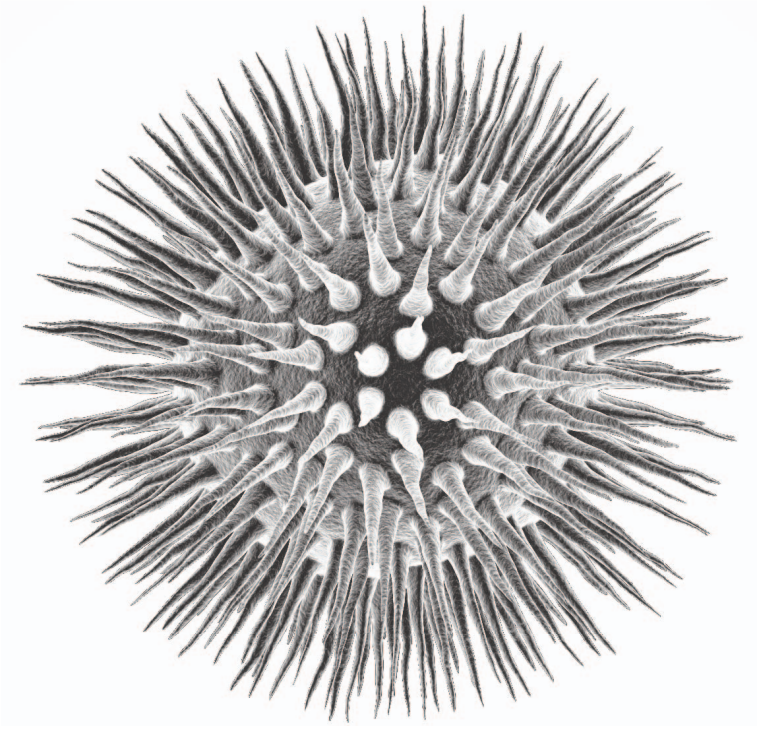
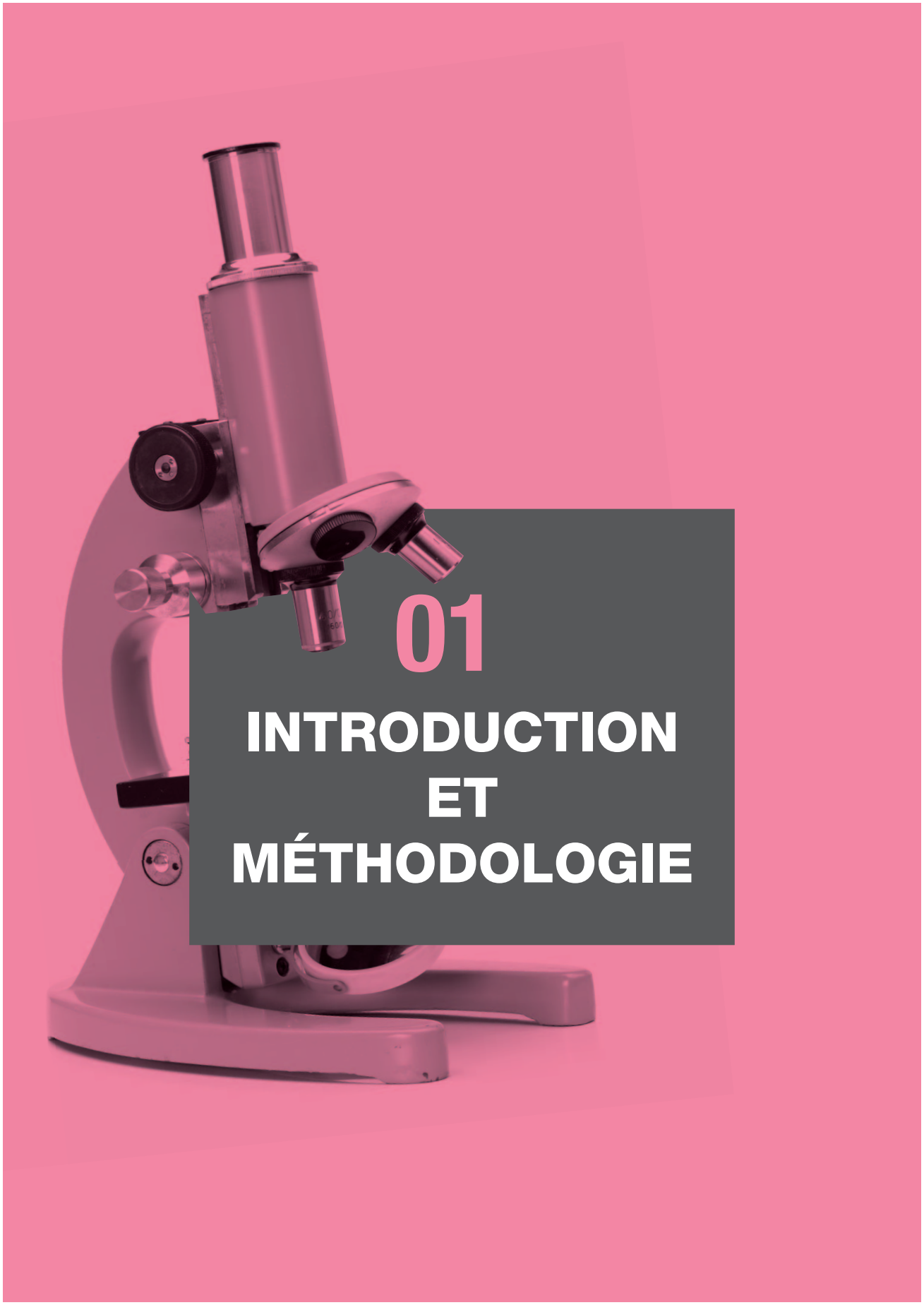
Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.



CHECK POINT
RAPPORT SÉCURITÉ
2014

CHECK POINT
RAPPORT SÉCURITÉ 2014



01

INTRODUCTION ET MÉTHODOLOGIE

01 INTRODUCTION ET MÉTHODOLOGIE

SUR LA SORTIE PAPIER, JE POUVAIS VOIR LE PIRATE TENTER SA CHANCE SUR MILNET. IL A ESSAYÉ QUINZE ORDINATEURS DE L'ARMÉE DE L'AIR LES UNS APRÈS LES AUTRES, DANS LES BASES D'EGLIN, DE KIRTLAND ET DE BOLLING. SANS SUCCÈS. IL SE CONNECTAIT À CHAQUE ORDINATEUR, ESSAYAIT D'OUVRIR LA PORTE UNE FOIS OU DEUX FOIS, PUIS PASSAIT AU SYSTÈME SUIVANT. JUSQU'À CE QU'IL ESSAIE LES SYSTÈMES DE LA DIVISION DU SPACE COMMAND. IL A D'ABORD TENTÉ D'OUVRIR LA PORTE EN ESSAYANT LEUR COMPTE SYSTEM AVEC LE MOT DE PASSE « MANAGER ». SANS SUCCÈS. PUIS LE COMPTE GUEST AVEC LE MOT DE PASSE « GUEST ». AUCUN EFFET. PUIS LE COMPTE FIELD AVEC LE MOT DE PASSE « SERVICE » [...] COMME PAR MAGIE, LA PORTE S'EST GRANDE OUVERTE. IL AVAIT RÉUSSI À SE CONNECTER EN TANT QU'ANTENNE DU SERVICE ADMINISTRATIF. PAS SEULEMENT UN UTILISATEUR ORDINAIRE. UN COMPTE COMPLÈTEMENT PRIVILÉGIÉ. [...] QUELQUE PART EN CALIFORNIE DU SUD, À EL SEGUNDO, UN ORDINATEUR VAX ÉTAIT INFILTRÉ PAR UN PIRATE INFORMATIQUE SITUÉ À L'AUTRE BOUT DU MONDE.

Clifford Stoll, *The Cuckoo's Egg*[1]

Il y a plus de vingt-cinq ans, un administrateur UNIX a remonté le fil d'une erreur de facturation de 75 cents jusqu'à un réseau d'espionnage du bloc de l'Est qui tentait de voler des secrets du gouvernement et de l'armée des États-Unis. Le récit de son cheminement, de la découverte des anomalies initiales jusqu'à son combat contre la plus grande intrusion, est retracé dans *The Cuckoo's Egg*, qui reste un modèle pour les défis de la cyberdéfense.

Les technologies impliquées, les moyens de connexion et les méthodes d'intrusion, ont énormément évolué depuis la fin des années 1980, mais l'identification des systèmes compromis, la réponse aux incidents, et la protection des systèmes et des données contre de futures attaques restent les principaux défis à relever pour les entreprises dans le monde entier, indépendamment de leur taille et de leur secteur d'activité.

En 2013, la sécurité de l'information a pris une place importance dans la conscience publique en raison de la forte médiatisation des fuites de données. Le vol et la divulgation d'informations appartenant au renseignement américain ont fait la une des actualités en 2013 et ont secoué les relations diplomatiques à travers le monde. Des vols à grande échelle de données de cartes bancaires ont été signalés tout au long de l'année et ont ruiné la saison des soldes des grandes enseignes et de nombreux consommateurs. La cyberguerre et « l'hacktivisme »[2] ont remodelé la nature des conflits entre les peuples et les nations, de même que l'émergence de « l'Internet des objets »[3] expose plusieurs aspects de nos vies quotidiennes et les rend vulnérables.

Dans le milieu de la sécurité, la flambée des logiciels malveillants inconnus, pas seulement les nouvelles menaces, mais de nouvelles façons de créer et déployer des menaces indétectables à très grande échelle, a remis en question la viabilité des stratégies et des technologies existantes. De plus en plus de logiciels malveillants courants deviennent obstinément résistants aux défenses en place, tandis que la mobilité, la consumérisation et « l'informatique de l'ombre », ont considérablement accru la complexité des problématiques de sécurité.

5 QUESTIONS QUE VOUS DEVEZ VOUS POSER

1. COMMENT L'ÉVOLUTION RAPIDE DU PAYSAGE DE LA SÉCURITÉ A AFFECTÉ VOTRE ENTREPRISE ?

2. QUELLES MENACES AVEZ-VOUS RENCONTRÉ, ET QUELS SONT LES RISQUES ÉMERGENTS QUI VOUS PRÉOCCUPENT LE PLUS ?

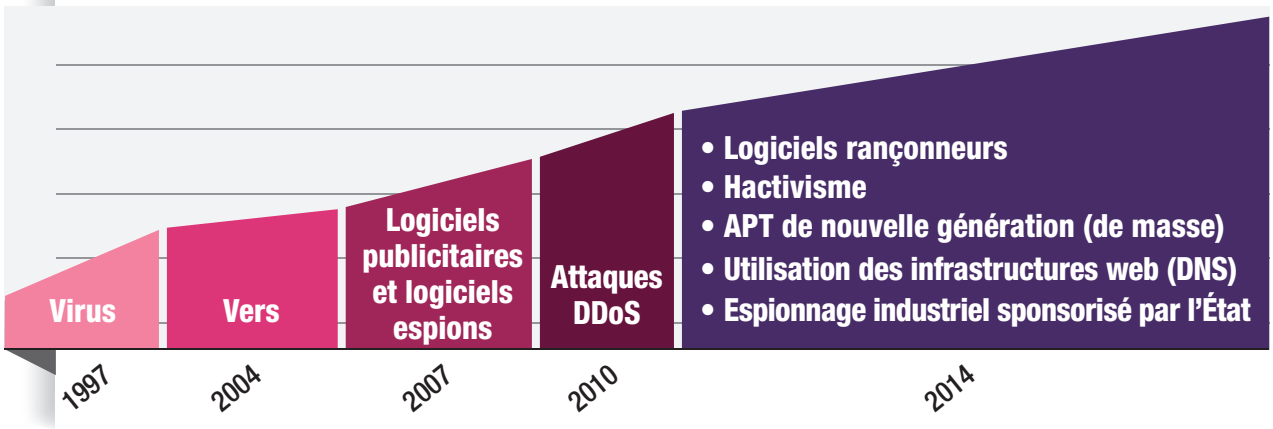
3. PENSEZ-VOUS AVOIR LA BONNE STRATÉGIE ET LES BONS OUTILS POUR RELEVER LES DÉFIS, OU ÊTES-VOUS DE PLUS EN PLUS DÉPASSÉS PAR D'INCESSANTES VAGUES DE DÉVELOPPEMENTS INQUIÉTANTS ?

4. QUELLES NOUVELLES MESURES ALLEZ-VOUS ADOPTER DURANT L'ANNÉE ?

5. COMMENT ALLEZ-VOUS AIDER VOTRE ENTREPRISE À RENFORCER SA SÉCURITÉ ?

Les chercheurs de Check Point ont analysé les événements de plus de 10 000 entreprises sur une année complète pour identifier les tendances de sécurité informatique et les logiciels malveillants critiques de 2013 auxquels les entreprises doivent faire face en 2014 et au-delà. Le *Rapport Sécurité 2014* de Check Point présente les résultats de cette analyse. Cette analyse en profondeur des menaces et des tendances de 2013 aidera les décideurs à comprendre les différentes menaces qui pèsent sur leur entreprise. Le rapport comprend également des recommandations sur la manière de se protéger contre ces menaces et de futures menaces. Les points clés de notre étude sont :

Tendances des logiciels malveillants



UNE JOURNÉE TYPIQUE EN ENTREPRISE

Toutes les **1 mn**, un hôte accède à un site web malveillant

Toutes les **3mn**, un bot communique avec son centre de commande et de contrôle

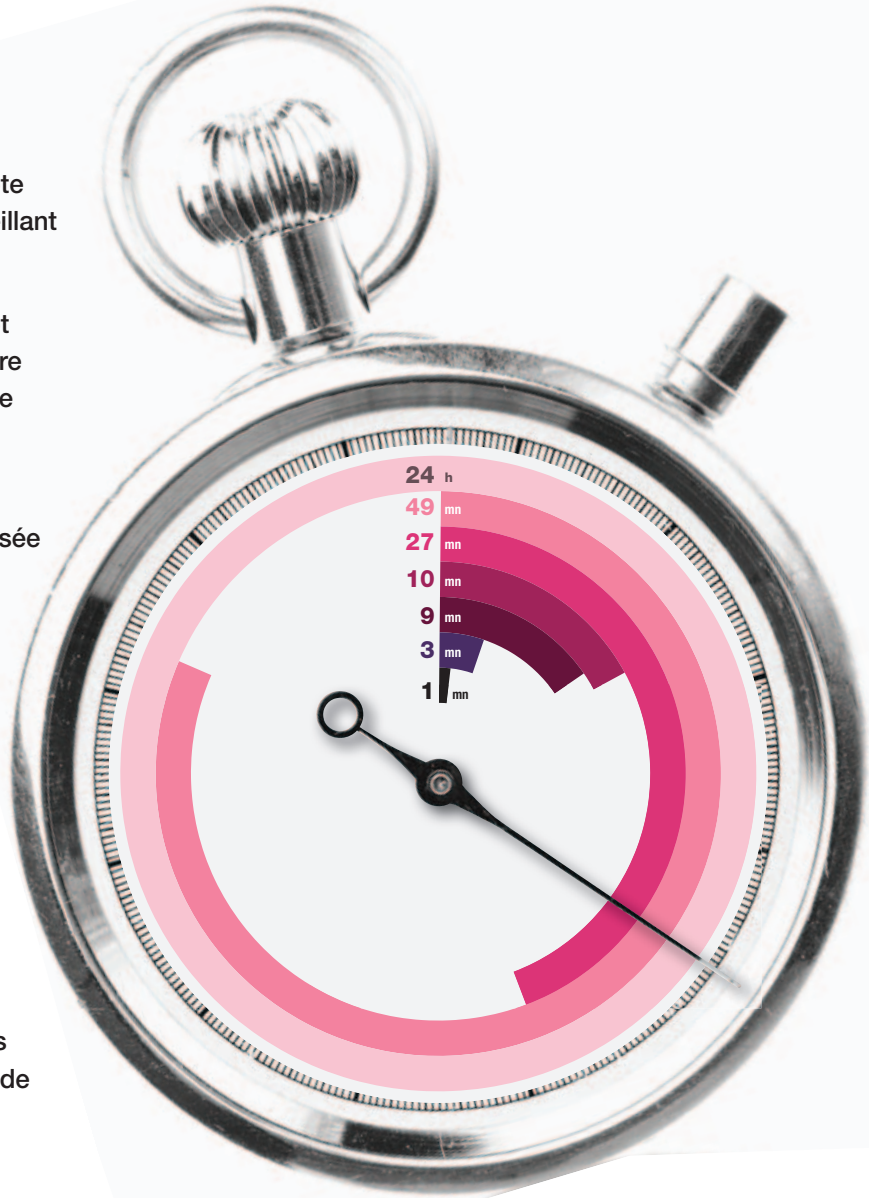
Toutes les **9mn**, une application à risque est utilisée

Toutes les **10mn**, un logiciel malveillant connu est téléchargé

Toutes les **27 mn**, un logiciel malveillant inconnu est téléchargé

Toutes les **49mn**, des données confidentielles sont envoyées à l'extérieur de l'entreprise

Toutes les **24h**, un hôte est infecté par un bot



Graphique 1-1

Source : Check Point Software Technologies

TABLEAU COMPLET DES MENACES

Environnement informatique : utilisateurs, données et systèmes

Objectifs métiers

Paysage des menaces : logiciels malveillants

COMPRENDRE VOTRE SÉCURITÉ

- L'utilisation de logiciels malveillants inconnus a explosé avec la tendance de la « personnalisation de masse »[4] des logiciels malveillants : 2,2 logiciels malveillants inconnus en moyenne (des logiciels malveillants qui n'ont jamais été vu avant) frappent les entreprises toutes les heures
- Le nombre d'infections a augmenté, ce qui reflète le succès croissant des campagnes de logiciels malveillants ciblées : en 2013, 73% des entreprises ont détecté au moins un bot, par rapport à 63% en 2012
- Chaque catégorie d'application à risque est de plus en plus présente dans les entreprises dans le monde entier : par exemple, 63% des entreprises ont constaté l'utilisation de BitTorrent, par rapport à 40% en 2012
- Le nombre d'incidents de fuites de données ont augmenté dans tous les secteurs et pour tous les types de données : 88% des entreprises ont connu au moins une fuite de données, contre 54% en 2012

Les sources de données de ce rapport

Le *Rapport Sécurité 2014* de Check Point repose sur des études collaboratives et des analyses des événements de sécurité provenant des rapports d'analyse des passerelle de sécurité de Check Point (Security Checkup),[5] des capteurs de Check Point Threat Emulation,[6] de Check Point ThreatCloud™,[7] et des rapports de Check Point Endpoint Security.[8]

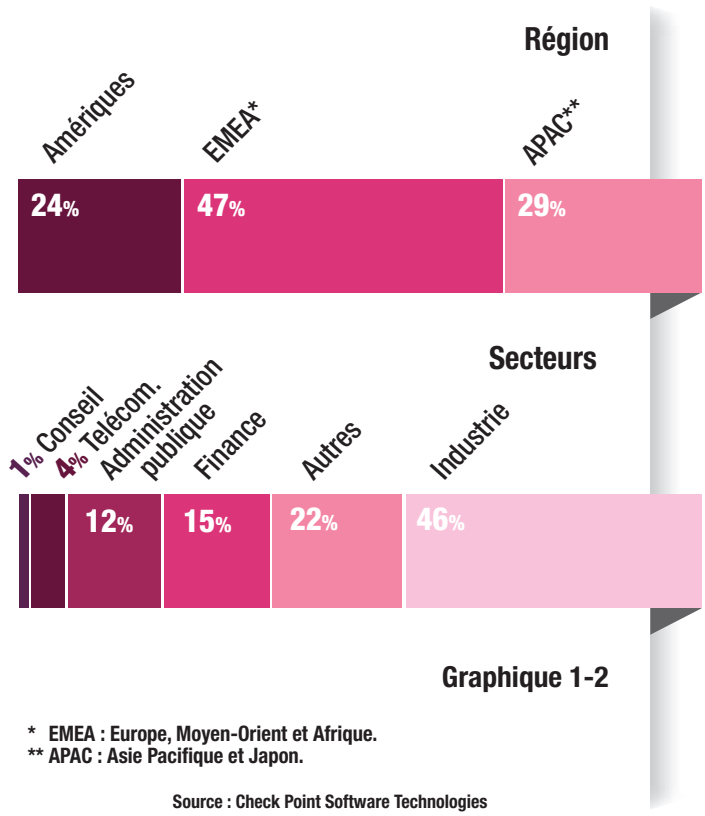
Une méta-analyse des événements de sécurité réseau de 996 entreprises a été effectuée à partir des données recueillies via des études Check Point Security Checkup, qui ont analysé en direct le trafic entrant et sortant de ces entreprises. Ce trafic a été inspecté grâce à la technologie multicouche Check Point Software Blades[9] afin de détecter différents types d'applications à risque, de tentatives d'intrusions, de virus, de bots, de fuites de données confidentielles et autres menaces. Le trafic réseau de chaque entreprise était surveillé en temps réel via le mode en ligne ou le mode surveillance des passerelles de sécurité Check Point,[10] pendant 216 heures en moyenne.

Les entreprises étudiées sont issues d'un large éventail de secteurs et sont situées dans le monde entier comme le montre le Graphique 1-2.

En outre, des événements provenant de 9 240 passerelles de sécurité ont été analysés à l'aide des données générées par Check Point ThreatCloud. ThreatCloud est une base de données massive mise à jour en temps réel à partir de données de sécurité provenant d'un vaste réseau mondial de capteurs placés stratégiquement autour du globe. ThreatCloud collecte des informations sur les menaces et les attaques de logiciels malveillants, et permet d'identifier les nouvelles tendances mondiales de sécurité et de menaces, pour constituer un réseau collaboratif de lutte contre la cybercriminalité. Pour notre étude, les données de ThreatCloud recueillies sur une période de 12 mois ont été consolidées puis analysées.

Des données sur les logiciels malveillants inconnus ont été recueillies par les capteurs de Check Point Threat Emulation, entre juin et décembre 2013. Check Point Threat Emulation place les fichiers suspects détectés par les passerelles Check Point dans un bac à sable dans le cloud et les analyse dynamiquement. Des données anonymes provenant de Threat Emulation depuis 848 passerelles de sécurité ont été relayées dans ThreatCloud pour agrégation, corrélation et analyse avancée.

Enfin, une méta-analyse de 1 036 rapports de sécurité de postes de travail provenant de différentes entreprises a été effectuée. Cette analyse de la sécurité évaluait notamment chaque hôte pour estimer les risques de fuites de données, les risques d'intrusions et les risques liés aux logiciels malveillants. L'analyse a été réalisée au moyen d'un outil de reporting Check Point Endpoint Security pour vérifier la présence d'un antivirus sur les hôtes, s'il est à jour, si les logiciels utilisés sont les dernières versions, et plus encore. Cet outil est gratuit et disponible publiquement. Il peut être téléchargé depuis le site de Check Point.



