Rapport Microsoft sur les données de sécurité
Volume 8 (juillet à décembre 2009)

Résumé des conclusions principales

Introduction

Le volume 8 du *Rapport Microsoft® sur les données de sécurité* offre une présentation détaillée des logiciels malveillants et potentiellement indésirables, des codes malveillants visant l'exploitation logicielle, des violations de la sécurité, des vulnérabilités logicielles dans les logiciels Microsoft® comme dans ceux de tiers. Microsoft a mis au point ces perspectives basées sur l'analyse détaillée de ces dernières années, en mettant l'accent sur le second semestre 2009 (2S09)[1].

Ce document synthétise les principales conclusions du rapport. Le *Rapport complet sur les données de sécurité* contient également une analyse approfondie de tendances constatées dans plus de 26 pays/régions du Monde et propose des stratégies, des mesures de prévention et des contre-mesures pour vous aider à gérer les menaces qui figurent dans le rapport.

Le *Rapport complet sur les données de sécurité*, ainsi que les volumes précédents de ce rapport et les vidéos associées peuvent être téléchargées à partir de www.microsoft.com/france/sir.

L'environnement des menaces informatiques évolue en permanence. Au fur et à mesure que les menaces poursuivent leur évolution, depuis des pirates malfaisants à la recherche de célébrité jusqu'à des membres du crime organisé qui volent des données à but lucratif, la préoccupation du public continue de croître. Microsoft a créé l'initiative pour l'Informatique digne de Confiance (TwC) en 2002 pour s'engager dans une stratégie visant à fournir des expériences informatiques plus sécurisées, plus confidentielles et plus fiables à nos clients.

TwC Security comprend des centres technologiques qui collaborent étroitement pour traiter les problèmes de sécurité et fournir les services, les informations et les réponses nécessaires à une meilleure compréhension de l'évolution des menaces, mieux protéger les clients des menaces en ligne, et partager des connaissances avec un écosystème de sécurité plus large. Ces trois centres de sécurité comprennent :

- Centre de protection Microsoft contre les programmes malveillants
- Centre de réponse aux problèmes de sécurité Microsoft (MSRC)
- Microsoft Security Engineering Center

Les blogs des trois centres de sécurité, ainsi que d'autres blogs comme le blog Data Privacy Imperative se trouvent à l'adresse www.microsoft.com/twc/blogs.

Les données et l'analyse présentes dans ce *Résumé des conclusions principales* et dans le *Rapport complet sur les données de sécurité* sont présentées du point de vue de ces trois centres et de leurs partenaires dans les différents groupes de produit Microsoft.

[1] La nomenclature utilisée dans le présent rapport pour se référer à différentes périodes de déclaration est nSAA, où nS représente soit le premier (1), soit le second (2) semestre de l'année, et AA représente l'année. Par exemple, 2S09 représente la période couvrant le second semestre de 2009 (du 1er juillet au 31 décembre), et 2S08, la période couvrant le second semestre 2008 (du 1er juillet au 31 décembre).

Conclusions du centre de protection Microsoft contre les programmes malveillants

Tendances globales des logiciels malveillants et potentiellement indésirables

Les produits de sécurité Microsoft rassemblent, avec le consentement des utilisateurs, les données de plus de 500 millions d'ordinateurs dans le monde entier et de services en ligne parmi les plus actifs sur Internet. L'analyse de ces données offre une perspective complète et unique sur l'activité liée aux programmes malveillants et potentiellement indésirables dans le monde.

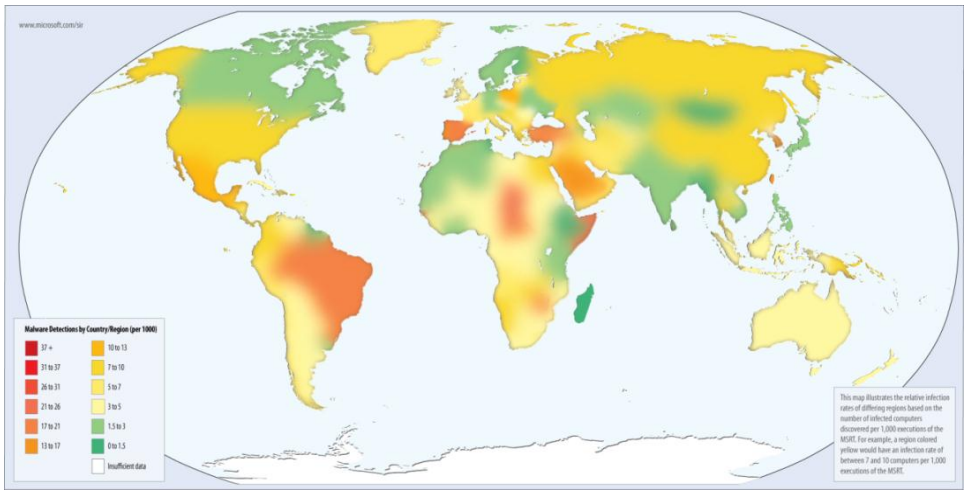
Tendances géographiques

Figure 1 : 15 principaux endroits présentant le plus fort taux d'ordinateurs nettoyés par les produits anti-programmes malveillants Microsoft pour ordinateurs de bureau 2S09 (Le *rapport complet* contient les 25 premiers endroits.)

	Pays/Région	Ordinateurs nettoyés (2S09)	Ordinateurs nettoyés (1S09)	Changement
1	États-Unis	15 383 476	13 971 056	10,1 % ▲
2	Chine	3 333 368	2 799 456	19,1 % ▲
3	Brésil	2 496 674	2 156 259	15,8 % ▲
4	Royaume-Uni	2 016 132	2 043 431	-1,3 % ▼
5	Espagne	1 650 440	1 853 234	-10,9 % ▼
6	France	1 538 749	1 703 225	-9,7 % ▼
7	Corée	1 367 266	1 619 135	-15,6 % ▼
8	Allemagne	1 130 632	1 086 473	4,1 % ▲
9	Canada	967 381	942 826	2,6 % ▲
10	Italie	954 617	1 192 867	-20,0 % ▼
11	Mexique	915 786	957 697	-4,4 % ▼
12	Turquie	857 463	1 161 133	-26,2 % ▼
13	Russie	677 601	581 601	16,5 % ▲
14	Taïwan	628 202	781 214	-19,6 % ▼
15	Japon	609 066	553 417	10,1 % ▲
	Monde entier	41 024 375	39 328 515	4,3 % ▲

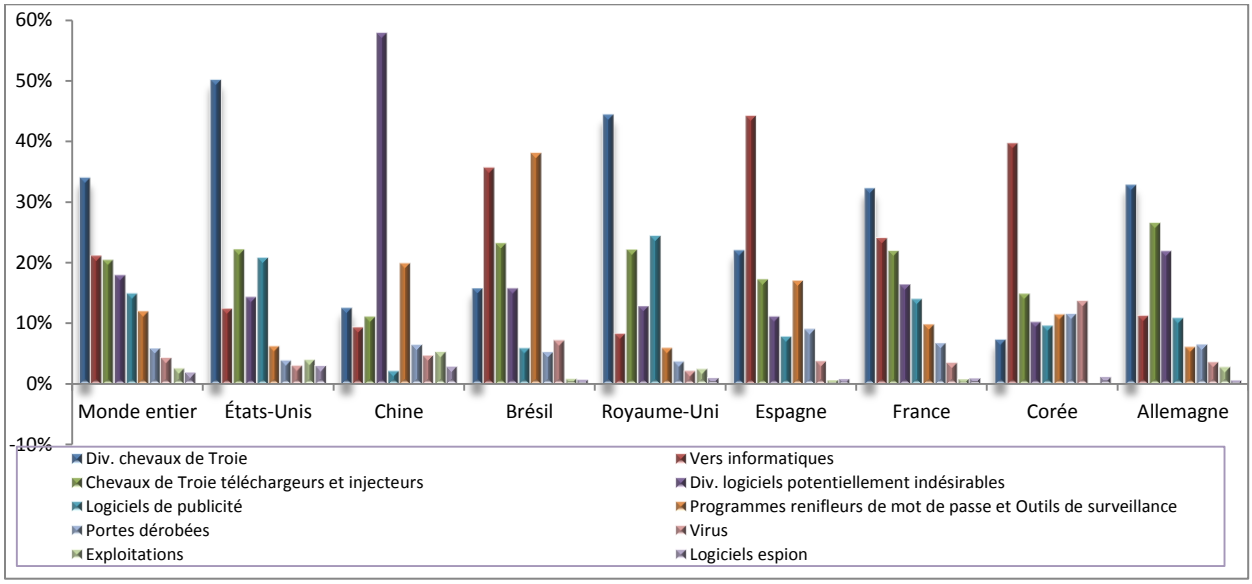
- Deux des plus fortes augmentations du nombre d'ordinateurs nettoyés ont été enregistrées par la Chine et le Brésil, qui ont respectivement augmenté de 19,1 % et 15,8 % depuis 1S09 respectivement. Cette augmentation est en grande partie due à la publication en septembre 2009 de Microsoft Security Essentials, une solution anti-programme malveillant pour les ordinateurs domestiques disponible gratuitement pour les utilisateurs détenteurs d'une licence Windows. La Chine et le Brésil ont adopté Security Essentials très tôt.
- Un certain nombre de régions ont connu une baisse de leur taux d'infection :
  - Le déclin le plus important du nombre d'ordinateurs nettoyés est celui de la Turquie, de 26,2 %, qui peut être attribué majoritairement à la baisse de la prédominance de Win32/Taterf et Win32/Frethog, deux renifleurs de mot de passe visant les joueurs en ligne.
  - Cette baisse de prédominance de Taterf et Frethog est une des principales raisons de la baisse de 19,6 % constatée à Taïwan.
  - La régression de 20 % en Italie est quant à elle le résultat de l'important déclin du nombre de détections de chevaux de Troie de la famille Win32/Wintrim.

