Rapport Microsoft sur les données de sécurité, volume 6 (juillet à décembre 2008)

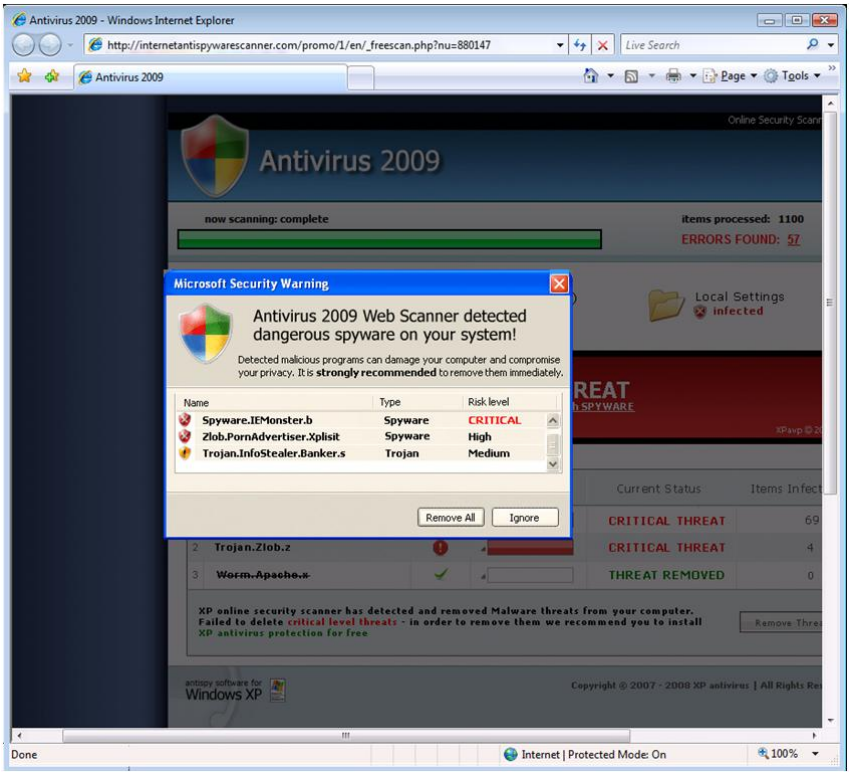
Synthèse des principaux constats

Ce sixième volume du rapport Microsoft® sur les données de sécurité présente l'ensemble des vulnérabilités logicielles (pour les logiciels Microsoft comme pour ceux d'éditeurs tiers), codes exploitant une vulnérabilité de sécurité, logiciels malveillants et logiciels potentiellement indésirables observés par Microsoft au cours des dernières années, avec une attention particulière sur le deuxième semestre 2008 (2S08)[1]. Le rapport contient également des informations sur les faux logiciels de sécurité (rogues), les attaques sur les navigateurs et sur les formats de documents courants, ainsi que des informations actualisées sur la sécurité et le non-respect de la vie privée.

Ce document constitue une synthèse des principaux constats du rapport. Le rapport intégral sur les données de sécurité propose également des stratégies de réduction des risques ainsi que des mesures défensives. Il est téléchargeable à l'adresse suivante : http://www.microsoft.com/france/sir.

Faux logiciels de sécurité

- La prédominance des faux logiciels de sécurité a augmenté de manière significative au cours des trois dernières périodes (voir la figure 16 sur les divers chevaux de Troie ci-dessous). Les faux logiciels de sécurité ont recours à des stratégies basées sur la peur et l'agacement pour convaincre les victimes d'acheter une « version complète » censée leur permettre de se protéger des logiciels malveillants, de les supprimer et de stopper les alertes ou avertissements continuels. Des exemples avec captures d'écran de techniques d'ingénierie sociale liés aux faux logiciels de sécurité peuvent être trouvés dans la version complète du Rapport sur les données de sécurité. Ce rapport met également en relief les actions en justice intentées contre les distributeurs de faux logiciels de sécurité.



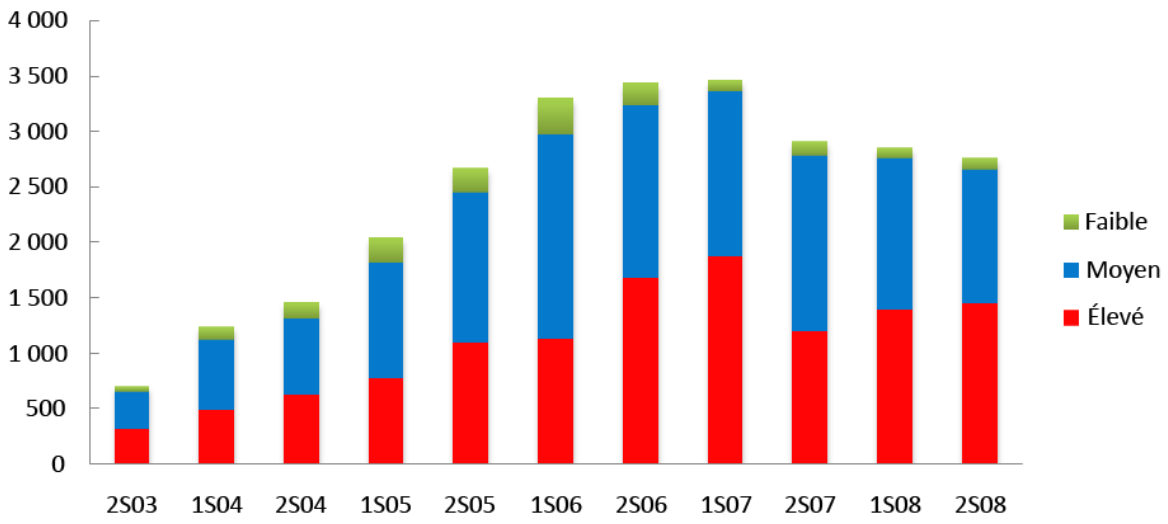
[1] La convention utilisée dans l'ensemble de ce document pour faire référence à différentes périodes d'étude du rapport est nSAA, où nS désigne le premier (1) ou le second (2) semestre de l'année et AA représente l'année. Par exemple, 2S08 représente le second semestre 2008 (du 1er juillet au 31 décembre 2008), tandis que 1S08 représente le premier semestre 2008 (du 1 janvier au 30 juin 2008).

Divulgations de vulnérabilités

Les vulnérabilités sont définies comme les points faibles d'un logiciel permettant à un attaquant de compromettre l'intégrité, la disponibilité ou la confidentialité de ce logiciel. Dans le pire des cas, ces vulnérabilités peuvent permettre aux pirates d'exécuter du code arbitraire sur des systèmes compromis. Les données relatives aux vulnérabilités présentées dans cette section ont été recueillies auprès de sources tierces, dans des rapports publiés et parmi les données Microsoft.

- Le nombre total de divulgations de vulnérabilités uniques dans le secteur a diminué sur 2S08 de 3 % par rapport à 1S08. Pour l'ensemble de l'année 2008, le nombre total de divulgations a diminué de 12 % par rapport à 2007.
- À l'inverse, les vulnérabilités d'indice Élevé, tel que défini par le Common Vulnerability Scoring System (CVSS)[2], ont augmenté de 4 % sur 1S08, représentant 52 % de l'ensemble des vulnérabilités. Sur l'année 2008, le nombre total de vulnérabilités d'indice Élevé a diminué de 16 % par rapport à 2007.