Graphique 1-2

*** EMEA : Europe, Moyen-Orient et Afrique.**
**** APAC : Asie Pacifique et Japon.**

Source : Check Point Software Technologies

Les données au cœur du *Rapport Sécurité 2014* de Check Point sont complétées par des exemples d'incidents réels qui illustrent la nature des menaces actuelles, leur impact sur les entreprises concernées et leurs implications pour la communauté de la sécurité. Des experts émettent également des recommandations et des conseils afin que votre stratégie et vos solutions de sécurité soient pertinentes et efficaces pour vous protéger contre les risques d'aujourd'hui. Le rapport est divisé en chapitres traitant des logiciels malveillants inconnus, des logiciels malveillants connus, des applications à risque et des fuites de données.

02

LA FLAMBÉE DES LOGICIELS MALVEILLANTS INCONNUS

02 LA FLAMBÉE DES LOGICIELS MALVEILLANTS INCONNUS

LE CONNU EST FINI,
L'INFINI EST INCONNU.

Thomas Henry Huxley[11]

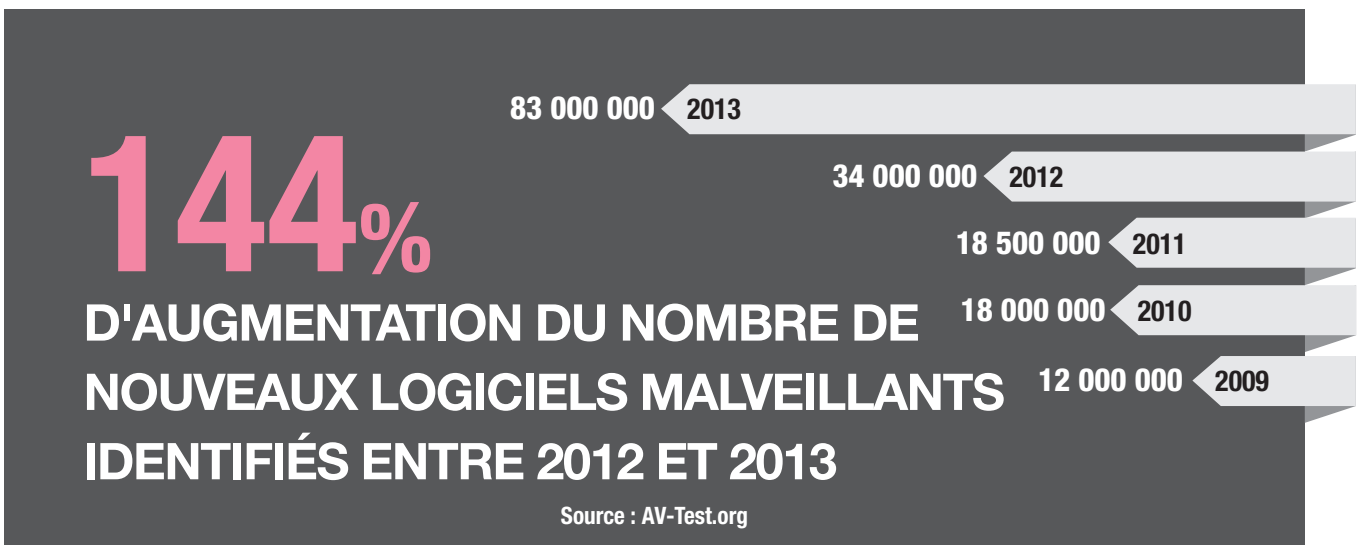
La menace des logiciels malveillants inconnus

Les technologies traditionnelles de sécurité telles que les antivirus et les systèmes de prévention d'intrusions (IPS) sont les plus efficaces pour détecter les tentatives d'exploitation des vulnérabilités connues des logiciels, et dans une certaine mesure, elles offrent également une protection préventive contre les attaques inconnues. Les pirates ont bien compris cela et s'offrent le luxe de tester leurs nouveaux logiciels malveillants sur ces technologies afin de vérifier s'ils sont détectés.

La course aux armements entre les éditeurs de solutions de sécurité et les pirates conduit à une évolution rapide des techniques utilisées par ces derniers, qui essaient continuellement d'utiliser des vulnérabilités inconnues (également appelées « exploitations de vulnérabilités zero-day » car il faut habituellement quelques heures ou quelques jours pour les détecter et fournir les protections adéquates) et des méthodes d'infection inconnues dans le but de contourner les défenses.

Fin 2013, les chercheurs de Check Point travaillant avec le service Threat Emulation ont découvert et analysé une nouvelle variante de logiciel malveillant qui employait une combinaison sophistiquée de techniques pour échapper aux proxies et aux solutions antimalwares. Dénommé « HIMAN »[12] par les chercheurs, ce logiciel malveillant illustre parfaitement le type d'attaques ciblées complexes auxquelles sont confrontés les entreprises et les professionnels de la sécurité informatique à travers le monde.

La passerelle de sécurité d'un client Check Point abonné au service Threat Emulation, a analysé un document Microsoft Word joint à un email provenant de l'adresse « boca_juniors@aol.com » avec pour ligne d'objet « Invitation à une réception ». Lors de l'ouverture dans un bac à sable, le document a exploité une vulnérabilité connue (CVE-2012-0158) afin de déposer un fichier nommé « kav.exe » dans le dossier « Local Settings\



Graphique 2-1

2,2

LOGICIELS MALVEILLANTS INCONNUS FRAPPENT LES ENTREPRISES TOUTES LES HEURES

Temp » de l'ordinateur cible de l'utilisateur. Le nom de ce fichier semblait être un leurre destiné à ressembler à l'exécutable[13] de l'antivirus Kaspersky, et le logiciel malveillant lui-même semblait lié à des campagnes de logiciels malveillants précédentes que les chercheurs ont attribué à un ou plusieurs groupes d'attaquants chinois. L'analyse a révélé que le fichier procédait en deux étapes, en se renommant en cours d'installation sur le système cible puis en s'accrochant au processus « explorer.exe » afin de charger une DLL malveillante.

Check Point a effectué des recherches dans les bases de données de logiciels malveillants connus et a constaté qu'aucun éditeur d'antivirus n'était capable de détecter ce logiciel malveillant au moment où il a été découvert.

Ce dernier injectait une bibliothèque malveillante (mswins64.dll) à l'aide d'une série d'appels de fonctions Windows et de contrôles d'exclusion mutuelle, afin d'installer le logiciel malveillant dans le système client sans être détecté par les solutions antimalwares existantes. Une fois installé, le logiciel malveillant ajoutait une entrée dans la base de registre différente de celles bien connues qui sont couramment utilisées par les processus des logiciels malveillants, et qui sont donc plus étroitement surveillées par les logiciels antimalwares. Cette combinaison d'appels de fonctions API et d'entrées dans la base de registre moins utilisées permettait au logiciel malveillant d'augmenter ses chances d'échapper à toute détection.

HIMAN démontre comment les auteurs de logiciels malveillants mettent à profit leur expertise du système Windows, du comportement du système d'exploitation et du fonctionnement des outils antimalwares pour échapper à toute détection, sans aller jusqu'à développer ou acheter un véritable kit d'exploitation de vulnérabilité zero-day. Cette sophistication s'étend également aux communications de commande et de contrôle et aux processus d'exfiltration : HIMAN peut s'attaquer à des proxies sortants via des méthodes de force brute à l'aide d'identifiants stockés, chiffrer les données recueillies à l'aide d'AES,[14] et utiliser des techniques d'obscurcissement pendant l'exfiltration afin de se soustraire au filtrage sortant.

Une fois installé, et après avoir établi une connexion à un serveur de commande et de contrôle, HIMAN s'adapte dynamiquement et exécute un script qui recueille des données sur les services utilisés, les comptes locaux ayant des droits administrateur, d'autres informations sur la configuration du système et les parties du réseau local qui sont visibles à la machine infectée. Armés de cette information, les assaillants possèdent une carte du réseau local et un moyen d'accès à l'entreprise ciblée pour continuer à l'étudier, l'explorer, exfiltrer des données, et attaquer les serveurs, les systèmes et les processus métiers.

Utilisant différentes techniques pour établir une tête de pont dans le réseau d'une entreprise ciblée et dérober des données confidentielles, le logiciel malveillant HIMAN démontre à la fois la flexibilité des développeurs

MOINS DE 10% DES MOTEURS ANTIVIRUS DÉTECTENT LES LOGICIELS MALVEILLANTS INCONNUS LORSQU'ILS SONT CAPTURÉS POUR LA PREMIÈRE FOIS

CRÉER UN

INCONNU EST SI FACILE QU'UN ENFANT POURRAIT LE FAIRE

de logiciels malveillants et des agresseurs, et les défis auxquels les professionnels de la sécurité ont été confrontés en 2013.

Comment en sommes-nous arrivés là ? L'évolution des logiciels malveillants inconnus

Depuis plusieurs années, les dangers des attaques ciblées et des menaces persistantes avancées (APT) ont fortement suscité l'attention des professionnels de la sécurité de l'information. Les APT ont fait leur entrée sur scène en 2010 avec l'attaque ciblée Stuxnet,[15] dans laquelle un logiciel malveillant hautement spécialisé a déstabilisé le système de contrôle d'une centrifugeuse nucléaire iranienne dans le cadre de cyberattaques parrainées par des États.

Ce nouveau type de logiciels malveillants a réussi à percer la plupart des défenses antimalwares classiques de trois manières. Tout d'abord, Stuxnet était très spécialisé. Il a été étudié et conçu pour un système spécifique, dans un environnement spécifique, et avec un objectif précis en tête. Deuxièmement, il était très rare, ce qui signifie qu'il n'avait jamais été exposé aux réseaux de collecte et d'analyse que les éditeurs d'antivirus ont mis au point pour rester au fait du « marché de masse » des virus et des bots qui avait défini le paysage des logiciels malveillants depuis une décennie, et il était resté silencieux pendant un laps de temps indéterminé de potentiellement plusieurs années. Enfin, le motif derrière Stuxnet différait nettement de celui des virus et de la plupart des vers très médiatisés, tels que Code Red[16] et Sasser,[17] qui ont suivis. En regard de ce motif, il est clair que le ou les auteurs de Stuxnet étaient persévérants.

En bref, Stuxnet représentait un nouveau type de logiciels malveillants ciblé, rare et motivé, que les technologies antivirus et de prévention d'intrusions existantes étaient mal équipées pour le combattre. En ce sens, il était à l'avant-garde d'une vague de logiciels malveillants sur mesure exigeant un nouvel ensemble d'outils et de stratégies. L'émergence de HIMAN souligne l'évolution continue de cette tendance et la menace qu'elle représente.

33%

DES ENTREPRISES ONT TÉLÉCHARGÉ AU MOINS UN FICHIER INFECTÉ PAR UN LOGICIEL MALVEILLANT INCONNU

ATTAQUE CIBLÉE, CAMPAGNE MONDIALE

Le 22 octobre 2013, une entreprise de médias a reçu six emails suspects qui ont été analysés par le service Check Point Threat Emulation.

- De : No-Replay@UPS.COM
- Objet : Notification de livraison UPS
- Pièce jointe : factureBQW8OY.doc (MD5 ad0ef249b1524f4293e6c76a9d2ac10d)

Pendant la simulation automatique dans un bac à sable virtuel d'un utilisateur ouvrant un fichier potentiellement malveillant, plusieurs comportements anormaux ont été détectés :

- Microsoft Word a cessé de fonctionner et s'est relancé avec un document vide
- Une clé de registre a été configurée
- Un nouveau processus a été lancé sur le poste

Check Point Threat Emulation a déterminé en conséquence que ce fichier était malveillant.

Une analyse plus approfondie effectuée par les chercheurs de Check Point a mis en évidence que les documents des six emails étaient identiques et exploitaient la vulnérabilité CVE-2012-0158 affectant Microsoft Word. Cette vulnérabilité, également appelée MSCOMCTL.OCX RCE,[18] permet l'exécution de code à distance sur le poste.

L'analyse a identifié le code malveillant comme étant une variante personnalisée du cheval de Troie Zbot,[19] qui dérobe des données via des attaques de type « man-in-the-browser », enregistrement de frappe, détournement de formulaires et autres méthodes. La consignation de ces échantillons dans la base de données VirusTotal[20] a révélé un faible taux de détection (< 10%) à la fois pour la pièce jointe malveillante et la variante de Zbot au moment de la consignation.

Les chercheurs de Check Point ont analysé les différentes URL à partir desquelles les documents malveillants ont été téléchargés et ont déterminé que la liste des paramètres uniques passés aux serveurs infectant était en fait un désignateur de cible chiffré en Base64 contenant l'adresse email ciblée. Ces URL uniques représentaient les adresses email des utilisateurs de grandes entreprises ciblées par les attaques, y compris de grandes entreprises internationales, dont des institutions financières, des constructeurs automobiles internationaux, des opérateurs de télécoms, des organismes gouvernementaux, des institutions d'enseignement et des organismes municipaux en Amérique du Nord. Les attaques faisaient partie d'une campagne ciblée visant à capturer des identifiants utilisateur, des informations bancaires et d'autres informations pouvant être utilisées pour accéder aux données les plus confidentielles des entreprises ciblées.

35%

DES FICHIERS INFECTÉS PAR DES LOGICIELS MALVEILLANTS INCONNUS SONT AU FORMAT PDF

2013 : Un début prometteur, une fin décevante

Les administrateurs sécurité sont de plus en plus habitués aux attaques ciblées, mais également aux nouveaux outils nécessaires pour les combattre. Les technologies automatisées d'analyse en bac à sable des logiciels malveillants sont des outils bien connus des équipes de sécurité des grandes entreprises et des organismes publics, qui les ont déployés pour renforcer leur infrastructure de sécurité actuelle et détecter les logiciels malveillants ciblés qui pourraient autrement échapper aux défenses existantes des passerelles et des postes reposant sur des signatures et l'évaluation de la réputation.

Cependant, 2013 a connu une augmentation spectaculaire de la fréquence des « logiciels malveillants inconnus », c'est-à-dire des attaques appliquant les techniques d'obscurcissement et de contournement des APT à des logiciels malveillants connus dans des campagnes ciblées de portée mondiale (Encart : *Attaque ciblée, campagne mondiale*). Non seulement les attaques hyper ciblées utilisant des logiciels malveillants hautement spécialisés demeurent une problématique, la « personnalisation de masse » signifie maintenant que l'efficacité accrue des logiciels malveillants ciblés est également à la portée de campagnes de grande envergure motivées par l'appât du gain.

« Inconnu » ou « zero-day »

Il est important de distinguer les logiciels malveillants inconnus de ce qui est sont souvent dénommé exploitation de vulnérabilités « zero-day ». Les logiciels malveillants zero-day exploitent des vulnérabilités jusqu'alors inconnues et non déclarées pour lesquelles il n'existe pas de correctif. Les logiciels malveillants inconnus contiennent du code malveillant qui exploite des vulnérabilités ou des faiblesses connues, mais qui ne peuvent être détectés au moment de leur découverte, même par des antivirus, des antibots et des systèmes de prévention d'intrusions à jour. La fenêtre d'efficacité d'un logiciel malveillant inconnu est souvent de 2 ou 3 jours seulement, car son existence donne aux éditeurs d'antivirus le temps de le détecter sur leurs réseaux mondiaux et de développer des signatures.

Cette distinction est cruciale, car elle nous permet de comprendre la vraie nature des logiciels malveillants qui ont pris le devant de la scène en 2013.

Rendre l'inconnu connu

En 2013, les moteurs d'émulation de Check Point, une forme avancée d'analyse automatisée de logiciels malveillants en bac à sable, déployés dans le monde entier, ont découvert que 2,2 logiciels malveillants inconnus frappaient les entreprises toutes les heures, soit un taux quotidien de 53.

Les chercheurs de Check Point ont déterminé que deux principaux facteurs étaient à l'origine de cette soudaine augmentation de la fréquence :

1. Les pirates employaient des mécanismes automatisés de création de logiciels malveillants inconnus furtifs à grande échelle, puis ciblaient les entreprises à travers le monde grâce à des campagnes coordonnées pour maximiser leur efficacité.

Fonctionnement des analyses en bac à sable

Fichier reçu sous forme de pièce jointe d'un email ou téléchargé

Les fichiers suspects sont envoyés à un bac à sable virtuel local ou hors site

Ouvrir et exécuter le fichier inconnu dans un système d'exploitation virtuel. Rechercher les actions malveillantes :
- Base de registre
- Système de fichier
- Services
- Connectivité réseau

S'il est sain, le transmettre à sa destination. S'il est malveillant, les actions possibles sont :
- Le transmettre à sa destination avec une alerte
- Le bloquer

Graphique 2-2

2. Les processus d'enquête et d'intervention manuels utilisés pour atténuer les attaques ciblées étaient incapables de faire face à ce nouveau volume élevé d'incidents.

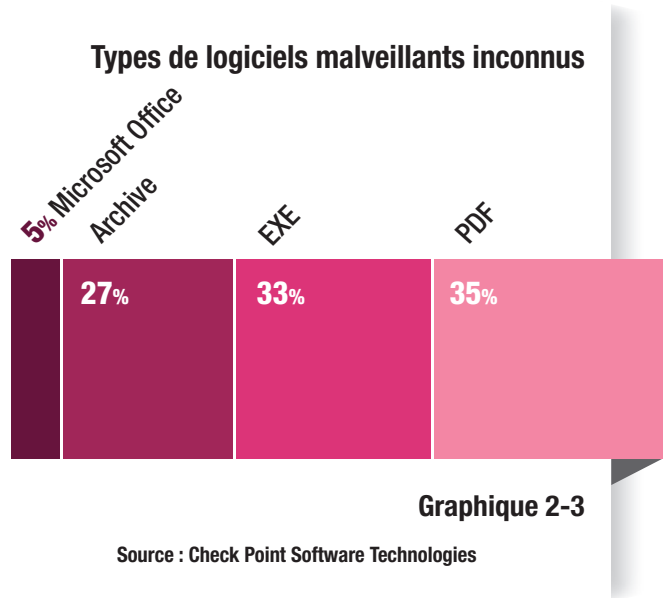
L'analyse des détections de 2013 a montré que la majorité des logiciels malveillants inconnus était diffusée à des clients ciblés par email, le plus souvent via des pièces jointes. En 2013, le format PDF était le plus populaire, représentant près de 35% des fichiers détectés par les mécanismes d'émulation des logiciels malveillants inconnus et conçus pour exploiter des versions non corrigées d'Adobe Reader. (Graphique 2-3) Nos recherches montrent que les formats EXE et archives sont également populaires, représentant 33% et 27% des fichiers malveillants analysés, respectivement.

Parmi les formats de fichiers Microsoft Office, le plus populaire était Word (.doc), bien que les analyses des données des bacs à sable ont montré que les agresseurs étendaient leurs attaques à d'autres formats également. En tout, nous avons détecté des programmes malveillants inconnus dans 15 types de fichiers Office différents, y compris les fichiers de modèles pour Word et PowerPoint, et différents formats Excel. Bien que la majorité des fichiers d'archives malveillantes étaient au format ZIP, sans doute parce que tous les systèmes Windows sont capables d'ouvrir des archives ZIP, les analyses Check Point ont néanmoins détecté des logiciels malveillants dans tous les autres types majeurs de fichiers archive, tels que TAR, RAR, 7z et CAB.

2,2 LOGICIELS MALVEILLANTS INCONNUS FRAPPENT LES ENTREPRISES TOUTES LES HEURES, SOIT UN TAUX **QUOTIDIEN DE 53**

Un flot de nouveaux logiciels malveillants

Les analyses de Check Point sur les données des logiciels malveillants en 2013 ont mis en évidence la fréquence à laquelle les programmes malveillants inconnus ont été détectés au niveau des passerelles réparties dans le monde entier. Des données provenant de sources externes ont confirmé ces résultats. AV-TEST,[21] un institut de recherche indépendant sur la sécurité informatique et les antivirus, enregistre plus de 220 000 nouveaux programmes malveillants chaque jour. AV-TEST a enregistré plus de 80 millions de nouveaux logiciels malveillants en 2013, soit plus du double de 2012.



Graphique 2-3

Source : Check Point Software Technologies

Nos recherches portant sur 2013 jettent beaucoup plus de lumière sur cette tendance et son impact généralisé. Sur l'ensemble de nos échantillons, un tiers des entreprises ont téléchargé au moins un fichier infecté par des logiciels malveillants inconnus.

LES CONTES DE CRYPTER

Afin de contourner les mécanismes de détection des solutions antimalwares, les auteurs de logiciels malveillants modernes utilisent des outils de masquage spécialisés appelés « crypters ». Pour vérifier que leurs variantes ne sont pas détectées, les auteurs de logiciels malveillants évitent les plates-formes d'analyse antivirus en ligne telles que VirusTotal et autres qui communiquent les échantillons avec les éditeurs de solutions antimalwares, et utilisent à la place des services privés tels que RazorScanner, Vscan (appelé également NoVirusThanks) et chk4me. Les crypters sont classés par les communautés de pirates comme étant UD (indétectable) ou FUD (totalement indétectable), en fonction de leur degré de réussite à échapper à la détection antivirus.

En 2013, Check Point Threat Emulation a détecté une variante de logiciel malveillant chiffrée jusqu'alors inconnue, conçue pour diffuser l'outil d'administration à distance DarkComet.[23] Dans le cas de notre échantillon détecté, une chaîne de caractères intégrée a révélé qu'il s'agissait d'un produit du crypter iJuan, qui est disponible en ligne à la fois sous forme de version gratuite (UD) et payante FUD).

Techniquement classifié comme étant un « packer » (empaqueteur) d'exécutables portable (PE),[24] à ne pas confondre avec les logiciels rançonneurs chiffreurs tels que CryptoLocker,[25] ces crypters déguisent des exécutables au moyen de différents systèmes de chiffrement et d'encodage, habilement combinés et recombinés, souvent plus d'une fois.

Cet échantillon détecté, qui a réussi à échapper à la plupart des solutions antivirus, a été comparé à une détection similaire dans un autre pays. Nous avons pu déterminer qu'il s'agissait d'une version masquée différemment du même outil DarkComet, communiquant avec le même serveur de commande et de contrôle. Réunis ensembles, ces facteurs indiquent que ces deux détections distinctes, l'une en Europe et l'autre en Amérique latine, font en fait partie de la même campagne.

Ces détections soulignent les rouages internes des familles d'attaques avancées qui transforment à la fois le paysage des menaces, et la gamme de solutions dont les responsables de la sécurité ont besoin pour défendre leur réseau et leurs données.

Cette explosion du nombre de logiciels malveillants inconnus est due en partie à l'accessibilité des techniques d'obscurcissement qui nécessitaient des compétences ou des outils spécialisés dans le passé, voire les deux (Encart : *Les contes de Crypter*).[22] Les cas que nous avons étudiés dans ce chapitre illustrent le haut degré de sophistication atteint par les logiciels malveillants actuellement diffusés, habituellement réservé à de simples variantes. Cette sophistication aggrave la problématique qu'ils représentent, car ils nécessitent le déploiement de capacités de détection et d'analyse intelligentes et plus subtiles à une échelle bien supérieure aux ressources de suivi, de réponse et de gestion des incidents présentes dans de nombreuses entreprises.