Figure 2 : Taux d'infection par pays/région, 2S09, exprimé en CCM[2], pour les endroits du monde ayant eu une moyenne d'au moins 1 000 000 d'exécutions de MSRT par mois au 2S09



Les CCM de plus de 200 pays/régions sont disponibles dans le *Rapport complet sur les données de sécurité*.

Figure 3 : Catégories de menace dans le monde entier et dans les huit endroits présentant le plus fort taux d'ordinateurs nettoyés, par incidence parmi tous les ordinateurs nettoyés à l'aide des produits Microsoft anti-programme malveillant au 2S09



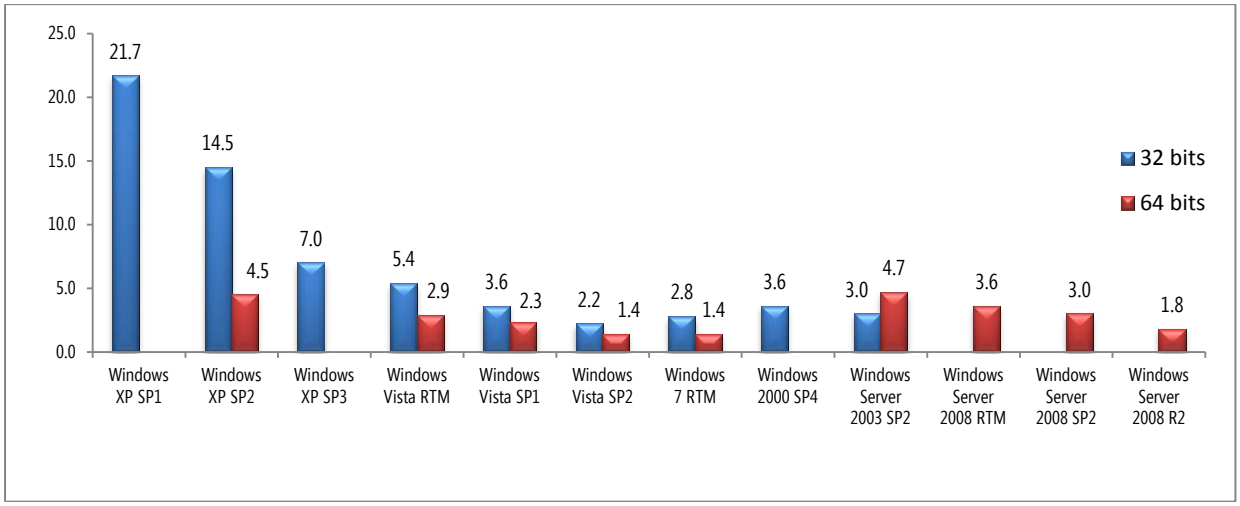
- Les environnements de menaces aux États-Unis et au Royaume-Uni sont très similaires. Les deux sites présentent à peu près la même proportion de catégories et ont en commun 7 de leurs 10 familles principales. Les chevaux de Troie divers représentent la principale catégorie simple de menace. Les familles telles que celles de Win32/FakeXPA, Win32/Renos et Win32/Alureon sont bien classées dans les deux endroits.

[2] Pour mesurer de façon cohérente les infections et utiliser les résultats obtenus pour comparer entre elles les différentes populations d'ordinateurs de différents endroits, les taux d'infection de ce rapport sont exprimés au moyen du CCM (Computers cleaned per thousand, ordinateurs nettoyés par milliers), unité qui représente le nombre d'ordinateurs signalés comme nettoyés toutes les 1 000 exécutions de l'outil MRST.

- En Chine, nombre des menaces parmi les plus prédominantes sont des familles localisées, qui n'apparaissent dans la liste des principales menaces d'aucune autre région. Parmi elles, certaines des versions de Win32/BaiduSobar, une barre d'outils de navigateur en langue chinoise et des programmes renifleurs de mot de passe tels que Win32/Lolyda et Win32/Ceekat, qui ciblent plusieurs jeux populaires en ligne en Chine.
- Au Brésil, les programmes renifleurs de mot de passe et d'outils de surveillance représentent la principale catégorie commune, principalement parce qu'un certain nombre de renifleurs de mots de passe en langue portugaise ciblent les utilisateurs en ligne des banques. Win32/Bancos est le plus répandu de ces programmes renifleurs de mot de passe.
- La Corée est dominée par les vers, principalement le Win32/Taterf, qui cible les joueurs en ligne. La prédominance de Taterf en Corée est due à la propension des vers à se répandre facilement dans les cafés Internet et les centres de jeux en réseau local, très populaires dans ce pays.

Tendances des systèmes d'exploitation

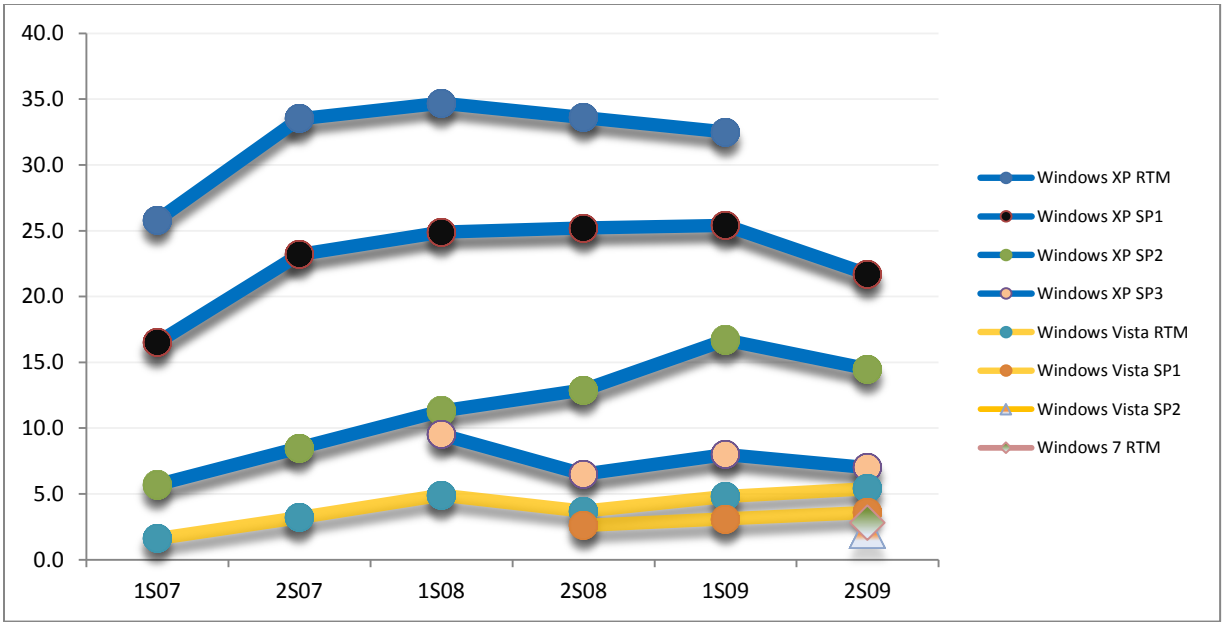
Figure 4 : Nombre d'ordinateurs nettoyés pour chaque 1 000 exécutions de l'outil MSRT par système d'exploitation en 2S09



- Comme dans les périodes précédentes, les taux d'infection des systèmes d'exploitation et des Service Packs les plus récents sont sensiblement inférieurs à ceux de leurs prédécesseurs, que ce soit pour des plateformes serveur ou client.
- Windows 7, sorti au 2S09 et Windows Vista® avec le Service Pack 2 présentent des taux d'infection inférieurs à toutes les autres plateformes du schéma.
  - Les versions 64 bits de Windows 7 et Windows Vista SP2 ont présenté des taux d'infection inférieurs (1,4 pour les deux) à ceux de toutes les autres configurations au 2S09, bien que les versions 32 bits présentent déjà toutes les deux des taux d'infection inférieurs de moitié à ceux de Windows XP avec son Service Pack le plus récent, SP3.
- Pour les systèmes d'exploitation ayant des Service Packs, chaque Service Pack présente un taux d'infection inférieur à son prédécesseur.
  - Le taux d'infection pour Windows XP avec SP3 représente moins de la moitié de celui de SP2, et moins d'un tiers de celui de SP1.
  - De même Windows Vista SP2 présente un taux d'infection inférieur à celui de SP1, qui lui-même a un taux d'infection inférieur à celui de Windows Vista RTM.
  - Pour les systèmes d'exploitation serveur, le taux d'infection de Windows Server® 2008 avec SP2 est de 3,0, soit de 20 % inférieur à celui de son prédécesseur, Windows Server 2008 RTM.