Figure 1. Divulgations de vulnérabilités par semestre (de 1S03 à 2S08) pour l'ensemble du secteur, classées par degré de gravité selon le standard CVSSv2

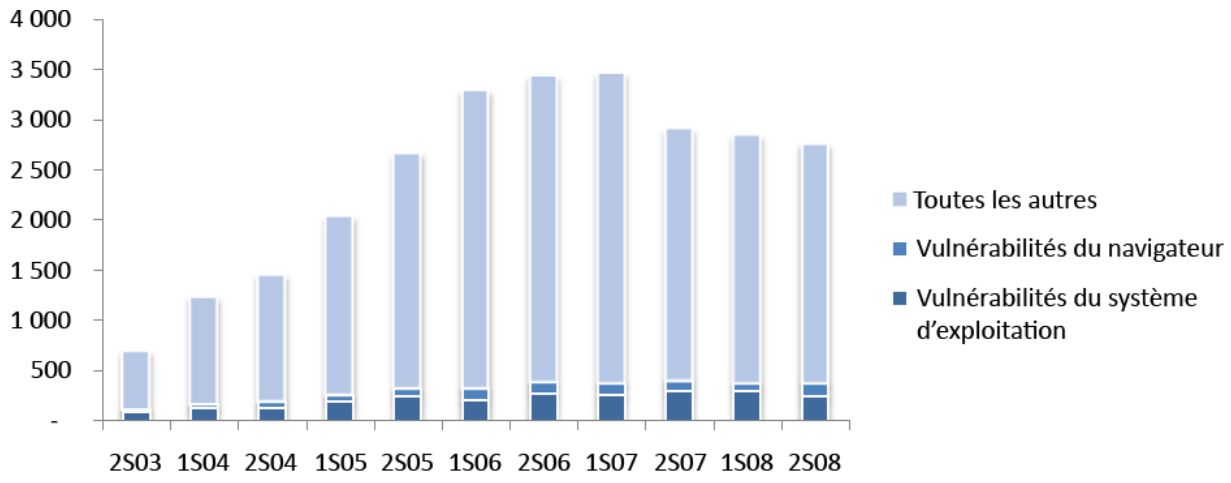


- S'ajoutant au problème soulevé par les vulnérabilités d'indice Élevé, le pourcentage des vulnérabilités faciles à exploiter a augmenté, atteignant maintenant 56 %[3].
- La part des vulnérabilités divulguées concernant les systèmes d'exploitation de l'ensemble des éditeurs continue à diminuer : plus de 90 % des vulnérabilités déclarées concernent des applications ou des navigateurs.

[2] Le CVSS est un standard utilisé par les différents éditeurs pour évaluer le niveau de gravité des vulnérabilités logicielles. Consultez http://www.first.org/cvss/ pour obtenir plus d'informations sur CVSS.

[3] Définition tirée de : Mell, Peter, Karen Scarfone et Sasha Romanosky. « A Complete Guide to the Common Vulnerability Scoring System Version 2.0 » (http://www.first.org/cvss/cvss-guide.html) section 2.1.2.

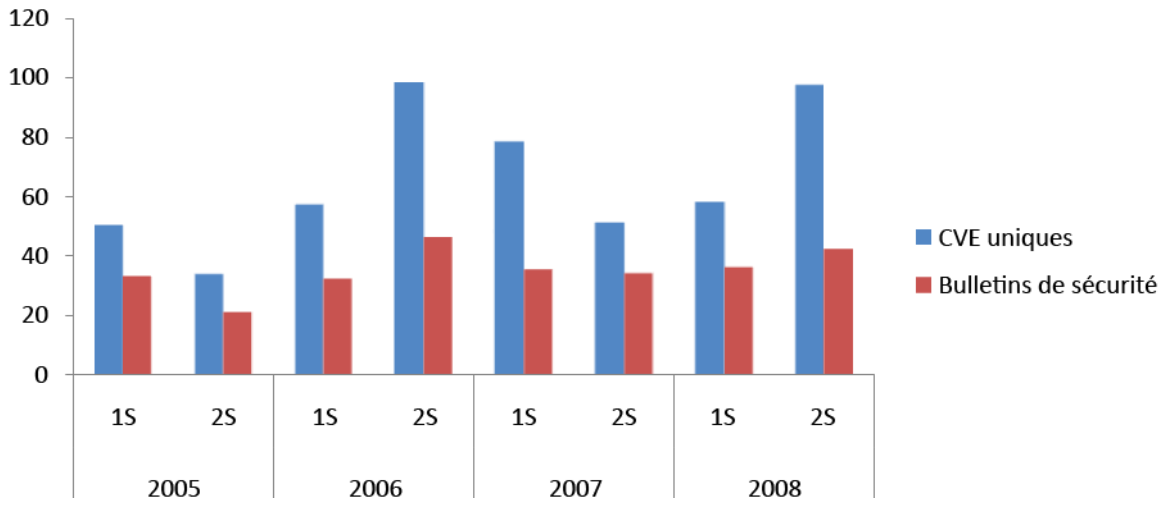
Figure 2. Vulnérabilités de systèmes d'exploitation, navigateurs et autres pour l'ensemble du secteur, 2S03–2S08



Précisions sur les vulnérabilités concernant Microsoft au cours du second semestre 2008

Au cours du second semestre 2008, Microsoft a publié 42 bulletins de sécurité concernant 97 vulnérabilités CVE (Common Vulnerabilities and Exposures), un chiffre en hausse de 67,2 % par rapport au premier semestre 2008. Pour l'ensemble de l'année 2008, Microsoft a diffusé 78 bulletins de sécurité concernant 155 vulnérabilités, soit une hausse de 16,8 % par rapport à 2007.

Figure 3. Bulletins de sécurité publiés et vulnérabilités CVE traitées par semestre, 1S05-2S08

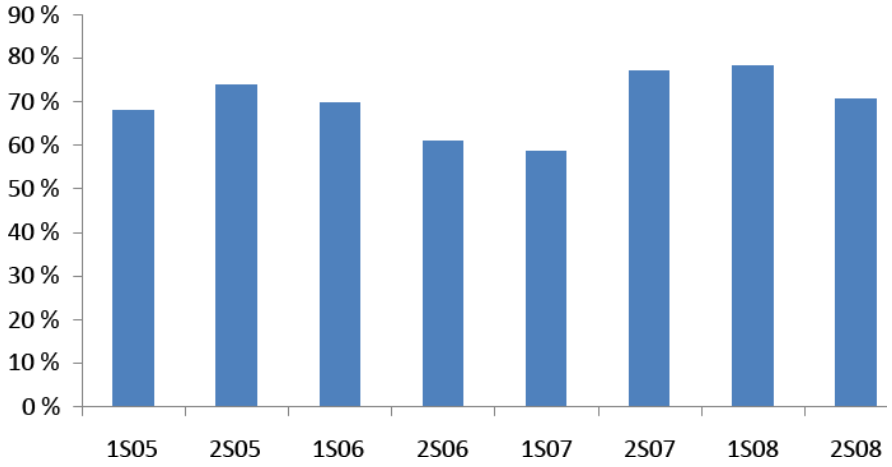


Divulgation responsable

L'expression « *divulgation responsable* » est le respect de la confidentialité lors de la communication d'une vulnérabilité à l'éditeur afin qu'il puisse la corriger avant qu'elle ne soit rendue publique. La sécurité des utilisateurs est ainsi renforcée, les personnes malveillantes n'étant pas en mesure de prendre connaissance des nouvelles vulnérabilités avant que les mises à jour ne soient disponibles.

- Au cours du second semestre 2008, 70,6 % des divulgations de vulnérabilités Microsoft ont respecté cette pratique de divulgation responsable, une baisse par rapport aux 78,2 % constatés le premier semestre de cette même année. Le pourcentage de divulgations responsables pour l'ensemble de l'année 2008 est nettement supérieur à celui de l'année précédente.
- Grâce aux relations directes avec la communauté sécurité et au traitement proactif des problèmes de sécurité, la majorité des vulnérabilités ont été signalées de manière responsable.

