FireEye
SECURITY REIMAGINED

RAPPORT SPÉCIAL

LA LIGNE MAGINOT DE LA CYBERSÉCURITÉ — LA SUITE :

Résultats de nouveaux tests en conditions réelles

LA SÉCURITÉ
RÉINVENTÉE

SOMMAIRE

RÉSUMÉ

Les cyberpirates contournent les défenses informatiques traditionnelles presque à leur guise, compromettant des systèmes partout dans le monde et dans pratiquement tous les secteurs d'activité. C'est le constat sévère qui se dégage des nouvelles données recueillies par plus de 1 600 capteurs FireEye déployés sur des appliances pour réseau et messagerie électronique dans des environnements réseau réels. La présente étude compare les données de notre premier rapport *La ligne Maginot de la cybersécurité : Un audit grandeur nature du modèle de défense en profondeur*, publié en mai 2014, avec celles qui ont été récoltées dans les mois qui ont suivi.

Opérant derrière d'autres couches de sécurité, les capteurs FireEye nous offrent un point de vue unique pour évaluer les performances d'autres outils de sécurité. La totalité des menaces observées par FireEye dans le cadre de la première étude avaient réussi à contourner tous les autres dispositifs de défense.

Les nouvelles données corroborent nos conclusions initiales. Elles montrent que les attaques passent outre les multiples couches des outils de défense en profondeur traditionnels, dans la grande majorité de déploiements.

Cette nouvelle série de données nous permet également de dégager certaines tendances.

Les secteurs ci-dessous ont enregistré une hausse substantielle du pourcentage de systèmes compromis au cours de la période couverte par la présente étude :

COMMERCE

5 % d'augmentation

(100 % de systèmes compromis)

SOINS DE SANTÉ ET INDUSTRIE PHARMACEUTIQUE

4 % d'augmentation

(100 % de systèmes compromis)

Nous avons constaté de nettes augmentations des attaques exploitant des logiciels malveillants avancés[1] dans les secteurs suivants :

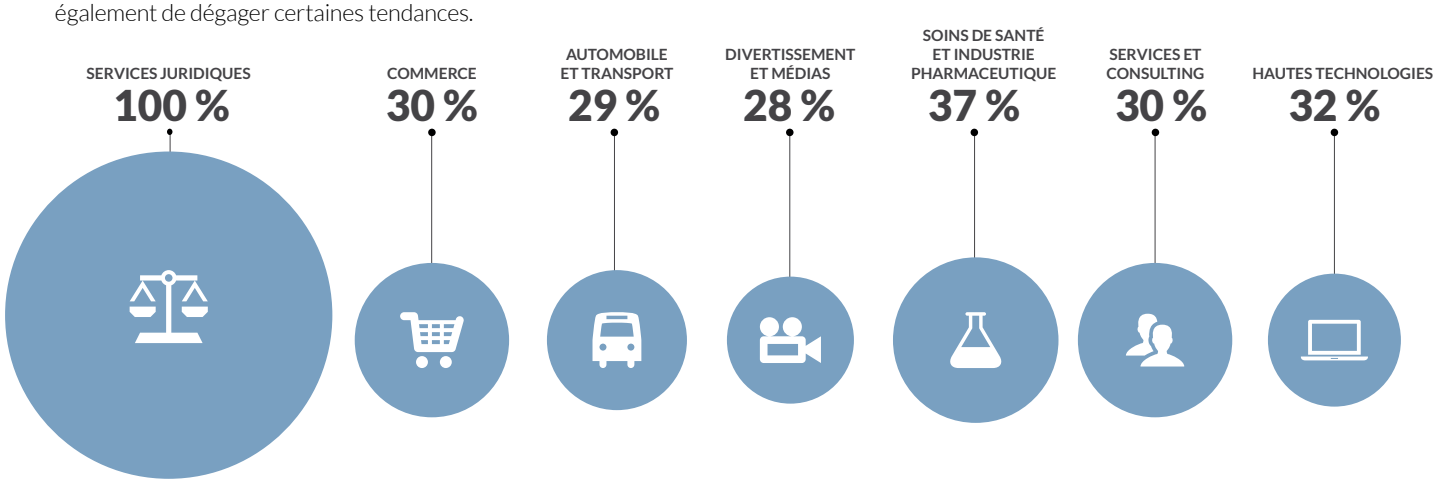
Sur l'ensemble des secteurs d'activité, 96 % des systèmes ont été compromis en moyenne. En outre, 27 % des violations de sécurité impliquaient des logiciels malveillants avancés.

Au vu des lacunes généralisées des déploiements de sécurité traditionnels, les entreprises doivent impérativement revoir leur approche de la sécurisation de leurs actifs informatiques.

Elles doivent abandonner leurs systèmes de défense passifs et peu intégrés, qui n'offrent qu'une vue fragmentée des menaces et sont incapables d'établir les liens indispensables pour déjouer une attaque avancée. Elles ont besoin d'une architecture agile et étroitement intégrée qui favorise une vigilance globale.

Aujourd'hui, les équipes responsables de la sécurité informatique ne peuvent se permettre d'attendre passivement qu'une attaque survienne. Elles doivent au contraire adopter une approche leur permettant d'anticiper et de traquer activement les nouvelles menaces non identifiées.

FireEye a baptisé cette approche Adaptive Defense™, ou défense adaptative.



[1] Par souci de concision, nous utilisons dans ce rapport l'expression « logiciels malveillants avancés » pour faire référence aux outils qui présentent les caractéristiques de ceux employés dans le cadre d'attaques de type « menaces persistantes avancées » (APT, Advanced Persistent Threats), même si d'autres types d'attaques ont largement recours à ces outils.

CONTEXTE :

En mai 2014, FireEye et Mandiant, une entreprise FireEye, ont publié le rapport *La ligne Maginot de la cybersécurité : Un audit grandeur nature du modèle de défense en profondeur*. Cette étude, la première en son genre, analysait les données issues de plus de 1 200 systèmes de sécurité d'organisations implantées dans 63 pays et actives dans plus de 20 secteurs.

Pour les architectures de sécurité conventionnelles, le verdict est accablant. En effet, dans la grande majorité des réseaux, les cybermenaces avaient réussi à franchir toutes les couches d'outils de défense en profondeur des organisations.

Notre premier rapport faisait un parallèle entre cette brèche de sécurité et la ligne Maginot : un dispositif impressionnant mais qui s'est finalement révélé inefficace. À l'instar de celle-ci, l'architecture de protection multiniveau complexe élaborée par le secteur de la cybersécurité est impuissante face à des menaces d'un nouveau genre.

Contrairement aux tests de laboratoire habituels, qui évaluent les outils de sécurité par rapport à des échantillons de logiciels malveillants triés sur le volet, avec des paramètres très contrôlés, notre audit portait sur des données issues d'environnements réseau existants. Ces données ont été générées par 1 614 appliances FireEye pour réseau et messagerie électronique lors d'essais de validation. Installés derrière d'autres couches de sécurité, ces déploiements d'essai nous ont offert un point de vue unique pour évaluer les performances d'autres outils de sécurité. La totalité des menaces observées par FireEye dans le cadre de l'étude avaient réussi à passer outre tous les autres dispositifs de défense censés protéger le réseau d'entreprise.

LE RÉSULTAT :

En dépit des milliards investis chaque année dans des dispositifs de sécurité traditionnels, les pirates semblent n'avoir aucun mal à infiltrer les réseaux. Peu importe le fournisseur ou la combinaison d'outils de défense en profondeur conventionnels que les entreprises déploient, ou encore les performances de ces outils lors de tests de laboratoire. Les pirates les contournent tous en situation réelle.

VOICI UN APERÇU DES CONCLUSIONS DU PREMIER RAPPORT :

97 %

des organisations ayant participé à l'étude ont subi une compromission au cours de la période d'évaluation.

> 1/4

Plus d'un quart ont connu des incidents suggérant l'emploi d'outils et de tactiques propres à des pirates connus pour utiliser des menaces persistantes avancées (APT).

Trois quarts des organisations présentaient des communications de commande et de contrôle (CnC) actives, indiquant que les pirates contrôlaient les systèmes compromis et recevaient peut-être déjà des données de ceux-ci.

> 1 fois par semaine

Même après la compromission d'une organisation, les pirates tentaient généralement de lancer une attaque plus d'une fois par semaine en moyenne.