La figure ci-dessous montre la cohérence de ces tendances sur la durée. Elle montre les taux d'infection des différentes versions des éditions 32 bits de Windows XP et de Windows Vista pour chaque semestre entre 1S07 et 2S09.

Figure 5 : Tendances CCM pour les versions 32 bits de Windows XP et Windows Vista, 1S07 à 2S09



Tendances par catégories dans le monde

Figure 6 : 10 principales familles de logiciels malveillants ou potentiellement indésirables détectés par les produits anti-programme malveillant en 2S09 (Le *rapport complet sur les données de sécurité* contient les 25 principales familles.)

	Famille	Catégorie la plus significative	Ordinateurs nettoyés (2S09)
1	Win32/Taterf	Vers informatiques	3 921 963
2	Win32/Renos†	Chevaux de Troie téléchargeurs et injecteurs	3 640 697
3	Win32/FakeXPA*	Chevaux de Troie divers	2 939 542
4	Win32/Alureon†	Chevaux de Troie divers	2 694 128
5	Win32/Conficker†	Vers informatiques	1 919 333 [3]
6	Win32/Frethog	Programmes renifleurs de mot de passe et Outils de surveillance	1 823 066
7	Win32/Agent	Chevaux de Troie divers	1 621 051
8	Win32/BaiduSobar	Divers logiciels potentiellement indésirables	1 602 230
9	Win32/GameVance	Logiciels de publicité	1 553 646
10	Win32/Hotbar	Logiciels de publicité	1 476 838

Les astérisques (*) désignent les familles de logiciels de sécurité.
Les croix (†) désignent des familles qui ont été observées comme téléchargeant des logiciels de sécurité factices.

- Dans l'ensemble, les détections des principales menaces ont considérablement baissé depuis le premier semestre de 2009.
  - Le 1S09, sept familles ont été supprimées d'au moins 2 millions d'ordinateurs par les outils anti-programme malveillant Microsoft, par rapport à 4 le 2S09.
  - Même Win32/Taterf, la principale famille de 2S09, a été supprimée d'environ 1 000 000 d'ordinateurs de moins que pour la période du 1S09.

[3] La Shadowserver Foundation, qui assure le suivi des infections actives par Win32/Conficker a signalé que 4,6 millions d'ordinateurs infectés par Conficker ont été suivis par des serveurs sinkholes exécutés par Shadowserver dans les derniers jours du 2S09, ce qui représente une baisse par rapport aux 5,2 millions des derniers jours du 1S09. Le nombre de logiciels malveillants détectés et nettoyés par les logiciels antivirus peut s'avérer très différent des estimations issues de l'observation d'ordinateurs infectés actifs, et il n'existe pas d'accord général sur la méthode à privilégier.

- Le chiffre de 3,9 millions d'ordinateurs infectés par Taterf au 2S09 est largement inférieur à celui des ordinateurs infectés par la famille principale du 1S09, Win32/Zlob, qui a été retirée de 9 millions d'ordinateurs au cours de cette période.
- De nombreux attaquants utilisent des chevaux de Troie téléchargeurs et injecteurs, tels que Win32/Renos et ASX/Wimad (les seconde et onzième familles dominantes au 2S09, respectivement) pour distribuer d'autres menaces telles que les botnets, les logiciels de sécurité factices et les renifleurs de mot de passe.

- En général, l'environnement des logiciels malveillants en 2S09 se distingue par des familles modérément prédominantes, avec en tête de liste des familles dominantes moins nombreuses, mais supprimées d'un grand nombre d'ordinateurs. L'adoption rapide de Microsoft Security Essentials est peut-être en partie responsable du déclin des suppressions.

Tendances dans la prolifération d'échantillons

Les créateurs de logiciels malveillants tentent d'échapper à la détection en publiant constamment de nouvelles variantes afin de prendre de vitesse la diffusion de nouvelles signatures par les fournisseurs d'antivirus. Une des façons de déterminer les familles et les catégories de logiciels malveillants les plus actifs est de compter les échantillons uniques.

Figure 7 : Échantillons uniques soumis au Centre de protection Microsoft contre les programmes malveillants (MMPC, Microsoft Malware Protection Center) par catégorie, 1S09 à 2S09

Catégorie	2S09	1S09	Différence
Virus	71 991 221	68 008 496	5,9 % ▲
Chevaux de Troie divers	26 881 574	23 474 539	14,5 % ▲
Chevaux de Troie téléchargeurs et injecteurs	9 107 556	6 251 286	45,7 % ▲
Divers logiciels potentiellement indésirables	4 674 336	2 753 008	69,8 % ▲
Logiciels de publicité	3 492 743	3 402 224	2,7 % ▲
Exploitations	3 341 427	1 311 250	154,8 % ▲
Vers informatiques	3 006 966	2 707 560	11,1 % ▲
Programmes renifleurs de mot de passe et Outils de surveillance	2 217 902	7 087 141	-68,7 % ▼
Portes dérobées	812 256	589 747	37,7 % ▲
Logiciels espions	678 273	269 556	151,6 % ▲
Total	**126 204 254**	**115 854 807**	**8,9 %**

- Plus de 126 millions d'échantillons malveillants ont été détectés au cours du 2S09.
- La baisse de la catégorie des renifleurs de mot de passe et des outils de surveillance est en grande partie due à Win32/Lolyda, qui est passée de 5,7 millions d'échantillons pour 1S09 à moins de 100 000 pour 2S09.
- L'augmentation de la catégorie des logiciels espions a été principalement causée par Win32/ShopAtHome, qui compte déjà cinq fois plus d'échantillons au 2S09 que pour la période précédente.
- Un nombre élevé d'échantillons de virus est dû au fait que les virus peuvent infecter de nombreux fichiers différents, chacun d'eux constituant un échantillon unique. Les nombres d'échantillons de virus ne doivent donc pas être considérés comme indiquant qu'il existe un grand nombre de variantes réelles pour ces familles.

Logiciels de sécurité factices

Les logiciels de sécurité factices (logiciels affichant de fausses alertes ou des alertes trompeuses au sujet d'infections et de vulnérabilités sur les ordinateurs de la victime et proposant de résoudre le problème supposé moyennant finance) sont devenus pour les attaquants un des moyens les plus utilisés pour soutirer de l'argent à leurs victimes.

