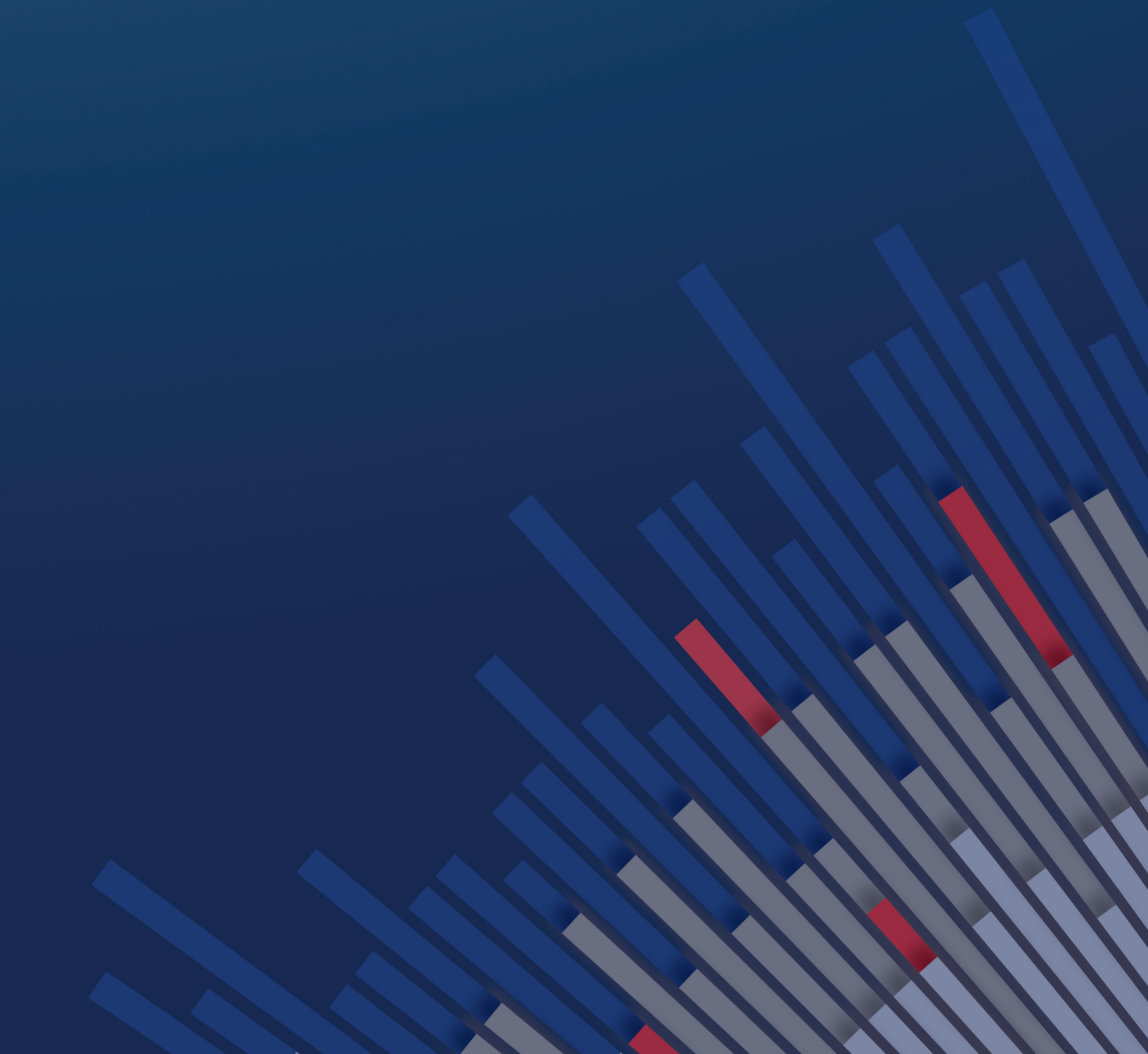
Partager le rapport

Figure 25 : Rétrospectives, délai de détection moyen et délai de détection médian, décembre 2014-mai 2015



Source : Cisco Security Research

Analyses et constats



Des solutions de cybersécurité toujours plus innovantes

Les experts en sécurité de Cisco indiquent que des changements sont imminents dans le secteur de la cybersécurité. Une vague de consolidation et d'intégration est nécessaire pour développer des solutions de sécurité innovantes, adaptables et fiables qui peuvent réduire les délais de détection et empêcher les attaques. En outre, nos experts géopolitiques donnent une idée de l'importance de la cybergouvernance pour l'innovation et la croissance économique de l'entreprise à l'échelle globale.