Figure 4. Pourcentage des divulgations responsables par rapport à l'ensemble des divulgations, 1S05-2S08



Attaques basées sur le navigateur

Pour estimer la prédominance relative des attaques véhiculées par navigateur sur 2S08, Microsoft a analysé un échantillon de données obtenues à partir d'incidents signalés par les utilisateurs, de codes malveillants soumis et de rapports d'erreur de Microsoft Windows®. Ces données englobent plusieurs versions de systèmes d'exploitation et de navigateurs, de Windows XP à Windows Vista®. Elles comprennent également des données de navigateurs tiers qui intègrent le moteur de rendu d'Internet Explorer, appelé Trident.[4]

- L'anglais américain a été la langue des systèmes d'exploitation la plus touchée par ces attaques véhiculées par navigateur (32,4 %), suivi par le chinois simplifié (25,6 %).
- Les vulnérabilités Microsoft ont représenté 40,9 % des attaques véhiculées par navigateur sous Windows XP (42,0 % au 1S08). Sur les ordinateurs exécutant Windows Vista, la part des vulnérabilités Microsoft a été bien moindre, seulement 5,5 % du nombre total, un chiffre en baisse par rapport aux 6,0 % du premier semestre 2008.

[4] Pour plus d'informations sur Trident, consultez l'article à l'adresse http://msdn.microsoft.com/library/aa939274.

Figure 5. Attaques basées sur le navigateur ciblant les logiciels Microsoft, ciblant les logiciels tiers, sous Windows XP, 2S08

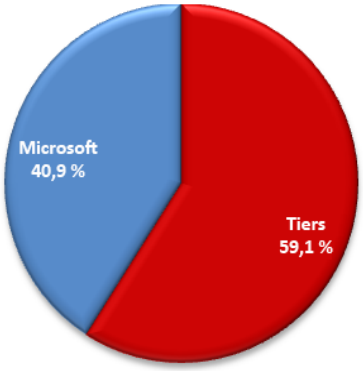
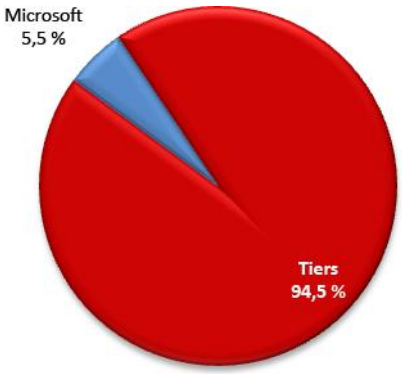


Figure 6. Attaques basées sur le navigateur ciblant les logiciels Microsoft, ciblant les logiciels tiers, sous Windows Vista, 2S08



- Les logiciels Microsoft comprennent 6 des 10 vulnérabilités basées sur le navigateur ayant fait l'objet d'attaque sous Windows XP au cours de 2S08, mais aucune sur les ordinateurs fonctionnant sous Windows Vista - ce qui est similaire à ce qui a été observé au premier semestre. Les chiffres ci-dessous présentent les 10 vulnérabilités basées sur le navigateur ayant fait l'objet d'attaques sous Windows XP et sous Windows Vista. Ces vulnérabilités sont référencées par leur numéro de bulletin CVSS ou de Bulletin de sécurité Microsoft.

Figure 7. 10 principales attaques de vulnérabilités basées sur le navigateur sous Windows XP, 2S08

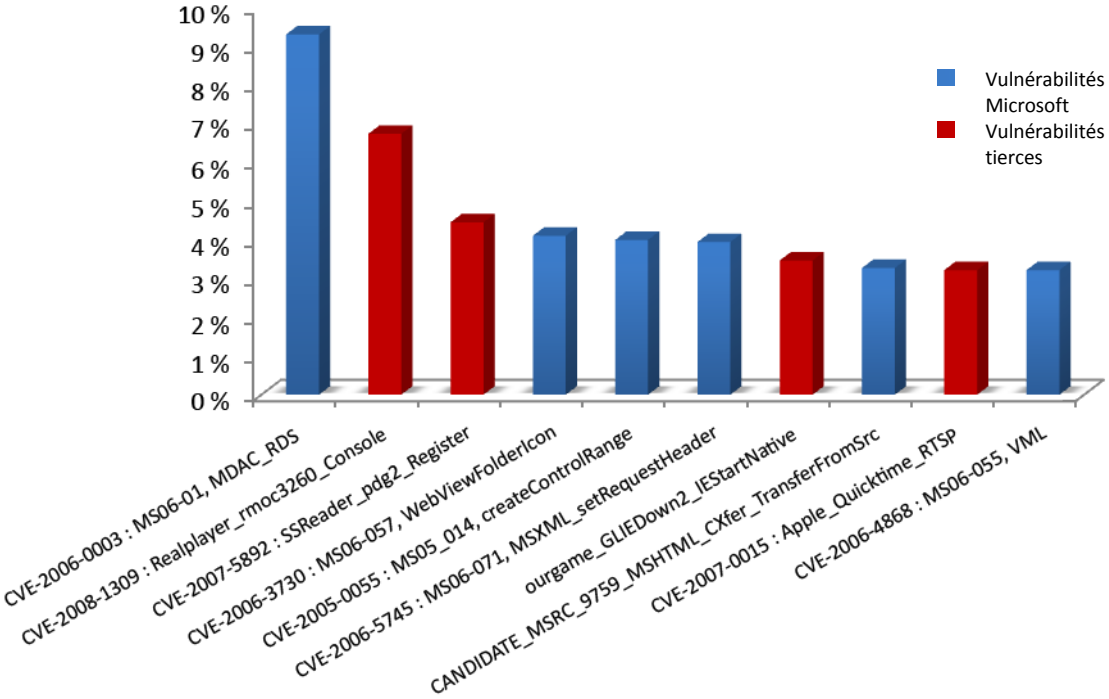
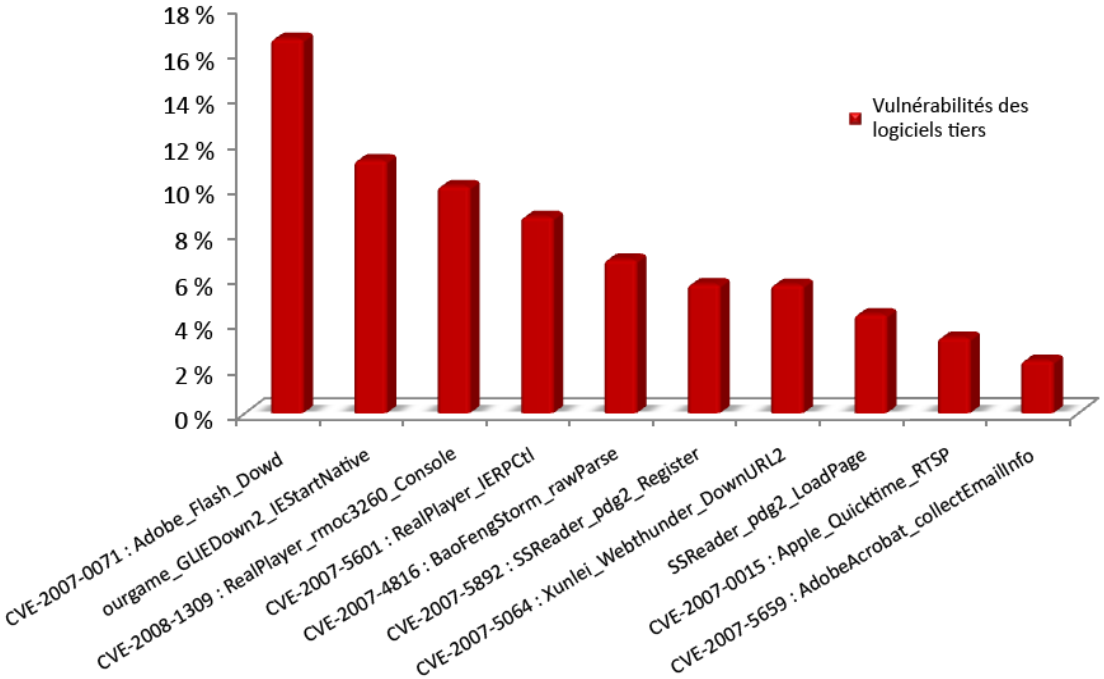


