Rapport sur les données de sécurité Microsoft

Volume 11

Une vue en profondeur des infections et vulnérabilités logicielles, des menaces de code malveillant et des logiciels potentiellement indésirables pour le premier semestre de l'année 2011

RÉSULTATS CLÉS

Microsoft

Rapport sur les données de sécurité Microsoft

Sommaire

Rapport sur les données de sécurité Microsoft, Volume 11

Le volume 11 du *Rapport sur les données de sécurité de Microsoft®* (*Microsoft Security Intelligence Report* ou *SIRv11*) propose des vues approfondies relatives aux vulnérabilités et infections logicielles, aux menaces de code malveillant et aux logiciels potentiellement indésirables concernant des logiciels Microsoft ou d'autres logiciels tiers. Microsoft a élaboré ces vues sur base d'analyses de tendances détaillées réalisées au cours des dernières années, en se concentrant sur le premier semestre de 2011.

Ce document récapitule les résultats clés de ce rapport. Le rapport complet inclut également une analyse en profondeur des tendances enregistrées dans plus de 100 pays/régions du monde et propose des méthodes vous permettant de gérer les risques liés à votre organisation, à vos logiciels, ainsi qu'à votre personnel.

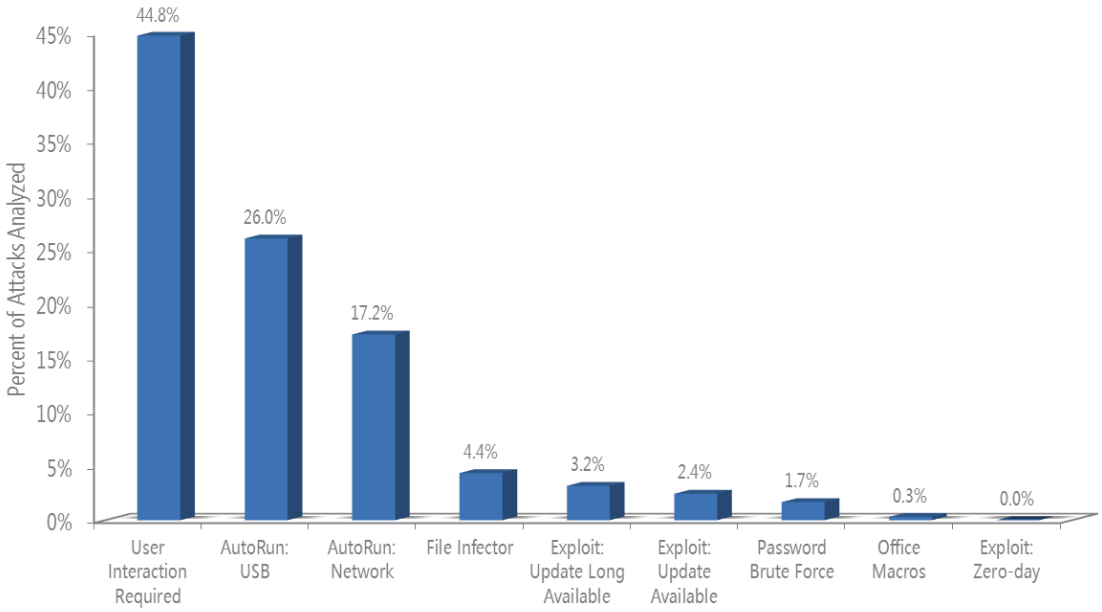
Le rapport complet, ainsi que les volumes précédents et les vidéos associées peuvent être téléchargés depuis www.microsoft.com/sir.

Focalisation sur les méthodes de propagation des logiciels malveillants

Microsoft a entrepris une analyse afin de mieux comprendre la fréquence des attaques « 0 day », ainsi que les risques associés auxquels les utilisateurs sont confrontés. Cette analyse a été conduite pour fournir aux professionnels de la sécurité des informations qu'ils peuvent utiliser pour hiérarchiser leurs problèmes et gérer efficacement leurs risques. Comme tout un chacun, les responsables des départements informatiques sont confrontés à des contraintes de temps, de budget, de personnel et de ressources lorsqu'ils planifient et exécutent leurs tâches. Des informations précises et à jour sur l'étendue des menaces permettent aux professionnels de la sécurité d'organiser efficacement leurs systèmes de défense et de préserver la sécurité de leurs réseaux, logiciels et personnel.