Dans un monde où les atteintes aux utilisateurs et aux systèmes sont garanties et supposées, la détection des attaques masquées est bien évidemment une priorité nécessaire pour les entreprises et les équipes de sécurité. Les attaques, notamment les activités provenant d'états-nations, sont en augmentation. De nombreuses entreprises réfléchissent donc de plus en plus sérieusement à l'élaboration de plans de continuité des activités pouvant les aider à récupérer les services critiques suite à une cyberattaque contre leur entreprise ou l'infrastructure qui la sous-tend.

Cependant, nous observons aussi une demande importante des entreprises et des utilisateurs individuels pour que le secteur de la cybersécurité développe des fonctionnalités qui soient plus efficaces pour éviter, et ne pas uniquement détecter, les cyberattaques. Pour le moins, ils recherchent des solutions permettant d'accélérer les délais de détection et de résolution.

La complexité de la sécurité ne permet pas de satisfaire ces demandes, pour le moment

D'un côté du secteur de la cybersécurité on trouve des acteurs bien établis, de grande envergure, qui développent des suites de sécurité basées sur un ou plusieurs produits qui se démarquent. Cependant, ces suites peuvent également contenir d'autres solutions qui ne sont pas aussi efficaces que, ou ne sont pas compatibles avec, d'autres solutions majeures.

Des fournisseurs spécialisés, de leur côté, développent des produits permettant de traiter des failles de sécurité spécifiques. De nombreuses entreprises se précipitent pour investir dans la dernière innovation qui leur permettra de combler une lacune connue, au lieu de prendre du recul pour examiner la sécurité de manière globale.

Le résultat est toute une série de produits fragmentés qu'il est difficile de gérer pour les équipes de sécurité. Les solutions peuvent comporter des fonctionnalités qui se recoupent, ne répondent pas toujours aux normes du secteur et ne sont probablement pas interopérables. Les technologies ciblées qui ne peuvent pas être déployées à grande échelle pour répondre aux besoins des utilisateurs courants sont généralement de courte durée, quelque soit leur efficacité.

En outre, de nombreuses technologies de sécurité obligent les entreprises à repenser leur architecture de sécurité uniquement pour l'adapter aux nouveaux risques. Ces technologies, qu'elles soient d'un côté ou de l'autre du spectre du secteur de la sécurité, ne sont pas capables d'évoluer au rythme des attaques. Ce modèle n'est pas durable.

Consolidation des offres de cybersécurité et protection intégrée contre les menaces

Nos experts en sécurité indiquent que le besoin en solutions modulables conduira à d'importants changements dans le secteur de la cybersécurité au cours des cinq années à venir. Nous allons assister à la consolidation des offres de cybersécurité et à une évolution vers une architecture intégrée de défense contre les attaques, proposant de la visibilité, du contrôle, des informations et du contexte pour de nombreuses solutions.

Ce cadre de détection-réponse permettra une réaction plus rapide aux attaques connues et émergentes. Le cœur de cette architecture est une plate-forme de visibilité qui fournit des informations contextuelles complètes. Elle devra être mise à jour en permanence pour évaluer les attaques, relier l'expertise locale et globale et optimiser les défenses. L'expertise locale fournira le contexte de l'infrastructure alors que l'expertise globale reliera tous les événements détectés et les indicateurs d'atteintes à des fins d'analyse et de protection immédiate et partagée.