NOUVELLES DONNÉES, MÊMES CONCLUSIONS

Depuis l'élaboration du premier rapport, nous avons continué à recueillir des données à partir des déploiements de validation afin de vérifier nos résultats initiaux et de dégager des tendances. Les déploiements appartenaient à des organisations qui avaient installé les appliances FireEye à des fins de test, sans être encore complètement protégées par la plate-forme FireEye.

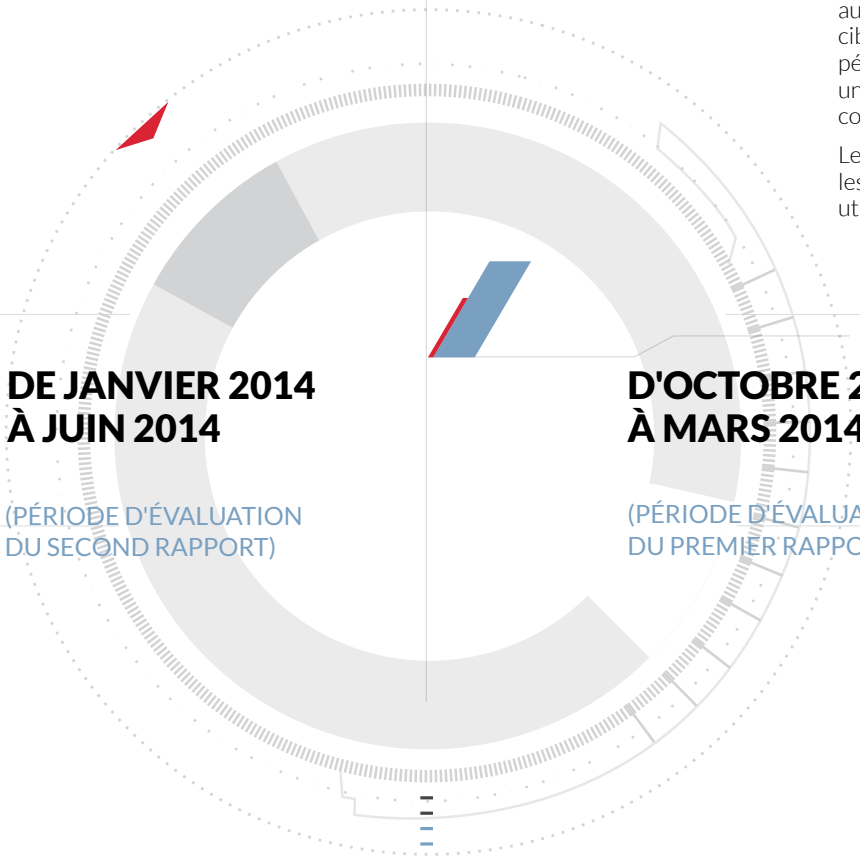
Nous avons examiné les données issues de 1 214 déploiements de sécurité sur deux périodes de six mois se chevauchant :

Ce rapport met en évidence les changements observés entre la première et la seconde période d'évaluation. Les nouvelles données corroborent nos conclusions initiales. Les pirates continuent à contourner les outils de sécurité conventionnels et à compromettre la grande majorité des architectures de sécurité. De plus, environ un quart des systèmes compromis l'ont été à l'aide d'outils et de techniques qui rappellent ceux employés par des auteurs d'attaques de type APT connus.

Cette nouvelle série de données nous permet également de dégager pour la première fois certaines tendances. Si le bilan général reste le même, un grand nombre de détails ont changé.

Tout d'abord, nous avons constaté une augmentation sensible des attaques avancées ciblant divers secteurs d'activité au cours de la période étudiée. Ensuite, nous avons enregistré une forte hausse du pourcentage de systèmes compromis dans différents secteurs.

Les sections ci-après décrivent ces changements et les familles de logiciels malveillants avancés les plus utilisées dans ces secteurs.



DE JANVIER 2014 À JUIN 2014

(PÉRIODE D'ÉVALUATION DU SECOND RAPPORT)

D'OCTOBRE 2013 À MARS 2014

(PÉRIODE D'ÉVALUATION DU PREMIER RAPPORT)

Les nouvelles données corroborent nos conclusions initiales. Les pirates continuent à contourner les outils de sécurité conventionnels et à compromettre la grande majorité des architectures de sécurité.

LES MENACES PERSISTANTES AVANCÉES, UN FLÉAU QUI MÉRITE TOUTE NOTRE ATTENTION

FireEye surveille d'innombrables variantes de logiciels malveillants dans le monde. Nous portons toutefois une attention particulière à celles qui sont fréquemment utilisées dans le cadre d'attaques exploitant des menaces persistantes avancées, ou menaces APT (Advanced Persistent Threats). Dans la terminologie FireEye, ces menaces sont désignées par l'acronyme APT présent dans leur sous-type. Citons par exemple la famille de logiciels malveillants Gh0stRAT, que nous appelons BACKDOOR.APT.GH0STRAT.

Les auteurs de menaces APT sont généralement commandités par un État et bénéficient de son soutien. Que leur mission soit de subtiliser des données, de perturber l'activité ou de causer des dommages à l'infrastructure, ils poursuivent leur objectif avec ténacité, s'aidant d'une multitude d'outils et de tactiques.

La présence d'un logiciel malveillant associé à une menace APT sur vos systèmes ne signifie pas pour autant que vous êtes en proie à un auteur de menace APT. En effet, les attaques par APT recourent souvent à des outils courants pour dissimuler leurs activités ou simplement par facilité. Autrement dit, cette intrusion peut être le fait de n'importe qui. Des informations relatives au logiciel malveillant ne suffisent généralement pas à identifier le coupable : un contexte plus large est nécessaire.

Quoi qu'il en soit, votre équipe de sécurité doit être très attentive lorsque ses outils de sécurité détectent un logiciel malveillant associé à de précédentes attaques de type APT.

Bien qu'un auteur de menace APT ne se cache pas forcément derrière le logiciel malveillant, l'éventualité n'est pas à exclure et exige une analyse plus poussée. Les motivations des auteurs d'attaques de type APT ne sont pas toujours claires. Il se peut que vous possédiez, sans le savoir, des données qu'ils chercheront à dérober parce qu'elles ont de la valeur à leurs yeux, ou que vous entreteniez des relations avec d'autres personnes ou entités qui disposent de telles données.

De plus, la présence de la mention « APT » dans l'appellation d'un logiciel malveillant indique souvent qu'il est de nature avancée. Même entre les mains d'un pirate non spécialisé dans les APT, le logiciel malveillant pourrait se révéler difficile à analyser et à neutraliser. Il est cependant essentiel de le détecter et de prendre les mesures correctives nécessaires au plus vite.

Ce rapport met en évidence certains des principaux logiciels malveillants détectés au sein de secteurs d'activité qui ont connu une forte augmentation des logiciels malveillants associés aux APT ; il décrit leur fonctionnement ainsi que leur impact sur les activités.

Par souci de concision, l'expression « logiciels malveillants avancés » est utilisée pour faire référence aux outils qui présentent les caractéristiques de ceux employés dans le cadre d'attaques de type APT, même si d'autres types d'attaques ont largement recours à ces outils.

Des informations relatives au logiciel malveillant ne suffisent généralement pas à identifier le coupable : un contexte plus large est nécessaire. Quoi qu'il en soit, votre équipe de sécurité doit être très attentive lorsque ses outils de sécurité détectent un logiciel malveillant associé à de précédentes attaques de type APT.

PROGRESSIONS LES PLUS FORTES DU NOMBRE DE COMPROMISSIONS

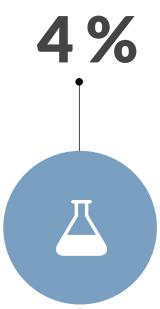
Si le pourcentage de systèmes compromis est resté globalement stable, il a fortement augmenté dans les secteurs du commerce et des soins de santé.

COMMERCE

Le nombre de systèmes compromis chez les commerçants a augmenté de plus de 5 %. Au terme de la période d'évaluation, les 58 déploiements qui composaient notre échantillon avaient été infiltrés, et 17 % d'entre eux l'avaient été par un logiciel malveillant avancé.