Pour les besoins de l'analyse, les menaces détectées par l'outil de suppression des logiciels malveillants au cours du premier semestre de 2011 ont été classées selon les moyens de propagation que chaque famille de menaces utilise pour infecter ses victimes. Pour les menaces signalées comme utilisant plusieurs méthodes pour infecter des utilisateurs, le nombre d'infections signalées par l'outil pour cette famille a été divisé et réparti équitablement entre les différentes méthodes. La Figure 1 reprend les résultats de cette analyse.

Figure 1. Logiciels malveillants détectés par l'outil de suppression des logiciels malveillants au cours du premier semestre de 2011, selon les méthodes de propagation signalées



- Les différentes méthodes de propagation des menaces employées par les logiciels malveillants reprises dans la Figure 1 sont décrites comme suit :

  - **Intervention de l'utilisateur requise** (User Interaction Required). Lorsqu'un utilisateur doit effectuer une action pour que l'ordinateur soit compromis. Dans ce contexte, « action » correspond à une action intentionnelle à distinguer par certains points de l'utilisation ordinaire de l'ordinateur.

  - **Exécution automatique : USB** (AutoRun : USB). La menace profite de la fonction Exécution automatique de Windows pour infecter les périphériques de stockage USB, ainsi que d'autres volumes amovibles.

  - **Exécution automatique : Réseau** (AutoRun : Network). La menace profite de la fonction Exécution automatique de Windows pour infecter des volumes réseau mappés sur des lettres de lecteur.

  - **Infecteur de fichiers** (File Infector). La menace se répand en modifiant des fichiers, souvent assortis d'une extension .exe ou .src, en recopiant ou en écrasant certains segments de code.

- **Attaque : Mise à jour disponible depuis longtemps** (Exploit: Update Long Available). Le fournisseur a publié une mise à jour de sécurité pour traiter la vulnérabilité plus d'un an avant l'attaque.

- **Attaque : Mise à jour disponible** (Exploit: Update Available). Le fournisseur a publié une mise à jour de sécurité pour traiter la vulnérabilité moins d'un an avant l'attaque.

- **Attaque de mot de passe par force brute** (Password Brute Force). La menace se répand en lançant des attaques de mot de passe par force brute sur les volumes disponibles de manière similaire à la commande `net use`.

- **Macros Office** (Office Macros). La menace se répand en infectant les documents Microsoft Office par le biais de macros malveillantes Visual Basic® pour Applications (VBA).

- **Attaque « 0 day »** (Exploit: Zero-day). Le fournisseur n'a pas publié de mise à jour de sécurité pour traiter la vulnérabilité au moment de l'attaque.

- Plus d'un tiers des détections de logiciels malveillants analysées ont été associées à des logiciels malveillants se servant de la fonction Exécution automatique de Windows®.

  - Les menaces en question ont été scindées en deux catégories : celles qui se répandent via des volumes amovibles (26 % du nombre total) et celles qui se propagent par le biais de volumes réseau (17 %).

  - Pour lutter contre ces menaces, Microsoft a pris plusieurs mesures pour protéger les utilisateurs, en publiant notamment une mise à jour automatique pour les plateformes Windows XP et Windows Vista® en février 2011. Cette initiative permet de garantir un niveau de sécurité supérieur pour la fonction Exécution automatique (autorun), similaire au niveau par défaut de Windows 7.

- Environ 6 % des détections par l'outil de suppression des logiciels malveillants analysées ont été associées à des *attaques*. Il s'agit, en d'autres termes, de code malveillant tentant d'exploiter des vulnérabilités d'applications ou de systèmes d'exploitation.