Recommandations

L'explosion en 2013 du nombre de logiciels malveillants inconnus signifie que les entreprises doivent reconsidérer les outils et les processus déployés principalement pour détecter et répondre à de faible volume d'attaques ciblées. Les mécanismes de détection qui nécessitent des interventions manuelles sans possibilité de blocage automatique laissent les équipes de sécurité démunies face à la vague de logiciels malveillants inconnus frappant leur réseau.

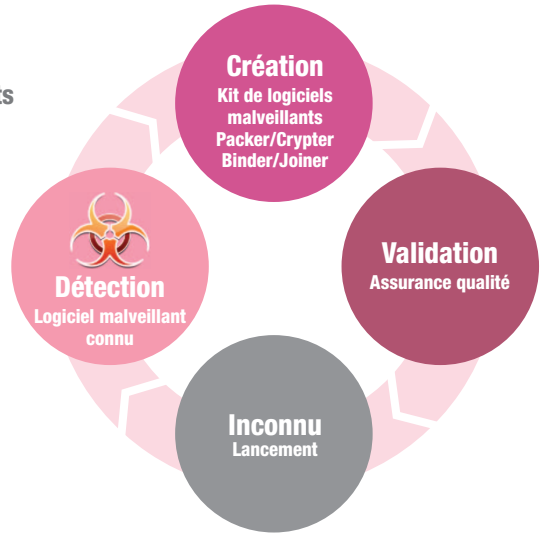
L'émulation, ou l'analyse automatisée des logiciels malveillants en bac à sable, est désormais une solution incontournable pour toute entreprise. Même les solutions antivirus, antibots et IPS les plus réactives doivent compter avec une fenêtre de 2 à 3 jours durant laquelle les logiciels malveillants inconnus ne sont pas détectés ; un laps de temps plus que suffisant pour permettre à des agresseurs de prendre pied dans une entreprise.

Cycle de vie d'un logiciel malveillant

Kit de logiciels malveillants
Spy Eye
Zeus Builder
Citadel Builder

Crypter/Packer
UPX GUI
PFE CX
Indectables.net

Joiner/Binder
File Joiner
ExeBundle



Assurance qualité
Analyse multimoteur
NoVirusThanks

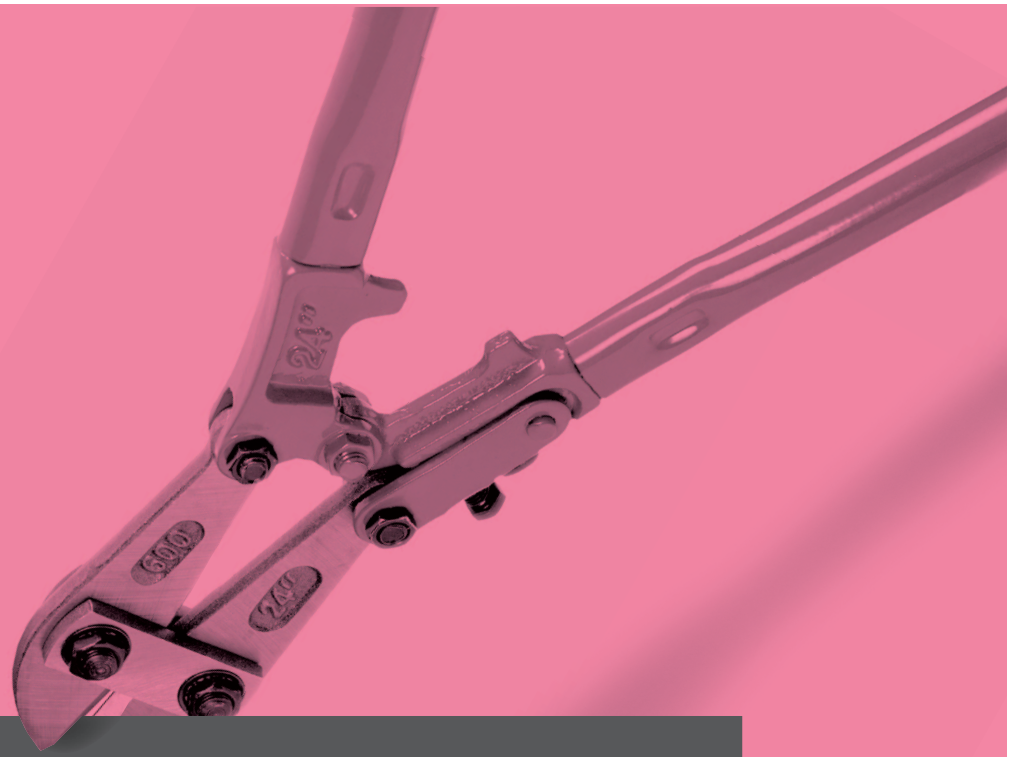
Ces solutions doivent toutefois faire partie intégrante de l'infrastructure de sécurité de l'entreprise plutôt que d'exister dans une couche distincte de l'infrastructure. Les entreprises devraient rechercher des solutions d'émulation capables de fournir :

- **Intégration** — L'intégration transparente avec les passerelles, les infrastructures de messagerie et les postes existants, est la seule méthode de déploiement évolutive qui n'augmente ni la complexité ni le coût. L'intégration avec la messagerie est particulièrement critique puisque le courrier électronique est le principal vecteur d'attaque contre les clients à la fois à l'intérieur et à l'extérieur du réseau.
- **Prévention** — Les approches employant la détection seule ne sont plus suffisantes pour les gros volumes de logiciels malveillants inconnus. Les entreprises doivent rechercher des solutions axées sur la prévention qui permettent de détecter et de bloquer automatiquement les logiciels malveillants inconnus avant qu'ils n'atteignent leur destination.

L'ÉMULATION, OU L'ANALYSE AUTOMATIQUE AVANCÉE DE LOGICIELS MALVEILLANTS EN BAC À SABLE, EST DÉSORMAIS UNE **SOLUTION INCONTOURNABLE** POUR TOUTE ENTREPRISE

- **Automatisation** — L'élimination des processus manuels pour l'analyse et les interventions permet aux entreprises de faire face à ces attaques, et répond à d'autres objectifs de sécurité et métiers. La prévention automatique est déterminante, tout comme le sont le reporting et l'intégration des flux de travail pour des notifications et des interventions efficaces.

La hausse rapide du nombre de logiciels malveillants inconnus change clairement la donne en matière de sécurité, appelant à de nouvelles stratégies et technologies ainsi qu'à une approche de la sécurité capable de fournir une protection efficace sans surcharger les ressources de l'entreprise. L'adaptation à ces nouvelles exigences devrait être une priorité urgente pour toutes les entreprises. En parallèle, les types d'attaques les plus courants et établis de longue date continuent de poser de sérieuses menaces, et nécessitent une vigilance continue et des contre-mesures proactives. Les toutes dernières tendances sur les logiciels malveillants connus sont décrites dans le chapitre suivant.



03

UN DANGER BIEN CONNU

Les logiciels malveillants dans l'entreprise

03

UN DANGER BIEN CONNU : LES LOGICIELS MALVEILLANTS DANS L'ENTREPRISE

La sécurité de l'information a dominé l'actualité en 2013, avec des révélations sur les programmes de cybersurveillance financés par l'État et le piratage d'entreprises de médias telles que le *Washington Post* et Yahoo, des épidémies malveillantes telles que CryptoLocker et des fuites de données client à une échelle éclipsant tout ce qui a pu être signalé précédemment.

> NOUS NOUS INQUIÉTONS DES ARMES DE DESTRUCTION MASSIVE DEPUIS DES DÉCENNIES. IL EST MAINTENANT TEMPS DE NOUS INQUIÉTER DE CE NOUVEAU TYPE D'ARMES DE PERTURBATION MASSIVE.
>
> **John Mariotti[26]**

L'année écoulée fait que 2012 semble calme en comparaison, sauf que 2012 n'était absolument pas une année calme du point de vue des cyberattaques. Cette année-là s'est distinguée par la quantité et l'ampleur de ses cyberattaques, y compris la flambée de l'hacktivisme, du piratage parrainé par l'État sur les médias et les entreprises, et des fuites de données d'institutions financières à travers le monde. Les principales tendances de 2012 en matière de logiciels malveillants relevées dans le *Rapport Sécurité 2013*[27] de Check Point étaient :

- La démocratisation des menaces persistantes avancées
- L'omniprésence des botnets
- L'augmentation du nombre de vulnérabilités étendant la surface d'attaque

Durant nos études, nous avons constaté que ces tendances ont non seulement continué en 2013, mais ont accéléré dans presque tous les domaines, que ce soit la fréquence à laquelle les logiciels malveillants entrent dans les entreprises, ou l'étendue et la gravité des infections de bots.

84%

DES ENTREPRISES ONT TÉLÉCHARGÉ DES LOGICIELS MALVEILLANTS

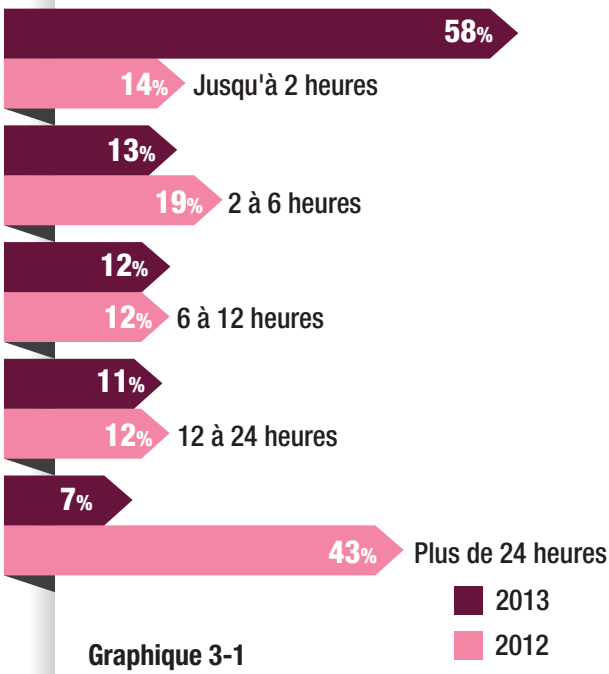
Plus rapide ne signifie pas toujours mieux

S'il existe une statistique unique en 2013 qui illustre le mieux les défis que rencontrent aujourd'hui les administrateurs de sécurité, c'est bien la fréquence croissante avec laquelle les logiciels malveillants ont été téléchargés par les entreprises que nous avons étudiées (Graphique 3-1). En 2012, près de la moitié (43%) des entreprises que nous avons analysées ont téléchargé des logiciels malveillants à un taux de moins de un par jour, tandis que les autres entreprises (57%) ont téléchargé des logiciels malveillants toutes les 2 à 24 heures.

En 2013, en revanche, près des deux tiers (58%) des entreprises ont téléchargé des logiciels malveillants toutes les deux heures ou moins. Cette accélération du rythme des cyberattaques sur les entreprises se reflète dans toutes les statistiques de notre dernière étude sur la sécurité. Dans ce chapitre, nous examinons les détails de ce changement et ses implications pour la sécurité et les responsables, avec un premier regard sur les vulnérabilités qui créent de la surface d'attaque pour les auteurs de logiciels malveillants et les pirates.

58% DES ENTREPRISES ONT TÉLÉCHARGÉ DES LOGICIELS MALVEILLANTS **TOUTES LES DEUX HEURES OU MOINS**

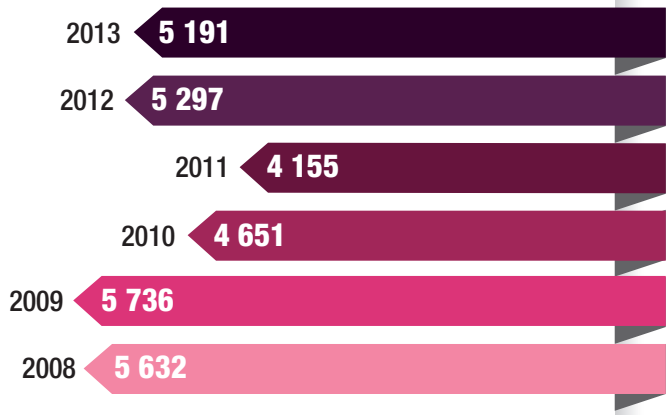
Fréquence de téléchargement des logiciels malveillants (% des entreprises)



Graphique 3-1

Source : Check Point Software Technologies

Nombre total de vulnérabilités courantes



Graphique 3-2

(Source : Base de données CVE (vulnérabilités courantes

Moins de vulnérabilités, ou un faux espoir ?

Le seul facteur de risque du paysage de la sécurité de l'information qui n'a pas augmenté en 2013 est le nombre de vulnérabilités signalées. À première vue, cela semble être un certain soulagement après les indications de 2012 qui suggéraient que la tendance à la baisse du nombre de vulnérabilités signalées était renversée, vu que leur nombre avait bondi de 27% par rapport à 2011 pour atteindre 5 297 (Graphique 3-2). En effet, 2012 a vu un paysage de vulnérabilités élargir les opportunités pour les agresseurs, et augmenter également la zone que les administrateurs, déjà aux prises avec l'entrée des appareils mobiles et des services grand public dans les réseaux d'entreprise, devaient défendre.

TOUTES LES 60 SECONDES DES HÔTES ACCÈDENT À DES SITES WEB MALVEILLANTS

Pourquoi alors 2013 ne représente pas vraiment une tendance positive ? À certains égards, oui. La protection des vulnérabilités implique généralement deux approches principales :

- L'application des correctifs émis par les éditeurs pour corriger les vulnérabilités. Pour les systèmes clients, c'est maintenant généralement fait automatiquement, sans requérir de test. Pour les serveurs, des tests supplémentaires sont souvent nécessaires afin de vérifier que les correctifs n'entraînent pas d'effets indésirables.
- Le déploiement de systèmes de prévention d'intrusions (IPS) pour détecter et, le cas échéant, bloquer les tentatives d'exploitation des vulnérabilités connues. Cela se fait parfois comme mesure provisoire jusqu'à ce qu'une mise à jour puisse être appliquée dans le cadre du cycle de correction normal. Dans d'autres cas, l'IPS est le

ZERO-DAY, GROS SOUS

Malgré l'augmentation des primes proposées aux chercheurs par les éditeurs pour découvrir des vulnérabilités, la valeur élevée des véritables vulnérabilités zero-day sur le marché conduit les chercheurs à les vendre à des organismes gouvernementaux[28] qui travaillent avec des pirates pour étendre leurs cyberdéfenses, et des entreprises de tests de pénétration. Un marché noir des logiciels malveillants souterrain encore plus lucratif attire les pirates. Les prix des vulnérabilités non déclarées y varient selon la plate-forme cible, allant de 5 000 dollars pour Adobe Reader jusqu'à 250 000 dollars pour Apple iOS. La disponibilité des exploitations de vulnérabilités zero-day place les cyberattaques avancées à la portée de toute organisation, indépendamment de ses compétences techniques.

PLATE-FORME CIBLÉE	PRIX
Adobe Reader	De 5 000 à 30 000 dollars
Mac OS X	De 20 000 à 50 000 dollars
Android	De 30 000 à 60 000 dollars
Plug-ins Flash ou Java pour navigateurs	De 40 000 à 100 000 dollars
Microsoft Word	De 50 000 à 100 000 dollars
Microsoft Windows	De 60 000 à 120 000 dollars
Navigateurs Firefox et Safari	De 60 000 à 150 000 dollars
Navigateurs Chrome et Internet Explorer	De 80 000 à 200 000 dollars
Apple iOS	De 100 000 à 250 000 dollars

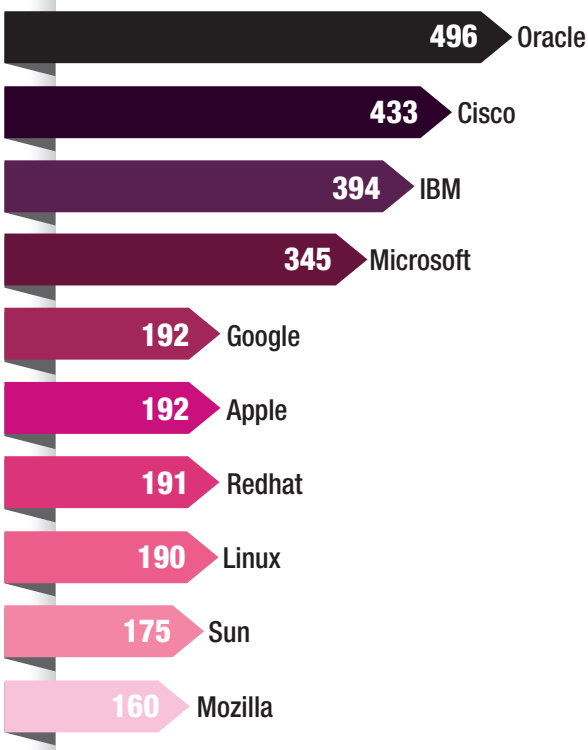
Source : Forbes

TOUTES LES 10 MINUTES, UN HÔTE TÉLÉCHARGE DES LOGICIELS MALVEILLANTS

principal moyen de défense à long terme pour les systèmes qui ne peuvent être corrigés pour une variété de raisons.

Le nombre de vulnérabilités nouvellement signalées a tendance à avoir une corrélation positive directe sur la charge de travail des services de sécurité et des services informatiques. Dans cette optique, 2013 semble bien avoir apporté de bonnes nouvelles aux responsables de la sécurité surmenés. La base de données CVE a confirmé une diminution du nombre de vulnérabilités signalées pour l'année, à 5 191, soit une baisse modeste de 2% par rapport à 2012, avec une baisse de 9% du nombre de vulnérabilités « critiques » signalées.

Principales vulnérabilités en 2013 par éditeur
(nombre de vulnérabilités)



Graphique 3-3

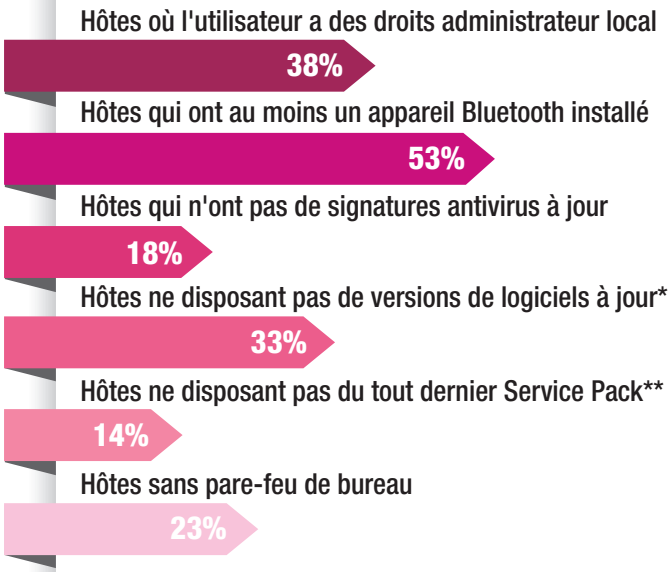
(Source : Base de données CVE (vulnérabilités courantes

Mais tout n'est pas aussi clair que cela puisse paraître. Même si moins de vulnérabilités ont été signalées, les experts s'entendent pour dire qu'un nombre croissant de vulnérabilités critiques est siphonné par les marchés gris et noir ; une tendance potentiellement plus désastreuse (Encart : *Zero-day, gros sous*).

Quand bien même de nouvelles vulnérabilités « disparaissent » pour tomber potentiellement dans les mains des auteurs de logiciels malveillants, la répartition des vulnérabilités signalées souligne une autre problématique pour les responsables informatiques (Graphique 3-3). Oracle est resté la plate-forme la plus vulnérable en 2013, avec de nombreuses vulnérabilités signalées dans les produits Java qui sont largement utilisés dans les serveurs et les applications clientes, présentant ainsi de grandes opportunités pour les agresseurs. Microsoft a été rétrogradé en quatrième position, et plus de vulnérabilités ont été signalées dans les produits Cisco et IBM, y compris les serveurs et les composants d'infrastructure réseau à grande échelle qui ne sont pas toujours couverts par des politiques de protection IPS.

La plupart des entreprises ont des processus bien définis pour le déploiement des correctifs de Microsoft. Il n'en est pas de même pour les applications clientes

Vulnérabilités et erreurs de configuration des postes en entreprise
(% des hôtes)



* Les logiciels suivants ont été analysés : Acrobat Reader, Flash Player, Java, Internet Explorer

** Les plates-formes Microsoft Windows analysées : Windows XP, Windows 2003, Vista, 2008, 2008 R2, Windows 7

Graphique 3-4

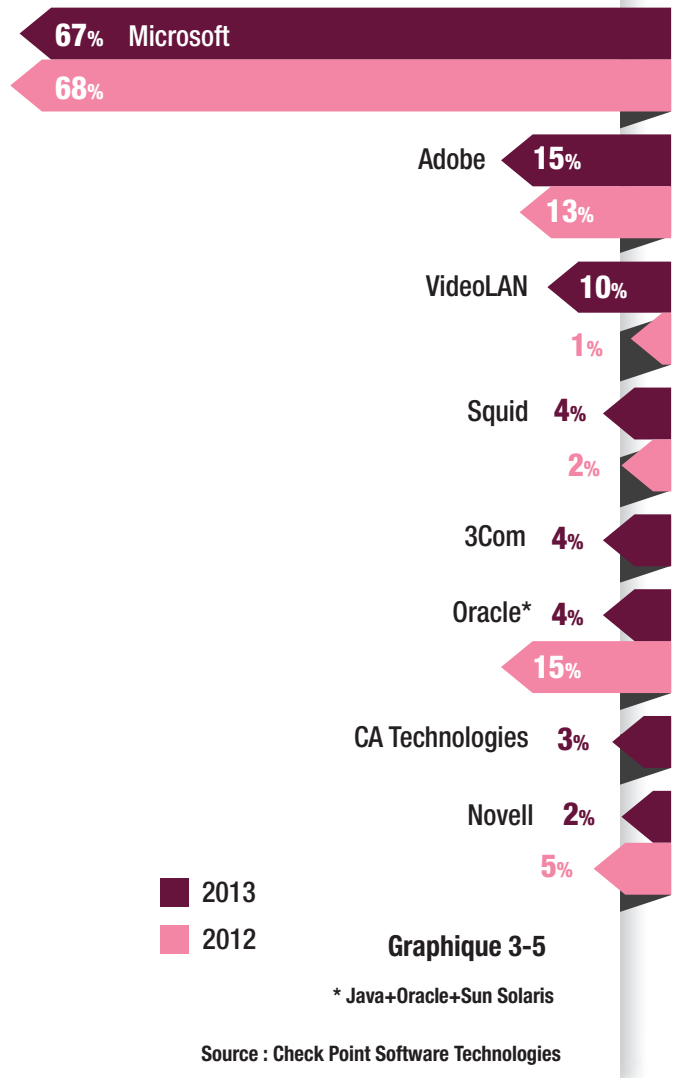
Source : Check Point Software Technologies

telles que Java et Adobe Reader. Cet écart les expose à des attaques d'hameçonnage via navigateur (emails de phishing ciblés) et des attaques de type « watering hole » (point d'eau), par lesquelles un agresseur compromet un site web populaire et y incorpore des logiciels malveillants capables d'infecter un client vulnérable qui le consulte.