Figure 8. 10 principales attaques de vulnérabilités basées sur le navigateur sous Windows Vista, 2S08



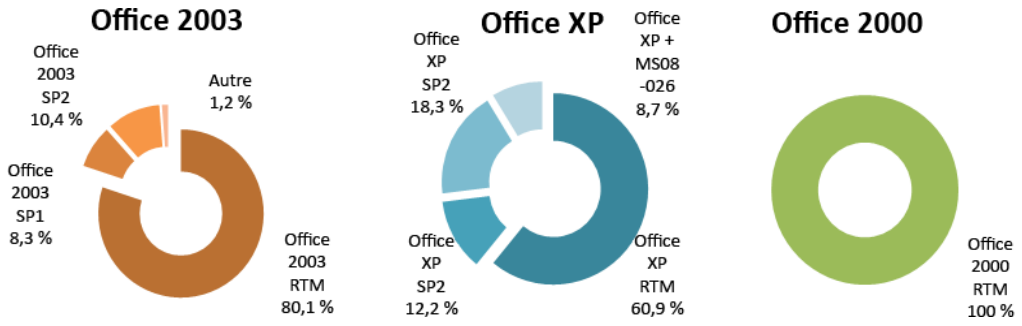
Codes d'exploitation concernant les formats de documents

De plus en plus, les attaquants utilisent les formats de fichier courants comme vecteur d'attaque. Les programmes de messagerie électronique ou instantanée les plus modernes sont configurés pour bloquer la transmission de fichiers potentiellement dangereux en fonction de leur extension. Cependant, ces programmes autorisent généralement la transmission de formats de fichier courants comme ceux de Microsoft Office ou d'Adobe PDF (Portable Document Format). Ces formats sont utilisés par de nombreuses personnes chaque jour. Par conséquent, il est difficile de les bloquer. Ils sont donc devenus une cible de choix pour les créateurs de codes malveillants.

Fichiers au format Microsoft Office

- Les vulnérabilités Microsoft Office les plus fréquemment exploitées sont également les plus anciennes. 91,3 % des attaques étudiées exploitaient une seule vulnérabilité pour laquelle un correctif de sécurité était disponible depuis plus de deux ans (CVE-2006-2492).
- L'anglais américain a été la langue la plus touchée (32,5 %), suivi par le chinois simplifié (15,7 %).
- Dans la plupart des cas, les applications attaquées n'avaient pas le niveau de service pack à jour. Pour chaque version, une nette majorité des attaques concernait la version RTM (Release to Manufacturing) de la suite d'applications sur laquelle aucun service pack n'était installé. Pour Office 2000 par exemple, 100 % des attaques concernaient la version RTM, lancée en 1999, malgré les nombreux service packs et autres mises à jour de sécurité publiés.

Figure 9. Attaques par niveau de mise à jour pour Office 2003, Office XP et Office 2000, parmi les ordinateurs infectés, 2S08

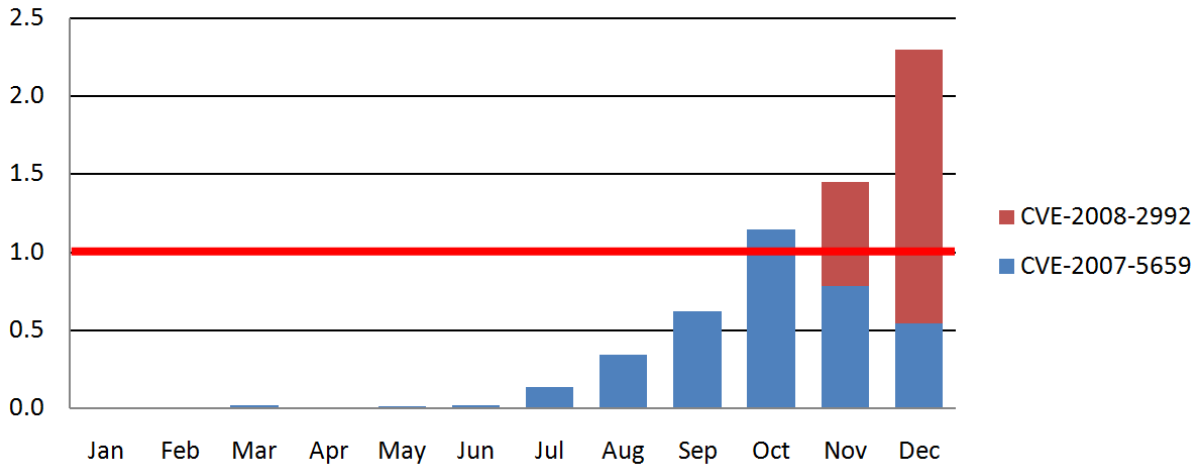


Fichiers au format Adobe PDF

L'utilisation du format PDF comme vecteur d'attaque a explosé au second semestre 2008. Le nombre d'attaques du mois de juillet représente en effet une hausse de plus de 100 % par rapport à l'ensemble des attaques du premier semestre 2008. Ce pourcentage double ou presque pour chacun des derniers mois de l'année.

- Deux vulnérabilités représentent l'ensemble des attaques dans les fichiers échantillon étudiés (CVE-2008-2992 et CVE-2007-5659). Ces deux vulnérabilités sont traitées par des mises à jour de sécurité Adobe ; aucune n'existe dans les versions actuelles des produits Adobe affectés.

Figure 10. Exploits concernant Adobe Reader par mois en 2008, indexées sur la moyenne de 2S08



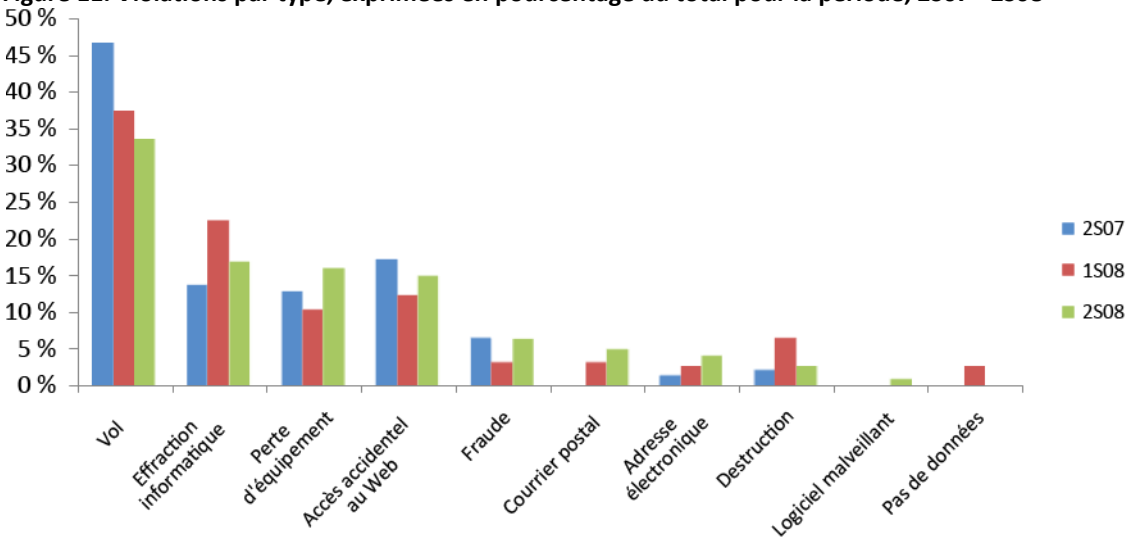
Tendances des violations de sécurité

Cette section du rapport examine en détail les violations de sécurité enregistrées dans le monde, en s'appuyant sur des données fournies par la base de données Data Loss Database de l'Open Security Foundation, consultable à l'adresse suivante : http://datalossdb.org.