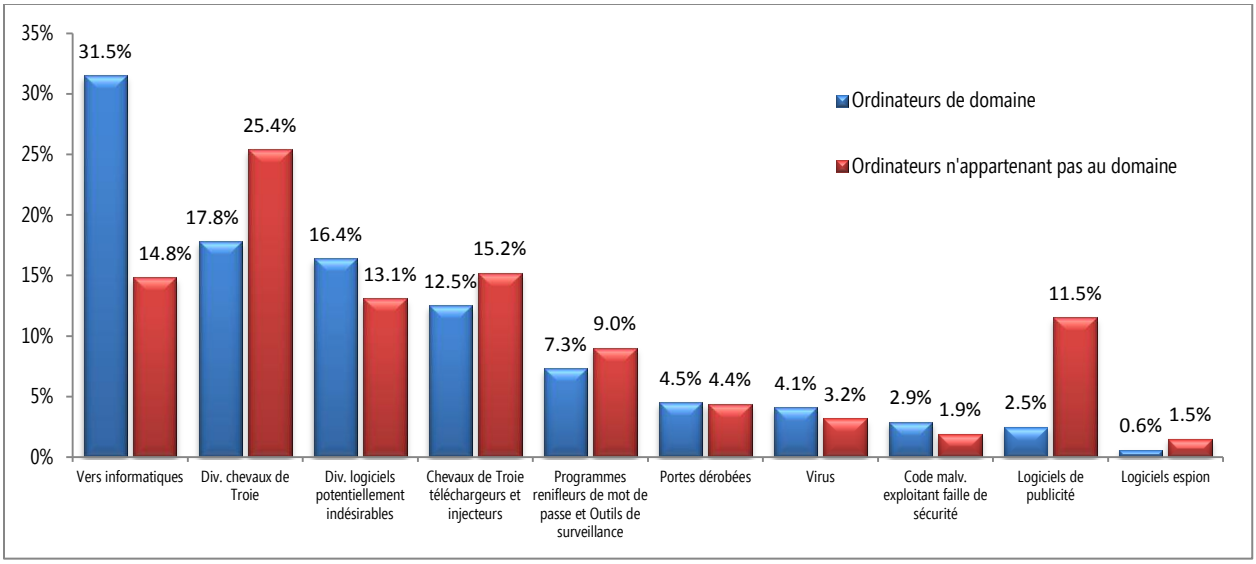
Figure 8 : « Analyses de sécurité » factices effectuées par des variantes de Win32/FakeXPA, famille de logiciels de sécurité factices dominante pour le 2S09

- Les produits Microsoft de sécurité ont retiré de 7,8 millions d'ordinateurs des logiciels malveillants de type logiciels de sécurité factices au 2S09, plus qu'au 1S09, où ils avaient traité 5,3 millions d'ordinateurs, soit une augmentation de 46,5 %, ce qui suggère que les logiciels de sécurité factices procurent à ceux qui les distribuent des profits importants, supérieurs à ceux issus d'autres types de menaces.
- Une famille de logiciels de sécurité factices, Win32/FakeXPA, se classait troisième au niveau mondial parmi les menaces dominantes détectées par les produits Microsoft de sécurité d'ordinateurs au 2S09. Trois autres familles (Win32/Yektel, Win32/Fakespypro et Win32/Winwebsec) se sont respectivement classées onzième, quatorzième et dix-septième.
- Vous trouverez dans le *Rapport Microsoft complet sur les données de sécurité* une répartition géographique complète des endroits où Microsoft détecte le plus grand nombre de logiciels de sécurité factices et les principales familles de menaces pour chaque région.
- Trois nouvelles vidéos pour le grand public ont été publiées sur http://www.microsoft.com/france/athome/security. Elles sont conçues pour informer les particuliers de la menace croissante que représentent les logiciels de sécurité factices pour leur sécurité et leur vie privée.

Panorama des menaces à la maison et en entreprise

Les données d'infection fournies par les produits et les outils Microsoft anti-programme malveillant contiennent des informations sur les ordinateurs infectés appartenant à un domaine Active Directory®. Les domaines sont principalement utilisés dans les environnements d'entreprise, et les ordinateurs n'appartenant pas à un domaine sont le plus souvent utilisés chez des particuliers ou dans d'autres contextes, hors entreprise. La comparaison des menaces rencontrées par les deux types d'environnements peut apporter des réponses quant aux moyens qu'utilisent les attaquants pour cibler les entreprises et les utilisateurs à domicile, et donc, sur les menaces qui sont susceptibles d'aboutir dans chacun des environnements.

Figure 9 : Répartition de la catégorie de menaces pour les ordinateurs faisant partie d'un domaine ou les autres, au cours du 2S09



- Les ordinateurs joints à un domaine sont plus susceptibles de rencontrer des vers que les autres, en raison de la façon dont les vers se propagent. Les vers se propagent plus efficacement par les partages de fichiers et les volumes de stockage amovibles, deux éléments largement répandus dans les environnements d'entreprise, et moins communs à domicile.
  - Les vers représentent quatre des 10 familles principales détectées sur les ordinateurs joints à un domaine.
  - Win32/Conficker, qui utilise plusieurs méthodes de propagation fonctionnant plus efficacement dans un environnement réseau d'entreprise classique que via Internet, arrive largement en tête de la liste.
  - De même, Win32/Autorun, qui cible les disques amovibles, se retrouve plus communément dans les environnements de domaine dans lesquels ce type de volume est utilisé pour l'échange de fichiers.
- Les catégories Logiciels de publicité et Chevaux de Troie divers se rencontrent plus souvent dans les ordinateurs hors domaine.

Menaces par courrier électronique

Les données figurant dans cette section sont issues des messageries électroniques filtrées par le logiciel Microsoft Forefront Online Protection for Exchange (FOPE), qui fournit des services de filtrage contre le courrier indésirable, l'hameçonnage et les logiciels malveillants à des milliers de clients d'entreprise.

Le courrier indésirable associé aux fraudes financières (également appelées « scam 419 ») et aux jeux ont augmenté de façon significative au 2S09. La plupart des autres catégories sont restées stables en termes de pourcentage.

- Une fraude financière est une arnaque très répandue fondée sur la confiance, dans laquelle l'expéditeur d'un message affirme avoir droit à une grosse somme d'argent qu'il ne peut, pour toutes sortes de raisons, récupérer directement. En règle générale, la raison invoquée est liée à une lourdeur administrative ou à un contexte politique. L'expéditeur demande à la victime potentielle un prêt temporaire qu'il utilisera pour soudoyer des fonctionnaires ou payer les taxes permettant d'obtenir la somme complète. En échange, il promet de reverser une partie de sa fortune, ce qui donne un montant bien supérieur à celui du prêt.
- Ces messages sont fréquemment associés au Nigéria (« 419 » fait référence au numéro de l'article du code nigérian sanctionnant ce type de fraude) et à d'autres pays d'Afrique Occidentale, notamment le Sierra Leone, la Côte d'Ivoire et le Burkina Faso.

Figure 10 : Messages entrants bloqués par les filtres de contenu de FOPE par catégorie, 2S08 à 2S09

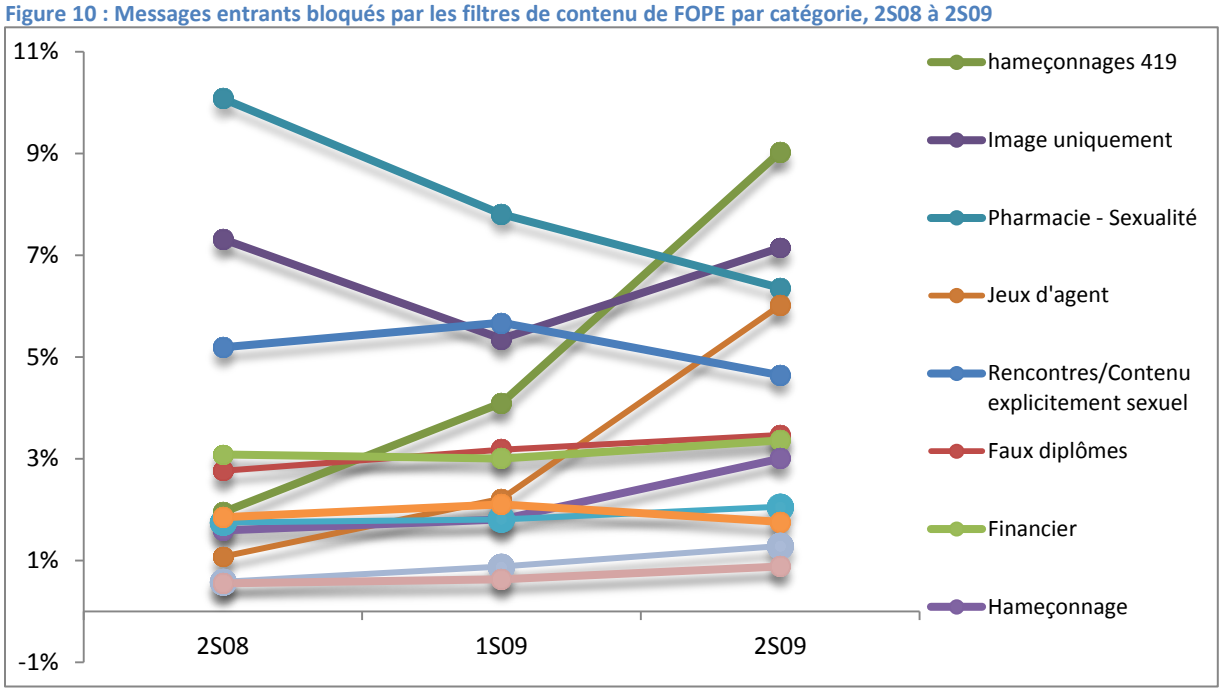
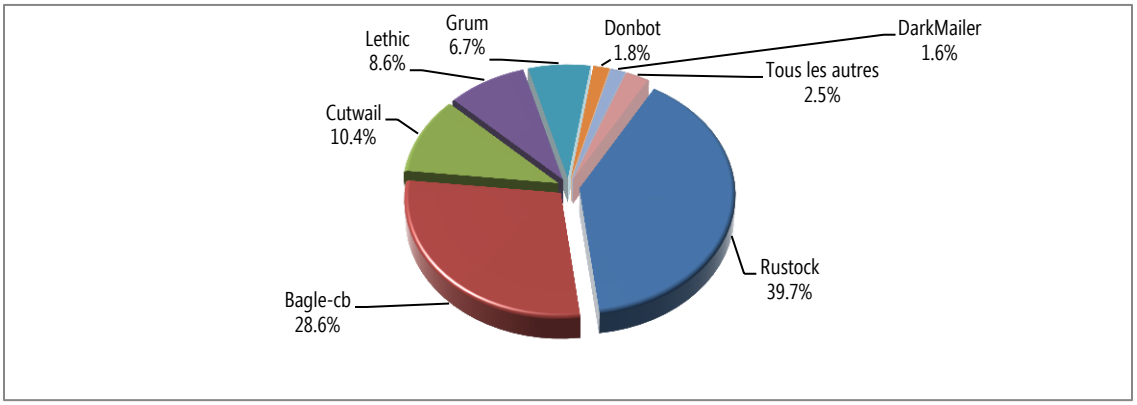