Postes : aucun correctif, aucune restriction et aucune préparation

Les statistiques Endpoint Security de notre étude 2013 confirment que la gestion des correctifs reste un défi majeur, en particulier pour les systèmes clients (Graphique 3-4). Malgré l'adoption généralisée de processus réguliers d'application de correctifs Microsoft, 14% des postes analysés ne disposent pas des tous derniers Service Packs Microsoft Windows, qui intègrent tous les correctifs et mises à jour précédentes. Plus important encore, 33% des postes en entreprise ne disposent pas des toutes dernières versions des logiciels clients tels qu'Adobe Reader, Adobe Flash Player, Java et Internet Explorer, laissant ces clients vulnérables à de nombreuses attaques.

Incidents de sécurité par éditeur
(% des entreprises)



Graphique 3-5

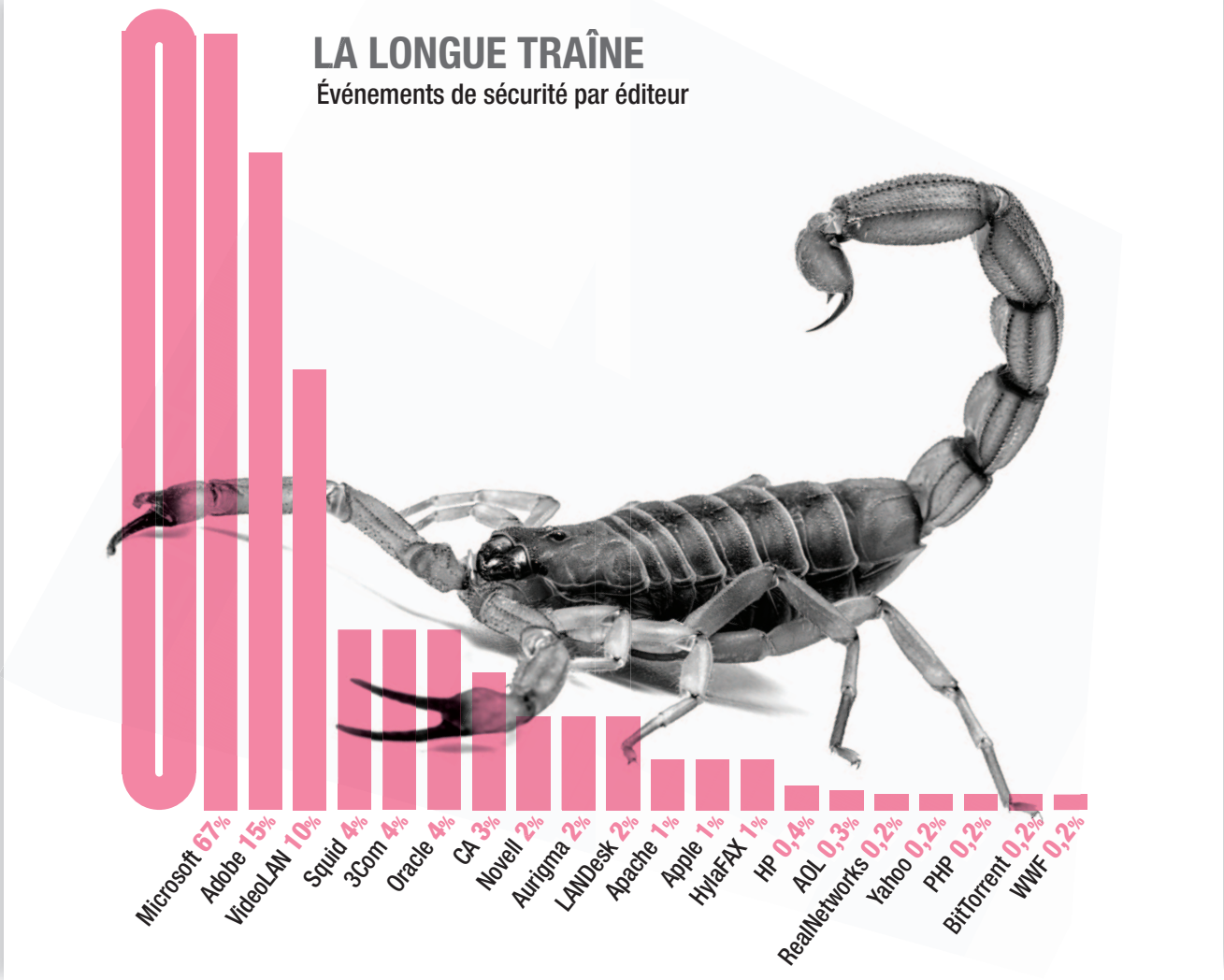
* Java+Oracle+Sun Solaris

Source : Check Point Software Technologies

La vulnérabilité de ces systèmes est aggravée par le fait que près d'un cinquième (18%) des postes étudiés ne disposent pas des toutes dernières signatures pour leur solution antivirus. Les conséquences de ces défaillances peuvent être considérables. Un agresseur qui a réussi à établir une tête de pont dans un client vulnérable peut ainsi disposer d'une plate-forme solide pour explorer le reste du réseau de l'entreprise ciblée. Parmi les postes analysés en entreprise, 38% d'entre eux sont configurés avec des privilèges d'administrateur local, permettant l'exécution de logiciels malveillants dans le contexte du système (root), plutôt que de limiter l'exécution au contexte de l'utilisateur.

Loin d'offrir de l'espoir aux responsables informatiques, l'environnement de 2013 s'avère avoir été très favorable aux agresseurs :

- Plus de vulnérabilités sur le marché noir, où elles restent non signalées et non corrigées.
- Clients non protégés.
- Report du nombre de vulnérabilités sur des applications et plates-formes qui sont moins régulièrement corrigées.



Graphique 3-6 **Source : Check Point Software Technologies**

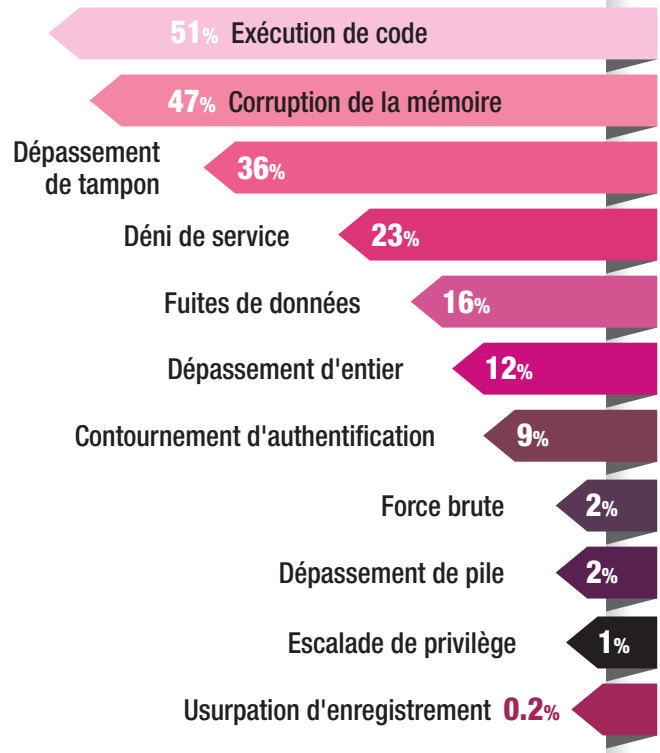
33%

DES HÔTES N'ONT PAS DE LOGICIELS À JOUR

Les pirates voient au-delà de Windows

Les données relatives aux attaques dans notre étude de 2013 montrent comment les agresseurs s'adaptent à ces opportunités dans les réseaux ciblés des entreprises (Graphique 3-5). Même si Microsoft reste la plate-forme la plus attaquée en 2013, visée par au moins une attaque dans 67% des entreprises analysées, cela représente une légère diminution par rapport à 2012. L'augmentation des attaques contre Adobe (Reader et Flash Player) et VideoLAN (le lecteur de médias VLC) reflète le ciblage accru des applications utilisateur, tandis que l'attention portée aux plates-formes et aux dispositifs d'infrastructure est évidente comme le montre l'augmentation du nombre d'attaques sur les systèmes de Squid (proxy et cache web), 3Com (commutation et routage) et CA (analyse et identité). En fait, la répartition des attaques sur différentes plates-formes reflète l'effet de « longue traîne » décrit par l'auteur Chris Anderson[29]

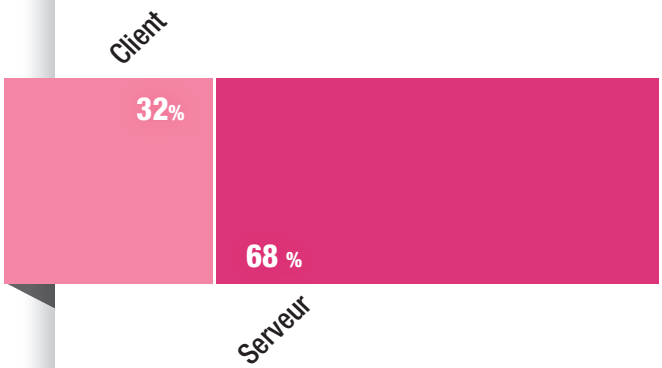
Principaux vecteurs d'attaque
(% des entreprises)



Graphique 3-8

Source : Check Point Software Technologies

Incidents de sécurité par plate-forme
2013 % du total



Graphique 3-7

Source : Check Point Software Technologies

en 2006 (Graphique 3-6). La suite de plates-formes ciblées est un ensemble de « marchés de niche à l'infini » qui atteste du modèle économique et des motivations économiques des cyberattaques modernes.

Les serveurs sont là où se trouve l'argent

L'étude de Check Point a constaté en 2013 que les serveurs restent la cible principale des attaques détectées par les systèmes de prévention d'intrusions, soit près du double (Graphique 3-7). Compte tenu de la faiblesse des systèmes clients décrits plus haut, on peut se demander : Pourquoi attaquer des serveurs s'ils sont susceptibles d'être plus corrigés et bien gardés ? Pour la même raison que Willie Sutton s'attaquait en son temps à des banques, car selon lui : « c'est là ou se trouve l'argent. »[30] Les serveurs d'application sont exposés au réseau et parfois même à Internet dans une zone démilitarisée, et les attaques automatisées sont bien adaptées aux serveurs car ils peuvent exploiter les vulnérabilités des services ou des applications sans nécessiter d'interaction avec les utilisateurs finaux. Les serveurs peuvent être analysés depuis l'extérieur du réseau ou d'un client interne compromis, puis ciblés par des attaques spécifiques à la version des applications ou de leur système d'exploitation. Les nombreuses attaques fournissent un contrôle à distance du système aux agresseurs en cas de réussite.

Les principaux vecteurs d'attaque observés dans notre étude de 2013 (Graphique 3-8) penchent fortement pour l'exécution de code à distance (RCE),[31] les trois premiers étant l'exécution de code, la corruption de la mémoire et les dépassements de tampon. Même les attaques de déni de service (DoS) peuvent soutenir les attaques menées contre des serveurs en servant d'écran de fumée pour détourner l'attention. Lorsque la fumée se dissipe, l'attaque est terminée et le serveur ciblé est compromis.

LA BLAGUE DU JOUR : LES UTILISATEURS RESTENT UN MAILLON FAIBLE

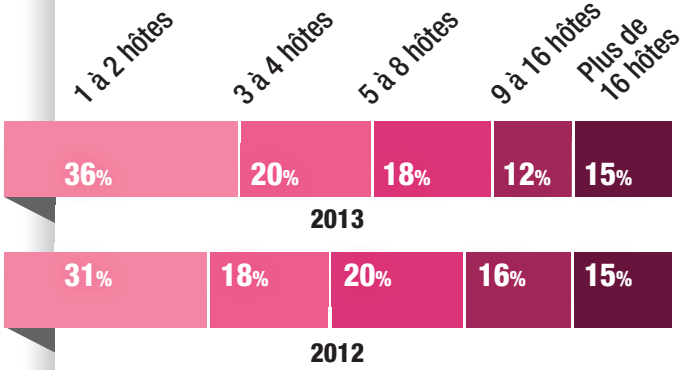
La messagerie reste le vecteur de propagation privilégié des logiciels malveillants. Un exemple de 2013 montre que même aujourd'hui, les utilisateurs restent imprudents face à de simples attaques, ce qui donne ainsi aux logiciels malveillants un mécanisme de diffusion dans de nombreuses entreprises.

En octobre 2013, un utilisateur travaillant chez un grand fabricant en France a reçu un email avec « Blagounette du jour »[33] pour ligne d'objet. Un fichier Microsoft Excel de 6 Mo était joint à l'email.

L'analyse automatique de documents suspects dans un bac à sable virtuel a révélé que le fichier Excel contenait une image et qu'il la plaçait dans le système de fichiers de l'ordinateur, puis modifiait la base de registre pour mettre la nouvelle image en fond d'écran. En raison du caractère humoriste de l'image, l'utilisateur était susceptible de partager cette « blague » sans méfiance, en transmettant l'email à ses amis et collègues. Une analyse plus poussée a révélé que c'est exactement ce qui s'est produit. Le document a été transmis à au moins trois grandes entreprises françaises supplémentaires.

Heureusement pour ces entreprises, ce document n'intégrait pas de code malveillant et n'avait pas été conçu pour causer des dommages aux ordinateurs des utilisateurs qui l'ouvraient. Toutefois, tous les ingrédients d'une campagne de logiciels malveillants ciblée sont présents. Les utilisateurs qui ont ouvert ce document ont exposé leur ordinateur et leur entreprise à un risque important, aggravé par ceux qui l'ont transmis à des collègues et des amis travaillant dans d'autres entreprises, qui sont devenus un vecteur supplémentaire de propagation d'une blague du jour qui n'avait vraiment rien de drôle.

Accès à des sites malveillants par nombre d'hôtes
(% des entreprises)



Graphique 3-9

Source : Check Point Software Technologies

Clients : aucun correctif, aucune restriction et aucune préparation

Les clients sont également de bonnes cibles, en particulier pour les attaques réseau qui tentent de se propager à travers un réseau interne ou dans un réseau public non protégé. En plus des correctifs et Service Packs manquants qui corrigent les services connus et facilement ciblés tels que RPC,[32] les clients sont souvent vulnérables en raison de la désactivation d'importantes protections. Par exemple, près d'un quart (23%) des postes en entreprise analysés par Check Point ne disposent pas d'un pare-feu de bureau activé, et plus de la moitié (53%) ont Bluetooth activé, ce qui les expose à des attaques via réseau sans fil dans les espaces publics.

Les systèmes clients offrent également de nombreuses autres vulnérabilités, notamment par l'exploitation du comportement des utilisateurs avec la messagerie et la navigation web. Dans ces domaines, les données de notre étude de 2013 reflètent à la fois l'accélération de l'activité des logiciels malveillants et le passage à la personnalisation de masse.

En 2013, le nombre d'hôtes accédant à des sites malveillants a continué d'augmenter. Notre étude montre qu'en moyenne, un hôte accède à un site web malveillant toutes les 60 secondes. À l'exception de la fourchette de « 1 à 2 hôtes », le Graphique 3-9 montre que la répartition du nombre d'hôtes accédant à des sites malveillants est restée relativement stable par rapport à 2012. Ces bonnes nouvelles apparentes démentent un problème plus profond, car c'est un effet des campagnes d'hameçonnage ciblant un nombre limité d'utilisateurs au sein d'une entreprise et de profilage social pour créer un email qui est plus susceptible d'être ouvert par les destinataires. Plutôt que de submerger toute l'entreprise d'emails de phishing facilement détectables, ces attaques ciblent un ou deux utilisateurs. Cette approche plus efficace a permis une augmentation de 20% du nombre d'hôtes accédant à des sites malveillants par rapport à 2012.

49% DES ENTREPRISES ONT
7 HÔTES OU PLUS INFECTÉS PAR DES BOTS

DANS 73%

DES ENTREPRISES, AU MOINS UN BOT A ÉTÉ DÉTECTÉ, CONTRE 63% EN 2012

BLOCAGE DE CRYPTOLOCKER

CryptoLocker est une souche de logiciel malveillant appelé « rançonneur » qui a été identifié pour la première fois début septembre 2013. Comme d'autres formes de rançonneurs, CryptoLocker s'installe sur l'ordinateur d'une victime et chiffre ses différents fichiers de données en tâche de fond, à l'insu de l'utilisateur.

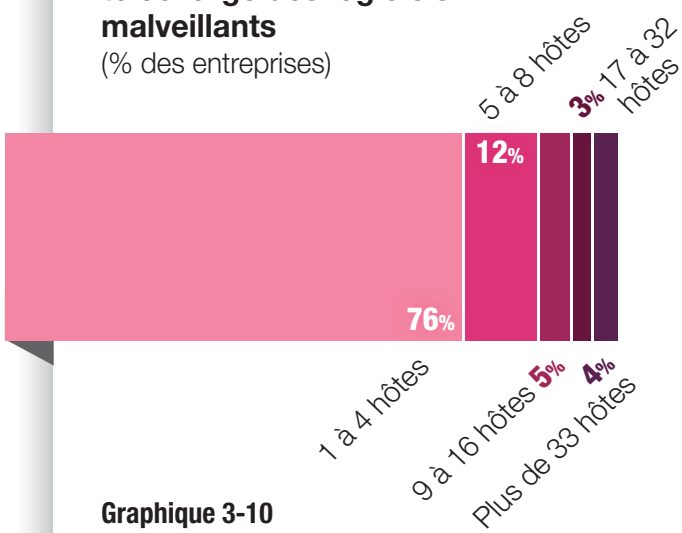
Lorsque la phase de chiffrement est terminée, CryptoLocker affiche un message informant l'utilisateur que ses fichiers ont été « pris en otage » et exige le paiement d'une rançon aux criminels pour déchiffrer les fichiers. Le message indique que si l'utilisateur ne se conforme pas à cette demande dans un certain délai (souvent moins de quatre jours), la clé privée nécessaire au déchiffrement sera supprimée du serveur des criminels, ce qui rend les données de la victime définitivement irrécupérables.

Il n'existe actuellement aucune méthode connue pour rétablir l'accès aux fichiers chiffrés.

Un trait important de CryptoLocker est que l'agent logiciel malveillant a besoin de trouver et d'établir une communication avec un serveur de commande et de contrôle avant de pouvoir commencer le processus de chiffrement des fichiers. Le moyen le plus efficace de vaincre CryptoLocker est donc de détecter et de bloquer la première tentative de communication de l'agent, avant qu'il puisse se connecter au serveur de commande et de contrôle et commencer le processus de chiffrement.

CryptoLocker a montré que la détection des bots, souvent considérée une mesure réactive, peut également jouer un rôle proactif dans une défense préventive de pointe. Durant l'épidémie CryptoLocker de fin 2013, les entreprises qui employaient des solutions antibots intelligentes étaient en mesure d'atténuer les dommages causés par les infections de CryptoLocker dans leur réseau, en identifiant non seulement les clients infectés mais en bloquant également la communication initiale critique avec le serveur de commande et de contrôle.

Nombre d'hôtes qui ont téléchargé des logiciels malveillants
(% des entreprises)



Graphique 3-10

Source : Check Point Software Technologies

Cette tendance explique également la hausse en 2013 du nombre d'hôtes téléchargeant des logiciels malveillants. De 1 à 4 hôtes dans 76% des entreprises analysées ont téléchargé des logiciels malveillants, soit une augmentation de 69% par rapport à 2012, tandis que les fréquences sont restées stables ou ont diminué dans toutes les autres fourchettes (Graphique 3-10).

Un petit nombre d'hôtes accédant à des sites malveillants et téléchargeant des logiciels malveillants dans un plus grand nombre d'entreprises a contribué à l'accélération globale de l'activité des logiciels malveillants en 2013. En moyenne, un hôte accède à un site web malveillant toutes les minutes, et un logiciel malveillant est téléchargé toutes les dix minutes.

EN MOYENNE, UN HÔTE ACCÈDE À UN SITE WEB MALVEILLANT **TOUTES LES MINUTES**, ET UN LOGICIEL MALVEILLANT EST TÉLÉCHARGÉ **TOUTES LES DIX MINUTES**

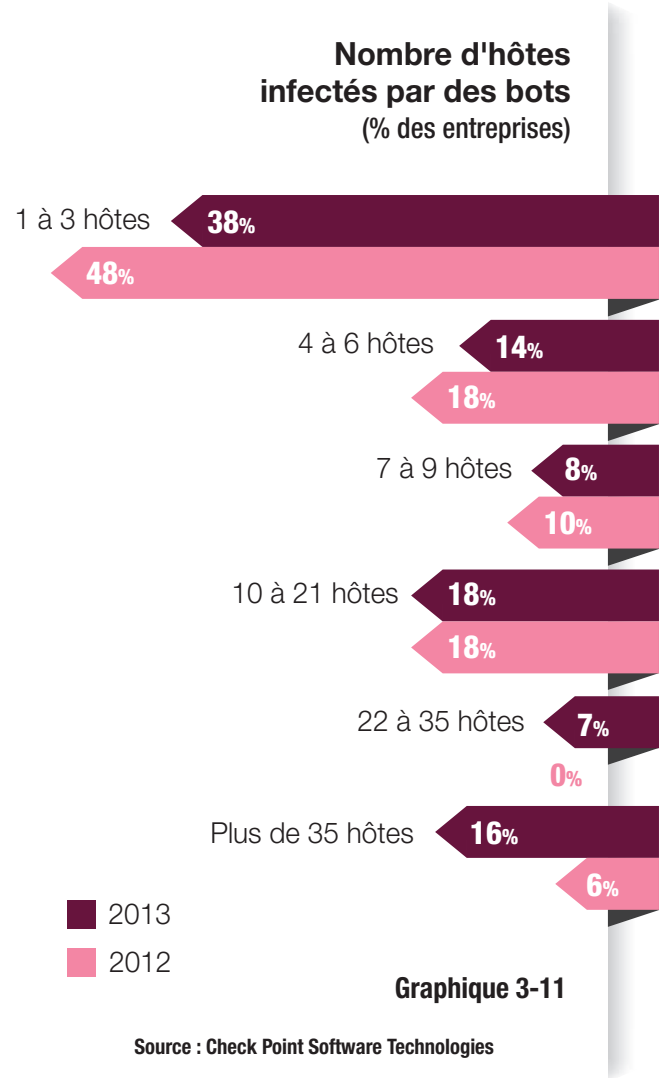
Les bots étendent leur portée

Comme on pouvait s'y attendre de cette augmentation des activités d'infiltration, les chercheurs de Check Point ont trouvé une augmentation correspondante des infections et de l'activité des bots en 2013. Si pour les infiltrations, le thème était une baisse du volume des attaques plus ciblées, pour les bots, l'inverse est vrai : volume élevé et haute fréquence. En 2013, le nombre d'entreprises comprenant 22 ou plusieurs hôtes infectés par des bots a augmenté de près de 400% (Graphique 3-11), tandis que les plus petites infestations de bots ont diminué.