- La principale raison invoquée lors de la perte de données consécutive à une violation de sécurité au cours de 2S08 est toujours le vol d'équipement, tel que les ordinateurs portables (33,5 % de toutes les pertes de données). La perte et le vol d'équipement représentent ensemble 50 % des incidents signalés.
- Les violations de sécurité liées aux attaques de pirates ou les incidents relatifs aux logiciels malveillants représentent moins de 20 % du total.
- Ces constats confirment la nécessité de mettre en place des procédures et des stratégies de gouvernance appropriées concernant la protection des données[5].

[5] Microsoft fournit des conseils et des ressources sur la gouvernance de données à l'adresse suivante : http://www.microsoft.com/france/securite/twc/privacy/datagovernance/default.mspx

Figure 11. Violations par type, exprimées en pourcentage du total pour la période, 2S07 - 2S08



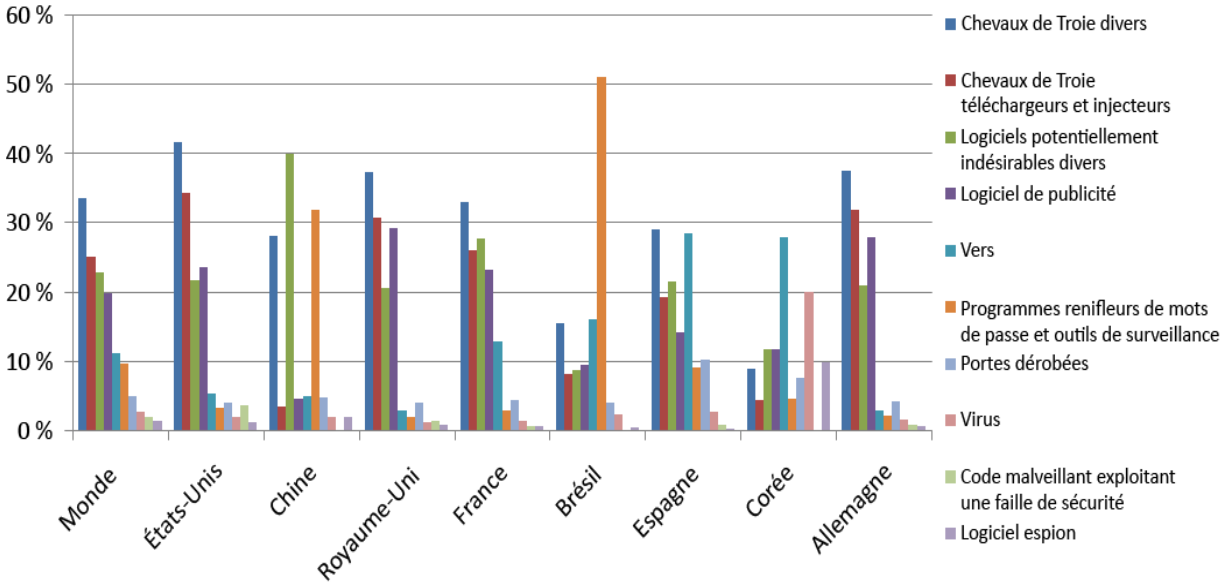
Logiciels malveillants et potentiellement indésirables

Tendances mondiales

Les produits de sécurité Microsoft recueillent, avec le consentement des utilisateurs, des informations en provenance de millions d'ordinateurs et de services en ligne parmi les plus populaires d'Internet. L'analyse de ces données présente de manière complète et unique les événements concernant les programmes malveillants et les logiciels potentiellement indésirables signalés dans le monde entier.

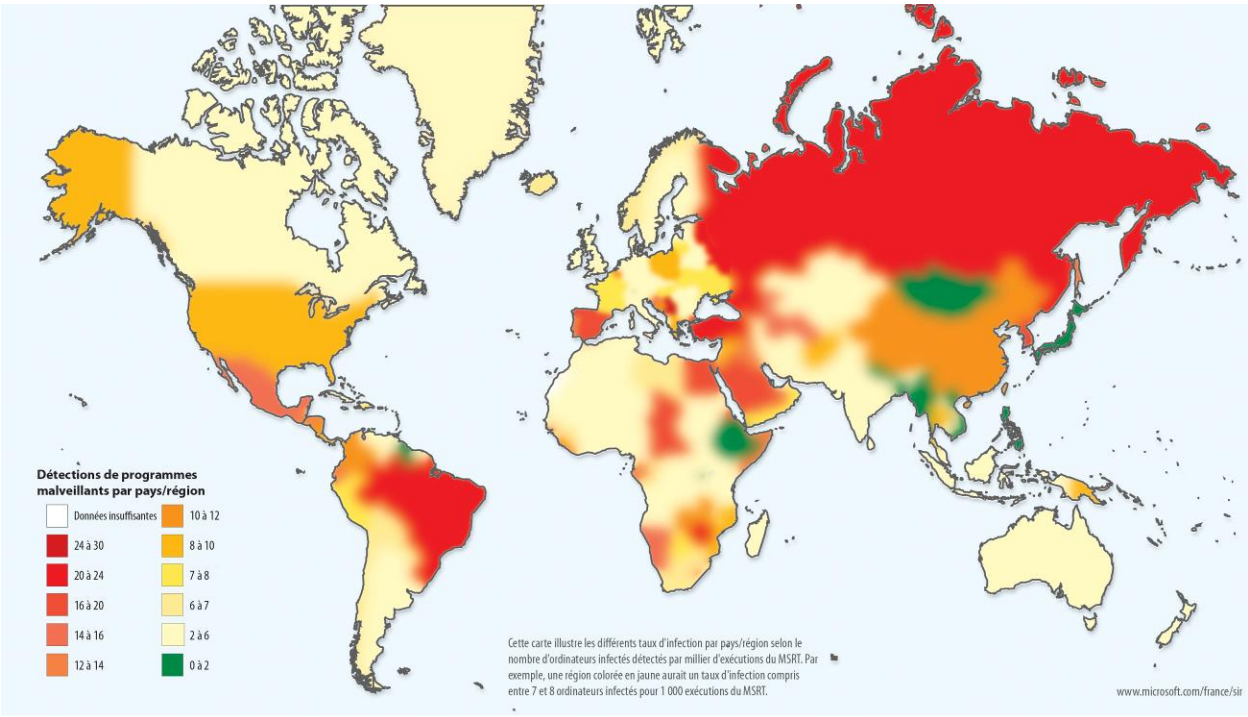
- Internet est, par définition, de nature globale. Cependant, il existe des différences dans les menaces ciblant les internautes selon les régions du monde. Plus les logiciels malveillants utilisent l'ingénierie sociale, plus les menaces dans le monde dépendent de facteurs linguistiques et culturels : en Chine, plusieurs modificateurs malveillants de navigateur sont très répandus, au Brésil il s'agit de logiciels malveillants visant les utilisateurs de services bancaires en ligne et en Corée des virus tels que Win32/Virut et Win32/Parite.

Figure 12. Catégories de menaces au niveau mondial et dans les huit pays possédant le plus grand nombre d'ordinateur nettoyés, par incidence sur l'ensemble des ordinateurs nettoyés, 2S08



- La carte suivante illustre les taux d'infection de diverses régions du monde, exprimés en nombre d'ordinateurs nettoyés par millier[6].