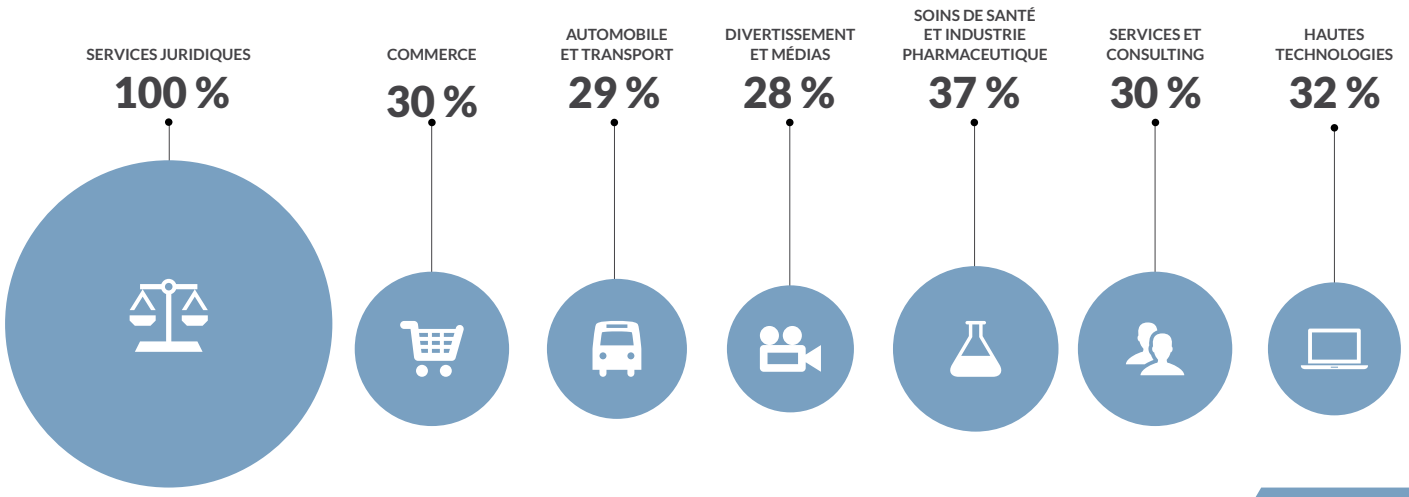
SOINS DE SANTÉ ET INDUSTRIE PHARMACEUTIQUE

Le nombre de systèmes compromis au sein des établissements de soins de santé et des entreprises pharmaceutiques s'est accru de plus de 4 %. Au terme de la période d'évaluation, les 54 déploiements qui composaient notre échantillon avaient été victimes d'une compromission, ayant pour origine un logiciel malveillant avancé pour 37 % d'entre eux.



PROGRESSIONS LES PLUS FORTES DE L'ACTIVITÉ DES LOGICIELS MALVEILLANTS AVANCÉS

Globalement, le pourcentage de compromissions qui impliquaient un logiciel malveillant avancé est resté stable, à environ 27 %. Plusieurs secteurs ont toutefois connu une augmentation à deux voire trois chiffres de l'activité de ces menaces.



SERVICES JURIDIQUES

Le pourcentage de compromissions mettant en cause un logiciel malveillant avancé subies par les cabinets d'avocats a doublé par rapport à la période d'évaluation précédente, passant à 10 %. Même si la vaste majorité des compromissions recensées dans ce secteur au cours de la seconde période d'évaluation n'étaient pas attribuables à un logiciel malveillant avancé, cette augmentation de 100 % est largement la plus élevée parmi tous les secteurs.

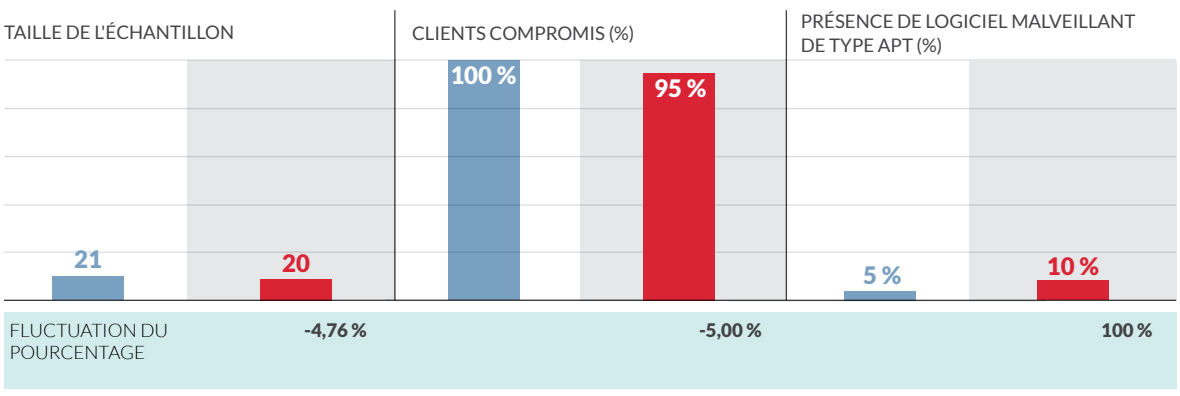
Le principal coupable était **TROJAN.APT.PINGBED**, suivi de loin par **TROJAN.APT.HEARTBEAT**.

100 % D'AUGMENTATION DES LOGICIELS MALVEILLANTS AVANCÉS

Découvert pour la première fois en août 2011, Pingbed cible les PC Windows et a principalement sévi aux États-Unis. En règle générale, les pirates qui l'utilisent incitent les utilisateurs à ouvrir ou à décompresser des fichiers PDF ou Microsoft Word malveillants. Une fois le fichier en question ouvert, le cheval de Troie télécharge, installe et exécute des fichiers malveillants. Il peut également effectuer d'autres actions :

- Configurer des délais de temporisation, une méthode évoluée de contournement des environnements restreints (*sandbox*)
- Collecter des informations sur les processus en cours d'exécution sur l'ordinateur infecté et informer le pirate des logiciels vulnérables éventuellement présents
- Arrêter des processus en cours d'exécution sur l'ordinateur, y compris des mécanismes de sécurité
- Exécuter des lignes de commande

LES PRINCIPAUX VECTEURS D'ATTAQUE sont la messagerie électronique et le Web. Les attaques menées à l'aide de Pingbed altèrent généralement le navigateur Web de l'utilisateur et volent des données, notamment des stratégies juridiques ou des informations confidentielles relatives aux clients et aux parties adverses. Pour la victime, une attaque de cette nature peut compliquer le traitement des dossiers et occasionner d'autres problèmes d'ordre juridique.



COMMERCE

De récentes attaques visant des géants de la grande distribution ont contribué à sensibiliser le public à la question de la cybersécurité puisqu'elles ont touché plusieurs millions de clients. Vous ne serez donc probablement pas surpris d'apprendre que le nombre de compromissions impliquant un logiciel malveillant avancé a grimpé de 30 % dans le secteur du commerce et que celles-ci représentent 17 % des attaques.

BACKDOOR.APT.GH0STRAT, l'une des variantes de logiciels malveillants les plus répandues au cours des derniers mois, tous secteurs confondus, a été identifié le plus souvent sur les systèmes compromis. Nous avons également détecté **TROJAN.APT.SIDEBARDLL**, **TROJAN.APT.HANGOVER** et **BACKDOOR.APT.1PHP**, mais beaucoup moins souvent.

QUAND LES CYBERPIRATES PIQUENT DANS LA CAISSE : LA GRANDE DISTRIBUTION CONFRONTÉE AUX LOGICIELS MALVEILLANTS

(ADAPTÉ D'UN ARTICLE DE BLOG PUBLIÉ PAR NART VILLENEUVE, CHERCHEUR EN CHEF SPÉCIALISÉ EN RENSEIGNEMENTS SUR LES MENACES CHEZ FIREEYE)

Depuis 2013, nous avons constaté une nette augmentation des logiciels malveillants ciblant les systèmes de terminaux de paiement.

La raison est simple : d'énormes quantités de données précieuses sont hébergées sur les réseaux des commerçants, et les cybercriminels sont nombreux à les convoiter.