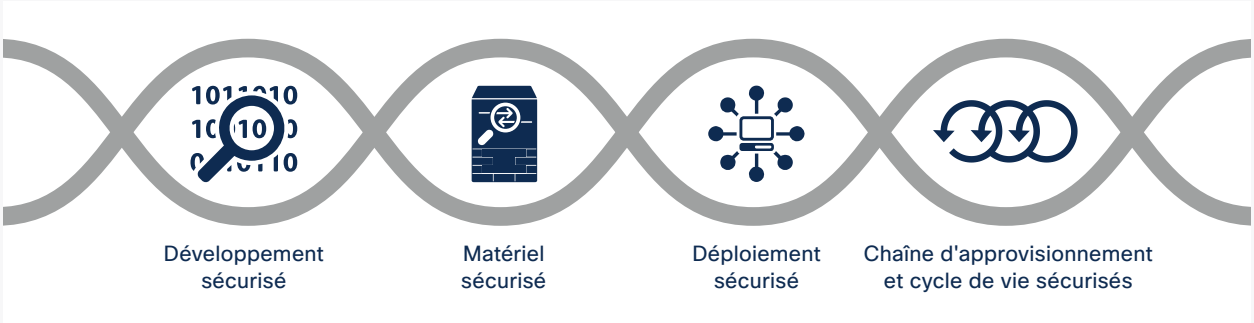
L'objectif de la plate-forme de visibilité est d'établir une base sur laquelle tous les fournisseurs peuvent travailler et à laquelle ils peuvent tous contribuer. Ce système s'alimentera du volume massif d'informations de sécurité disponible au sein de la communauté de sécurité. La visibilité qu'il apportera donnera aux équipes de sécurité un meilleur contrôle, afin d'offrir une meilleure protection contre davantage de nouveaux vecteurs d'attaque et de repousser un plus grand nombre d'attaques.

C'est la direction que le secteur de la cybersécurité doit prendre pour permettre à tous les utilisateurs de se défendre contre les tactiques sophistiquées des hackers actuels. Cependant, le développement d'une protection intégrée, telle que décrite ici, nécessite une meilleure coopération, un meilleur dialogue et une action mieux coordonnée parmi tous les fournisseurs de sécurité, que ce soient des innovateurs spécialisés ou des acteurs de longue date.

Le secteur fait de grands progrès dans le partage d'informations, en étant plus proactif et en utilisant des méthodes appropriées, notamment par le biais de partenariats. Mais un échange automatisé, en temps réel, d'informations sur les attaques est indispensable pour encourager l'innovation nécessaire à la défense et pour apporter une réponse systémique dans la pile de sécurité déployée. Plus le secteur de la cybersécurité pourra distribuer rapidement ses connaissances et son expertise sur tout le réseau, de façon cohérente et acceptable, moins les adversaires seront susceptibles de réussir et de rester dans l'anonymat.

Des produits fiables

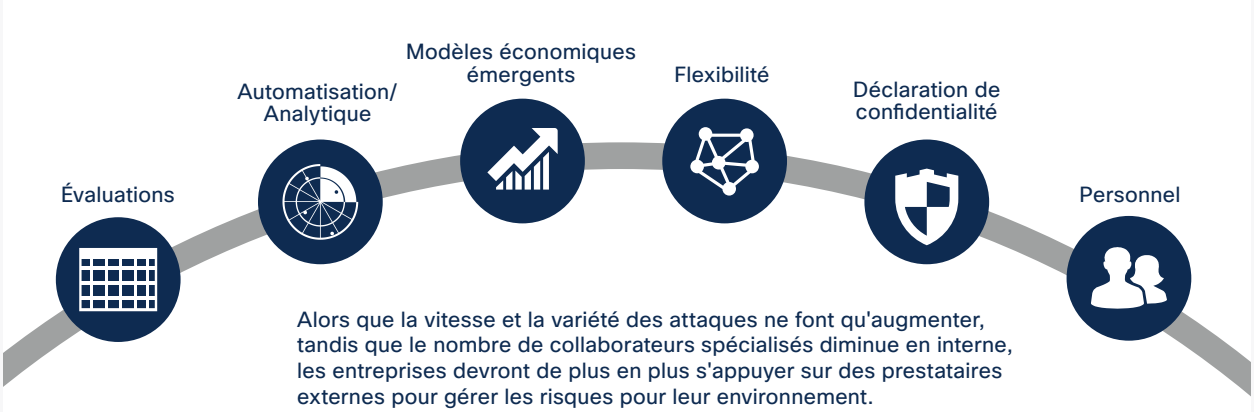
Partager le rapport



À mesure que la consolidation et l'intégration se développeront dans le secteur de la sécurité au cours des cinq prochaines années, les entreprises achetant de nouveaux produits et services de sécurité devront s'assurer que ces solutions sont efficaces, durables et fiables.