Figure 11 : Cinq principaux lieux à l'origine du plus grand nombre de spams, par pourcentage, au cours du 2S09

	Pays	Pourcentage
1	États-Unis	27,0 %
2	Corée	6,9 %
3	Chine	6,1 %
4	Brésil	5,8 %
5	Russie	2,9 %

Les réseaux botnets et de courrier indésirable des ordinateurs infectés par des logiciels malveillants contrôlés à distance par un attaquant sont à l'origine de la plupart du courrier indésirable envoyé aujourd'hui. Pour mesurer l'impact des botnets sur le secteur du courrier indésirable, FOPE contrôle les messages indésirables envoyés à partir d'adresses IP désignées comme étant associées à des botnets connus.

Figure 12 : Quelques botnets sont à l'origine de quasiment tout le courrier indésirable de botnets observés au 2S09 (plus de détails dans le *Rapport complet Microsoft sur les données de sécurité*)



Sites Web malveillants

Comme l'indiquent les volumes précédents du Rapport Microsoft sur les données de sécurité, les réseaux sociaux ont connu le plus haut volume d'impressions d'hameçonnage, ainsi que le plus haut taux d'impressions d'hameçonnage par site d'hameçonnage. Les institutions financières ont reçu le plus bas volume d'impressions d'hameçonnage par site tout en étant de loin la cible du plus grand volume total de sites frauduleux distincts. La figure qui suit représente le pourcentage d'impressions d'hameçonnage enregistré par Microsoft pour chaque mois de 2S09, pour chaque type d'institution le plus souvent ciblée.

Figure 13 : Gauche : Impressions pour chaque type de site d'hameçonnage au 2S09 Droite : Sites d'hameçonnage suivis chaque mois, par type de cible, au 2S09

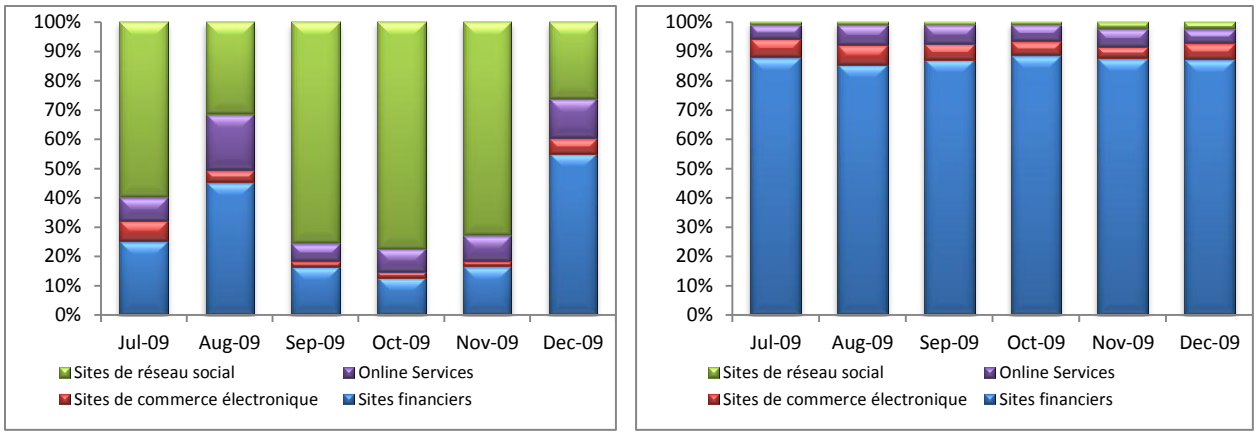
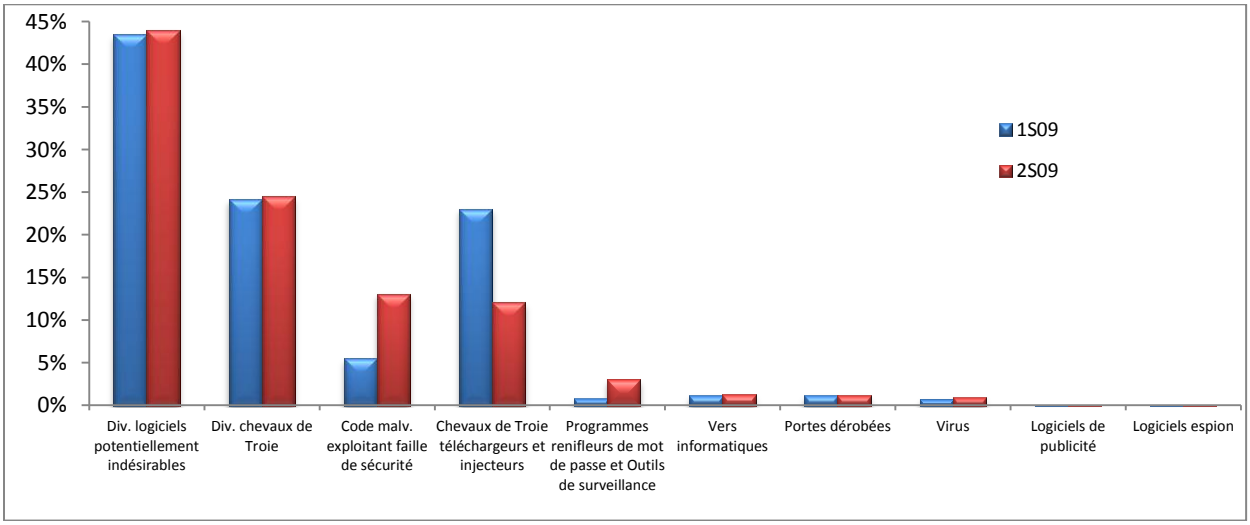


Figure 14 : Distribution par catégorie des menaces hébergées sur des URL bloquées par le filtre SmartScreen au cours des 1S09 et 2S09



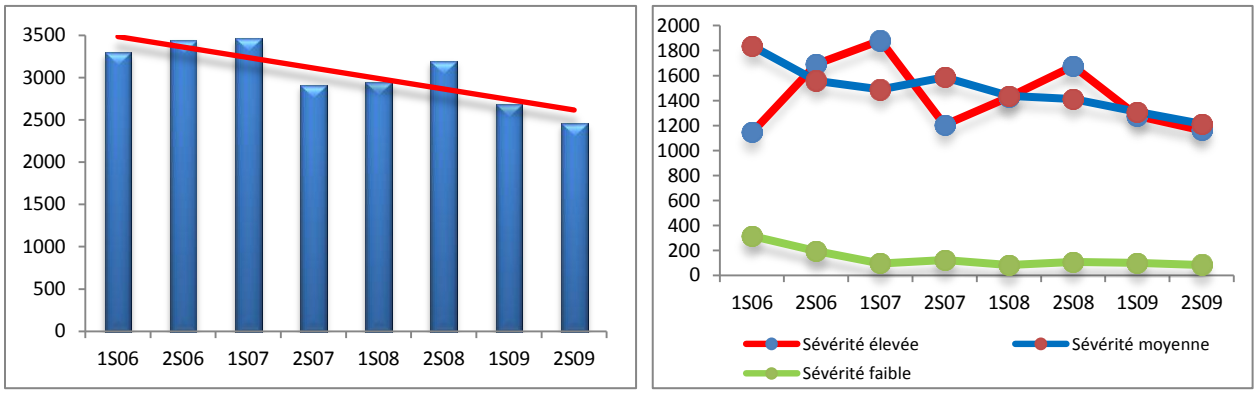
- Les catégories Divers logiciels potentiellement indésirables et Divers chevaux de Troie étaient en tête de liste au cours des deux périodes.
- La catégorie Chevaux de Troie téléchargeurs et injecteurs était pratiquement aussi prédominante que Chevaux de Troie divers au 1S09, mais a baissé de quasi 50 % au cours du second semestre de l'année, tandis que le nombre d'exploitations doublait.