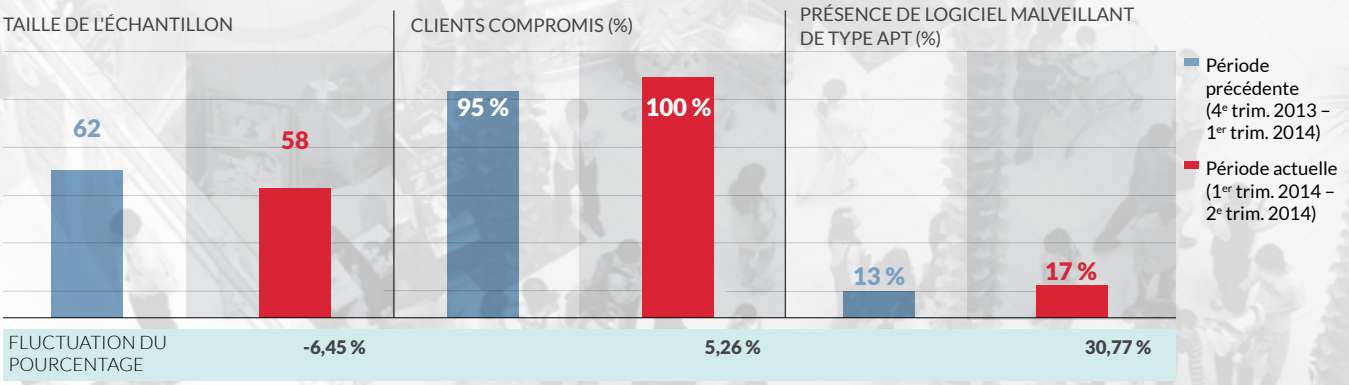
(Suite page 19)

30 % D'AUGMENTATION DES LOGICIELS MALVEILLANTS AVANCÉS

Mis au jour en août 2012, Gh0stRAT confère aux cyberpirates un contrôle étendu sur les systèmes infectés. Ce logiciel malveillant de type porte dérobée (*backdoor*) peut effectuer les opérations suivantes :

LES PRINCIPAUX VECTEURS D'ATTAQUE sont la messagerie électronique et le Web. Les attaques qui tirent parti de Gh0stRAT poussent généralement les utilisateurs à ouvrir un document malveillant. Ensuite, le composant *backdoor* altère le navigateur Web de l'utilisateur et tente de subtiliser des données, en particulier des numéros de carte de crédit. Malgré les gros titres consacrés aux compromissions de grande ampleur contre des enseignes américaines de la grande distribution, ce sont leurs homologues de Corée du Sud qui ont été majoritairement victimes de Gh0stRAT.

L'impact de ces compromissions sur les activités inclut des coûts tangibles ; citons par exemple la perte de ventes lorsque les clients méfiants évitent ces enseignes ou que l'entreprise concernée se trouve dans l'obligation d'informer les clients touchés.



AUTOMOBILE ET TRANSPORT

Bien que les attaques contre les entreprises des secteurs de l'automobile et du transport n'aient pas fait beaucoup parler d'elles dans les médias, nous avons constaté une progression de 29 % du nombre de compromissions faisant appel à un logiciel malveillant avancé, un pourcentage quasiment identique à celui observé pour le secteur du commerce. Peut-être plus alarmant encore : 40 % des systèmes compromis ont été infectés par un logiciel malveillant avancé — l'un des pourcentages les plus élevés de tous les secteurs.

Le logiciel malveillant rencontré le plus souvent sur ces systèmes était **BACKDOOR.APT.IXESHE.** Nous avons également détecté **TROJAN.APT.SHIQIANG**, **BACKDOOR.APT.LECNA** et **BACKDOOR.APT.HUPIGON**, mais beaucoup moins fréquemment.

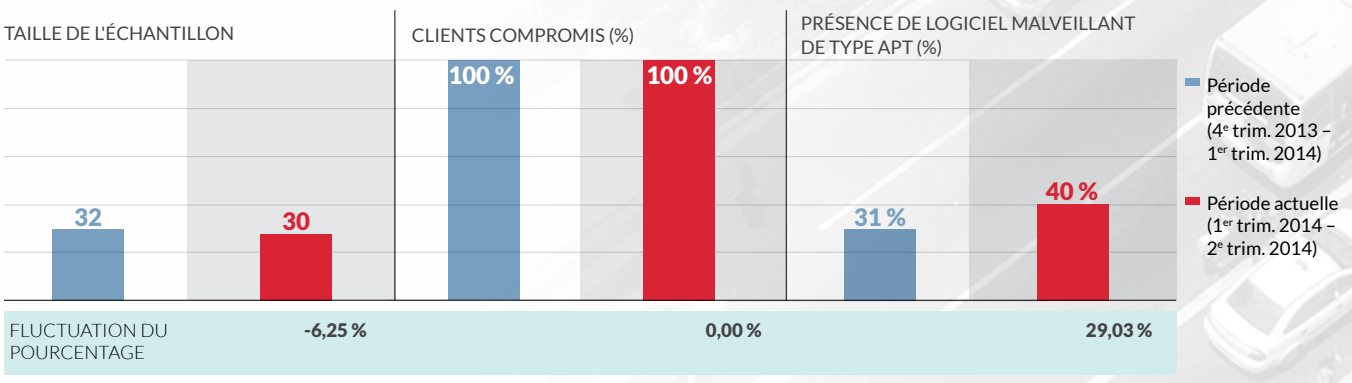
29 % D'AUGMENTATION DES LOGICIELS MALVEILLANTS AVANCÉS

Identifié pour la première fois en novembre 2011, Ixeshe (prononcé « aïe-sushi ») incite les utilisateurs à ouvrir un document piégé, en général un fichier PDF. Une fois le document ouvert, le logiciel malveillant extrait des mots de passe de l'emplacement protégé de Microsoft Internet Explorer afin de pouvoir s'authentifier auprès de serveurs proxy. Il peut exécuter les opérations suivantes :

- Transmettre et télécharger des fichiers
- Afficher et traiter des listes de processus pour surveiller le réseau compromis
- Exécuter des commandes
- Chiffrer le trafic afin de dissimuler l'activité malveillante (variantes récentes)

Ixeshe configure des serveurs de commande et de contrôle (CnC) au sein d'autres réseaux compromis, en vue de limiter autant que possible le trafic externe à destination d'adresses IP suspectes. Ce tour de passe-passe peut rendre Ixeshe extrêmement difficile à détecter[1].

LES PRINCIPAUX VECTEURS D'ATTAQUE sont la messagerie électronique et le Web. Le logiciel malveillant a été le plus souvent détecté lors d'attaques à l'encontre d'entités américaines. Il peut dérober des données et des éléments de propriété intellectuelle à l'organisation prise pour cible, ou encore extraire des identifiants utilisateur, afin de lancer de nouvelles attaques.



[1] Tim Wilson (*InformationWeek*). *New Advanced Persistent Threat, IXESHE, On The Rise*, mai 2012

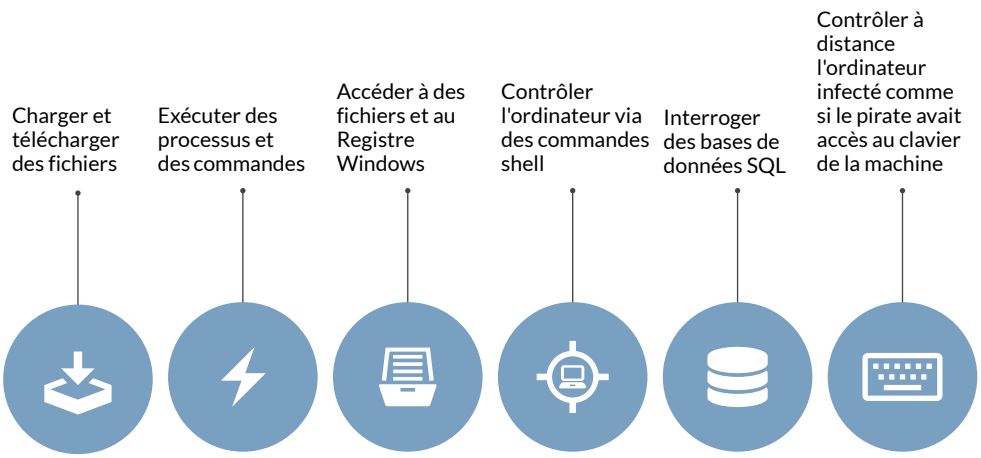
DIVERTISSEMENT ET MÉDIAS

La concentration des compromissions impliquant un logiciel malveillant avancé et visant des entreprises de ce secteur a augmenté de plus de 28 %, celles-ci représentant environ 18 % des attaques recensées au cours de la seconde période d'évaluation.