Elles devront prendre le temps de comprendre ce que les fournisseurs de sécurité et autres produits informatiques font pour assurer la sécurité dans leurs produits. Elles devront vérifier que ces produits restent fiables à chaque point de la chaîne d'approvisionnement qui leur fournit ces produits. Mais aussi, elles devront demander aux fournisseurs de démontrer que leurs produits sont fiables et de s'engager par contrat.

La valeur de l'expertise



Les fournisseurs de solutions de sécurité ont un rôle important à jouer pour aider les utilisateurs à comprendre l'importance d'investir dans des solutions fiables et de conserver les technologies de sécurité à jour. Les entreprises qui s'appuient sur une infrastructure obsolète exposent leurs données, systèmes et utilisateurs à des risques.

La pénurie grandissante d'experts de la sécurité signifie que de nombreuses entreprises ne disposent pas d'un personnel qualifié pour suivre les évolutions des risques et des fournisseurs. Le manque d'accès à une expertise en sécurité interne explique l'approche fragmentaire que de nombreuses entreprises adoptent lors de la création de leurs défenses de sécurité (voir page 32).

Le recours à une expertise tierce offre aux entreprises la possibilité de suivre l'évolution des risques et attaques. Les fournisseurs de services de sécurité sont bien placés pour apporter une approche globale de la sécurité et permettre aux entreprises d'investir et de tirer le meilleur parti de leurs investissements en matière de sécurité.

En plus d'étoffer des équipes de sécurité réduites, les experts tiers peuvent proposer des évaluations pour tester la sécurité d'une entreprise. Ils peuvent aider à établir les stratégies efficaces qui permettent de faire face aux vulnérabilités et autres risques. Ils peuvent également aider les entreprises à déployer l'automatisation et à gérer des solutions permettant l'analyse et la corrélation des attaques en temps réel nécessaires pour combattre les nouveaux types d'attaques difficiles à détecter.

Certaines entreprises font appel aux fournisseurs de services de sécurité pour être conseillées pendant le développement d'activités basées sur les technologies de la mobilité, de l'interactivité, du cloud et autres technologies émergentes. Certaines veulent de l'aide pour comprendre les exigences liées à la souveraineté et à la confidentialité des données sur les marchés où ils travaillent. D'autres, notamment les PME qui cherchent à tirer parti des technologies et des opérations de sécurité que les plus grandes entreprises utilisent, demandent aux experts de les aider à trouver des modèles gérés et hébergés qui répondent aux besoins de leurs activités.

Un cadre de cybergouvernance mondial pour promouvoir l'innovation

Les entreprises du monde entier dépendent de plus en plus d'Internet pour leurs modèles économiques qui les rendent plus compétitifs et sont avantageux pour leurs consommateurs. Mais elles doivent faire face à des pirates qui déploient des tactiques pouvant affecter leur réussite. S'ils ne sont pas pris en compte, les risques liés à la cybersécurité ont des conséquences importantes sur l'innovation et la croissance économique pour toutes les entreprises.

Les experts géopolitiques de Cisco considèrent un cadre de cybergouvernance cohérent, à plusieurs intervenants, comme une étape positive vers une innovation et une croissance économique durables sur la scène mondiale, protégeant les investissements des entreprises dans l'économie numérique. Cependant, le cadre de gouvernance actuel ne protège pas les entreprises des cyberattaques. Celles-ci n'incluent pas seulement celles qui entraînent des violations de données ou le vol de propriété intellectuelle, mais aussi celles capables de perturber les chaînes d'approvisionnement internationales, d'endommager les infrastructures critiques, voire pire.