Principales conclusions du Centre de réponse aux problèmes de sécurité Microsoft

Vulnérabilités observées dans le secteur

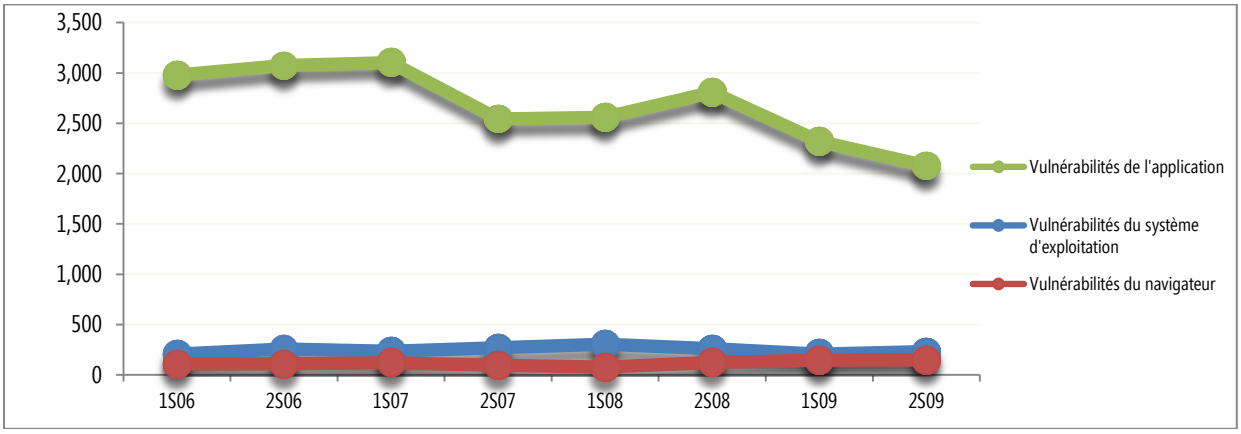
Les *vulnérabilités* sont des faiblesses du logiciel permettant à un attaquant de compromettre l'intégrité, la disponibilité ou la confidentialité de celui-ci. Les pires vulnérabilités peuvent notamment permettre aux attaquants d'exécuter des codes arbitraires sur un ordinateur compromis. Une divulgation, qui est le terme utilisé dans le rapport, est la révélation de la vulnérabilité d'un logiciel au grand public. Elle ne fait pas référence à un type de divulgation privée ou limitée à un certain nombre de personnes.

Figure 15 : Gauche : Divulgations de vulnérabilités observées dans le secteur pendant les semestres 1S06 à 2S09 | Droite : Divulgations de vulnérabilités observées par sévérité, aux 1S06 à 2S09.



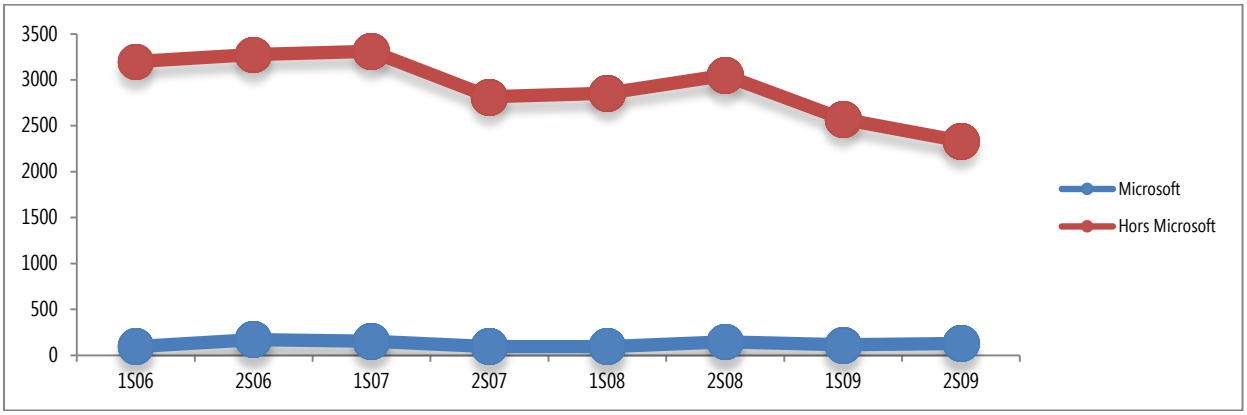
- Les divulgations de vulnérabilités pour le 2S09 ont baissé de 8,4 % par rapport au premier semestre, ce qui s'inscrit dans la continuité de la tendance générale au déclin modéré constatée depuis 2006.
- Les vulnérabilités de faible sévérité comptaient pour seulement 3,5 % du total au 2S09, soit 4,1 % de moins que pour le premier semestre de l'année.
- Les vulnérabilités de sévérité élevée au cours du 2S09 ont baissé de 9 % depuis le premier semestre de l'année, et de 30,7 % par rapport au 2S08.
    - La prédominance persistante des divulgations de sévérité moyenne et élevée est en partie due de la tendance des attaquants et des chercheurs de sécurité à donner la priorité à la recherche des vulnérabilités les plus sérieuses.

Figure 16 : Vulnérabilités de systèmes d'exploitation, de navigateur et d'application au niveau du secteur aux 1S06 à 2S09



- Les vulnérabilités d'application comptent parmi les plus nombreuses au 2S09, bien que le nombre total de vulnérabilités d'application ait baissé de façon significative depuis les 2S08 et 1S09.
- Les vulnérabilités de système d'exploitation et de navigateur sont toutes les deux restées stables, et chacune compte pour une petite proportion du total.

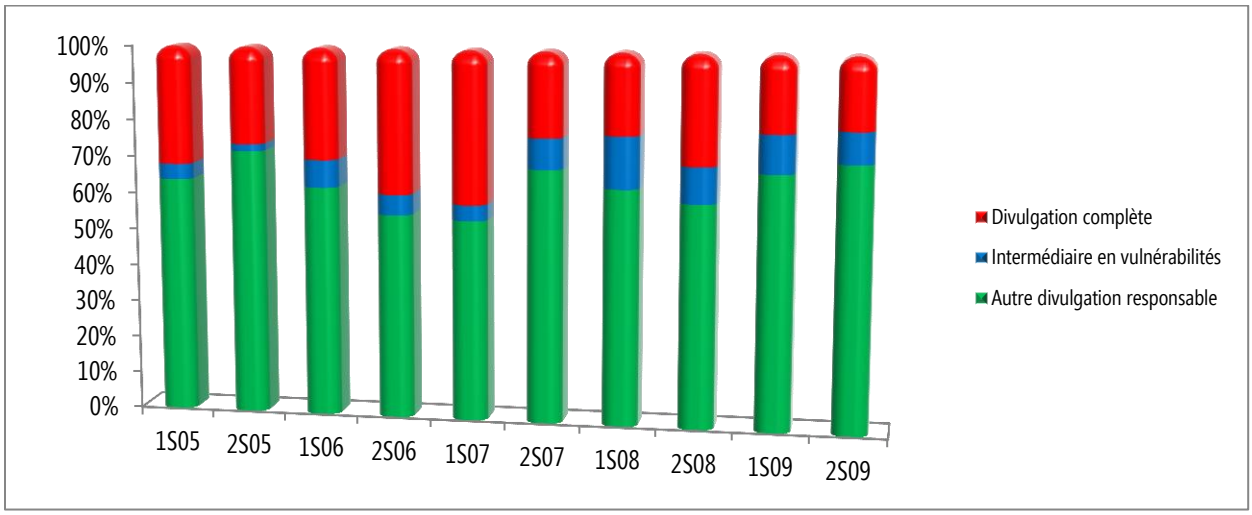
Figure 17 : Divulgations de vulnérabilité pour les produits Microsoft et non Microsoft pour 1S06 à 2S09



- Les divulgations de vulnérabilité pour les produits Microsoft ont atteint 127 au 2S09, contre 113 au 1S09.
- En règle générale, les tendances de divulgation de vulnérabilité Microsoft reflètent celles de l'ensemble du secteur qui on connu un pic durant les semestres 2S06 à 1S07, puis de nouveau au 2S08.
- Au cours des quatre dernières années, les divulgations de vulnérabilité ont sensiblement contribué aux divulgations de l'ensemble du secteur, dans une proportion de 3 à 5 %.