La famille de logiciels malveillants la plus fréquente était **BACKDOOR.APT.KABA**, suivie de loin par **TROJAN.APT.SISPROC** et **BACKDOOR.APT.GH0STRAT**, aux deuxième et troisième rangs respectivement.

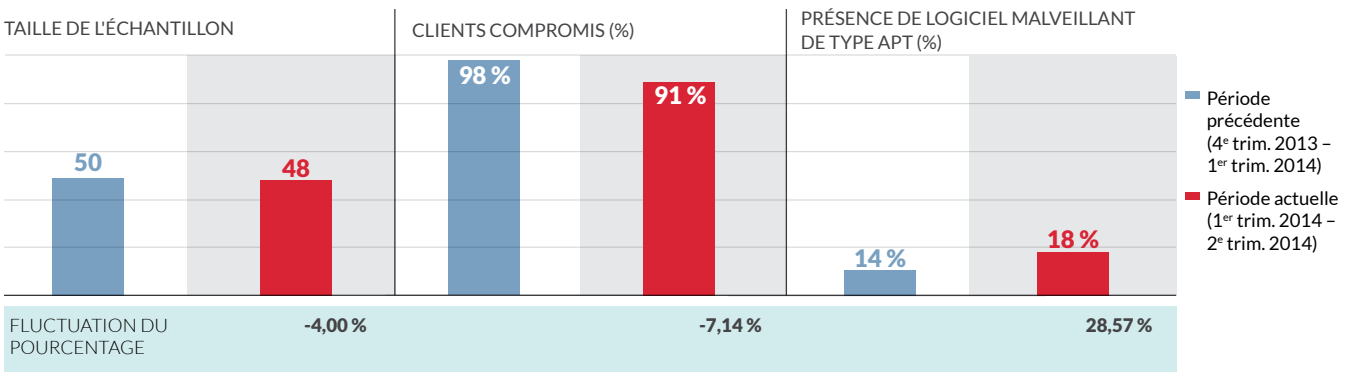
28 % D'AUGMENTATION DES LOGICIELS MALVEILLANTS AVANCÉS

Kaba, également connu sous le nom de PlugX, a été repéré pour la première fois en janvier 2012. Cet outil d'accès à distance (RAT, Remote Access Tool) bien connu procure à l'auteur d'attaque un contrôle total sur les systèmes infectés. Kaba peut exécuter les opérations suivantes :



LES PRINCIPAUX VECTEURS D'ATTAQUE sont la messagerie électronique et le Web. La plupart du temps, Kaba exploite une faille de Microsoft Office. Pour échapper à la détection, Kaba charge le fichier exécutable malveillant en mémoire, mais ne l'écrit jamais sur le disque, ce qui pourrait permettre à un analyseur antimalware de l'identifier.

Kaba a principalement pris pour cible des entreprises du divertissement implantées aux États-Unis. Une compromission peut exposer l'entreprise au vol de propriété intellectuelle (plans marketing subtilisés ; albums, films ou séries piratés avant même leur sortie, etc.) et autres données de valeur.



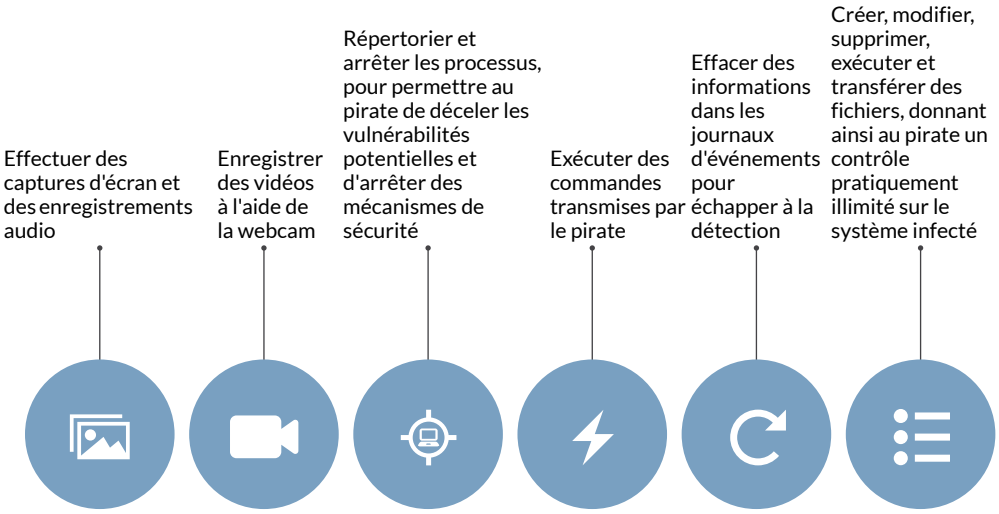
SOINS DE SANTÉ ET INDUSTRIE PHARMACEUTIQUE

Le pourcentage de systèmes infectés par des logiciels malveillants avancés parmi les établissements de soins de santé et les entreprises pharmaceutiques a bondi de plus de 37 %. Ces compromissions ont représenté 22 % de l'ensemble des compromissions détectées dans ces secteurs au cours de la seconde période d'évaluation.

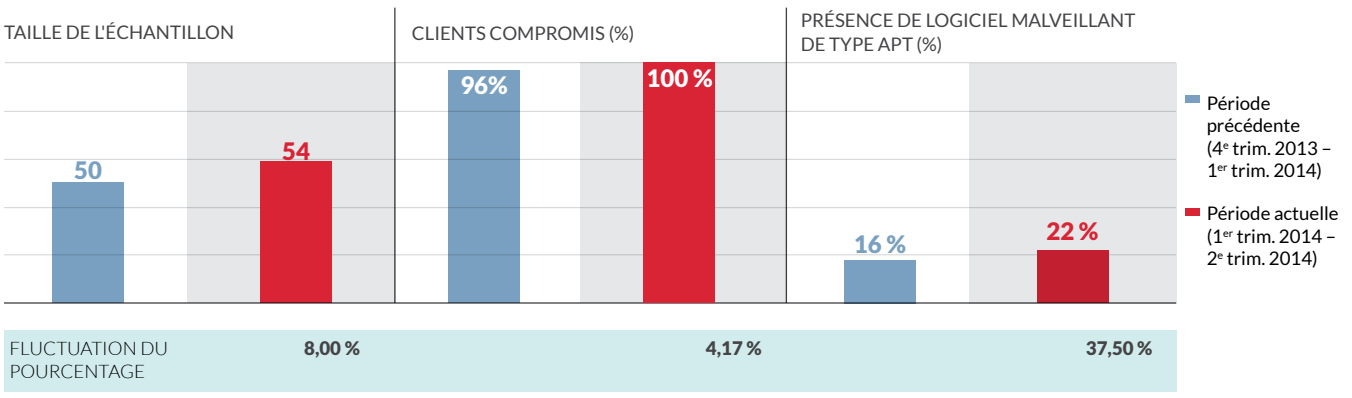
BACKDOOR.APT.GH0STRAT était le plus souvent en cause, suivi de **TROJAN.APT.SISPROC** et de **TROJAN.APT.MOLERAT**.

37 % D'AUGMENTATION DES LOGICIELS MALVEILLANTS AVANCÉS

Comme expliqué dans la section « Commerce » à la page 3, Gh0stRAT est un outil d'accès à distance répandu qui procure à l'auteur de l'attaque un contrôle étendu sur les systèmes infectés. Les données subtilisées sur les systèmes infiltrés peuvent être aussi diverses que des données de patient, des plans de développement ou des formules de nouveaux médicaments.



LES PRINCIPAUX VECTEURS D'ATTAQUE sont la messagerie électronique et le Web. Les attaques qui tirent parti de Gh0st RAT poussent généralement les utilisateurs à ouvrir un document malveillant. Ensuite, le composant *backdoor* altère le navigateur Web de l'utilisateur et tente de subtiliser des données, en particulier des numéros de carte de crédit.