De nombreuses entreprises ne recherchent pas de solutions aux cyberattaques, car elles ne disposent pas du soutien des services de police d'autres pays. Cependant, de plus en plus de gouvernements s'ouvrent au concept de l'attribution publique des attaques et de l'imposition de sanctions.

Le manque de cybergouvernance globale efficace peut également empêcher la collaboration dont a besoin le secteur de la cybersécurité pour créer des technologies adaptatives qui peuvent détecter et déjouer les nouvelles attaques. Des modifications récentes ont été proposées pour l'Arrangement de Wassenaar[7], une entente multinationale volontaire destinée à gérer l'exportation de certaines technologies « à double usage », notamment les logiciels intrusifs tels que les outils de surveillance numérique. Ces propositions menacent de restreindre ce contrôle et d'empêcher les analystes de sécurité de partager des informations avec leurs homologues sans charges réglementaires lourdes. Ce développement peut avoir un impact considérable sur les capacités de recherche concernant la cybersécurité et amplifier la pénurie d'experts dans le secteur.

Une meilleure harmonisation des règles : une solution d'avenir ?

La question des frontières (en particulier en ce qui concerne la manière dont les gouvernements collectent les données sur les citoyens et les entreprises et partagent, ou ne partagent pas, ces informations entre juridictions) est un obstacle important au type de coopération nécessaire pour réussir une cybergouvernance cohérente. Alors que l'Internet des objets se précise et que le monde devient de plus en plus interconnecté, les secteurs, les états et la société vont devoir collaborer plus efficacement pour relever les défis croissants de la confidentialité et de la sécurité.

Actuellement, la coopération, et la confiance, entre les entités de la scène mondiale est limitée au mieux à certains acteurs, et non existante parmi d'autres. Même les entités avec des partenariats solides ont des philosophies concurrentes sur la cybergouvernance et sont naturellement centrées sur la promulgation de lois protégeant leurs intérêts souverains et leurs citoyens. Tout comme les discussions concernant le changement climatique, seule une poignée d'acteurs participent aux débats et il est difficile d'atteindre un consensus, même pour les petites mesures.

Au niveau régional, au moins, des efforts ont lieu pour aller au-delà des frontières nationales. Par exemple, dans l'Union européenne, il existe un mouvement pour améliorer la coordination du partage des informations par le biais d'une proposition de directive sur la sécurité des informations et des réseaux (NIS). Cette directive « vise à assurer un niveau élevé et commun de cybersécurité dans l'Union européenne » en « améliorant la coopération entre les états membres et entre les secteurs public et privé », entre autres[8].

L'Union européenne et les États-Unis semblent également s'approcher de la signature d'une « entente globale » sur la protection des données qui définira les normes de protection des données partagées entre les autorités de contrôle. Cet accord ne répondra pas aux questions plus importantes concernant la manière d'accéder aux données et le type de données. Mais il peut aider à améliorer l'atmosphère tendue entre les deux puissances, qui a failli placer les entreprises au milieu du conflit juridictionnel. Les équipes juridiques, techniques et de sécurité des entreprises qui opèrent dans l'Union européenne et aux États-Unis devront travailler ensemble sur les conditions d'accès si l'entente globale est signée.

7 « Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items », *Federal Register* : https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items.

8 « Network and Information Security (NIS) Directive », European Commission : http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive.