Cela ne devrait pas être interprété comme signifiant que l'ensemble des infections de bots a diminué, puisque plus d'un tiers (38%) des entreprises avait encore au moins 1 à 3 hôtes infectés par des bots.

Les enjeux des infections de bots sont sans doute également en train d'augmenter avec l'avènement d'une nouvelle génération de logiciels rançonneurs, illustré par l'épidémie de CryptoLocker fin 2013 (Encart : *Blocage de CryptoLocker*).

Non seulement les entreprises sont aux prises avec des infestations plus étendues de bots dans leur environnement, mais les bots sont également plus actifs. La fréquence des communications des bots avec les serveurs de commande et de contrôle a augmenté de façon spectaculaire en 2013, avec 47% des entreprises détectant des tentatives de communication avec des serveurs de commande et de contrôle à un taux de plus d'une par heure, soit une augmentation de 88% par rapport à 2012 (Graphique 3-12). Remis à l'échelle de l'échantillon entier de notre étude, un bot tente de communiquer avec son serveur de commande et de contrôle toutes les trois minutes. Chacune de ces tentatives de communication est l'occasion pour le bot de recevoir des instructions et potentiellement exfiltrer des données confidentielles hors de l'entreprise ciblée. Cette accélération de la fréquence des communications avec les serveurs de commande et de contrôle représente une grave menace pour les entreprises qui luttent pour protéger leurs données et leurs systèmes.



Graphique 3-11

Source : Check Point Software Technologies

77%

DES BOTS SONT ACTIFS PENDANT PLUS DE 4 SEMAINES

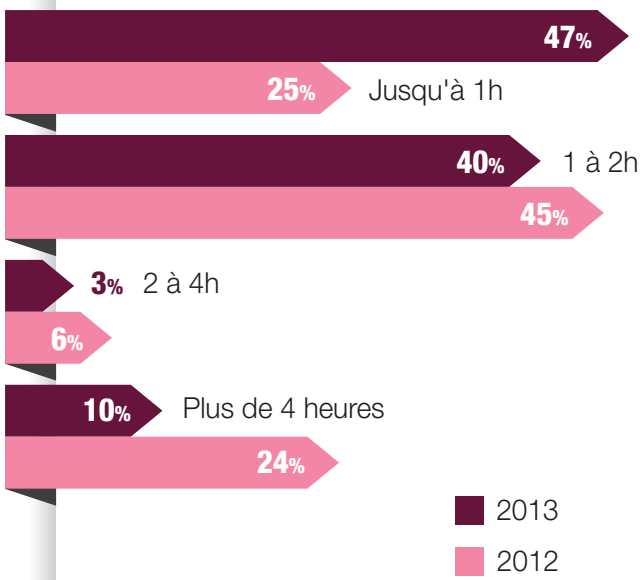
77% plus de 4 semaines

moins de 4 semaines **23%**

Source : Check Point Software Technologies

Fréquence des communications des bots avec leur serveur de commande et de contrôle

(% des entreprises)



Graphique 3-12

Source : Check Point Software Technologies

Les défenses antibots deviennent plus vitales et plus problématiques

L'augmentation de la fréquence permet également aux responsables de la sécurité de détecter, bloquer et stopper les infections de bots dans leur réseau. La détection des communications des bots est souvent la tâche la plus facile, tandis que l'éradication des bots sans réinstaller le système infecté peut présenter un plus grand défi. Le blocage efficace des communications des bots devient la partie la plus difficile de la guerre antibots en raison des nouveaux canaux plus sophistiqués de commande et de contrôle utilisés par les réseaux de zombies pour échapper au filtrage et aux outils de blocage traditionnels (Encart : *Ce n'est pas la partie de pêche de votre père*).[34]

UN BOT ESSAIE DE COMMUNIQUER AVEC SON SERVEUR DE COMMANDE ET DE CONTRÔLE

TOUTES LES TROIS MINUTES

CE N'EST PAS LA PARTIE DE PÊCHE DE VOTRE PÈRE

En 2013, les campagnes de phishing analysées par les chercheurs de Check Point ont mis en évidence des techniques de plus en plus sophistiqués employées aujourd'hui par les attaques de phishing pour échapper aux listes noires qui sont au cœur de la plupart des défenses traditionnelles, y compris l'utilisation d'une certaine forme de schéma d'URL dynamique pour échapper à toute détection par les listes noires statiques. Dans le cas de la campagne de phishing du kit d'exploitations Nuclear, ce système résiste également aux analyses effectuées par les chercheurs.

L'analyse de CryptoLocker menée par nos chercheurs a révélé un autre aspect de cette tendance : en tant que botnet reposant sur un algorithme de génération de noms de domaine (DGA),[35] CryptoLocker emploie des noms de domaine dynamiques, apparemment générés aléatoirement pour établir des communications entre le bot et le serveur de commande et de contrôle. Les bots CryptoLocker génèrent 1 000 nouveaux domaines tous les jours, tandis que les exploitants de CryptoLocker enregistrent les mêmes 1 000 nouveaux domaines puis s'en débarrassent au bout de 24 heures. En conséquence, les domaines malveillants ont peu de chance d'être détectés et enregistrés par les ressources chargées de créer et maintenir les listes noires d'URL et de domaines malveillants connus.

Vues dans leur ensemble, ces récentes campagnes de logiciels malveillants mettent en évidence le rôle important des URL et des noms de domaine dynamiques dans ces attaques, en particulier pour éluder les listes noires statiques traditionnellement utilisées pour détecter et bloquer les bots et les tentatives de phishing. Les URL dynamiques et l'algorithme DGA tirent parti de l'infrastructure même d'Internet pour générer des variantes obscures ou à usage unique, capables de confondre les systèmes de défense reposant sur l'analyse et le blocage du trafic de et vers des adresses qui ont été précédemment détectées et classées comme étant malveillantes.

Ces observations reflètent une tendance beaucoup plus importante dans l'industrie du logiciel malveillant. Les pirates exploitent les faiblesses du système de nom de domaine et des méthodes traditionnelles de mise en liste noire des URL pour contourner les défenses existantes et atteindre leurs objectifs. Dans les conclusions de son étude pour le deuxième trimestre 2013, le Groupe de travail antiphishing (APWG)[36] a constaté que même si les noms de domaine de premier niveau (TLD)[37] .com restent les plus couramment utilisés dans les campagnes de phishing (44% au total contre 42% au 1er trimestre), les TLD de certains pays sont plus fréquemment utilisés dans les attaques de phishing qu'il n'y a de domaines réellement enregistrés. Le Brésil (.br) par exemple a seulement 1% de domaines enregistrés mais représente 4% des TLD dans les emails de phishing. Les auteurs de tentatives de phishing et de logiciels malveillants exploitent la quantité de TLD possibles des pays pour générer un nombre immense de noms de domaine et d'URL uniques, et les contrôles que beaucoup supposent en place pour empêcher ce genre d'abus ne fonctionnent pas. Le rapport de l'APWG, « Enquête mondiale sur le phishing, 1ère moitié de 2013 : Tendances et utilisation des noms de domaine »,[38] étudie le rôle des noms de domaine dans les attaques de phishing et constate que les bureaux d'enregistrement de noms de domaine ne s'aperçoivent soit de rien soit sont les complices des agresseurs.

Ce problème ne fera que s'aggraver. En 2013, l'ICANN (la société pour l'attribution des noms de domaine et des numéros sur Internet)[39] a annoncé un projet d'augmentation du nombre de domaines de premier niveau de 22 à 1 400, avec notamment des TLD en caractères non latins comme l'arabe, le chinois et le cyrillique. Alors que l'APWG note que des TLD en caractères non latins sont disponibles depuis des années et ne sont pas particulièrement utilisés par les agresseurs, il y a tout lieu de croire que ces derniers vont chercher des moyens de les exploiter puisque les éditeurs de solutions de sécurité réussissent maintenant à mieux identifier les URL et les domaines de phishing utilisant des caractères latins. Ils vont tester les limites de toutes les techniques de filtrage des URL et par listes noires qui s'appuient sur des listes d'URL malveillantes ou suspectes connues, en local ou dans le cloud, pour créer un pool quasi infini d'URL à usage unique pouvant être utilisées dans les emails de phishing, et de noms de domaine pouvant être utilisés pour les botnets via DGA.

Recommandations

L'analyse de Check Point du paysage de la sécurité en 2013 révèle que l'activité des logiciels malveillants a augmenté dans toutes les catégories. Cette augmentation avait trois principaux aspects :

- Une plus grande activité d'infiltration, dans laquelle les utilisateurs sont exposés à des logiciels malveillants via des sites web, des emails et des téléchargements malveillants.
- Des menaces post-infection accrues sous forme de grandes infections de bots avec des communications de commande et de contrôle plus fréquentes.
- Un plus grand nombre d'attaques sur un large éventail de plates-formes, ciblant des vulnérabilités non seulement sur les serveurs et les clients Windows, mais également dans les infrastructures réseau et serveur, et les applications moins supervisées.

Vue dans son ensemble, cette augmentation du nombre de cyberattaques représente un défi de taille pour les entreprises et les responsables de la sécurité s'efforçant déjà de relever les défis présentés par les logiciels malveillants décrits dans le *Rapport Sécurité 2013* de Check Point. La seule façon pour les entreprises de contrer efficacement cette accélération de l'activité des logiciels malveillants, et lutter contre l'accélération du rythme des attaques, des infections et des exfiltrations dans leur environnement, est d'automatiser et de coordonner plusieurs niveaux de défense. Les mesures essentielles comprennent :

- **Antivirus sur passerelle et sur poste avec filtrage des URL** — Les entreprises doivent être en mesure de détecter et de bloquer les logiciels malveillants et les tentatives de connexion à des sites connus pour diffuser des logiciels malveillants.
- **Passerelle antibots** — En plus de détecter les logiciels malveillants, ces solutions devraient être capables de limiter les communications des botnets via DGA.
- **Protection IPS étendue** — Au-delà de la supervision seule, vous devriez être en mesure de bloquer les attaques critiques. Le système devrait également prendre en charge les réseaux, les serveurs et les infrastructures informatiques de Cisco et d'autres fournisseurs, pas seulement Microsoft Windows.
- **Maintenance complète du système et des applications** — Veillez à ce que des processus de gestion et de correction des vulnérabilités soient en place pour tous les systèmes et les applications, y compris Java et Adobe Reader, pas seulement les clients et les serveurs Microsoft Windows.
- **Meilleures pratiques pour la configuration des clients et des serveurs** — Il s'agit notamment de restreindre l'utilisation des privilèges administrateur, désactiver Java et autres scripts, et limiter les applications que les utilisateurs peuvent installer sur leur poste.

Dans le prochain chapitre, nous examinons les résultats de notre étude de 2013 sur les applications et les risques qu'elles posent aux données et aux utilisateurs.

04

APP(ETITE) FOR DESTRUCTION :

Les applications à risque dans l'entreprise

04 APP(ETITE) FOR DESTRUCTION : LES APPLICATIONS À RISQUE DANS L'ENTREPRISE

Le contrôle des applications représente un défi interne qui aggrave les défis posés par les cyberattaques externes. Les applications sont essentielles à la productivité et au fonctionnement quotidien de chaque entreprise, mais elles créent également des degrés de vulnérabilité dans leur posture de sécurité. Du point de vue de la sécurité, elles ressemblent aux personnages du roman *La ferme des animaux*[41] de George Orwell : toutes les applications sont égales, mais certaines ont plus d'égalité que d'autres.

MAIS SI NOUS SOMMES EN LIGNE,
LE MONDE EST LOCAL.

Neal Stephenson, Cryptonomicon[40]

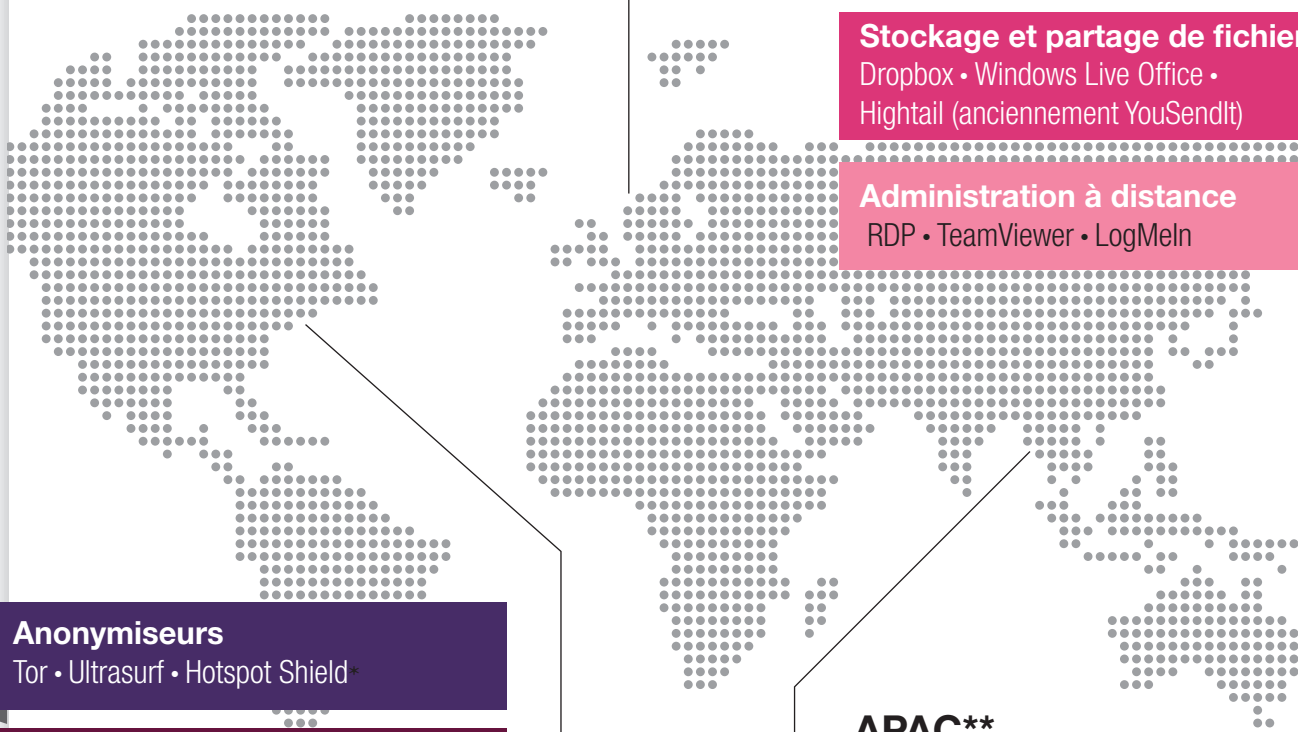
Les applications à risque incarnent ces problématiques. Contrairement aux applications de productivité telles que Microsoft Office et les applications web 2.0 de réseaux sociaux de plus en plus reconnues telles que Facebook, LinkedIn, Twitter, WebEx et YouTube, les applications à risque permettent de surfer sur le web de manière anonyme, de stocker des données dans le cloud et de partager des fichiers, d'utiliser des applications de bureau et données à distance, et partager des médias et autres fichiers entre utilisateurs et ordinateurs. Les applications à risque évoluent souvent en marge des solutions informatiques officiellement sanctionnées, voire totalement en dehors, et font partie de l'informatique de l'ombre ; c'est-à-dire l'ensemble des applications, des appareils et des services qui ne font l'objet d'aucune supervision.

86%

DES ENTREPRISES ONT AU MOINS UNE APPLICATION À HAUT RISQUE*

*** Partage de fichiers en P2P, anonymiseurs, stockage et partage de fichiers**

PRINCIPALES APPLICATIONS À RISQUE PAR RÉGION



EMEA*

Anonymiseurs
Tor • Hide My Ass! • OpenVPN

Partage de fichiers en P2P
Protocole BitTorrent • SoulSeek • Protocole EDonkey

Stockage et partage de fichiers
Dropbox • Windows Live Office • Hightail (anciennement YouSendIt)

Administration à distance
RDP • TeamViewer • LogMeIn

Amériques

Anonymiseurs
Tor • Ultrasurf • Hotspot Shield*

Partage de fichiers en P2P
Protocole BitTorrent • SoulSeek • Box Cloud

Stockage et partage de fichiers
Dropbox • Windows Live Office • Hightail (anciennement YouSendIt)

Administration à distance
RDP • LogMeIn • TeamViewer

APAC**

Anonymiseurs
Ultrasurf • Tor • Hide My Ass

Partage de fichiers en P2P
Protocole BitTorrent • Xunlei • SoulSeek

Stockage et partage de fichiers
Dropbox • Windows Live Office • Hightail (anciennement YouSendIt)

Administration à distance
TeamViewer • RDP • LogMeIn

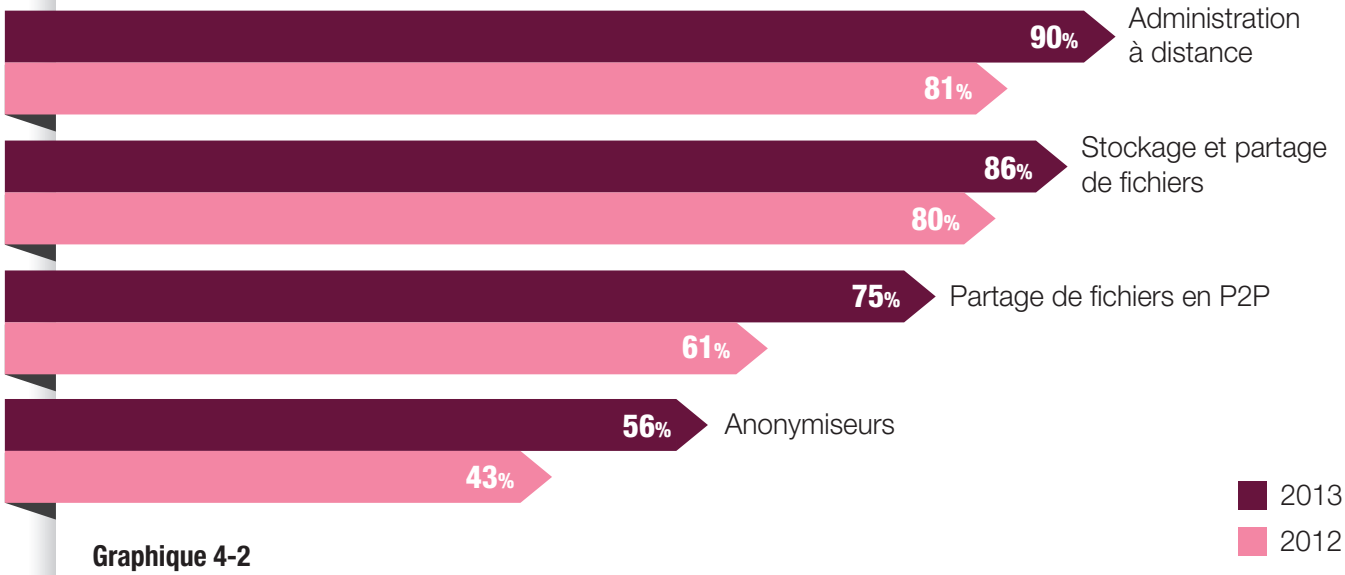
Graphique 4-1

*** EMEA : Europe, Moyen-Orient et Afrique**

**** APAC :** Asie Pacifique et Japon

Source : Check Point Software Technologies

Pourcentage des entreprises utilisant des applications à risque
(% des entreprises)



Graphique 4-2

Source : Check Point Software Technologies

En 2012, les chercheurs de Check Point ont constaté que les applications web 2.0 à risque étaient omniprésentes dans l'infrastructure de l'entreprise et posaient des risques importants de fuite de données, voire des failles de sécurité. Notre analyse de la sécurité des réseaux d'entreprise en 2013 a constaté que, malgré ces risques connus, le nombre d'applications à risque a augmenté dans toutes les catégories (Graphique 4-2). Ce chapitre examine les résultats de l'étude pour chaque catégorie et émet des recommandations pour atténuer ce problème.

LES CHERCHEURS ONT ENREGISTRÉ **UNE AUGMENTATION DE L'UTILISATION DES ANONYMISEURS** DANS LES RÉSEAUX D'ENTREPRISE, AVEC PLUS DE LA MOITIÉ (56%) DES ENTREPRISES ANALYSÉES ENREGISTRANT AU MOINS UN INCIDENT D'ANONYMISATION

Les dangers de l'anonymat

Les applications d'anonymisation fournissent principalement aux utilisateurs un moyen de surfer sur Internet et consulter des sites web tout en préservant leur anonymat. Elles reposent généralement sur la création d'un tunnel chiffré vers un ensemble de proxies HTTP qui permettent aux utilisateurs de contourner les pare-feux et les restrictions de filtrage des contenus. Certaines, telles que Tor, emploient des techniques supplémentaires d'obscurcissement du routage et même des logiciels spéciaux ou des plug-ins de navigateur pour permettre aux utilisateurs de brouiller les pistes et échapper à leur employeur, le gouvernement ou d'autres contrôles.

En 2013, les chercheurs de Check Point ont enregistré une augmentation globale de l'utilisation des proxies anonymes dans les réseaux d'entreprise, avec plus de la moitié (56%) des entreprises analysées comprenant au moins un incident d'anonymisation, soit une augmentation de 13% par rapport à 2012.