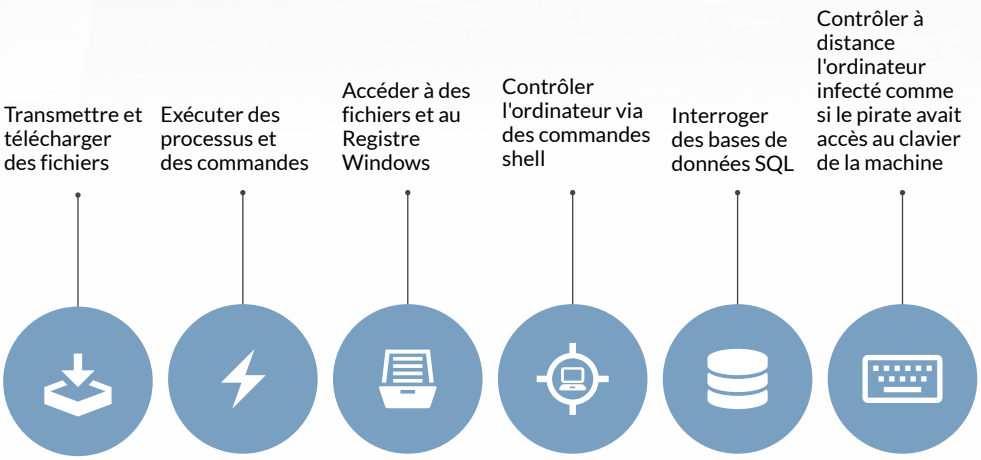
SERVICES ET CONSULTING

La concentration des compromissions par un logiciel malveillant avancé dans le secteur des services et du consulting a enregistré une hausse de 38 %. Celles-ci représentaient près de 30 % des toutes les compromissions ayant visé ce secteur au cours de la seconde période d'évaluation.

BACKDOOR.APT.KABA était le plus souvent à l'origine des attaques, suivi de **TROJAN.APT.HEARTBEAT** et de **BACKDOOR.APT.POISONIVY**.

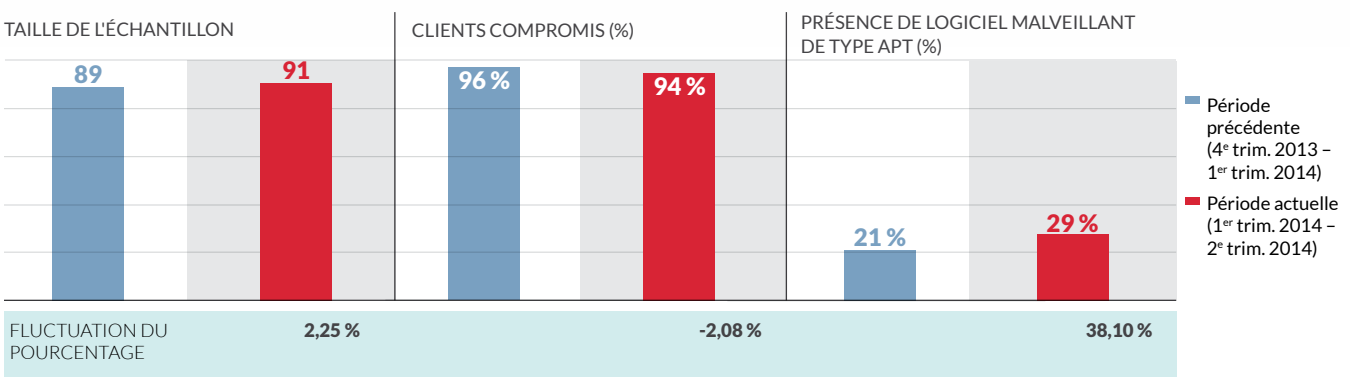
38 % D'AUGMENTATION DES LOGICIELS MALVEILLANTS AVANCÉS

Kaba, également connu sous le nom de PlugX, a été repéré pour la première fois en janvier 2012. Cet outil d'accès à distance (RAT, Remote Access Tool) bien connu procure à l'auteur d'attaque un contrôle total sur les systèmes infectés. Kaba peut exécuter les opérations suivantes :



LES PRINCIPAUX VECTEURS D'ATTAQUE sont la messagerie électronique et le Web. La plupart du temps, Kaba exploite une faille de Microsoft Office. Pour échapper à la détection, Kaba charge le fichier exécutable malveillant en mémoire, mais ne l'écrit jamais sur le disque, ce qui pourrait permettre à un analyseur antimalware de l'identifier.

Dans de nombreux cas, les auteurs d'attaques ciblent des entreprises de services/consulting pour dérober des informations sur leurs clients. Il peut notamment s'agir de renseignements sur les activités de fusion et acquisition, les tactiques de négociation et les stratégies juridiques.



HAUTES TECHNOLOGIES

La concentration des compromissions mettant en cause un logiciel malveillant avancé parmi les entreprises spécialisées dans les hautes technologies a grimpé de près d'un tiers. Celles-ci représentaient environ 32 % des attaques ciblant ce secteur au cours de la seconde période d'évaluation.

BACKDOOR.APT.XTREMERAT a été identifié le plus souvent, suivi de près par **BACKDOOR.APT.3128CREDS** et **BACKDOOR.APT.HOUDINI**.

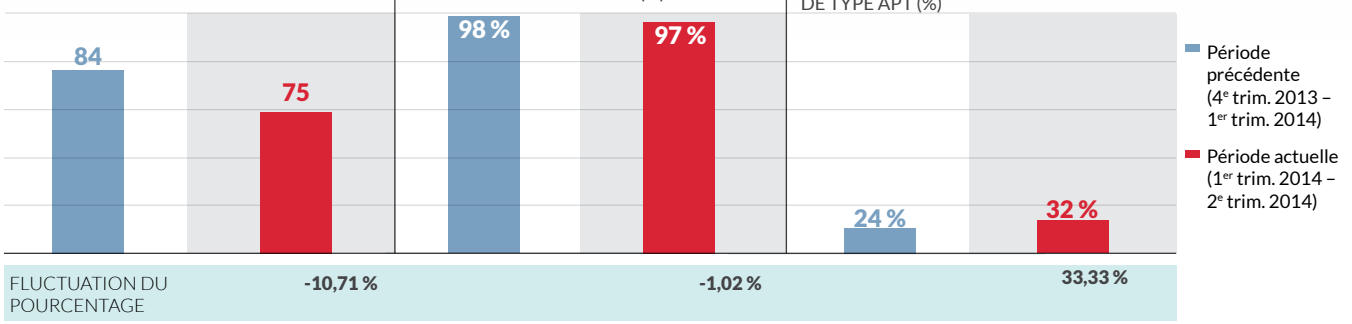
LES PRINCIPAUX VECTEURS D'ATTAQUE sont la messagerie électronique et le Web. XtremeRAT a été exploité dans un grand nombre d'attaques menées par des cybercriminels financés par des États ainsi que par des apprentis pirates. Plusieurs ont fait grand bruit au Moyen-Orient[2], mais le logiciel malveillant a été le plus souvent repéré dans des attaques contre des entités basées aux États-Unis.

Étant donné la simplicité d'emploi et l'étendue des fonctionnalités de XtremeRAT, son impact potentiel est difficile à mesurer. Il pourrait servir aussi bien au vol de simples données qu'à l'espionnage industriel.

32 % D'AUGMENTATION DES LOGICIELS MALVEILLANTS AVANCÉS

XtremeRAT, mis au jour en novembre 2012, est un outil RAT facilement disponible (et très polyvalent) qui peut effectuer les actions suivantes :

- S'exécuter sur Windows 8
- Interagir avec le système pris pour cible via un shell distant
- Transmettre et télécharger des fichiers
- Interagir avec le Registre
- Manipuler des services et des processus en cours d'exécution
- Effectuer des captures d'écran sur le poste de travail
- Réaliser des enregistrements via des équipements tels que la webcam ou le micro



[2] Nart Villeneuve et James T. Bennett (FireEye), *XtremeRAT: Nuisance or Threat?*, février 2014

LES PLUS FORTES CONCENTRATIONS EN LOGICIELS MALVEILLANTS AVANCÉS

La moitié des entreprises agricoles ont été victimes de compromissions par un logiciel malveillant avancé, soit le taux de concentration le plus élevé de tous les secteurs. Signalons néanmoins que l'échantillon évalué pour ce secteur était réduit et qu'aucune comparaison n'a été possible étant donné l'absence de déploiements au sein d'entreprises agricoles durant la première période d'évaluation. Le secteur du transport arrive en deuxième position, avec l'identification de logiciels malveillants avancés dans 40 % des compromissions. Le tableau 1 présente la répartition des taux de concentration des compromissions ayant pour origine un logiciel malveillant avancé entre les secteurs d'activité composant notre échantillon.