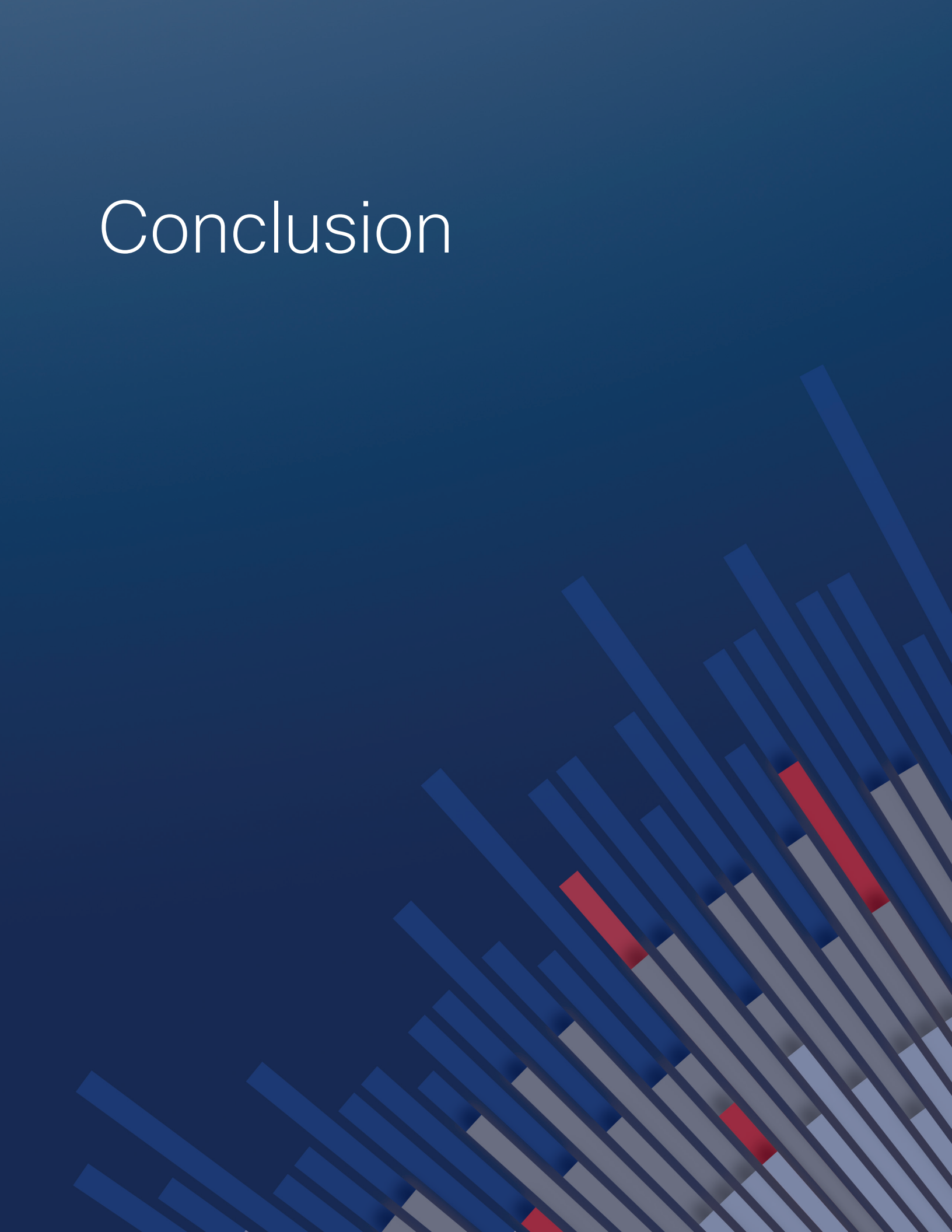
Cependant, d'autres réglementations sont en cours d'élaboration en Europe et elles pourraient induire la mise en place de plus de limites, particulièrement pour les entreprises. Les institutions de l'Union Européenne prévoient de finaliser la nouvelle réglementation sur la protection des données générale (GDPR) d'ici la fin de l'année, en remplacement de la directive européenne de protection des données.

Cette réglementation contient une définition générale des informations personnelles et des règles normatives sur la façon dont de telles données doivent être gérées sous peine d'amendes considérables. Elle aura un impact important sur la manière dont les entreprises qui travaillent avec et dans l'Union européenne collectent, enregistrent et utilisent les données des clients et comment elles doivent signaler les fuites de données. Destinée à imposer une plus grande responsabilité et une plus grande transparence, la nouvelle directive obligera au minimum de nombreuses entreprises à examiner leur approche de la confidentialité des données et de leur gouvernance et à adopter de bonnes pratiques.