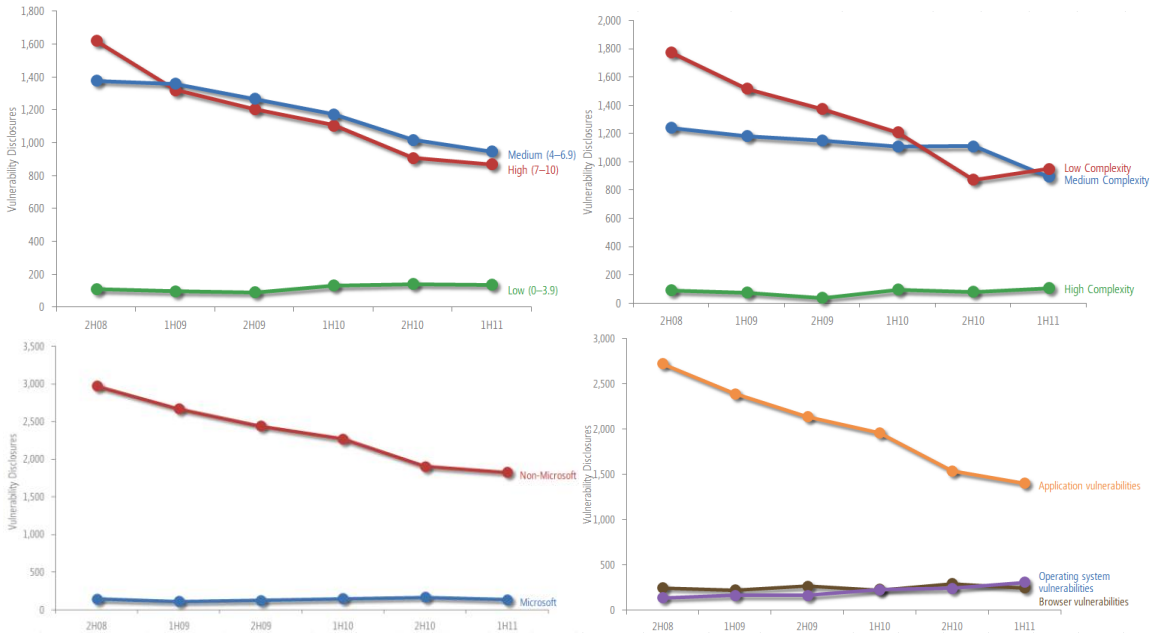
- Aucune des catégories les plus fréquentes détectées par l'outil de suppression des logiciels malveillants n'a été signalée comme procédant à des attaques « 0 day » au cours du premier semestre de 2011.

- Sur l'ensemble des exploitations de vulnérabilités détectées par l'outil, moins de1 % consistaient en des attaques « 0 day ».

Données sur les menaces dans le monde

Divulgations de vulnérabilités

Image 2. Tendances relatives à la gravité des vulnérabilités, à leur complexité, à leurs divulgations par fournisseur et par type



- La tendance globale de la sévérité des vulnérabilités (telle que définie par le dictionnaire CVE [Common Vulnerabilities and Exposures], numéro) est positive. Les vulnérabilités de sévérité moyenne et élevée divulguées au cours du premier semestre de 2011 ont chuté respectivement de 6,8 % et de 4,4 % par rapport au deuxième semestre de 2010.

- Les vulnérabilités de faible complexité (les plus faciles à exploiter) ont chuté de 41,2 % par rapport à la période de 12 mois précédente.

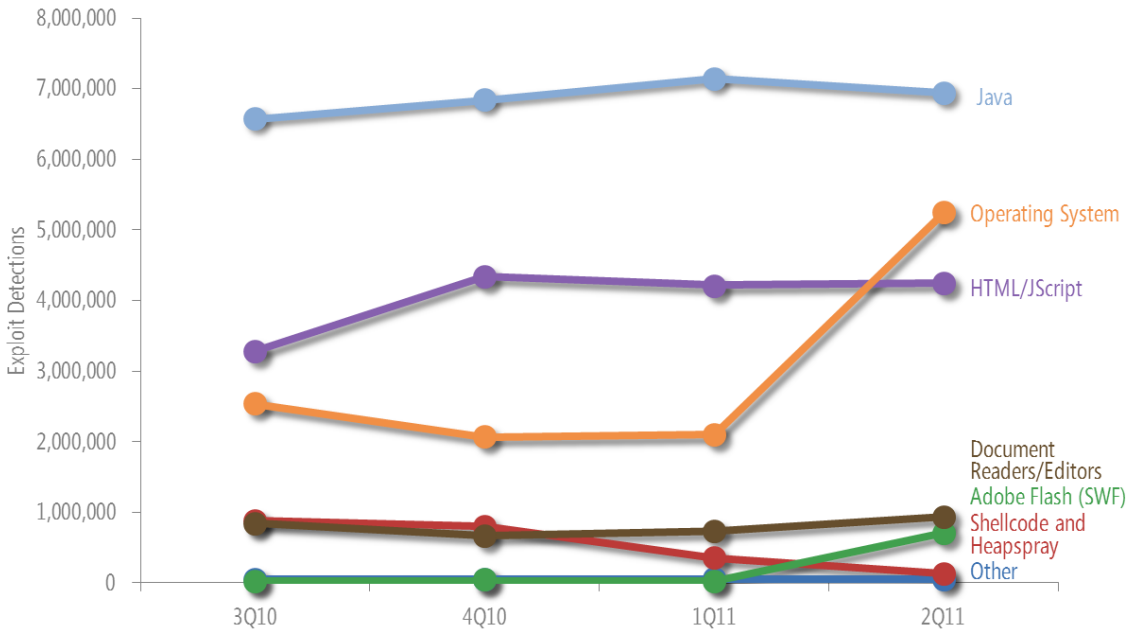
- Les chiffres relatifs aux divulgations de vulnérabilités au niveau des navigateurs et des systèmes d'exploitation ont manifesté une stabilité effective durant plusieurs années. Concrètement, ces catégories représentent respectivement 12,7 % et 15,7 % de l'ensemble des vulnérabilités divulguées durant le premier semestre de 2011.