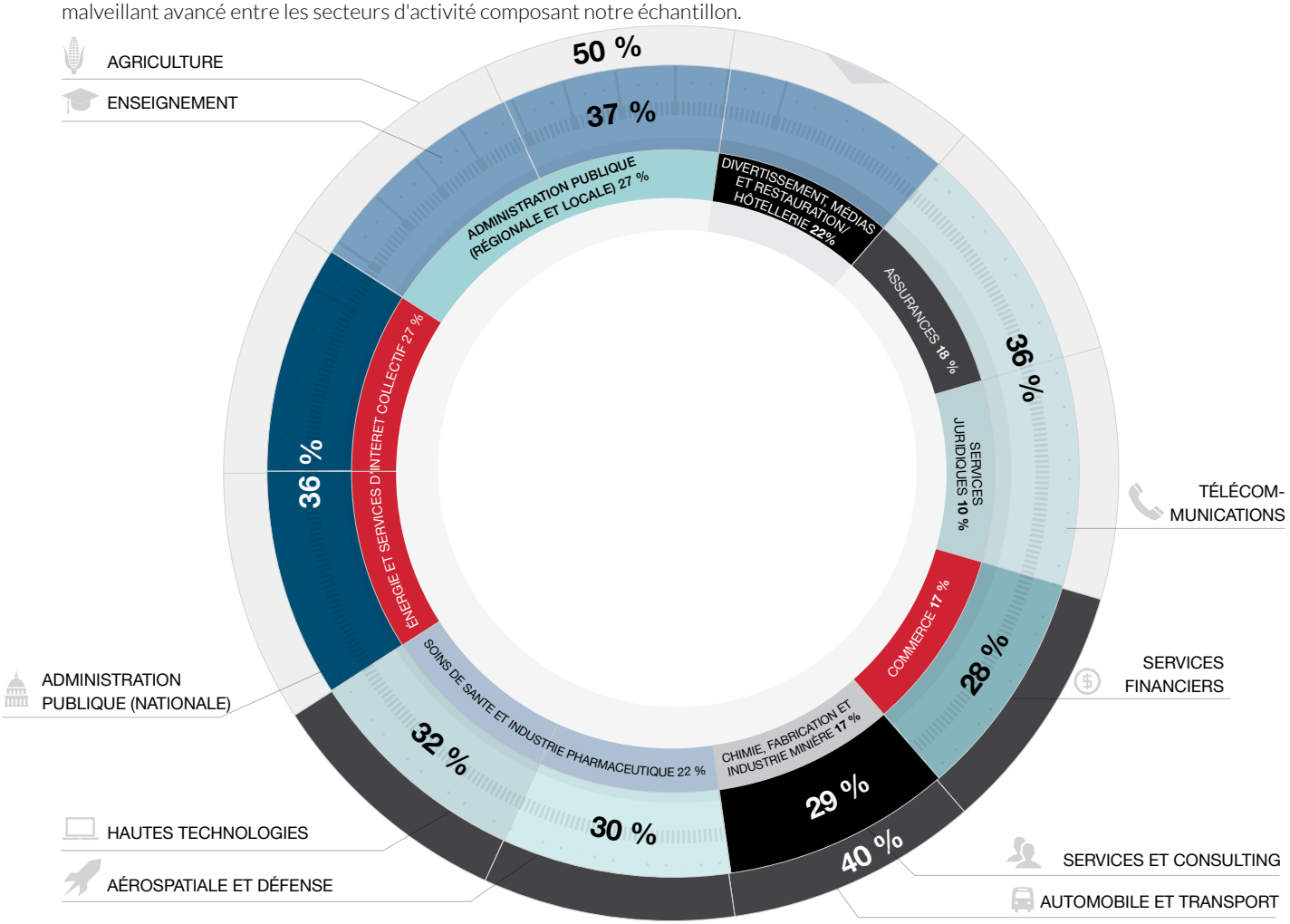


Tableau 1 — Concentration des compromissions par un logiciel malveillant avancé, par secteur d'activité

PRÉSENCE D'UN LOGICIEL MALVEILLANT					
Agriculture	50 %	Aérospatiale et défense	30 %	Divertissement, médias et restauration/ hôtellerie	18 %
Automobile et transport	40 %	Services et consulting	29 %	Assurances	18 %
Enseignement	37 %	Services financiers	28 %	Chimie, fabrication, industrie minière	17 %
Administration publique (nationale)	36 %	Énergie et services d'intérêt collectif	27 %	Commerce	17 %
Télécommunications	36 %	Administration publique (régionale et locale)	27 %	Services juridiques	10 %
Hautes technologies	32 %	Soins de santé et industrie pharmaceutique	22 %	Moyenne	27 %

LES PLUS FORTES CONCENTRATIONS EN COMPROMISSIONS

Comme le montre le tableau 2, plus de 96 % des déploiements de notre échantillon ont subi une compromission au cours de notre étude. C'est le cas de tous les déploiements des secteurs de l'agriculture, de l'automobile et du transport, de l'enseignement et du commerce. De plus, ce fut également le lot d'au moins 90 % des déploiements dans les autres secteurs, à une notable exception près.

En effet, 76 % « seulement » des entreprises de l'aérospatiale et de la défense ont été victimes d'une attaque. Bien qu'un tel chiffre soit inacceptable, il est toutefois nettement inférieur à celui enregistré dans les autres secteurs. Cette différence peut notamment s'expliquer par le fait que de nombreuses entreprises de ce secteur, longtemps une cible de choix des attaques financées par les États, ont renforcé leurs dispositifs de cyberdéfense. Toutefois, comme l'indiquent les données, ces mécanismes restent largement insuffisants.

Tableau 2 — Taux de compromissions par secteur

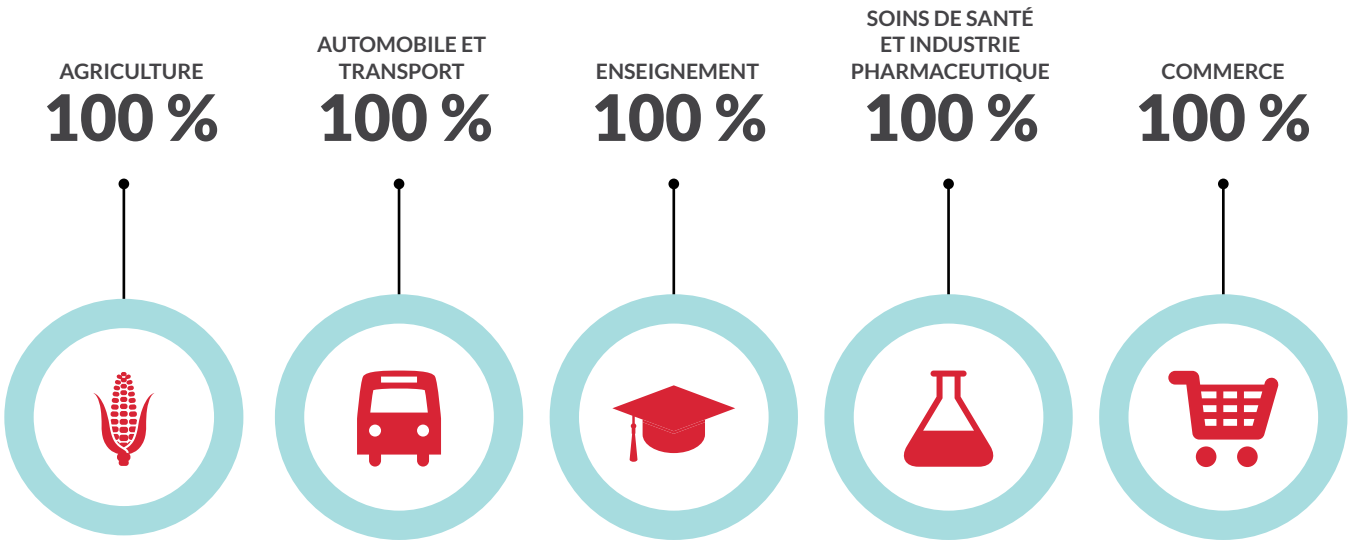


Tableau 2 — Taux de compromissions par secteur

ÉNERGIE ET SERVICES D'INTÉRÊT COLLECTIF	HAUTES TECHNOLOGIES	TÉLÉCOMMUNICATIONS	SERVICES FINANCIERS	ADMINISTRATION PUBLIQUE NATIONALE	ADMINISTRATION PUBLIQUE RÉGIONALE ET LOCALE
98 %	97 %	97 %	96 %	95 %	95 %