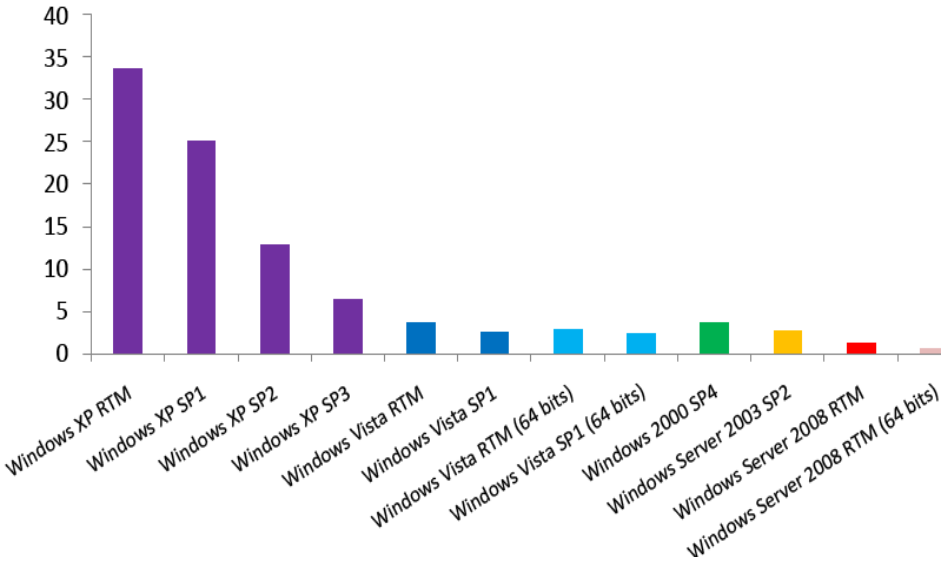
Figure 13. Taux d'infection par pays/région, 2S08



Tendances relatives aux systèmes d'exploitation

- Les différentes versions du système d'exploitation Microsoft Windows présentent différents taux d'infection en fonction de leur utilisation par les personnes et les organisations et des fonctionnalités et service packs disponibles pour chacune d'entre elles.

Figure 14. Nombre d'ordinateurs nettoyés pour 1 000 exécutions de MSRT, par système d'exploitation, 2S08



[6] Les taux d'infection contenus dans ce rapport sont exprimés à l'aide d'une mesure appelée CCM (Computers Cleaned per Mil), qui représente le nombre d'ordinateurs nettoyés pour mille exécutions du MSRT.

- Le taux d'infection pour Windows Vista est bien inférieur à celui de son prédécesseur, Windows XP, quelle que soit la configuration.
  - Par rapport aux derniers service packs de chaque version, le taux d'infection de Windows Vista SP1 est inférieur de 60,6 % à celui de Windows XP SP3.
  - Par rapport aux versions RTM de ces systèmes d'exploitation, le taux d'infection de la version RTM de Windows Vista est inférieur de 89,1 % à celui de la version RTM de Windows XP.
- Le taux d'infection de Windows Server 2008 version RTM, est inférieur de 52,6 % à son prédécesseur, Windows Server 2003 SP2.
- Plus le niveau du service pack est élevé, plus le taux d'infection est bas. Cette tendance s'observe à la fois au sein des systèmes d'exploitation serveur et client. Il y a deux raisons qui l'expliquent :
  - Les service packs incluent l'ensemble des mises à jour de sécurité déjà publiées. Ils peuvent également comporter des fonctionnalités de sécurité supplémentaires, des solutions d'atténuation des menaces et des modifications qui ont pu être apportées aux paramètres par défaut afin de protéger les utilisateurs.
  - En règle générale, les utilisateurs ayant recours aux service packs entretiennent mieux leurs ordinateurs que les autres et font également plus attention lorsqu'ils naviguent sur Internet, ouvrent des pièces jointes ou lors de diverses activités qui pourraient rendre leurs ordinateurs vulnérables aux attaques.
- Les versions serveur de Windows affichent un taux d'infection inférieur en moyenne à celui des versions client. En effet, les serveurs présentent généralement une surface d'attaque effective moindre par rapport aux ordinateurs exécutant des systèmes d'exploitation client, car ils sont souvent utilisés par des administrateurs expérimentés dans un environnement sous contrôle et ils bénéficient d'une ou de plusieurs couches de sécurité. En particulier, Windows Server 2003 et ses successeurs disposent d'une protection contre les attaques renforcée de différentes manières, ce qui reflète cette différence dans l'utilisation.

Les menaces contre les particuliers et les entreprises

Les ordinateurs exécutant Forefront Client Security (utilisé habituellement dans les environnements d'entreprise) ont été plus susceptibles d'avoir à traiter des vers que les ordinateurs de particuliers exécutant Windows Live OneCare. Les ordinateurs de particuliers ont également connu les pourcentages les plus élevés d'attaques par chevaux de Troie, chevaux de Troie téléchargeurs et injecteurs, logiciels de publicité et codes exploitant une vulnérabilité. Les deux produits ont détecté des pourcentages similaires d'attaques par portes dérobées et logiciels espion.

.

Figure 15. Catégories de menaces supprimées par Windows Live OneCare et ForeFront Client Security, par pourcentage du nombre total d'ordinateurs nettoyés par chaque programme, 2S08

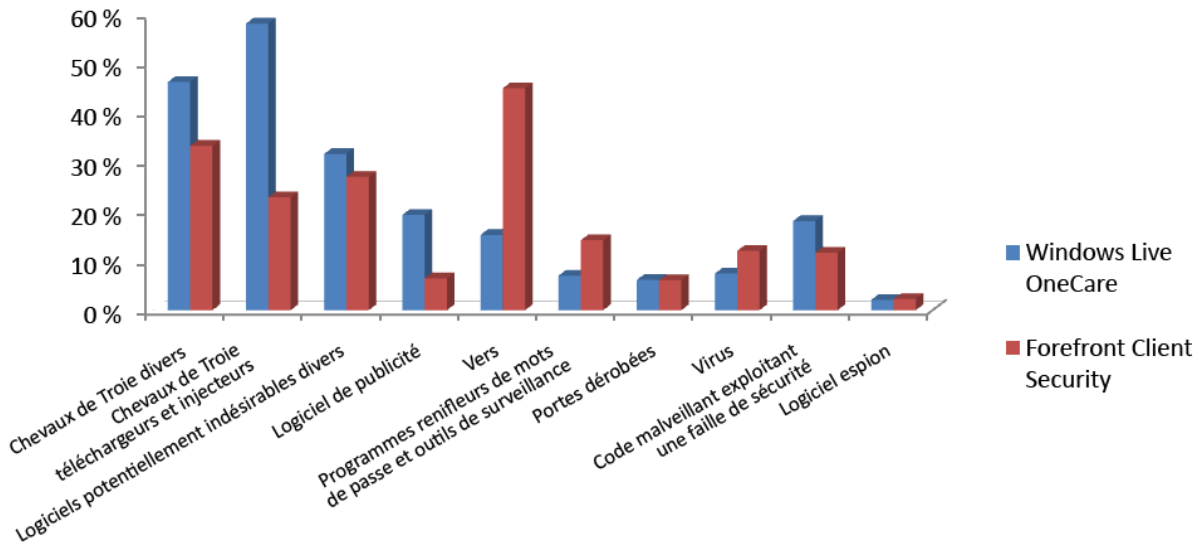
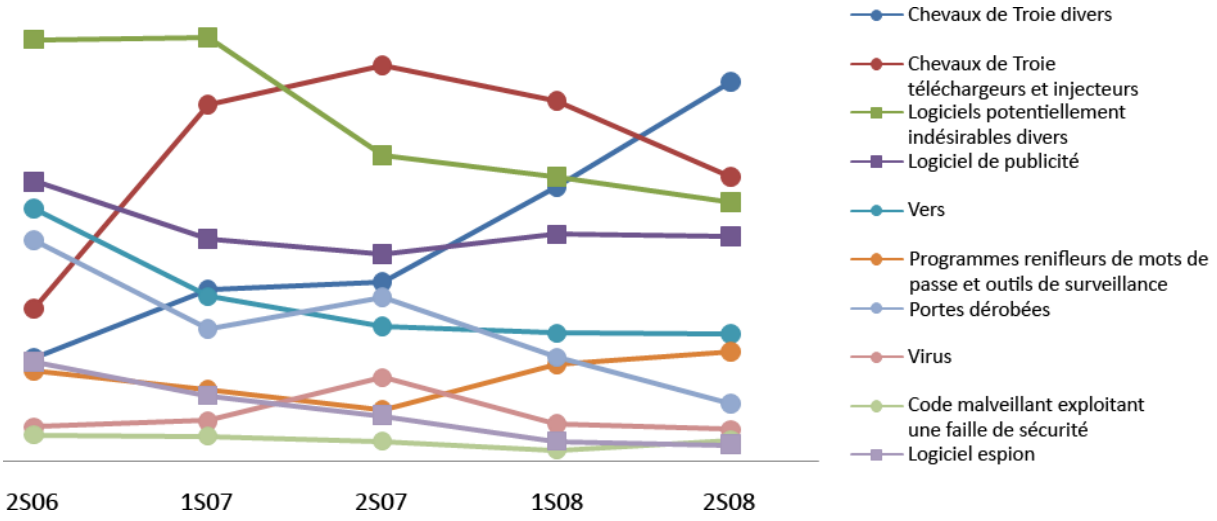