Divulgation responsable se réfère à la divulgation privée de vulnérabilités auprès d'un fournisseur affecté, afin qu'il puisse mettre au point une mise à jour de sécurité complète visant à éliminer la vulnérabilité avant que les détails ne parviennent à la connaissance du public.

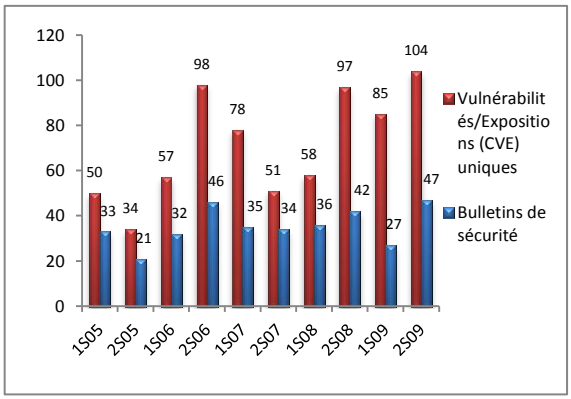
Figure 18 : Divulgations responsables en pourcentage de l'ensemble des divulgations impliquant des logiciels pour 1S05 à 1S09

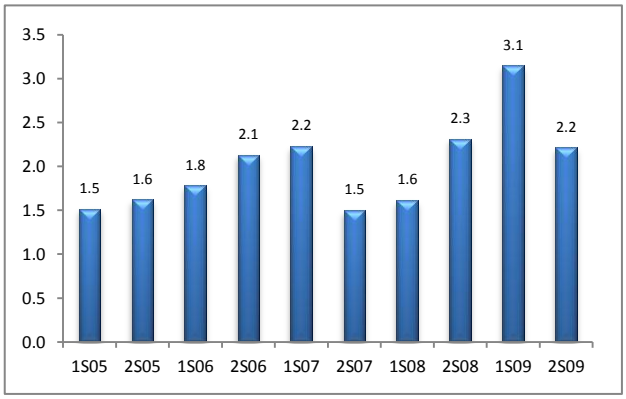


- Au 2S09, 80,7 % des vulnérabilités observées dans les logiciels Microsoft ont respecté les pratiques de divulgation responsables par rapport aux 79,5 % de 1S09 et sont supérieures à celles de la période de suivi précédente.

- Le pourcentage de divulgations soumis par les intermédiaires spécialistes de la vulnérabilité a légèrement décliné pour atteindre 8,6 % de l'ensemble des divulgations au 2S09, par rapport aux 10,5 % enregistrés lors du premier semestre.

Figure 19 : Gauche : Bulletins de sécurité et CVE émis adressés par Microsoft par semestre, entre 1S05 et 2S09 | Droite : Nombre moyen de CVE concernés adressés par le bulletin de sécurité, entre 1S05 et 2S09

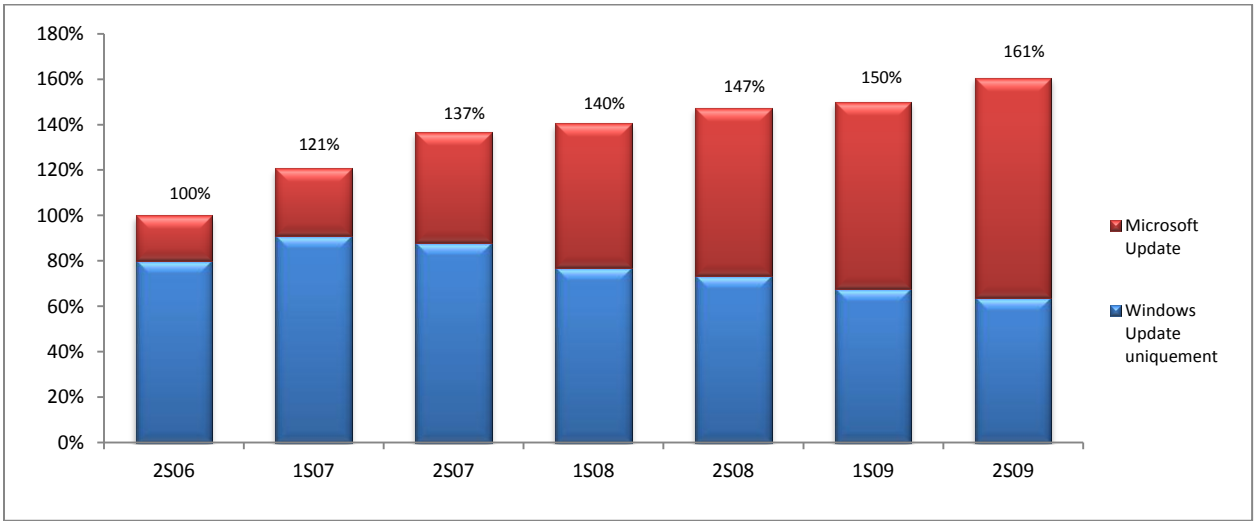




- Au 2S09, Microsoft a publié 47 bulletins de sécurité qui s'adressaient à 104 vulnérabilités individuelles identifiées dans la liste des vulnérabilités et expositions communes (CVE, Common Vulnerabilities and Exposures).
- Bien que le nombre total des bulletins expédiés (27 au 1S09) ait augmenté, le nombre de vulnérabilités traitées par bulletin a baissé de 3,1 à 2,2.

Comme le montre la figure suivante, l'adoption de Microsoft Update a sensiblement augmenté au cours des dernières années. Le nombre d'ordinateurs utilisant le service complet s'est accru de plus de 17 % depuis 1S09.

Figure 20 : Utilisation de Windows Update et de Microsoft Update, 2S06 à 2S09, indexée sur l'utilisation totale de 2S06



- **Windows Update** fournit des mises à jour pour les composants Windows et pour les pilotes de périphérique fournis par Microsoft et d'autres fournisseurs de matériel. Windows Update distribue également des mises à jour de signatures pour les produits anti-programme malveillant de Microsoft et la publication mensuelle du MSRT.

- **Microsoft Update** (http://update.microsoft.com/microsoftupdate) fournit toutes les mises à jour offertes via Windows Update et fournit des mises à jour pour les autres logiciels Microsoft. Les utilisateurs peuvent opter pour le service au moment de l'installation d'un logiciel maintenu à jour via Microsoft Update ou sur le site Web Microsoft Update. Microsoft conseille de configurer les ordinateurs afin qu'ils utilisent Microsoft Update au lieu de Windows Update, pour leur permettre de recevoir les mises à jour de sécurité destinées aux produits Microsoft en temps et en heure.

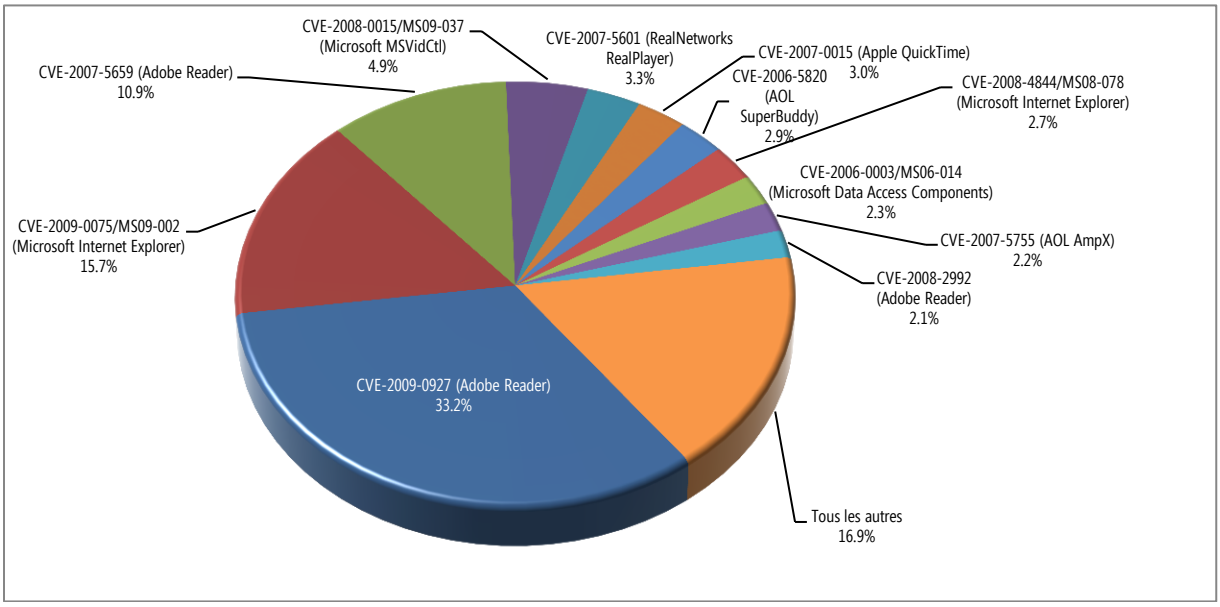
Principales conclusions du Microsoft Security Engineering Center

Science de la sécurité : Tendances des exploitations

Une *exploitation* est un code malfaisant conçu pour infecter un ordinateur sans le consentement de son utilisateur, et souvent, à son insu. Les exploitations sont souvent distribuées via des pages Web, bien que les attaquants utilisent également d'autres méthodes de distribution, comme les messages électroniques ou les services de messagerie instantanée. Les informations sur la façon dont les attaquants exploitent les navigateurs et les compléments peuvent offrir aux chercheurs en sécurité une meilleure compréhension des risques provoqués par les téléchargements en passant et les autres attaques basées sur le navigateur.