SERVICES JURIDIQUES	CHIMIE, FABRICATION, INDUSTRIE MINIÈRE	SERVICES ET CONSULTING	DIVERTISSEMENT, MÉDIAS ET RESTAURATION/ HÔTELLERIE	ASSURANCES	AÉROSPATIALE ET DÉFENSE
95 %	94 %	94 %	91 %	90 %	76 %

MOYENNE 96 %

QUAND LES CYBERPIRATES PIQUENT DANS LA CAISSE : LA GRANDE DISTRIBUTION CONFRONTÉE AUX LOGICIELS MALVEILLANTS

(ADAPTÉ D'UN ARTICLE DE BLOG PUBLIÉ PAR NART VILLENEUVE, CHERCHEUR EN CHEF SPÉCIALISÉ EN RENSEIGNEMENTS SUR LES MENACES CHEZ FIREEYE)

(Suite de la page 10)

Les marchés clandestins en plein essor et l'écosystème de la cybercriminalité offrent aux auteurs de menaces la logistique nécessaire pour élaborer et commercialiser leurs produits. Les familles les plus courantes de logiciels malveillants ciblant les systèmes de terminaux de paiement ainsi que leurs similitudes sont décrites ci-après :

1 Backoff

Des attaques impliquant Backoff ont été rendues publiques en juillet 2014, mais la campagne à proprement parler était déjà active en octobre 2013. D'après les signalements, les pirates avaient recours à des techniques d'attaque par force brute pour accéder à distance aux serveurs des terminaux et installer le logiciel malveillant Backoff. Backoff est capable d'extraire des informations de carte de paiement à partir des données de piste en mémoire puis de les exfiltrer via HTTP. Les serveurs de commande et de contrôle de Backoff sont connectés à ceux utilisés pour héberger Zeus, SpyEye et Citadel, ce qui donne à penser que Backoff peut être lié à un ensemble d'attaques plus vaste.

2 BrutPOS

Le logiciel malveillant BrutPOS a été documenté pour la première fois en juillet 2014. Il s'agit plus précisément d'un réseau de robots (*botnet*), qui balaie des plages définies d'adresses IP de serveurs de terminaux distants. En cas de détection d'un terminal de paiement, l'auteur de l'attaque peut déployer une autre variante qui passe au crible la mémoire des processus en cours d'exécution afin d'en extraire des informations de carte de paiement. BrutPOS exfiltre les données via le protocole FTP (File Transfer Protocol).

3 Soraya

Soraya, un logiciel malveillant visant les terminaux de paiement, a été découvert en juin 2014. Il parcourt les processus en cours d'exécution et accède à la mémoire pour en extraire des données de carte de paiement. Soraya possède également des fonctionnalités de récupération de formulaire et exfiltre les données via HTTP.

4 Nemanja

Les détails relatifs à Nemanja ont été divulgués en mai 2014, mais ce réseau de robots aurait été actif tout au long de l'année 2013. Les auteurs d'attaques ont compromis une série de terminaux exécutant des logiciels de paiement variés à travers le monde. Il semblerait qu'ils soient directement intervenus dans la production de fausses cartes de paiement et dans le blanchiment d'argent à l'aide de solutions pour terminaux de paiement mobiles.

5 JackPOS

Le logiciel malveillant JackPOS a été signalé pour la première fois en février 2014. Il semblerait qu'il se soit d'abord propagé par l'intermédiaire d'attaques de type téléchargement à l'insu de l'utilisateur (drive-by download). Ce logiciel malveillant, apparemment lié à Alina, peut extraire de la mémoire des informations de carte de paiement, puis les exfiltrer via HTTP. JackPOS est aujourd'hui largement disponible sur les forums clandestins et utilisé par une multitude de cyberpirates.

6 Decebal

Decebal a été signalé pour la première fois en janvier 2014. Le logiciel malveillant énumère les processus en cours d'exécution et récupère des données de carte de paiement. Il les exfiltre ensuite via HTTP.

7 ChewBacca

Les premières divulgations du logiciel malveillant ChewBacca remontent à décembre 2013. Celui-ci utilise deux expressions régulières qui font correspondre les formats de données de carte de paiement, énumère les processus en cours d'exécution et accède à la mémoire pour en extraire des informations. Il exploite le réseau d'anonymat Tor à des fins d'exfiltration des données.

8 BlackPOS

BlackPOS, apparemment mis en vente sur les forums clandestins par un individu surnommé « ree4 », a été signalé pour la première fois en mars 2013 et est aujourd'hui largement disponible. Le logiciel malveillant, qui possède une variante appelée KAPTOXA, inspecte la mémoire pour extraire des informations de carte de paiement. Ces données sont généralement transférées vers un emplacement local provisoire, puis exfiltrées par FTP. Son rôle dans plusieurs attaques très médiatisées l'a rendu tristement célèbre.

9 Alina

On attribue l'invention du logiciel malveillant pour systèmes de paiement Alina, divulgué pour la première fois en février 2013, au pirate connu sous le nom de « dice », qui a également participé au développement de Dexter. Il semblerait qu'Alina ait été distribué via des réseaux de robots Citadel. Le logiciel malveillant examine les processus en cours d'exécution (excepté ceux qui figurent sur une liste noire) et effectue un vidage de la mémoire pour rechercher des données de carte de paiement avant de les exfiltrer via HTTP. Utilisé par un nombre restreint de pirates au départ, il a ensuite été mis en vente sur des forums clandestins.

10 vSkimmer

Divulgué pour la première fois en janvier 2013, vSkimmer est disponible sur un large éventail de forums clandestins et exploité par une multitude d'auteurs d'attaques. Le logiciel malveillant parcourt les processus en cours d'exécution et accède à la mémoire pour en extraire des données de carte de paiement, qu'il exfiltre ensuite via HTTP.

CONCLUSIONS ET RECOMMANDATIONS

Depuis la publication de notre premier rapport, plus de six mois se sont écoulés mais les attaques n'ont pas cessé, comme en témoignent les innombrables compromissions de données d'envergure relayées dans les médias. Au vu de nos données les plus récentes, les compromissions de données demeurent monnaie courante.

Cette vulnérabilité est particulièrement alarmante lorsque l'on sait que pratiquement tous les logiciels malveillants avancés utilisés lors de ces compromissions sont bien connus des chercheurs en sécurité et des fournisseurs de solutions de protection. Pourtant, les outils conventionnels ne les arrêtent pas.

FireEye se réjouit de voir que d'autres se mobilisent pour sensibiliser l'opinion aux failles des systèmes traditionnels. Récemment, Delta Testing, une entreprise spécialisée dans les tests de sécurité basés sur des scénarios de déploiements réels, a publié un rapport révélant les graves lacunes des solutions de sécurité sophistiquées de nombreux fournisseurs bien connus. Ce rapport vient confirmer les thèses des précédentes études de FireEye sur la prévalence des logiciels malveillants avancés dans les entreprises, ainsi que les défis auxquels sont confrontés les fournisseurs de produits de sécurité traditionnels dans un paysage des menaces en perpétuelle évolution.

Comme nous le signalions dans notre premier rapport, les organisations doivent impérativement revoir leur approche de la sécurisation de leurs actifs informatiques. Elles doivent abandonner leurs systèmes de défense passifs et peu intégrés qui n'offrent qu'une vue fragmentée des menaces et sont incapables d'établir les liens indispensables pour déjouer une attaque avancée. Elles ont besoin d'une architecture agile et étroitement intégrée qui favorise une vigilance globale. Aujourd'hui, les équipes responsables de la sécurité informatique ne peuvent se permettre d'attendre passivement qu'une attaque survienne. Elles doivent au contraire adopter une approche leur permettant d'anticiper et de traquer activement les nouvelles menaces non identifiées.

FireEye a baptisé cette approche Adaptive Defense™, ou défense adaptative.

Pour en savoir plus sur la manière dont FireEye Adaptive Defense™ peut aider votre entreprise à prévenir, à détecter, à analyser et à neutraliser les menaces avancées actuelles, visitez notre site à l'adresse FireEye.fr.

Pour plus d'informations sur l'approche FireEye Adaptive Defense, rendez-vous sur notre site Web à l'adresse : **www.FireEye.fr**

FireEye, France | 4, place de la Défense, Paris La Défense Cedex 92974 | +33 1 58 58 01 76 | france@FireEye.com | **www.FireEye.fr**
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 | **www.FireEye.com**