- Les vulnérabilités constatées au niveau de produits Microsoft constituent 6,9 % de l'ensemble des vulnérabilités divulguées durant le premier semestre de 2011, ce qui représente une baisse par rapport aux 8,2 % enregistrés au cours du deuxième semestre de 2010.

Attaques

La Figure 3 illustre la prédominance de plusieurs types d'attaques pour chaque trimestre entre le troisième trimestre de 2010 et le deuxième de 2011.

Figure 3. Attaques détectées et bloquées par des produits Microsoft anti-logiciels malveillants entre le troisième trimestre de 2010 et le deuxième de 2011, classées par plateforme ou technologie ciblée



- Les types d'attaques les plus couramment observés au cours du premier semestre de l'année 2011 regroupaient les attaques ciblant des vulnérabilités dans l'environnement d'exécution Java d'Oracle (auparavant Sun), dans la machine virtuelle Java et au niveau de Java SE dans l'environnement Java Development Kit (JDK). Les exploitations de failles de sécurité au niveau de

Java ont été responsables de 30 à 50 % de l'ensemble des attaques observées au cours de chacun des quatre derniers trimestres.

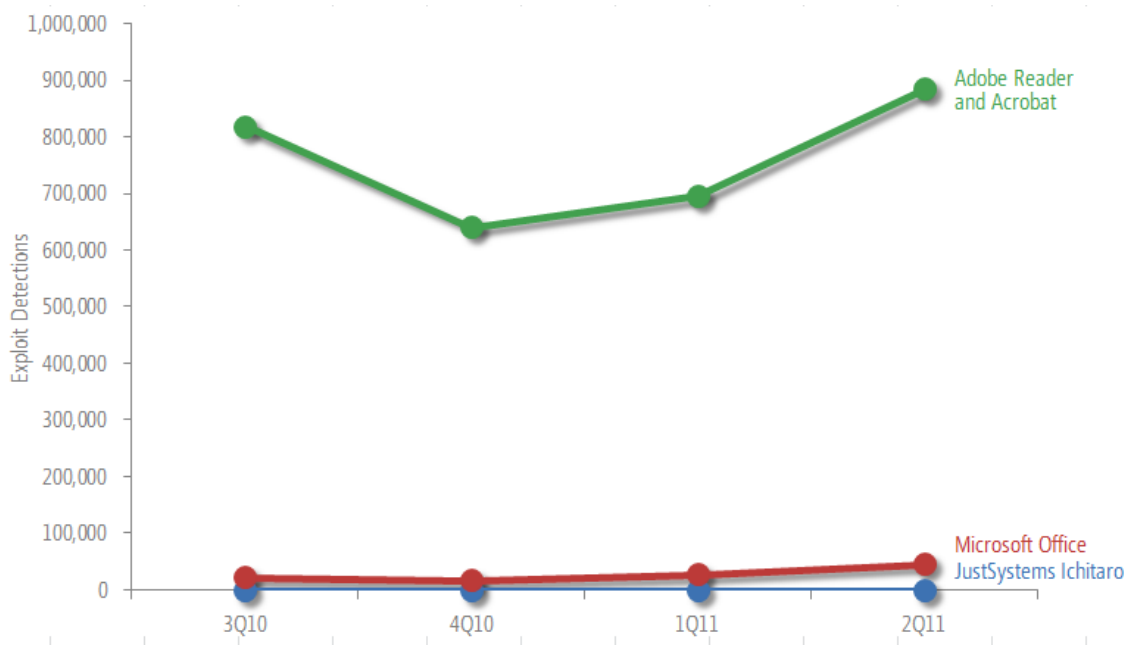
- Les détections d'attaques au niveau des systèmes d'exploitation ont sensiblement augmenté au cours du deuxième trimestre de 2011 du fait d'une augmentation des exploitations de la vulnérabilité CVE-2010-2568.