Les équipes techniques, par exemple, devront tenir compte des limites ou des difficultés liées au transfert de données au-delà des frontières. Ils devront prendre en considération les différentes sensibilités régionales par rapport à des données qui peuvent être considérées comme « personnelles » ou non. Les équipes de sécurité devront également prendre en compte les développements qui affectent le transfert de données, la définition des informations personnelles, la base juridique pour le traitement de la sécurité des réseaux et des informations et les exigences liées à la communication des fuites de données.

Une plus grande harmonisation des règles pourrait favoriser la définition d'un cadre de cybergouvernance qui encouragerait des négociations intergouvernementales sur les réglementations de protection des données et empêcherait dans le même temps le secteur de la cybersécurité de se retrouver coincé au milieu. En attendant, les experts de la sécurité doivent activement s'assurer que les décideurs de leurs entreprises comprennent l'impact potentiel que les réglementations émises par différents pays peuvent avoir sur leurs opérations. Les systèmes incompatibles, les exigences lourdes ou incohérentes concernant les données, les infractions aux lois de confidentialité et les exigences s'appliquant au transfert et à la gestion des données font partie de ces problématiques.

Conclusion



Conclusion

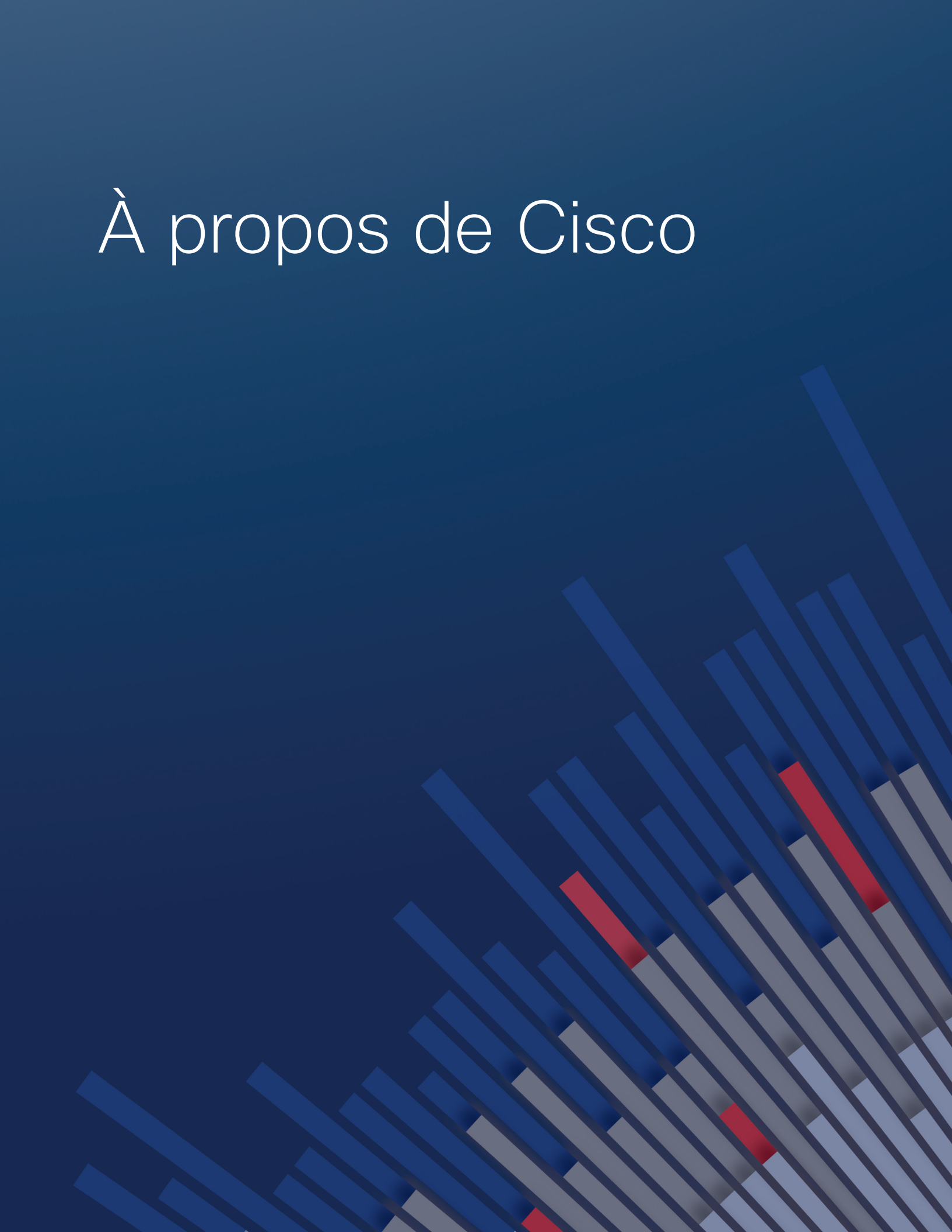
Les attaques abordées dans ce rapport ne représentent qu'un petit exemple des défis de cybersécurité auxquels doivent faire face les entreprises, les équipes de sécurité et les utilisateurs. Jusqu'ici, 2015 semble connaître une accélération sans précédent de l'innovation, de la résilience et de l'évitement des cyberattaques. Les cybercriminels sont déterminés à éliminer tous les obstacles à leur réussite. Dès que le secteur développe des technologies pour bloquer et détecter les attaques, les cybercriminels modifient leurs tactiques.