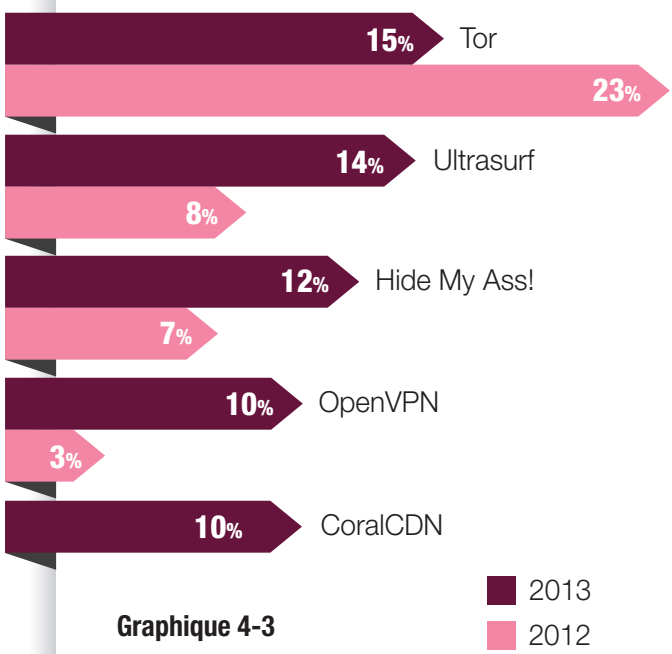
PORTAIL VERS LE WEB PROFOND

Appelé également « le routeur oignon », Tor[42] a de nouveau été l'application d'anonymisation la plus largement détectée dans notre étude de 2013. Tor était déjà bien connu comme véhicule pour la navigation anonyme contournant facilement les politiques de sécurité d'entreprise, mais en 2013, il a gagné une nouvelle notoriété en tant que portail vers le web profond, le côté ténébreux de l'Internet ouvert et consultable, ou « web surfacique ».[43] Caractérisé par son inaccessibilité à partir des outils de recherche standard, le web profond a attiré l'attention en 2013 en réponse aux préoccupations accrues aux États-Unis et à l'étranger concernant la surveillance et la vie privée, et en raison de l'arrestation du dirigeant de Silk Road.[44]

D'autres applications d'anonymisation posent un problème similaire, mais le rôle de Tor comme passerelle vers le web profond en font un risque particulier pour les responsables de la sécurité. Bien qu'il propose de l'anonymat et des places de marché underground, le web profond est également en proie à des logiciels malveillants et des escroqueries, et les entreprises ont raison de craindre que les employés qui utilisent Tor pour échapper à la surveillance réelle ou perçue finissent par exposer leur ordinateur et l'entreprise à un degré de risque élevé. Plus récemment, des chercheurs ont découvert que les données de cartes bancaires dérobées auprès de nombreux commerçants à l'aide du cheval de Troie d'accès à distance ChewBacca[45] ont été exfiltrées vers des serveurs grâce à Tor.

La liberté d'expression et l'anonymat sont des libertés essentielles et doivent être préservées pour les individus. Toutefois, pour les administrateurs de sécurité dans les environnements d'entreprise, la détection et le blocage de l'utilisation de Tor et d'autres anonymiseurs dans les systèmes et les réseaux d'entreprise doit être une priorité absolue en 2014 et au-delà.

Applications d'anonymisation les plus populaires
(% des entreprises)



Graphique 4-3

Source : Check Point Software Technologies

Les applications d'anonymisation individuelles ont cependant enregistré des gains inégaux. Tor a même été détecté dans moins d'entreprises qu'en 2012 : 15% en 2013, par rapport à 23% en 2012 (Graphique 4-3). Cela reflète une attention accrue, avec raison, à la restriction de Tor dans les politiques de sécurité d'entreprise (Encart : *Portail vers le web profond*). Cela pourrait également signifier que les employés surfent de manière anonyme moins fréquemment à partir des systèmes et réseaux d'entreprise, ou que les utilisateurs sont passés à d'autres applications d'anonymisation qui sont moins connues et donc moins susceptibles d'être bloquées par les politiques de sécurité.

Champions des défenseurs de la vie privée et de la liberté de parole, les outils d'anonymisation ont permis de protéger la confidentialité, et même la vie, des dissidents dans des pays en période de troubles. Plus récemment, les révélations en 2013 sur la surveillance orchestrée par des États ont augmenté leur adoption par les utilisateurs en Europe et en Asie comme refuge contre le cyberespionnage réel ou perçu. Les

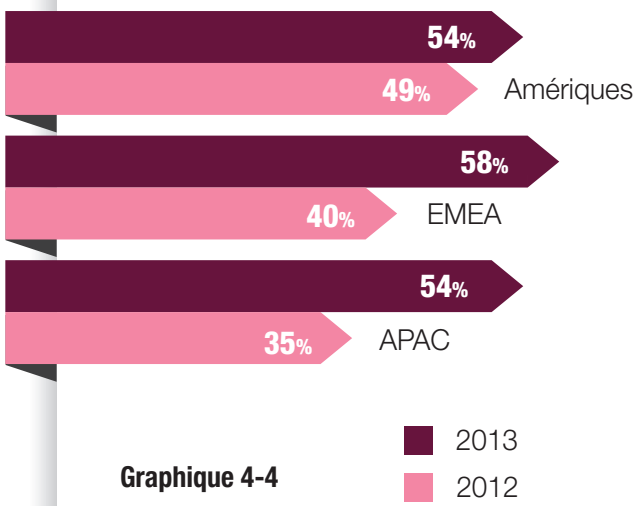
différences régionales dans les incidences d'utilisation des anonymiseurs dans les réseaux d'entreprise témoignent de ce facteur, et pointent également sur la réussite relative des administrateurs de sécurité des entreprises américaines à contraindre l'utilisation de cette catégorie d'applications à risque (Graphique 4-4).

Tout comme l'hydre mythique,[46] si les administrateurs ont réussi à couper la tête de Tor en 2013, ce n'était que pour voir six autres anonymiseurs prendre sa place. La fréquence d'utilisation des dix principaux outils d'anonymisation restants a augmenté par rapport à 2012.

Vous avez dit contrôle à distance ?

La catégorie d'applications à risque la plus largement détectée dans notre étude de 2013 était celle des applications d'administration à distance. L'application la plus connue est Microsoft RDP (Remote Desktop),[47]

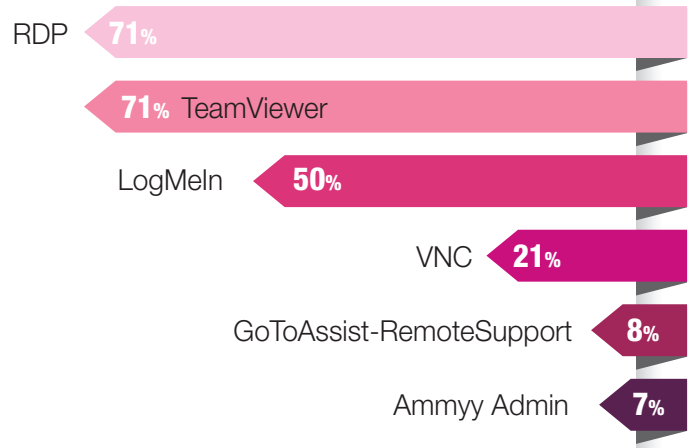
Utilisation des applications d'anonymisation par région
(% des entreprises)



Graphique 4-4

Source : Check Point Software Technologies

Principales applications d'administration à distance
(% des entreprises)



Graphique 4-5

Source : Check Point Software Technologies

mais beaucoup d'autres sont largement utilisées dans le monde, dont notamment TeamViewer qui gagne en popularité depuis 2012 (Graphique 4-5). Ces applications ont des usages légitimes lorsqu'elles permettent à des équipes d'assistance de gérer et maintenir les postes de travail des employés à travers le monde (Encart : *Outils d'administration à distance : le bon, la brute et le truand*).

De nombreuses entreprises ont cependant adopté ces outils au hasard, en fonction des besoins tactiques. Plutôt que de normaliser une seule application d'administration à distance, les services informatiques en utilisent trois ou plus, en fonction des plates-formes, des connexions et des tâches. En 2013, les applications d'administration à distance sont les seules pour lesquelles la fréquence d'utilisation la plus élevée a été détectée dans le secteur industriel, avec 90% des entreprises faisant état d'au moins un incident détecté lié à ces applications.

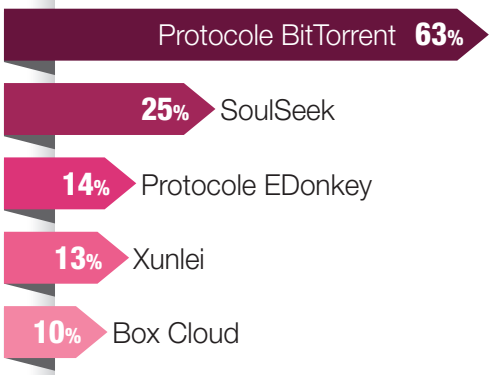
OUTILS D'ADMINISTRATION À DISTANCE : LE BON, LA BRUTE ET LE TRUAND

Les outils d'administration à distance sont parfois confondus avec les outils d'accès à distance en raison de leur similarité. En pratique, tandis que les outils d'administration à distance posent d'importants risques de sécurité, ceux-ci sont différents des risques associés aux outils d'accès à distance tels que ChewBacca, Poison Ivy,[48] DarkComet ou le célèbre Back Orifice.[49] Essentiellement des chevaux de Troie en pratique, les outils d'accès à distance n'ont pas un usage légitime dans un réseau d'entreprise, et en tant que menace majeure, leur détection doit entraîner une réponse rapide de suppression, d'assainissement et d'analyse de l'exposition potentielle des données.

Les outils d'administration à distance les plus connus, d'autre part, prolifèrent souvent dans les réseaux en raison des besoins des équipes d'assistance qui tentent de résoudre des problèmes, et pour fournir un accès aux applications et aux données à un ensemble toujours plus large d'appareils et de plates-formes utilisateur. L'outil d'administration à distance TeamViewer est un bon exemple de la tendance de ces outils. En 2013, la présence de TeamViewer sur les réseaux étudiés a bondi, grâce à l'arrêt de la version gratuite de son concurrent LogMeIn et de son ensemble de fonctionnalités comprenant la prise en charge étendue des plates-formes autres que Windows, ses fonctions de conférence et de collaboration, et ses performances sur différentes connexions sans avoir à modifier la configuration du pare-feu comme pour RDP.

Mais ces fonctionnalités ont un coût, car les caractéristiques qui en font un outil de choix pour les équipes informatiques sont également attrayantes pour les utilisateurs finaux qui souhaitent accéder à distance à leurs ordinateurs de travail depuis leur smartphone, tablette ou même PC personnel, ouvrant ainsi des portes dans le réseau de l'entreprise et compromettant la sécurité de l'entreprise. Dans ces cas, même un employé bien intentionné peut transformer un bon outil en un grave danger.

Principales applications de partage de fichiers en P2P
(% des entreprises)



Graphique 4-6

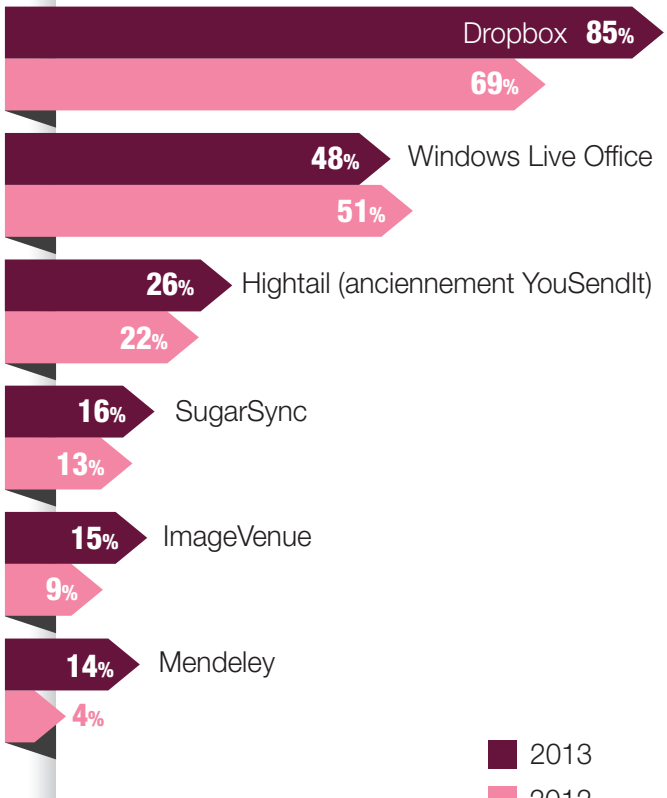
Source : Check Point Software Technologies

Partage de fichiers en P2P : Pas sûr pour le travail

Les applications de P2P (pair à pair) sont utilisées pour partager des fichiers entre utilisateurs. Souvent utilisé pour la distribution de contenus protégés, de logiciels légaux ou piratés, et autres médias, le partage de fichiers en P2P est le véhicule favori pour la diffusion de logiciels malveillants, qui peuvent être intégrés dans les fichiers partagés. En plus de livrer des logiciels malveillants à des utilisateurs peu méfiants ou non préparés, les applications de P2P peuvent créer des portes dérobées dans les réseaux d'entreprise, permettant ainsi à des agresseurs de pénétrer dans les réseaux et dérober des données confidentielles.

L'utilisation fréquente d'applications de P2P telles que BitTorrent pour distribuer de la musique et des films protégés, expose les entreprises à des poursuites de la part de la RIAA (Association de l'industrie du disque américaine), qui travaille agressivement avec les fournisseurs d'accès Internet pour identifier et

Principales applications de stockage et de partage de fichiers
(% des entreprises)



Graphique 4-7

Source : Check Point Software Technologies

poursuivre les sources de diffusion de contenus piratés ou sans licence (Graphique 4-6). En 2013, BitTorrent est resté l'application la plus populaire de partage de fichiers en P2P. Son utilisation est passée dans les entreprises de 40% en 2012 à 63% en 2013. La fréquence d'utilisation des applications de partage de fichiers en P2P a augmenté de façon constante dans toutes les régions.

Stockage et sur-partage de fichiers

La possibilité de créer et de partager facilement des contenus entre les appareils et les utilisateurs est un trait marquant des applications web 2.0. Les applications de stockage et de partage de fichiers y jouent un rôle important en facilitant l'enregistrement des contenus dans un dossier d'un appareil, puis en les répliquant automatiquement dans le cloud et en les synchronisant sur l'ensemble des appareils associés. Il suffit ensuite simplement d'envoyer un lien à d'autres utilisateurs pour partager des fichiers. Ces utilisateurs peuvent alors accéder aux fichiers partagés et même les modifier.

De toute évidence, cette facilité de partage expose les entreprises à un risque important de « sur-partage », si par inadvertance ou intentionnellement, des utilisateurs synchronisent les données confidentielles de l'entreprise depuis un système protégé vers d'autres appareils non protégés, et même dans des dossiers partagés avec d'autres utilisateurs.

En 2013, Dropbox est resté l'application de stockage et de partage de fichiers la plus courante, détectée dans 85% des réseaux analysés contre 69% en 2012 (Graphique 4-7). Cette situation contraste avec la quasi-totalité des autres applications de stockage et de partage de fichiers, dont la fréquence d'utilisation a diminué par rapport à 2012, ce qui signifie que les entreprises sanctionnent l'utilisation d'une seule application, et que la popularité continue de Dropbox parmi les utilisateurs le pousse dans les environnements d'entreprise dans le cadre de « l'informatique de l'ombre ».[50]

DROPBOX EST PRÉSENT DANS

85% DES ENTREPRISES

DROPBOX PREND UNE GIFLE

2013 est marquée comme étant l'année où les agresseurs et les chercheurs ont réalisé la capacité des applications de stockage et de partage de fichiers à infiltrer les entreprises et exfiltrer des données confidentielles. En mars, des pirates ont mis au point un mécanisme permettant d'utiliser Evernote pour prendre en charge les communications avec les serveurs de commande et de contrôle et les communications d'exfiltration des réseaux de bots.

Peu de temps après, en avril, un chercheur a décrit un mécanisme de propagation de logiciels malveillants dans une entreprise à l'aide des mécanismes de synchronisation de Dropbox. Appelée DropSmack,[51] l'attaque consiste à intégrer des commandes de macro dans un fichier portant l'extension .doc et un en-tête légitime, puis à placer ce fichier dans le dossier Dropbox d'un utilisateur d'une entreprise ciblée. Qu'il s'agisse d'un ordinateur managé par l'entreprise ou d'un appareil personnel ne fait aucune différence ; une fois DropSmack installé dans un appareil, les routines de synchronisation automatiques de Dropbox le répliquent dans le dossier Dropbox de chaque appareil associé à ce compte. DropSmack permet à un agresseur de contourner le périmètre et même la plupart des défenses anti-infiltration des appareils, de communiquer avec un serveur de commande et de contrôle, de se déplacer latéralement et d'exfiltrer des données.

L'introduction de nouvelles fonctionnalités de sécurité dans Dropbox telles que le chiffrement et l'authentification à deux facteurs répond certes aux préoccupations des responsables de la sécurité, mais DropSmack montre que ces applications ont encore un fort potentiel pour le partage de logiciels malveillants, et doivent donc être surveillées de près dans les environnements d'entreprise, si tant est qu'elles doivent être autorisées.

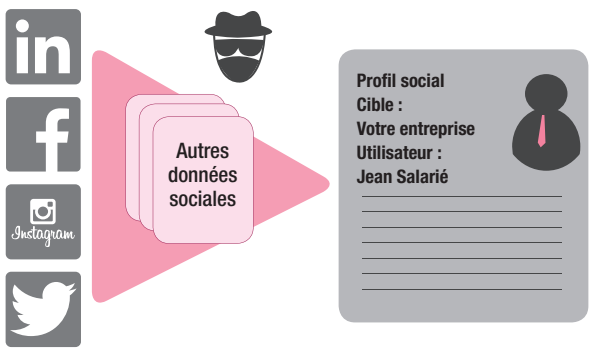
Créatures sociales

Les plates-formes de réseaux sociaux sont une caractéristique intégrale du web 2.0 et sont désormais acceptées, parfois au prix de grandes réticences, dans les environnements informatiques d'entreprise. Dans le *Rapport Sécurité 2013* de Check Point, nous avons décrit comment Facebook exposait les employés au piratage et à l'ingénierie sociale, et avons recommandé une meilleure sensibilisation des utilisateurs et de meilleures défenses pour les postes et le réseau.

En 2013, les risques sont les mêmes et sont exacerbés par le rôle croissant des réseaux sociaux comme outil essentiel pour les pirates dans la planification et l'exécution d'attaques ciblées.

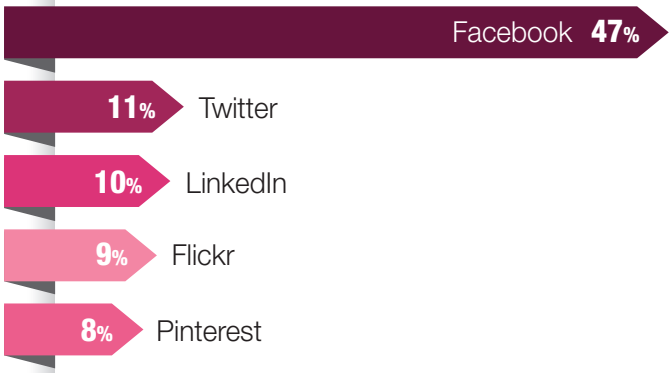
Une fois que les agresseurs ont ciblé une entreprise et identifié les employés qui ont accès aux données souhaitées, les agresseurs préparent le profil social de chaque employé ciblé (Graphique 4-8). Ce profil comprend des informations précieuses pour les agresseurs, telles que les sites web et les services de vente en ligne couramment utilisés par les employés, les amis qui sont susceptibles de leur envoyer des emails, et les événements importants auxquels ils ont récemment assisté ou assisteront. Armés de cette information, les agresseurs peuvent créer des emails d'hameçonnage ayant de fortes probabilités de réussite. Il nous suffit de regarder les conclusions du Chapitre 3 pour voir les effets de ce profilage.

Profil social



Graphique 4-8

Utilisation de la bande passante par les réseaux sociaux
(% des entreprises)



Graphique 4-9

Source : Check Point Software Technologies

Parmi les applications de réseaux sociaux, Facebook reste la plus populaire, mesurée en termes de consommation de bande passante dans les environnements d'entreprise que nous avons analysés pour notre étude de 2013 (Graphique 4-9).

Twitter et LinkedIn font également partie des trois principales applications de réseaux sociaux, mais leur fréquence d'utilisation globale a diminué par rapport à 2012, probablement moins en raison de la diminution de l'utilisation par les employés sur leur lieu de travail que de l'accès aux réseaux sociaux sur téléphones mobile. Bien que ce changement peut avoir l'avantage de réduire la pression sur les réseaux d'entreprise et diminuer les menaces immédiates sur les PC de l'entreprise, l'utilisation généralisée des applications de stockage et de partage de fichiers telles que Dropbox signifie qu'une infection sur la tablette ou le MacBook personnel d'un utilisateur peut facilement être transférée à leur système d'entreprise. (*Encart : Dropbox prend une gifle*).

Recommandations

Les applications à risque de toutes sortes restent une menace grandissante dans l'entreprise, alors même que les outils spécifiques plébiscités par les utilisateurs changent avec le temps. Tandis que certains d'entre eux, en particulier les anonymiseurs et les réseaux de P2P, n'ont pas un usage professionnel légitime et doivent être entièrement éliminés, les outils d'administration à distance et de partage et de stockage de fichiers peuvent répondre aux besoins légitimes des utilisateurs et des services informatiques, ce qui pose un défi plus complexe. Même les plates-formes de réseaux sociaux communément admises telles que Facebook, LinkedIn et YouTube, qui peuvent jouer un rôle important dans les activités et les stratégies marketing, peuvent présenter un vecteur attractif pour les attaques d'hameçonnage. Tandis que la protection antimalwares se concentre sur la détection, la prévention et l'éradication, les applications nécessitent une approche plus nuancée, devant inclure :

Le contrôle des applications par catégories — Les administrateurs doivent être en mesure de bloquer des familles entières d'applications, plutôt que d'avoir à procéder à des blocages individuels. L'administration s'en trouve non seulement simplifiée, mais cela permet également d'appliquer des contrôles à toute nouvelle application adoptée par les employés en remplacement des applications qui ont été bloquées ou restreintes.

La normalisation des applications sanctionnées — Les entreprises qui ont besoin d'outils d'administration à distance pour prendre en charge les fonctions du service informatique ou de l'entreprise doivent normaliser une seule application, puis surveiller leur réseau pour détecter d'autres outils d'administration à distance. Si le blocage n'est pas possible, leur présence devrait déclencher un processus de notification et d'enquête pour déterminer qui les utilise et comment ils sont utilisés, et vérifier si ce sont des exceptions à la politique en vigueur ou des digressions tactiques qui doivent être mises en conformité avec la politique. En outre, le suivi et la mise en application devraient être

liés à des utilisateurs ou des groupes d'utilisateurs autorisés spécifiques, afin de garantir que seuls les employés ayant un besoin métier légitime soient en mesure de les utiliser. Une approche similaire peut être utilisée pour les outils de stockage et de partage de fichiers. Le service informatique devrait mettre en place un service ou adopter une solution sécurisée pour répondre à ce besoin. Sinon, les utilisateurs se tourneront inévitablement vers des applications non sélectionnées pour permettre le partage de fichiers et la synchronisation multi-appareils que leur travail exige.

La sensibilisation des utilisateurs finaux — Compte tenu de l'impossibilité de bloquer entièrement certaines catégories d'applications, les responsables informatiques et de sécurité devraient élaborer des programmes afin d'informer les utilisateurs des menaces posées par les applications à risque. Les employés doivent comprendre les risques spécifiques posés par les différents types d'applications, notamment comment éviter les tentatives d'hameçonnage, les violations des droits d'auteur et autres menaces, et comment ils peuvent répondre à leurs besoins légitimes par des outils sélectionnés.