- Bien que cela semble extraordinaire par rapport à d'autres types d'attaques, les détections d'attaques ciblant Adobe Flash ont augmenté au deuxième trimestre de 2011 à raison de 40 fois le volume enregistré au cours du premier trimestre du fait de l'exploitation de deux vulnérabilités récemment détectées.

- Les attaques ciblant CVE-2010-2568, une vulnérabilité au niveau de Windows Shell, ont sensiblement augmenté au deuxième trimestre de 2011 et elles ont été responsables de l'augmentation des attaques au niveau des systèmes d'exploitation enregistrée au cours du deuxième trimestre de 2011. La vulnérabilité a initialement été détectée comme étant exploitée par la famille Win32/Stuxnet au milieu de l'année 2010.

Attaques au niveau de documents

Figure 4. Types d'attaques détectées et bloquées par des produits Microsoft anti-logiciels malveillants entre le troisième trimestre de 2010 et le deuxième de 2011



- Les attaques qui ont affecté Adobe Acrobat et Adobe Reader ont constitué la majorité des attaques au niveau des formats de document détectées au cours du premier semestre de 2011. Pratiquement toutes ces attaques impliquaient la catégorie générique d'attaques Win32/Pdfjsc.

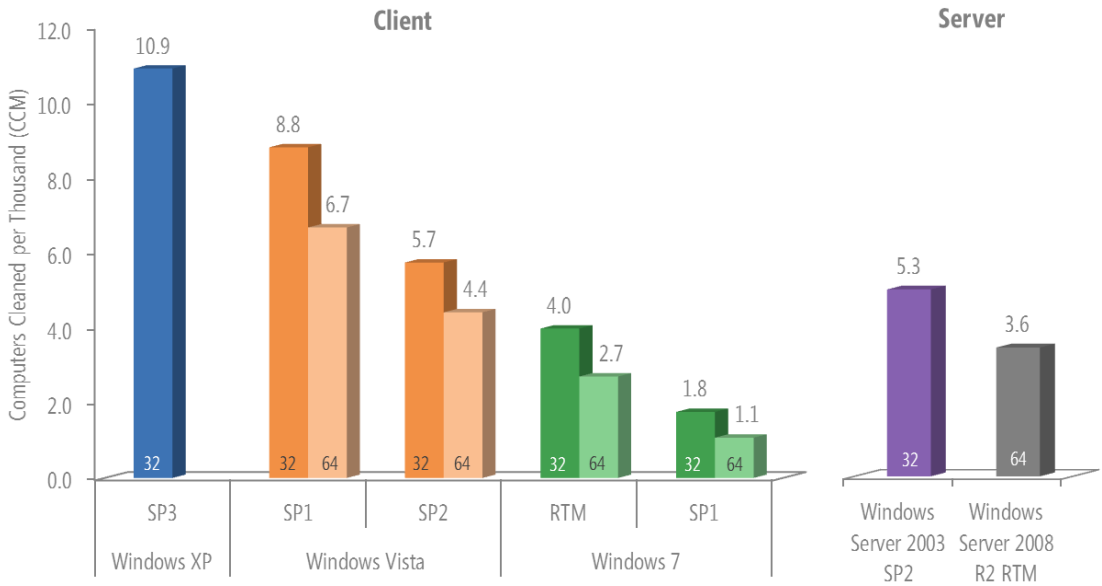
- Plus de la moitié des attaques au niveau de Microsoft Office impliquaient CVE-2010-3333, une vulnérabilité au niveau de l'analyseur RTF dans les versions de Microsoft Word.

Logiciels malveillants et logiciels potentiellement indésirables

Sauf indication contraire, les informations reprises dans cette section ont été collationnées à partir de données télémétriques générées à partir de plus de 600 millions d'ordinateurs dans le monde et de certains des services en ligne les plus utilisés sur Internet. Les taux d'infections sont exprimés en *ordinateurs nettoyés sur mille ordinateurs* ; ceux-ci correspondent au nombre d'ordinateurs signalés comme nettoyés sur un trimestre par tranche de mille exécutions de l'outil de suppression des logiciels malveillants. Consultez la section « Logiciels malveillants » du site Web du *Rapport sur les données de sécurité de Microsoft* pour plus d'informations sur la métrique en question.

Taux d'infection au niveau des systèmes d'exploitation

Figure 5. Taux d'infection (CCM) par système d'exploitation et par service pack au deuxième trimestre de 2011.



« 32 » = édition 32 bits ; « 64 » = édition 64 bits. SP = Service Pack. Systèmes d'exploitation pris en charge avec au moins 0,1 % du nombre total d'exécutions enregistrées pour le deuxième trimestre de 2011...