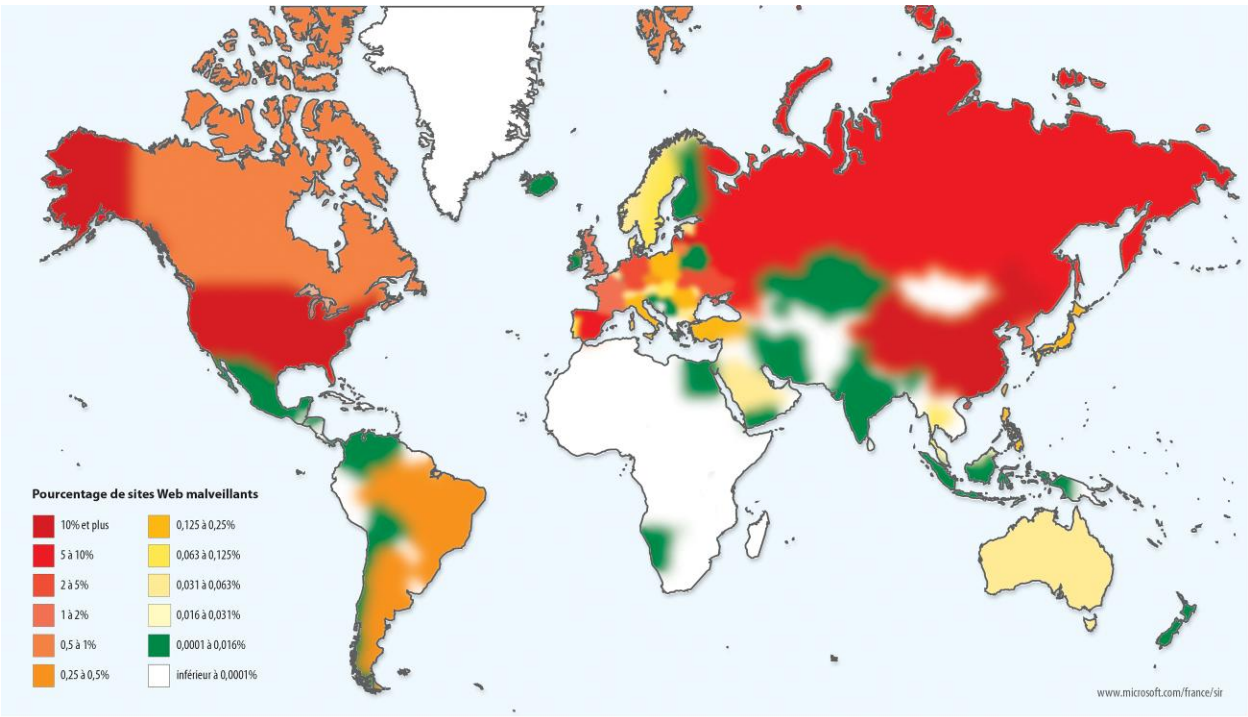
Figure 16. Ordinateurs nettoyés par catégorie de menace, en pourcentage, 2S06 - 2S08



Répartition géographique des pages malveillantes

L'hébergement des logiciels malveillants a tendance à être plus durable et moins réparti géographiquement que l'hébergement des sites de phishing. Ce phénomène résulte sans doute de l'utilisation encore assez récente de la neutralisation de serveurs et de la réputation sur le Web comme armes permettant de lutter contre la diffusion de logiciels malveillants. Ainsi, les distributeurs de logiciels malveillants n'ont pas été forcés à diversifier leurs méthodes d'hébergement. La figure 17 montre la répartition géographique des sites d'hébergement de logiciels malveillants signalés à Microsoft au niveau mondial au cours du second semestre 2008.

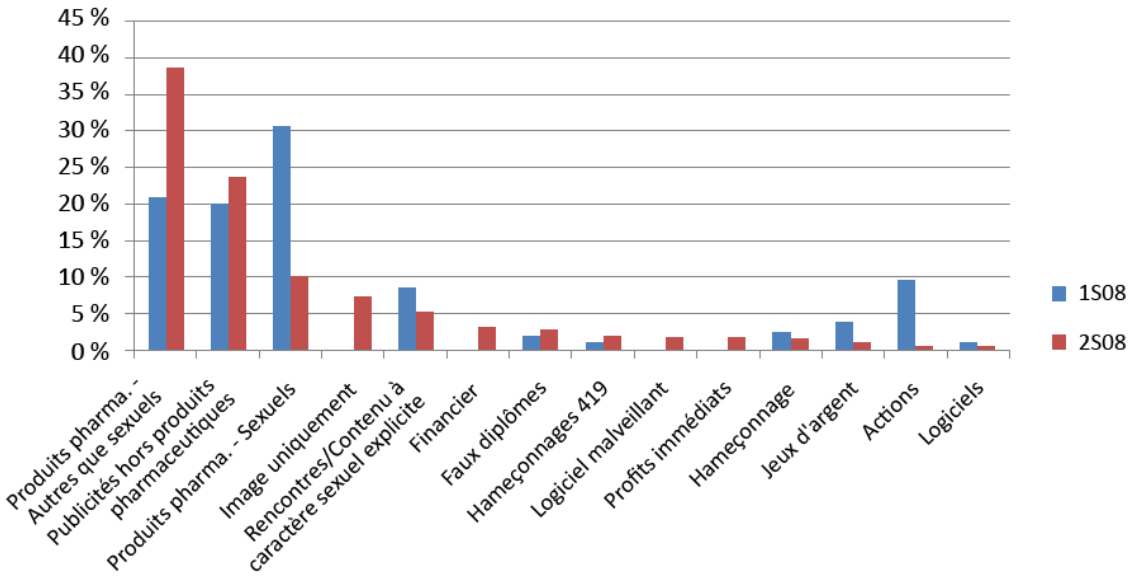
Figure 17. Sites d'hébergement de logiciels malveillants détectés par pays/région (nombre indexé sur la moyenne de l'ensemble des lieux), 2S08



Menaces par messagerie électronique

- Plus de 97 % des messages électroniques envoyés sont indésirables : ils comportent des pièces jointes malveillantes, véhiculent des attaques de phishing ou sont du spam.
- À l'instar des périodes précédentes, le spam constaté au second semestre 2008 était principalement constitué de publicités pour des produits divers, avec une majorité de produits pharmaceutiques (48,6 % du total). En incluant les publicités pour des produits non pharmaceutiques (23,6 % du total), les publicités pour des produits divers représentent 72,2 % du courrier indésirable reçu au cours du second semestre 2008.