Il ne suffit pas toujours d'un logiciel malveillant ou d'une application inappropriée pour exposer votre entreprise à des menaces. Bien que les logiciels malveillants jouent un rôle dans de nombreux incidents de fuites de données, de simples erreurs humaines sont trop souvent un facteur clé. Le chapitre suivant examine les incidents majeurs et les tendances de fuites de données en 2013.

05

PRÉVENTION DES FUITES DE DONNÉES : Le grand retour

05 PRÉVENTION DES FUITES DE DONNÉES : LE GRAND RETOUR

Les incidents de fuites de données ont acquis une nouvelle notoriété en 2013. Adobe Systems, Target, Neiman Marcus et d'autres entreprises de grande envergure ont été victimes de failles de sécurité exposant la confidentialité de millions de consommateurs.

Les données sont depuis longtemps la cible privilégiée des pirates, y compris les informations financières, la propriété intellectuelle, les informations commerciales et les informations d'authentification. Plus que jamais, les données peuvent facilement tomber dans de mauvaises mains. Les appareils mobiles et les applications de l'informatique de l'ombre fournissent de nouveaux vecteurs d'attaque, et augmentent les risques de fuites et d'exfiltration. L'Internet des objets ne fait qu'aggraver la situation puisque les appareils communiquent directement entre eux pour échanger des informations sur la consommation d'énergie à domicile, la localisation et l'état d'un véhicule, le suivi des colis, la santé personnelle et plus encore. Lorsqu'une plus grande quantité de données transite par encore plus de moyens, il devient de plus en plus difficile de les contrôler et les protéger.

> LES NUMÉROS DE SÉCURITÉ SOCIALE, DE COMPTES ET DE CARTES BANCAIRES, NE SONT PAS JUSTE DES DONNÉES. DANS DE MAUVAISES MAINS, ILS PEUVENT RÉDUIRE À NÉANT LES ÉCONOMIES DE TOUTE UNE VIE ET RUINER LA SANTÉ FINANCIÈRE D'UN INDIVIDU.
>
> **Melissa Bean**[52]

Les pirates ne sont pas la seule menace pour les données d'entreprise. De nombreux incidents se produisent par inadvertance, lorsque les utilisateurs envoient le mauvais fichier au bon destinataire, ou le bon fichier au mauvais destinataire, ou tout simplement

EN 2013, 88%

DES ENTREPRISES ONT SUBI AU MOINS UN INCIDENT POTENTIEL DE FUITE DE DONNÉES

VOUS PENSEZ NE COURIR AUCUN RISQUE DE FUITE DE DONNÉES ? RÉFLÉCHISSEZ BIEN...

De nombreuses entreprises continuent de négliger la mise en œuvre de politiques et de contrôles de protection des données parce qu'elles estiment qu'elles ne risquent aucune fuite. La douloureuse réalité est que les pirates ne ciblent pas seulement les grandes banques et les grandes enseignes commerciales, mais que chaque entreprise possède des données confidentielles qui peuvent être exposées par un simple email ou un ordinateur portable égaré. Ce ne sont que quelques-uns des exemples de 2013 :

Les renseignements personnels, y compris les numéros de sécurité sociale, de 3 500 patients ont été **dérobés** au Département de la Santé de l'État de Floride, par des employés qui ont ensuite transmis les données à un parent pour les utiliser dans des déclarations de revenus frauduleuses.[53]

Le gouvernement du conseil d'Islington (Londres) a été condamné à une amende de 70 000 livres après qu'une équipe interne ait **publié** par inadvertance des feuilles de calcul contenant les **renseignements personnels** de 2 375 habitants, y compris leur historique de santé, sur le site web public d'un organisme de logement.[54]

Rotech Healthcare a signalé **l'exposition accidentelle de données personnelles et de renseignements sur l'état de santé** de 3 500 employés par une ancienne employée des ressources humaines qui avait été autorisée à conserver son ordinateur personnel lorsqu'elle a quitté la société.[55]

Le bureau du Commissaire à l'information du Royaume-Uni a cité plus de soixante infractions de la Loi sur la protection des données par le conseil d'Anglesey (Pays de Galles) relatives à **l'accès non autorisé aux données personnelles des résidents**, y compris leur envoi par inadvertance à des sites web publics et par email.[56]

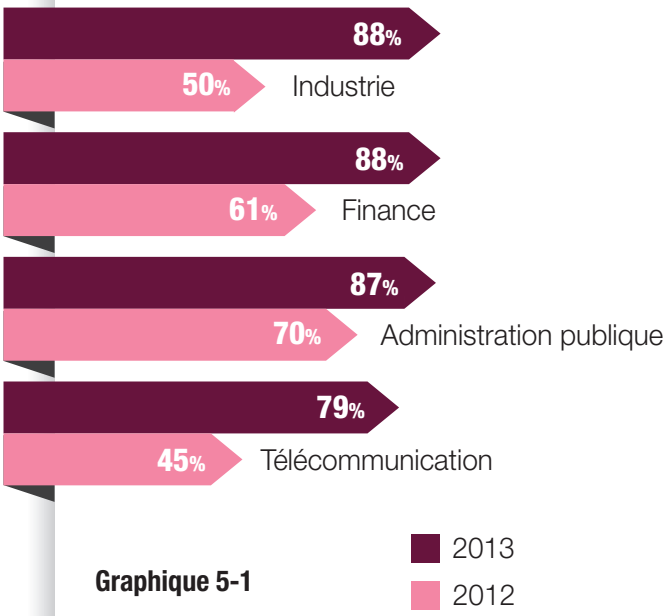
laissent un ordinateur portable sans surveillance au mauvais endroit. Les erreurs des employés ont joué un rôle clé dans un grand nombre d'incidents de fuites de données de l'année passée, mais intentionnel ou non, le résultat peut être le même : des données confidentielles exposées, des clients en colère, une réputation tâchée, des amendes pour non-conformité et de graves interruptions d'activité.

Le commerce de détail est peut-être le secteur qui a subi les pires fuites de données en 2013, mais selon les chercheurs de Check Point, des entreprises de tous les secteurs sont en train de perdre le contrôle de leurs données confidentielles, et elles le font à un rythme bien plus rapide qu'en 2012 (Graphique 5-1).

Il serait facile pour une petite entreprise de se considérer trop petite pour avoir à se soucier des fuites de données, mais rien n'est plus éloigné de la vérité (Encart : *Vous pensez ne courir aucun risque de fuite de données ? Réfléchissez bien...*). Heartland Payments,[57] une entreprise de 700 personnes, a été victime de la plus grande brèche jamais signalée lorsque des voleurs ont dérobé les informations numériques codées dans la bande magnétique des cartes bancaires. Chaque entreprise de la chaîne d'approvisionnement de l'information peut devenir une victime, et même un vol relativement petit peut fournir des données intéressantes aux pirates.

CHAQUE JOUR, UNE ENTREPRISE SUBIT
29 INCIDENTS DE FUITE POTENTIELLE
DE DONNÉES CONFIDENTIELLES.

Pourcentage d'entreprises avec au moins un incident de fuite de données potentielle par secteur d'activité (% des entreprises)



Graphique 5-1

Source : Check Point Software Technologies

TOUTES LES **49 MINUTES**, DES DONNÉES CONFIDENTIELLES SORTENT DES ENTREPRISES

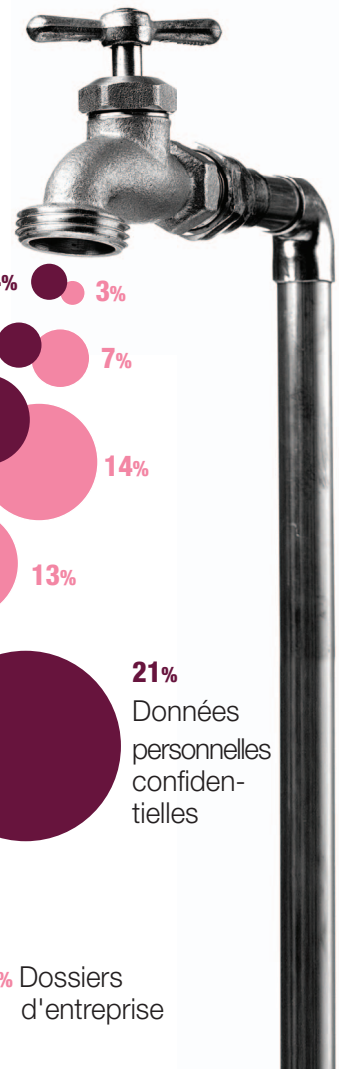
Les chercheurs de Check Point ont découvert que 88% des entreprises analysées ont été victimes de fuites de données, ce qui signifie que des données confidentielles ont été envoyées à l'extérieur des entreprises via email ou téléchargées via un navigateur web. Il s'agit d'une augmentation spectaculaire par rapport au chiffre déjà élevé de 54% que nous avons observé en 2012, et met en évidence la lutte continue des entreprises pour empêcher les données confidentielles d'être exposées accidentellement ou volontairement.

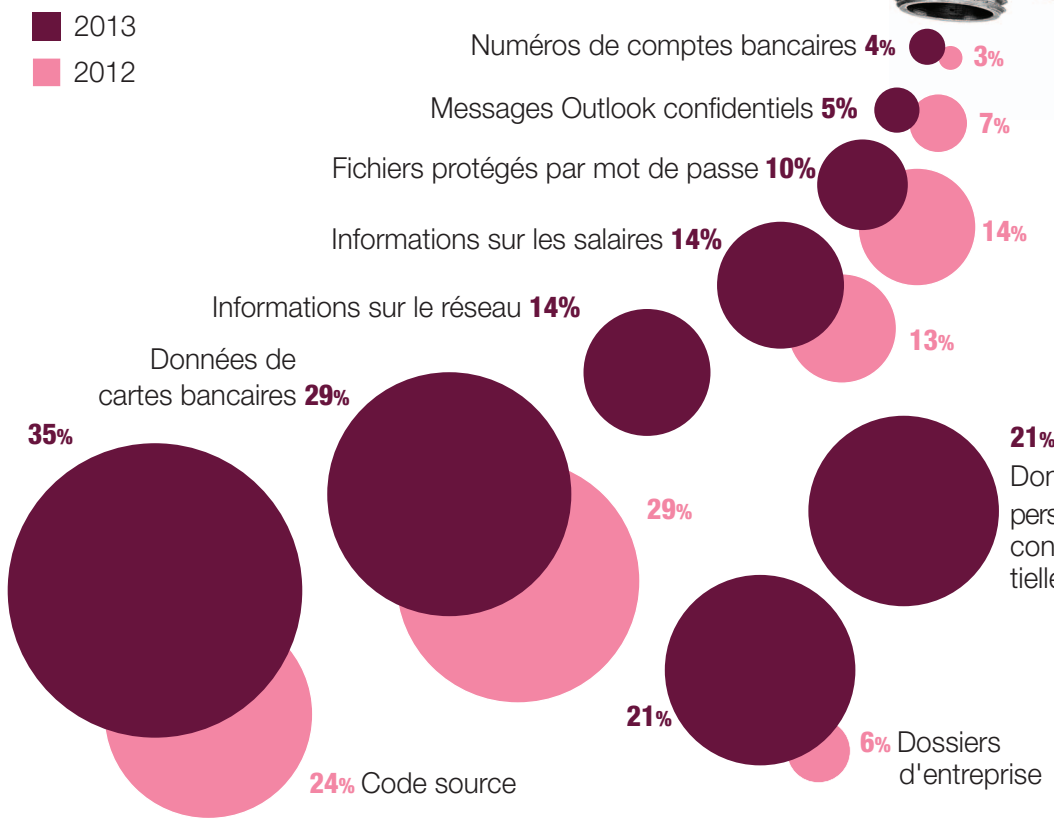
En d'autres termes, des données confidentielles sont envoyées à l'extérieur des entreprises toutes les 49 minutes. Chaque jour, une entreprise subit 29 incidents d'exposition potentielle de données confidentielles. Ce taux très élevé de fuites de données, affectant toutes les entreprises de tous les secteurs, met en évidence la nécessité d'un contrôle plus agressif des données confidentielles.

Les hausses les plus spectaculaires ont été observées dans les secteurs de l'industrie et du conseil. Ces augmentations ont plus de sens dans le contexte des types de données visés en 2013. (Graphique 5-2) Notre étude a révélé que le code source était le type de données le plus couramment envoyé à l'extérieur de l'entreprise en 2013, soit un bond de près de 50% par rapport à 2012.

Le code source, les dossiers clients et autres secrets commerciaux, représentent la majorité des actifs des entreprises, et sont constamment visés par des attaques. L'espionnage économique seul coûte aux entreprises américaines entre 250 et 500 milliards de dollars chaque année. Alors que les banques et les entreprises médicales sont depuis longtemps soumises à la pression des réglementations externes pour la protection des données des clients et des patients, les entreprises des secteurs de la fabrication, de l'énergie, du transport, de l'extraction minière et même des loisirs, n'ont pas toujours adopté une approche proactive de la sécurité des données. Ce sont les entreprises qui sont de plus en plus visées dans les campagnes utilisant des logiciels malveillants personnalisés ainsi que des attaques plus ciblées.

DONNÉES ENVOYÉES À L'EXTÉRIEUR DE L'ENTREPRISE PAR DES EMPLOYÉS (% des entreprises)





Graphique 5-2 **Source : Check Point Software Technologies**

33%

DES INSTITUTIONS FINANCIÈRES ONT ENVOYÉ DES INFORMATIONS DE CARTES BANCAIRES À L'EXTÉRIEUR DE L'ENTREPRISE

Les règlementations s'adaptent également

Malgré les nombreuses fuites de données de cartes bancaires qui se sont produites en 2013, les chercheurs de Check Point ont constaté que la fréquence des incidents de fuites de données liées à PCI dans les organismes financiers a légèrement baissé à 33%, contre 36% en 2012. Au sein des entreprises de soins et d'assurance, le nombre d'incidents liés à la règlementation HIPAA est passé de 16% des entreprises en 2012 à 25% en 2013.

La norme PCI-DSS 3.0[58] a été publiée en 2013. Elle comprend de nombreuses exigences qui arrivent à point nommé, concernant :

- Les pratiques de sécurité pour les systèmes tels que les points de vente et autres bornes.
- La sensibilisation accrue des utilisateurs aux attaques potentielles (phishing, USB, etc.) et à la manipulation responsable des données confidentielles.
- Les tests de pénétration des contrôles et des protections qui définissent la segmentation entre les données des titulaires de cartes bancaires et d'autres parties du réseau.
- Les identifiants utilisés par les fournisseurs de services pour l'accès à distance aux environnements des clients qui sont soumis à PCI-DSS.

Dans l'ensemble, ces exigences révisées mettent l'accent sur « la formation, la sensibilisation et la sécurité en tant que responsabilité partagée ». Les normes 3.0 ont pris effet au 1er Janvier 2014 et les incidents de 2013 ont contribué au sentiment d'urgence qui a poussé à l'adoption de ces nouvelles exigences.

Dans la perspective de 2014, les entreprises devront s'adapter à de nouvelles conformités et réglementations en matière de protection des données, y compris PCI-DSS 3.0 et ses exigences accrues autour de la protection des points de vente et de la sensibilisation des utilisateurs.

En Europe, la nouvelle directive de confidentialité des données de l'Union européenne, le règlement général sur la protection des données (GDPR),[59] prend également effet en 2014, et intègre des conditions plus strictes pour la protection des citoyens et des données client à la fois au sein des pays, et par-delà les frontières nationales et de l'UE. Les entreprises seront tenues de faire évoluer leurs politiques et pratiques de sécurité pour se conformer aux nouveaux règlements ou courront le risque de sanctions financières importantes.

Recommandations

Les incidents de fuites de données de grande envergure et très médiatisés de 2013, qui ont affecté certaines des marques les plus connues dans le monde ainsi que de nombreuses petites entreprises, montrent qu'il reste beaucoup à faire pour protéger les données personnelles et professionnelles. Cela ne fera qu'empirer avec les tendances de la mobilité et de l'Internet des objets qui exposent les données à de nouvelles façons de les dérober ou les exposer accidentellement. L'erreur humaine joue un rôle particulièrement central dans de nombreux incidents de fuites de données, et il faudra une approche véritablement globale et holistique pour que les données ne soient pas exposées à des menaces.

Dans un monde où les fuites de données sont un phénomène croissant, les entreprises doivent se charger elles-mêmes de la protection de leurs données confidentielles. La meilleure solution pour empêcher les fuites de données involontaires consiste à implémenter des règles de sécurité automatiques qui détectent les données protégées avant qu'elles ne quittent l'entreprise. Ces politiques peuvent être appliquées par une solution de prévention des fuites de données (DLP). Les produits de DLP intègrent un ensemble complet de fonctionnalités pour offrir aux entreprises plusieurs options de déploiement.

Avant de déployer une solution de DLP, les entreprises doivent développer des stratégies précises avec des critères concrets précisant : Ce qui est considéré comme étant des informations confidentielles Qui peut les expédier Où, comment et sur quels types d'appareils elles peuvent être utilisées Vous pouvez

LA CONFORMITÉ PCI DONNE-T-ELLE UN FAUX SENTIMENT DE SÉCURITÉ ?

Les fuites massives de données de cartes bancaires en fin 2013 ont redynamisé le débat sur la relation entre PCI-DSS et la sécurité, et en particulier de savoir si une entreprise certifiée comme étant « conforme aux normes PCI » est vraiment protégée contre le piratage.

Certains affirment que la certification de la conformité PCI favorise un faux sentiment de sécurité auprès des commerçants et du grand public. Les fuites de données qui se sont produites dans les entreprises conformes et la révocation rétroactive de la conformité PCI vont certainement engendrer du cynisme, tandis que l'évolution continue de la norme peut sembler en faire une cible mouvante.

Face à ces préoccupations, l'organisme PCI souligne à juste titre que les cas où les entreprises conformes telles que Target qui obéissait à de solides processus de sécurité, mais ont néanmoins subi des fuites de données, illustrent un problème fondamental dans la manière dont la sécurité est souvent implémentée, à savoir que ce n'est pas un produit, mais un processus.

Bob Russo, président du Conseil des normes de sécurité PCI, a souligné lors d'une intervention à ComputerWorld que la certification de la conformité PCI est un « instantané » à un moment donné. « Vous pouvez être en conformité aujourd'hui et totalement hors de conformité demain. »[60]

Les normes sont des outils précieux pour mesurer et comparer la posture de sécurité par rapport à des référentiels communs. Le danger de la certification de conformité est qu'elle donne aux entreprises le sentiment d'en « avoir terminé » avec la sécurité, plutôt que de s'engager dans un processus continu de réévaluation et d'adaptation pour faire face aux changements de leur environnement et des pratiques en matière de données.

ainsi implémenter la solution de façon optimale et la configurer pour répondre aux besoins uniques de votre entreprise en matière de productivité et de sécurité. Pour une prévention efficace des fuites de données, votre solution doit englober les mesures et les fonctionnalités suivantes :

Classification des données — L'identification fiable des données confidentielles est un composant essentiel de la solution de DLP. La solution de DLP doit être en mesure de détecter les informations personnellement identifiables, les données de conformité (HIPAA, SOX, PCI, etc.), et les données d'entreprise confidentielles, quel que soit leur type, généralisé ou personnalisé. Comme les données se déplacent dans l'entreprise et au-delà, la solution doit inspecter les flux de contenus et appliquer les règles de sécurité dans les protocoles TCP les plus couramment utilisés, y compris SMTP, FTP, HTTP, HTTPS et webmail, à l'aide de mécanismes d'analyse reposant sur des correspondances avec des modèles et des classifications de fichiers, pour identifier les types de contenu quel que soit l'extension appliquée aux fichiers ou leur compression. La solution de DLP doit être en mesure de reconnaître et de protéger les formulaires confidentiels, selon des modèles prédéfinis et la correspondance fichiers/formulaire.

Résolution des incidents par les utilisateurs — Les solutions de DLP traditionnelles peuvent détecter, classifier et même reconnaître des documents spécifiques et différents types de fichiers, mais elles ne peuvent déterminer l'intention des utilisateurs lorsqu'ils communiquent des informations confidentielles. La technologie seule est inadéquate car elle ne peut identifier cette intention et prendre les décisions qui s'imposent. Ainsi, une bonne solution de DLP doit engager les utilisateurs afin d'obtenir un résultat optimal, en leur permettant de remédier aux incidents en temps

réel. En d'autres termes, la solution de DLP doit informer les utilisateurs que leur action peut entraîner un incident de fuite de données, puis leur permettre de décider de stopper ou de poursuivre leur action. Cette méthodologie améliore la sécurité grâce à la sensibilisation aux politiques d'utilisation des données. Elle alerte les utilisateurs d'erreurs potentielles en temps réel et leur permet de remédier instantanément aux problèmes. L'impact des utilisateurs est réduit et les communications légitimes sont rapidement autorisées. L'administration est ainsi simplifiée, car les administrateurs peuvent suivre les événements de DLP pour les analyser, sans qu'il leur soit nécessaire de traiter personnellement les demandes d'envoi de données vers l'extérieur.

Protection contre les fuites de données internes — Une autre fonctionnalité importante de la DLP est la possibilité d'empêcher des données de quitter l'entreprise, mais également d'inspecter et de contrôler les emails confidentiels entre départements. Des règles de sécurité peuvent être définies pour empêcher des données confidentielles d'atteindre les mauvais départements, notamment les fichiers de rémunération, les documents confidentiels de ressources humaines, les documents de fusions/acquisitions et les formulaires médicaux

Protection des données dans les disques durs des postes — Les entreprises doivent protéger les données des ordinateurs portables dans le cadre de leur politique de sécurité pour empêcher des tiers d'obtenir des données importantes en cas de perte ou de vol des ordinateurs portables. Vous pouvez empêcher les utilisateurs non autorisés d'accéder aux informations en chiffrant les données sur tous les disques durs des postes de travail, y compris les données utilisateur, les fichiers du système d'exploitation, les fichiers temporaires et les fichiers supprimés.

Protection des données sur supports amovibles — Les employés combinent souvent des fichiers personnels (musique, photos et documents) avec des fichiers professionnels dans des appareils de stockage et des supports amovibles, ce qui rend encore plus difficile le contrôle des données d'entreprise. Les fuites de données peuvent être minimisées par le chiffrement des appareils de stockage amovibles.

Protection des documents — Des documents d'entreprise sont régulièrement envoyés sur le web par des applications de stockage de fichiers, envoyés sur des smartphones personnels, copiés sur des supports amovibles et partagés avec des partenaires commerciaux externes. Chacune de ces actions augmente les risques de fuites ou d'utilisation

25%

DES ENTREPRISES DES SECTEURS DE LA SANTÉ ET DES ASSURANCES ONT ENVOYÉ DES INFORMATIONS CONFIDENTIELLES À L'EXTÉRIEUR DE L'ENTREPRISE

QUE RETENIR DES ATTAQUES CONTRE LES POINTS DE VENTE ?