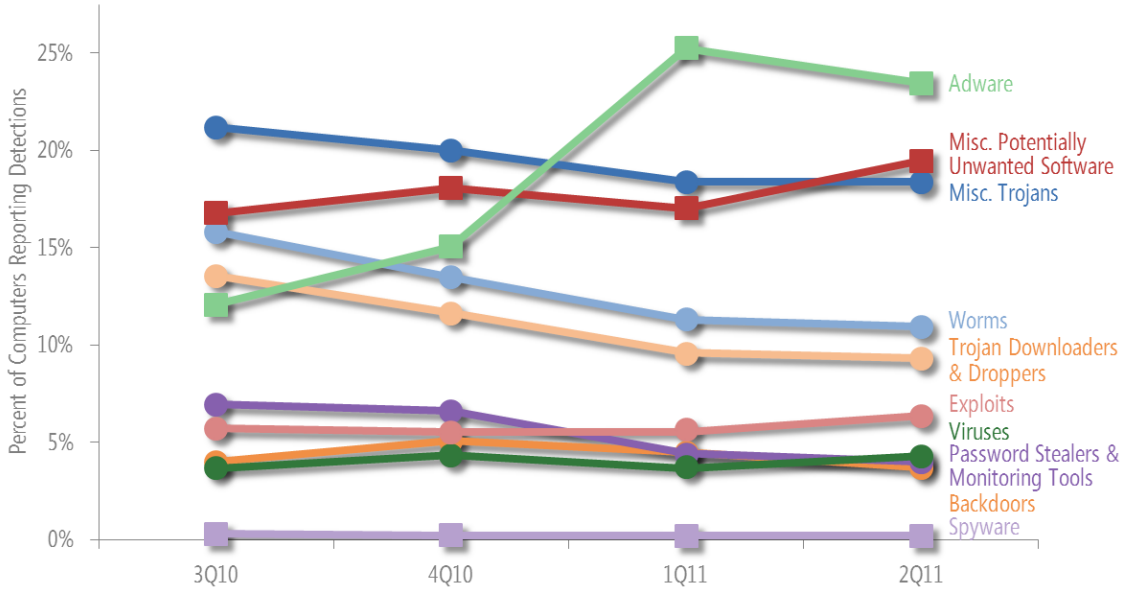
- Similairement aux périodes précédentes, les taux d'infection relatifs aux systèmes d'exploitation Microsoft et aux service packs plus récents sont sensiblement inférieurs aux taux précédents, au niveau des plateformes de clients et de serveurs. Windows 7 et Windows Server® 2008 R2, les versions

les plus récentes du client et du serveur Windows, enregistrent le taux d'infection le plus bas, comme le montre la Figure 4.

- Les taux d'infection pour Windows XP SP3 et Windows Vista ont chuté dès la publication, en février 2011, d'une mise à jour automatique qui a modifié la manière dont la fonction Exécution automatique fonctionne sur ces plateformes, afin que les fonctionnalités de ces dernières soient adaptées à Windows 7. L'effet de cette modification peut être observé dans les statistiques d'infection relatives à Win32/Rimecud, la neuvième catégorie de menaces la plus détectée et l'une des premières à exploiter la fonction Exécution automatique.

Familles et catégories de menaces

Figure 6. Détections par catégorie de menaces, entre le troisième trimestre de 2010 et le deuxième de 2011, par pourcentage de l'ensemble des ordinateurs signalant des détections



Les ronds correspondent aux catégories de logiciels malveillants, les carrés aux catégories de logiciels potentiellement indésirables.

- Win32/OpenCandy était la famille de menaces la plus couramment détectée de manière globale au premier semestre de 2011. OpenCandy est un logiciel de publicité qui peut être fourni avec certains programmes d'installation de logiciels tiers.

- JS/Pornpop, deuxième famille de menaces la plus communément détectée globalement au premier semestre de 2011, est un moyen de détection des

objets JavaScript spécialement conçus qui essaient d'afficher des publicités de type pop-under dans les navigateurs Web des utilisateurs.

- Win32/Hotbar, la famille de menaces la plus communément détectée au deuxième trimestre de 2011 et la troisième au premier semestre de 2011, est un logiciel de publicité qui installe une barre d'outils de navigateur qui affiche des annonces de type pop-up selon la manière dont il contrôle les activités de navigation Web.

- Les détections de Win32/FakeRean ont augmenté de plus de 300 % entre le premier et le deuxième trimestre de 2011 pour devenir la famille de logiciels de sécurité de serveurs non autorisés la plus communément détectée au second trimestre.