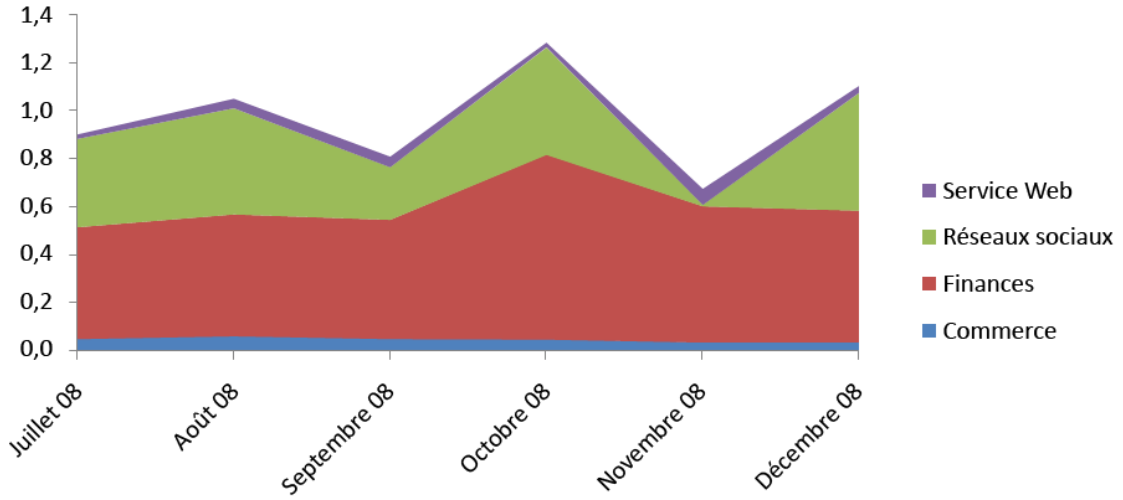
Figure 19. Messages entrants bloqués par les filtres de contenu Exchange Hosted Services, par catégorie, 1S08-2S08



Sites Web malveillants

La majorité des pages de phishing cible les organisations financières. Toutefois, en termes d'exposition (tentatives d'ouverture d'une page de phishing connue), les réseaux sociaux sont aussi fréquemment touchés.

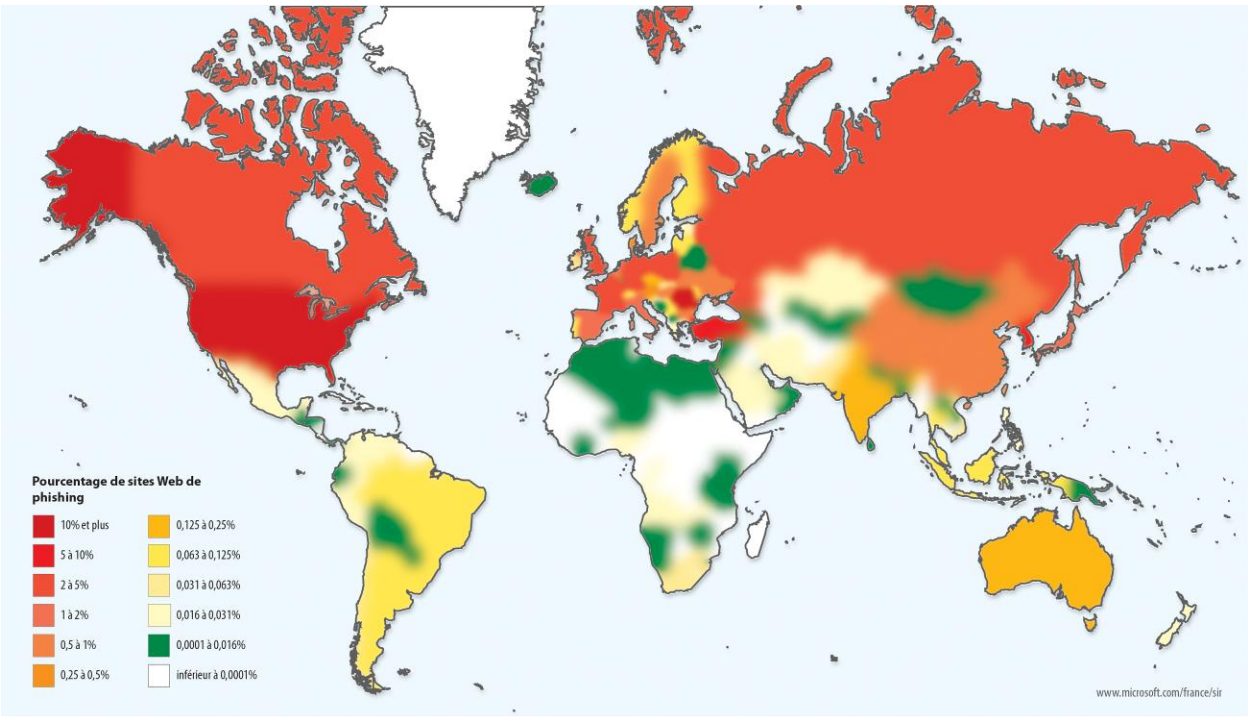
Figure 20. Expositions par mois pour chaque type de page de phishing (nombre indexé sur la moyenne des expositions mensuelles pour cette période), 2S08



- La fermeture de McColo courant novembre semble avoir eu un impact considérable sur les expositions au phishing. Celles-ci ont en effet chuté de 46,2 % entre octobre et novembre. Sur l'ensemble des expositions, les visites de pages de phishing ciblant les sites de réseaux sociaux sont passées de 34,1 % en octobre à 1,1 % en novembre.

- Les États-Unis étaient le pays hébergeant le plus grand nombre de sites de phishing, avec en tête le Texas.

Figure 21. Répartition mondiale des pages de phishing (nombre indexé sur la moyenne de l'ensemble des lieux), 2S08



Téléchargements furtifs

- Plus d'un million de pages déclenchant des téléchargements furtifs ont été détectées mensuellement par Live Search depuis le début du second semestre 2008. Ce chiffre équivaut à 0,07 % de l'ensemble des pages indexées (environ 1 sur 1 500).
- Les domaines de premier niveau présentant le taux le plus élevé de pages déclenchant des téléchargements furtifs étaient .name (0,23 % de l'ensemble des pages), .edu (0,19 %) et .net (0,19 %).
- Un faible nombre de serveurs hébergent les exploits utilisés par une large majorité des pages déclenchant des téléchargements furtifs.

Aidez Microsoft à améliorer le Rapport sur les données de sécurité

Nous vous remercions d'avoir pris le temps de lire ce tout dernier volume du Rapport Microsoft sur les données de sécurité. Nous nous efforçons de le rendre aussi fonctionnel et pertinent que possible pour nos clients. Pour tout commentaire sur ce volume ou pour toute suggestion visant à améliorer les prochains, n'hésitez pas à nous contacter à l'adresse : sirfb@microsoft.com.

Bien cordialement,

Microsoft Trustworthy Computing

Ce résumé est fourni à titre purement informatif. MICROSOFT N'OFFRE AUCUNE GARANTIE, EXPRESSE, EXPLICITE OU IMPLICITE CONCERNANT LES INFORMATIONS CONTENUES DANS CE RÉSUMÉ. Aucune partie de ce résumé ne peut être reproduite, stockée ou incluse dans un système de récupération de données ou transmise à quelque fin ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autre) sans l'autorisation expresse et écrite de Microsoft Corporation.
Microsoft peut détenir des brevets, avoir déposé des demandes de brevets ou être titulaire de marques, de droits d'auteur ou d'autres droits de propriété intellectuelle portant sur tout ou partie des éléments contenus dans le présent résumé. Sauf stipulation expresse contraire d'un contrat de licence écrit de Microsoft, ce résumé ne concède en aucun cas une licence sur ces brevets, marques, droits d'auteur ou autres droits de propriété intellectuelle.

Copyright © 2009 Microsoft Corporation. Tous droits réservés.

Microsoft, le logo Microsoft, Windows, Windows XP, Windows Vista et Microsoft Office sont des marques déposées ou des appellations commerciales de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. Les noms de société et de produit réels mentionnés dans ce document peuvent être des marques de leurs propriétaires respectifs.