La course à l'innovation entre les pirates et les fournisseurs de solutions de sécurité ne fait que s'accélérer et les entreprises risquent de devenir plus vulnérables aux attaques si elles n'agissent pas. Elles doivent être proactives dans l'identification et la prise en compte des attaques qui peuvent affecter leurs activités, et connecter les personnes, les processus et la technologie appropriés pour les aider à traiter ces problématiques.

« La sécurité doit faire partie de la vision globale des entreprises pour leurs activités », explique David Goeckeler, vice-président directeur et directeur général du groupe de sécurité de Cisco. « Les enjeux sont nombreux : leur marque, leur réputation, leur propriété intellectuelle et les données de leurs clients. Tous ces éléments sont exposés. Les entreprises doivent adopter une approche systémique pour réduire ces risques grâce à un niveau de sécurité approprié. »

Des produits fiables sont l'élément essentiel d'une sécurité efficace, indique John N. Stewart, responsable de la sécurité pour Cisco. « Les entreprises n'acceptent plus de s'entendre dire que les atteintes à la sécurité sont inévitables », déclare-t-il. « Elles attendent du secteur de la cybersécurité des produits fiables et résilients, capables d'intercepter même les attaques les plus sophistiquées. »

À propos de Cisco



À propos de Cisco

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

Les chercheurs de Cisco CSI, notre écosystème de collecte d'informations sur les menaces, regroupent l'ensemble des informations sur les risques issues des données télémétriques émanant des nombreux appareils et capteurs, des flux publics et privés, et de la communauté open source Cisco. Tous les jours, des milliards de requêtes web et des millions d'e-mails, d'échantillons de programmes malveillants et de données sur les intrusions dans les réseaux sont collectés.

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

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

Contributeurs du rapport semestriel 2015 Cisco sur la cybersécurité

Informations de veille collective

Cisco CSI est présent sur plusieurs solutions de sécurité et fournit une protection et une efficacité de pointe. Outre les chercheurs spécialisés, l'écosystème CSI repose sur l'infrastructure d'information, les données télémétriques des produits et des services, les flux publics et privés et la communauté open source.

Groupe de sécurité adaptative et de recherche Talos

Le groupe de sécurité adaptative et de recherche Talos se compose des meilleurs spécialistes de la cybersécurité, lesquels exploitent des systèmes sophistiqués afin d'établir un panorama des menaces permettant aux produits Cisco de détecter et d'analyser les attaques connues et émergentes, et d'y répondre. Talos gère les règles officielles de Snort.org, ClamAV, SenderBase.org et SpamCop ; son équipe est la source principale d'informations sur les menaces pour l'écosystème Cisco CSI.

Équipe IntelliShield

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

Équipe d'analyse des attaques actives

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

Cognitive Threat Analytics (CTA)

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

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

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

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

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

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