Menaces au niveau des entreprises

- Les familles de vers occupent les trois premières places des familles de logiciels malveillants les plus couramment détectés sur des ordinateurs appartenant à un domaine, une configuration plus commune aux environnements d'entreprises qu'aux environnements domestiques.

- Les familles de logiciels malveillants significativement plus fréquentes sur des ordinateurs appartenant à un domaine comprennent Win32/Conficker et le logiciel potentiellement indésirable Win32/RealVNC. RealVNC est un programme permettant à un ordinateur d'être contrôlé à distance, à l'instar des Services de Bureau à distance. Celui-ci compte un nombre d'utilisations autorisées, mais les utilisateurs malveillants l'ont également utilisé pour prendre le contrôle d'ordinateurs d'utilisateurs à des fins malveillantes.

- La famille de virus Win32/Sality, qui ne faisait pas partie des dix familles les plus détectées sur des ordinateurs appartenant à un domaine en 2010, occupe désormais la neuvième place du classement au premier semestre de 2011.

Menaces au niveau du courrier électronique

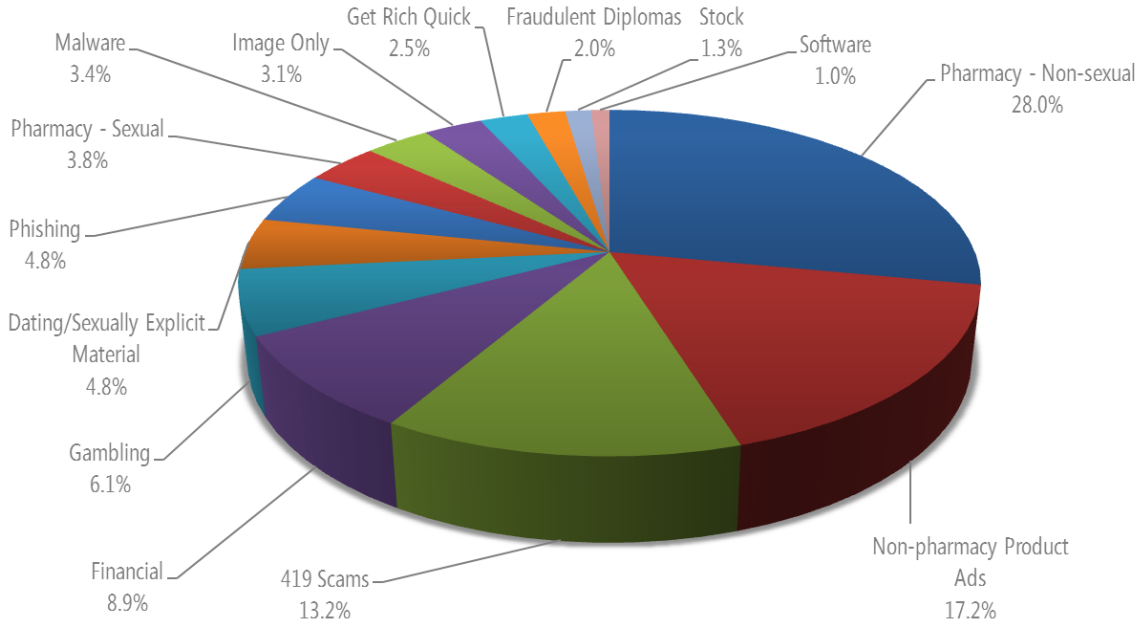
- Le volume de courrier indésirable bloqué par Microsoft Forefront® Online Protection for Exchange (FOPE) a sensiblement chuté au cours des 12 derniers mois, à savoir de 89,2 milliards de messages en juillet 2010 à 25 milliards en juin 2011, principalement en raison de la mise hors service des deux botnets principaux : Cutwail, mis hors service en août 2010, et

Rustock, mis hors service en mars 2011, à la suite d'une période de latence qui a débuté au mois de janvier[1].

- Similairement aux périodes précédentes, les publicités pour des produits pharmaceutiques non sexuels (28 % du total) et pour des produits non pharmaceutiques (17,2 %) représentent la majeure partie des messages indésirables bloqués par les filtres de contenu de FOPE au premier semestre de 2011.

- La proportion de messages indésirables composés uniquement d'une image a chuté à 3,1 % du total au premier semestre 2011, soit un recul par rapport aux 8,7 % de 2010.