Bien que le piratage des terminaux de point de vente dans le but de dérober les données des cartes bancaires a longtemps été techniquement possible, les agresseurs trouvaient que les serveurs de stockage de ces données étaient des cibles plus faciles. L'amélioration de la sécurité des serveurs de stockage des données de cartes bancaires et des données des clients a forcé les agresseurs à reporter leur attention sur la source des données. L'année 2013 a marqué un tournant dans le piratage des terminaux de point de vente. Même si l'ampleur de ces fuites de données ont été choquantes pour beaucoup, la variété de logiciels malveillants employés dans cette catégorie était tout aussi intéressante pour les professionnels de la sécurité.

Les logiciels malveillants pour points de vente varient en sophistication, de la simple récupération de données en mémoire de ChewBacca et de Dexter,[61] au complexe BlackPOS[62] et au logiciel malveillant encore plus ciblé découvert chez Neiman Marcus.[63] Cependant, ils partagent plusieurs caractéristiques qui permettent aux agresseurs d'infiltrer les systèmes des points de vente et dérober de grandes quantités de données de cartes bancaires :

- L'utilisation de systèmes d'exploitation obsolètes dans les terminaux des points de vente, qui restent souvent non corrigés pendant des mois, même si un correctif est disponible
- L'accès au système de point de vente par l'intermédiaire d'un client ou d'un serveur infecté dans l'enseigne ciblée
- La capacité à contourner le contrôle des applications et autres mesures de confinement du système, par exemple en infectant un serveur de mise à jour
- L'utilisation du chiffrement, de protocoles communs et de modèles de trafic réseau standards, pour cacher les données pendant leur exfiltration
- Dans de nombreux réseaux, l'accès direct à Internet à partir des points de vente même, car c'est souvent ainsi que la facturation réelle est effectuée

Aborder ces questions séparément ne résout pas le problème, car cela ne résout pas la cause : une segmentation faible ou inexistante des réseaux des points de vente et d'exploitation. Les réseaux des enseignes commerciales mettent en évidence l'importance de développer et mettre en œuvre une stratégie de segmentation obéissant aux meilleures pratiques, qui permet aux entreprises d'appliquer des politiques de confinement des hôtes compromis et définir les interactions à l'intérieur d'un segment pouvant être supervisées automatiquement. Par exemple, la surveillance de la direction et des types de trafic dans les segments contenant des terminaux de point de vente devrait restreindre les possibilités pour les logiciels malveillants de se propager et d'exfiltrer des données. À cet égard, les enseignes commerciales vont se retrouver à l'avant-garde de changements conduisant toutes les entreprises à définir et implémenter une segmentation logique et une mise en application reposant sur des politiques dans leur environnement informatique.

malintentionnée. Pour protéger les documents d'entreprise, la solution de sécurité doit être en mesure de les chiffrer via des règles de sécurité et ne permettre leur accès qu'à des individus autorisés.

Gestion des événements — La définition de règles de DLP qui répondent à la politique d'utilisation des données de l'entreprise doit s'accompagner de solides possibilités de supervision et de reporting. Votre solution de sécurité doit intégrer la surveillance et l'analyse des événements de DLP passés et en temps réel. Cela donne aux administrateurs de sécurité une visibilité claire et étendue sur les informations envoyées à l'extérieur et leurs sources, et la possibilité d'agir en temps réel si nécessaire.

Le chapitre suivant présente un schéma de sécurité de haut niveau pour une protection efficace.

06

SDP :
L'architecture de sécurité pour les menaces de demain

06 SDP : L'ARCHITECTURE DE SÉCURITÉ POUR LES MENACES DE DEMAIN

UN NOUVEAU PARADIGME EST NÉCESSAIRE POUR PROTÉGER LES ENTREPRISES DE MANIÈRE PROACTIVE

Le *Rapport Sécurité 2014* de Check Point présente les résultats de notre analyse approfondie des menaces et des tendances de 2013. Ce rapport peut aider les décideurs à comprendre l'éventail des menaces qui pèsent sur leur entreprise et envisager de nouvelles mesures pour améliorer la protection de leur environnement informatique.

Les points clés de notre étude sont :

- L'utilisation de logiciels malveillants inconnus a explosé avec la tendance de « personnalisation de masse » des logiciels malveillants.
- Le nombre d'infections a augmenté, ce qui reflète le succès croissant des campagnes de logiciels malveillants ciblées.
- Chaque catégorie d'application à risque est de plus en plus présente dans toutes les entreprises.
- Le nombre d'incidents de fuites de données a augmenté dans tous les secteurs et tous les types de données.

Relever les défis

Les conclusions de ce rapport indiquent clairement que le paysage des menaces continue d'évoluer alors que les stratégies et les technologies de sécurité utilisées dans de nombreuses entreprises sont insuffisantes face à des attaques de plus en plus sophistiqués et préjudiciables. L'explosion du nombre de logiciels malveillants inconnus rend les solutions de détection obsolètes. La quantité de logiciels malveillants connus écrase les défenses existantes et s'attaque à un large éventail de plates-formes. Les applications à risque, ainsi que les outils du web 2.0, de stockage et de partage de fichiers, et d'administration à distance ayant des utilisations légitimes, continuent de proliférer, ouvrant de nouveaux vecteurs de menaces lorsqu'elles se propagent. Les incidents de fuites de données malveillants et non intentionnels causent des dommages sans précédent aux entreprises de toute taille dans tous les secteurs d'activité, et la mobilité, la consumérisation et l'Internet des objets, aggravent encore plus la problématique de protection des données. Les entreprises ont besoin d'un meilleur contrôle sur la circulation et l'utilisation de l'information.

L'évolution des menaces n'est cependant pas le seul défi de l'environnement informatique. Les entreprises sont aujourd'hui de plus en plus dominées par la libre circulation de l'information, qui supprime les frontières clairement définies des réseaux d'entreprise. Les données des entreprises circulent dans le cloud et les appareils mobiles, et rayonnent à travers des idées et des messages dans les réseaux sociaux. L'utilisation des appareils personnels, la mobilité et le cloud computing ont révolutionné les environnements informatiques statiques, entraînant la naissance de réseaux et d'infrastructures dynamiques.

Dans ce monde fait d'infrastructures informatiques et de réseaux exigeants, où les périmètres ne sont plus

aussi bien définis et où les menaces deviennent chaque jour plus intelligentes, nous devons définir la meilleure façon de protéger les entreprises.

Il existe aujourd'hui une multitude de produits de protection, qui sont généralement de nature réactive et tactique, mais font abstraction de toute notion d'architecture. Les entreprises d'aujourd'hui ont besoin d'une architecture unique combinant des équipements de sécurité réseau haute performance avec des protections proactives en temps réel.

Un nouveau paradigme est nécessaire pour protéger les entreprises de manière proactive.

Architecture de sécurité SDP

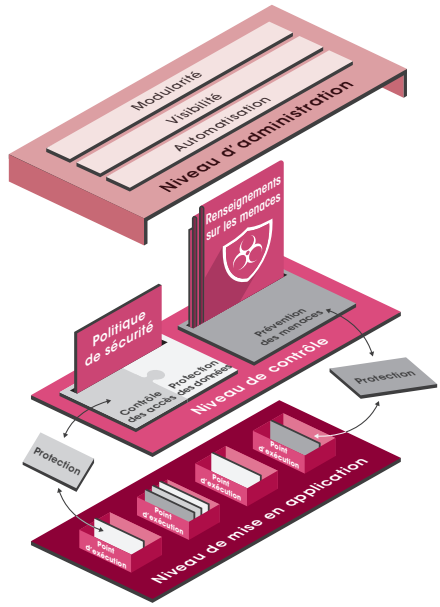
Pour répondre aux besoins actuels de protection contre les menaces en constante évolution, tout en prenant en charge les infrastructures informatiques exigeantes, Check Point a introduit SDP,[64] une nouvelle architecture et méthodologie pragmatiques de sécurité qui proposent une infrastructure modulaire, agile et surtout, SÉCURISÉE.

Grâce à l'architecture SDP, les entreprises de toute taille sont protégées en tout lieu : siège, succursales, smartphones ou appareils mobiles, ou lors de l'utilisation du cloud.

Les protections devraient automatiquement s'adapter à la nature des menaces, sans obliger les administrateurs de sécurité à garder un œil sur des milliers de notifications et de recommandations. Ces protections doivent s'intégrer harmonieusement dans l'environnement informatique, et l'architecture doit fournir une posture défensive s'appuyant sur des sources d'intelligence collaboratives internes et externes.

L'architecture SDP partitionne l'infrastructure de sécurité en trois niveaux interconnectés :

- Un **niveau de mise en application** qui repose sur des points d'exécution physiques et virtuels de la sécurité, segmente le réseau, et exécute la logique de protection dans des environnements exigeants.



Niveaux de l'architecture SDP

- Un **niveau de contrôle** qui analyse les différentes sources d'information sur les menaces et génère des protections et des politiques de sécurité exécutées par le niveau de mise en application.
- Un **niveau d'administration** qui orchestre l'infrastructure et apporte le plus haut degré d'agilité à l'ensemble de l'architecture.

En combinant le niveau de mise en application haute performance avec le niveau de contrôle logiciel hautement évolutif et dynamique, l'architecture SDP fournit non seulement une résilience fonctionnelle, mais fournit également une prévention proactive des incidents adaptée au paysage des menaces en constante évolution.

Implémentation du schéma de sécurité dans votre entreprise

Un des principaux avantages de l'architecture SDP est qu'elle propose une simple méthodologie d'implémentation du schéma de sécurité. Check Point SDP — Schéma de Sécurité Entreprise décrit en détail l'architecture SDP, ses avantages et une méthodologie d'implémentation claire. Il est disponible en ligne gratuitement sur checkpoint.com/sdp.

La section suivante décrit, niveau par niveau, comment SDP peut être intégré dans votre entreprise pour la protéger contre les menaces présentées dans ce rapport.

Niveau de mise en application

Le niveau de mise en application, conçu pour être fiable, rapide et simple, se compose de passerelles de sécurité réseau et de logiciels sur hôte qui agissent en tant que points d'exécution réseau. Ces points d'exécution peuvent être implémentés sous forme physiques ou virtuelles, ou encore sous forme de composants sur les postes du réseau de l'entreprise ou dans le cloud.

Où déployer ces points d'exécution dans notre réseau ? Lorsque les réseaux étaient simples, nous pouvions nous contenter d'appliquer des protections au niveau du périmètre. Mais lorsque le périmètre n'est pas bien défini, où déployer les points d'exécution ?

Chaque segment devient le nouveau périmètre. En divisant un environnement complexe en petits segments, en fonction de profils de sécurité, et en déployant un point d'exécution au périmètre de chaque segment, l'environnement est sécurisé !

Niveau de contrôle

L'élément suivant de l'architecture SDP est le niveau de contrôle. Il génère les protections et les politiques de sécurité, et les transmet aux points d'exécution. À l'aide de politiques de contrôle d'accès et de protection des données, les administrateurs peuvent définir des politiques reposant sur des règles pour contrôler les interactions entre les utilisateurs, les actifs, les données et les applications. Il s'agit essentiellement d'un pare-feu et d'un pare-feu de nouvelle génération.

Des politiques y sont définies pour contrôler l'accès aux applications à risque décrites au Chapitre 4, telles que les anonymiseurs et les applications de partage de fichiers en P2P, de stockage de fichiers et d'administration à distance. Ces politiques contrôlent également les flux de données en mouvement et au repos, et protègent contre les fuites de données telles que celles décrites au Chapitre 5.

Les politiques de contrôle d'accès et de protection des données ne sont pas suffisantes. Les entreprises doivent également se protéger contre les agresseurs et les menaces en constante évolution. Afin d'atteindre cet objectif, nous devons implémenter des protections qui permettent d'identifier les attaques connues et inconnues, telles que celles décrites aux Chapitres 2 et 3.

C'est le rôle de la prévention des menaces, la deuxième partie du niveau de contrôle. Les protections y sont mises à jour en temps réel et protègent automatiquement les points d'exécution de sorte qu'il n'est pas nécessaire de définir ici une politique spécifique, mais plutôt d'activer le mécanisme de prévention des menaces.

Les renseignements sur les menaces sont la clé d'une prévention efficace des menaces. Ces renseignements devraient provenir d'autant de sources que possible, et devraient être transformés et traduits en de nouvelles protections pour alimenter tous les points d'exécution en temps réel.

Niveau d'administration

Ce troisième niveau, qui permet à l'architecture SDP de prendre vie, est crucial pour gérer l'ensemble de l'architecture. Le niveau d'administration a 3 principales caractéristiques : modularité, automatisation et visibilité.

La modularité permet de séparer les tâches administratives pour une souplesse optimale. L'automatisation et l'ouverture permettent l'intégration de systèmes tiers pour créer des politiques et des protections en temps réel. Enfin, la visibilité, c'est-à-dire la possibilité de recueillir des renseignements de sécurité à partir de tous les points d'exécution, fournit une vue d'ensemble sur la posture de sécurité de l'entreprise.

L'architecture SDP fournit une infrastructure modulaire et dynamique, capable de s'adapter rapidement à l'évolution des menaces et des environnements informatiques.

07

À PROPOS DE CHECK POINT SOFTWARE TECHNOLOGIES

07 À PROPOS DE CHECK POINT SOFTWARE TECHNOLOGIES

Depuis maintenant 20 ans, la mission de Check Point est de sécuriser Internet. Après avoir inventé le pare-feu et être devenu le leader du marché de la sécurité réseau, Check Point se concentre dorénavant sur le développement de technologies de protection adaptées à l'évolution continue d'Internet.

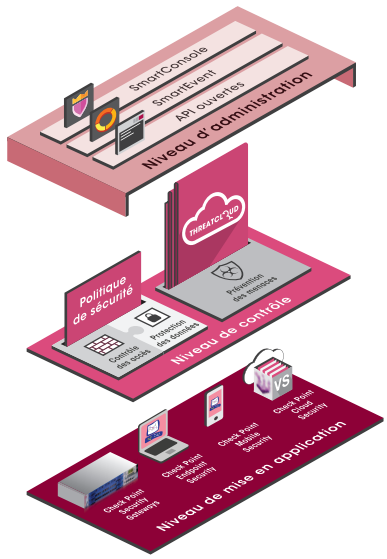
Internet n'est plus seulement une plate-forme pour mener des activités légitimes. C'est également un repère de cybercriminels. Compte tenu de cet environnement, Check Point a développé une architecture permettant de déployer des technologies de prévention des menaces multicouche qui proposent une protection maximale contre toutes les menaces, y compris les attaques zero-day.

Check Point SDP

Les protections Check Point définies par logiciel offrent la flexibilité nécessaire pour faire face aux nouvelles menaces et adopter de nouvelles technologies.

Check Point propose une gamme complète de points d'exécution, notamment sous forme d'appliances de sécurité réseau haute performance, de passerelles virtuelles, de logiciels sur hôte et d'applications pour appareils mobiles, pouvant être déployés dans un réseau d'entreprise ou dans le cloud.

En termes de niveau de contrôle, Check Point propose le pare-feu de nouvelle génération le plus avancé du marché, et ThreatCloud est la plus grande base ouverte de renseignements sur les menaces, qui alimente nos points d'exécution en temps réel.



Check Point SDP

Enfin, l'architecture Check Point est administrée à partir d'une console de sécurité unifiée, modulaire, hautement évolutive et ouverte aux systèmes tiers.

Check Point propose l'architecture de sécurité dont les entreprises ont besoin dès aujourd'hui pour se protéger contre les menaces de demain. Pour obtenir des informations complémentaires sur SDP, rendez-vous sur www.checkpoint.com/sdp

Check Point combine cette approche holistique de la sécurité avec ses solutions technologiques innovantes pour répondre aux défis posés par les menaces actuelles et intégrer la sécurité dans l'activité de l'entreprise.

Régulièrement identifié par les analystes comme leader du marché de la sécurité réseau, Check Point Software fournit à ses clients des solutions de sécurité de haut niveau et des meilleures pratiques depuis maintenant 20 ans. Check Point compte parmi ses clients les 100 plus grandes entreprises mondiales, et plus d'une centaine de milliers d'entreprises de toute taille.

RÉFÉRENCES

1 Stoll, Cliff. (2005). The Cuckoo's Egg : Tracking a Spy Through the Maze of Computer Espionage. New York : Pocket Books.

2 http://resources.infosecinstitute.com/hacktivism-means-and-motivations-what-else/

3 http://www.entrepreneur.com/article/231886

4 http://www.darkreading.com/advanced-threats/mass-customized-attacks-show-malware-mat/240154997

5 http://www.checkpoint.com/campaigns/securitycheckup/index.html

6 http://www.checkpoint.com/products/threat-emulation/

7 http://www.checkpoint.com/threatcloud-central/index.html

8 https://supportcenter.checkpoint.com/supportcenter/portal/role/supportcenterUser/page/default.psml/media-type/html?action=portlets.DCFileAction&eventSubmit_doGetdcdetails=&fileid=20602

9 https://www.checkpoint.com/products/softwareblades/architecture/

10 http://www.checkpoint.com/products/index.html#gateways

11 Huxley, Thomas Henry (1887). Sur la réception de l'Origine des espèces, http://www.todayinsci.com/H/Huxley_Thomas/HuxleyThomas-Quotations.htm

12 http://www.checkpoint.com/threatcloud-central/downloads/check-point-himan-malware-analysis.pdf

13 http://usa.kaspersky.com/

14 http://msdn.microsoft.com/en-us/magazine/cc164055.aspx

15 http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon

16 http://news.cnet.com/Code-Red-worm-claims-12,000-servers/2100-1001_3-270170.html

17 http://www.cnn.com/2004/TECH/internet/05/03/sasser.worm/

18 http://support.microsoft.com/kb/2664258

19 http://www.pcmag.com/article2/0,2817,2370016,00.asp

20 https://www.virustotal.com/

21 http://www.av-test.org/en/home/

22 http://www.checkpoint.com/threatcloud-central/downloads/10001-427-19-01-2014-ThreatCloud-TE-Thwarts-DarkComet.pdf

23 http://contextis.com/research/blog/malware-analysis-dark-comet-rat/

24 http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Portable_Executable.html

25 http://blog.malwarebytes.org/intelligence/2013/10/cryptolocker-ransomware-what-you-need-to-know/

26 Mariotti, John. (2010). The Chinese Conspiracy. Bloomington : iUniverse.com

27 http://www.checkpoint.com/campaigns/security-report/download.html?source=google-ngfw-us-sitelink-report&gclid=ClfK-JuOhrwCFZFxQgodsBYA_w

28 https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/3/html/Security_Guide/ch-risk.html

29 Anderson, Chris. (2006). The Long Tail : Why the Future of Business is Selling Less of More. New York : Hyperion.

30 http://www.fbi.gov/about-us/history/famous-cases/willie-sutton

31 http://searchwindowsserver.techtarget.com/definition/remote-code-execution-RCE

RÉFÉRENCES Suite

[32] http://searchsoa.techtarget.com/definition/Remote-Procedure-Call

[33] https://www.checkpoint.com/threatcloud-central/articles/2013-11-25-te-joke-of-the-day.html

[34] http://www.checkpoint.com/threatcloud-central/articles/2013-12-03-new-wave-url-domain-malware.html

[35] http://www.checkpoint.com/threatcloud-central/articles/2013-11-14-defeating-cryptocker.html

[36] http://www.apwg.org/

[37] http://www.checkpoint.com/threatcloud-central/articles/2013-12-03-new-wave-url-domain-malware.html

[38] http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2013.pdf

[39] http://newgtlds.icann.org/en/program-status/delegated-strings

[40] Stephenson, Neal. (2002). Cryptonomicon. New York : Avon.

[41] Orwell, George. (1956). La ferme des animaux. New York : Signet Books.

[42] https://www.torproject.org/

[43] http://www.pcworld.com/article/2046227/meet-darknet-the-hidden-anonymous-underbelly-of-the-searchable-web.html

[44] http://www.huffingtonpost.com/tag/silk-road-arrest

[45] http://www.pcworld.com/article/2093200/torenabled-malware-stole-credit-card-data-from-pos-systems-at-dozens-of-retailers.html

[46] http://www.britannica.com/EBchecked/topic/278114/Hydra

[47] http://msdn.microsoft.com/en-us/library/aa383015(v=vs.85).aspx

[48] http://www.securityweek.com/poison-ivy-kit-enables-easy-malware-customization-attackers

[49] http://www.checkpoint.com/defense/advisories/public/2005/cpai-20-Decf.html

[50] http://www.emea.symantec.com/web/ShadowIT-enduser/

[51] http://www.techrepublic.com/blog/it-security/dropsmack-using-dropbox-to-steal-files-and-deliver-malware/

[52] http://vote-il.org/politicianissue.aspx?state=il&id=ilbeanmelissa&issue=buscrime

[53] http://www.scmagazine.com/florida-health-department-employees-stole-data-committed-tax-fraud/article/318843/

[54] http://www.islingtongazette.co.uk/news/data_leak_lands_islington_council_with_70_000_fine_1_2369477

[55] http://healthitsecurity.com/2013/11/12/rotech-healthcare-reports-three-year-old-patient-data-breach/

[56] http://www.dailypost.co.uk/news/north-wales-news/anglesey-council-under-fire-over-6330304

[57] http://www.informationweek.com/attacks/heartland-payment-systems-hit-by-data-security-breach/d/d-id/1075770

[58] https://www.pcisecuritystandards.org/documents/DSS_and_PA-DSS_Change_Highlights.pdf

[59] http://ec.europa.eu/justice/newsroom/data-protection/news/130206_en.htm

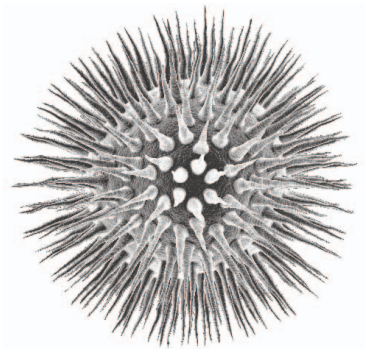
[60] http://www.computerworld.com/s/article/9245984/Despite_Target_data_breach_PCI_security_standard_remains_solid_chief_says

[61] http://www.csoonline.com/article/723630/dexter-malware-infects-point-of-sale-systems-worldwide-researchers-say

[62] http://www.darkreading.com/vulnerabilities---threats/securestate-releases-black-pos-malware-scanning-tool/d/d-id/1141216

[63] http://www.businessweek.com/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data

[64] http://www.checkpoint.com/sdp



Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

www.checkpoint.com

SIÈGE MONDIAL

5 HA'SOLELIM STREET, TEL AVIV 67897, ISRAËL
TÉL. : +972 3 753 4555 | FAX : +972-3-624-1100
EMAIL : INFO@CHECKPOINT.COM

SIÈGE FRANÇAIS

1 PLACE VICTOR HUGO, 92400 COURBEVOIE, FRANCE
TÉL. : +33 (0)1 55 49 12 00
EMAIL : INFO_FR@CHECKPOINT.COM