Image 7. Messages entrants bloqués par les filtres de FOPE au premier semestre de 2011, par catégorie



Sites Web malveillants

- Les hameçonneurs ont généralement ciblé des sites financiers plutôt que d'autres types de sites. Toutefois, la majeure partie des impressions de hameçonnage signalées au premier semestre de 2011 concernaient des sites

[1] Pour plus d'informations sur la mise hors service de Cutwail, consultez le *Rapport sur les données de sécurité de Microsoft, Volume 10 (juillet-décembre 2010)*. Pour plus d'informations sur la mise hors service de Rustock, consultez le rapport « Combattre la menace Rustock » disponible dans le Centre de téléchargement Microsoft.

qui ciblaient des réseaux sociaux, avec un pic de détections de 83,8 % pour le mois d'avril. (Une exposition à l'hameçonnage correspond à une instance où un utilisateur essaie de visiter un site de hameçonnage connu à l'aide de Windows Internet Explorer® qui se trouve être bloqué par le filtre SmartScreen®. Consultez la section « Sites Web malveillants » du site Web du Rapport sur les données de sécurité de Microsoft pour plus d'informations.) Dans l'ensemble, les expositions à l'hameçonnage qui ciblaient les réseaux sociaux ont représenté 47,8 % de l'ensemble des expositions à l'hameçonnage au premier semestre de 2011, suivies par celles ciblant des institutions financières (35 %).

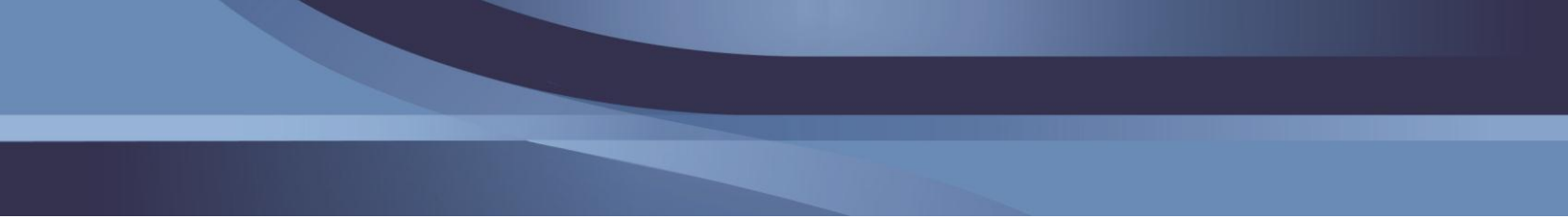
- En comparaison, les sites de hameçonnage qui ciblaient des institutions financières représentaient en moyenne 78,3 % des sites de hameçonnage actifs signalés chaque mois au cours du premier semestre de 2011, par rapport aux seuls 5,4 % de sites de hameçonnage ciblant les réseaux sociaux. Les institutions financières ciblées par des hameçonneurs peuvent se compter par centaines, et des approches de hameçonnage personnalisées sont nécessaires pour chacune d'elles. Le nombre de sites de réseaux sociaux étant nettement inférieur, les hameçonneurs s'attaquant à ces derniers peuvent cibler bien plus de personnes par site. Malgré tout, les possibilités d'accès illégal direct aux comptes bancaires des victimes impliquent que les institutions financières demeurent des sites de hameçonnage sollicités ; elles se placent à la deuxième, voire à la première place, du classement du nombre d'impressions par mois.

- Ce phénomène se rencontre également à échelle réduite au niveau des services en ligne et des sites de jeux. Un nombre réduit de services en ligne représente la majeure partie du trafic vers de tels sites ; ainsi les sites de hameçonnage qui ciblaient des services en ligne constituaient 11 % des impressions avec seulement 3,6 % de sites. Le trafic relatif aux jeux en ligne a tendance à s'étendre à un grand nombre de sites. De ce fait, les sites de hameçonnage qui ciblaient des destinations de jeux en ligne représentaient 8,9 % des sites actifs, mais n'enregistraient que 4,3 % des impressions.

Par ailleurs, les sites de hameçonnage qui ciblaient le commerce en ligne ne représentaient que 3,8 % des sites actifs et 1,9 % des impressions. Cette tendance indique que les hameçonneurs n'ont pas jugé que les sites de commerce en ligne étaient des cibles particulièrement intéressantes.

Vous trouverez des informations sur la Protection de votre organisation, de vos logiciels et de votre personnel à la section « Gestion du risque » du site Web du *Rapport sur les données de sécurité* de *Microsoft*

http://www.microsoft.com/sir



Microsoft
1 Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security