- Autrefois, les créateurs d'exploitations utilisaient quatre à six éléments par kit, afin d'augmenter les chances de réussir une attaque.
  - Cette moyenne est tombée à 3,2 exploitations par kit lors du premier semestre de 2009, alors que l'attaquant mettait à profit un certain nombre de vulnérabilités prédominantes, certaines de composants tiers, ce qui rendait inutile la multiplication des exploitations.
  - Cette tendance s'est poursuivie au cours de 2S09 ; le nombre moyen de logiciels malveillants tombant à 2,3.
  - Cependant, certains attaquants préfèrent toujours utiliser de grands nombres d'exploitations. Le plus important kit observé au 2S09 en contenait 23.

Figure 21 : Exploitations basées sur navigateur rencontrées au 2S09, par pourcentage

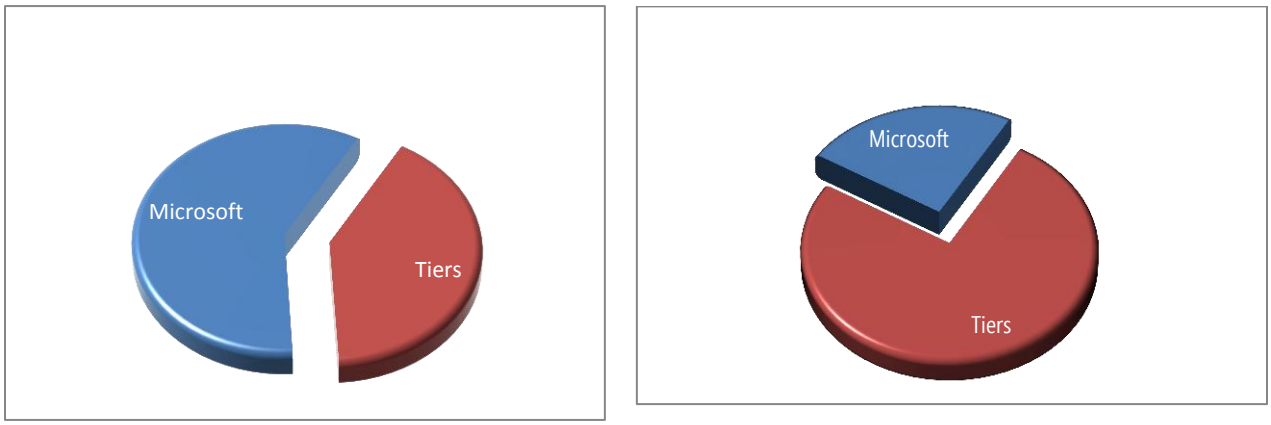


- CVE-2007-0071, la vulnérabilité exploitable en passant dans Adobe Flash Player qui était la vulnérabilité de navigateur la plus communément exploitée au 1S09, est passée à la vingt-troisième place lors du second semestre de l'année et a compté pour seulement 0,4 % des exploitations.

- Des évolutions significatives telles que celles-ci peuvent être mises en relation avec la tendance des créateurs de kits d'exploitation à remplacer les logiciels anciens par des nouveaux.
- Comme l'indique le graphique de la Figure 21, l'incidence de plusieurs exploitations très répandues a varié de façon significative d'un mois à l'autre lors du 2S09.

- Une des vulnérabilités répertoriées à la Figure 21 a été corrigée en 2006.
- Toutes les vulnérabilités traitées à la Figure 21 disposaient de mises à jour de sécurité avant la période concernée par le Rapport Microsoft sur les données de sécurité.

Figure 22 : Gauche : exploitations par navigateur ciblant les logiciels Microsoft et tiers sur les ordinateurs fonctionnant sous Windows XP pour 2S09 | Droite : exploitations par navigateur ciblant les logiciels Microsoft et tiers sous Windows Vista et Windows 7 pour 2S09



- La comparaison les exploitations visant les logicielsde Microsoft à celles visant des tiers (celles qui ciblent les vulnérabilités dans les logiciels proposés par d'autres fournisseurs) suggère que l'environnement des vulnérabilités de Windows Vista et Windows 7 est très différent de celui de Windows XP.
  - Dans Windows XP, les vulnérabilités Microsoft comptent pour 55,3 % des attaques de l'échantillon étudié.
  - Dans Windows Vista et Windows 7, la proportion de vulnérabilités de Microsoft est significativement plus petite, ne comptant que pour 24,6 % des attaques de l'échantillon étudié.
    - Ce chiffre est supérieur au pourcentage de 15,5 % enregistré au 1S09 (contenant Windows Vista uniquement) en raison des attaques croissantes sur CVE-2009-0075/MS09-002, une vulnérabilité d'Internet Explorer 7 qui affecte Windows Vista RTM et SP1 (mais pas Windows Vista SP2 ou Windows 7). Cette vulnérabilité a été résolue par une mise à jour de sécurité Microsoft en janvier 2009.

Les Figures 23 et 24 de la page qui suit montrent les 10 vulnérabilités exploitées le plus souvent dans Windows XP (Figure 23) et dans Windows Vista et Windows 7 (Figure 24).

Figure 23 : 10 vulnérabilités de navigateur exploitées le plus souvent sous Windows XP, par pourcentage de toutes les exploitations pour le 2S09

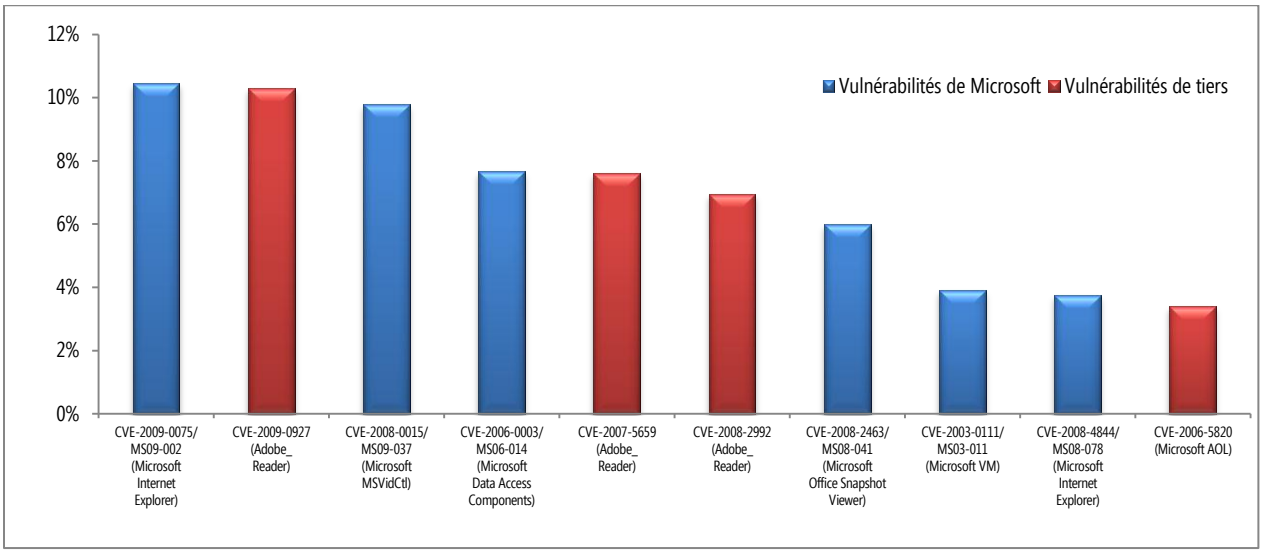
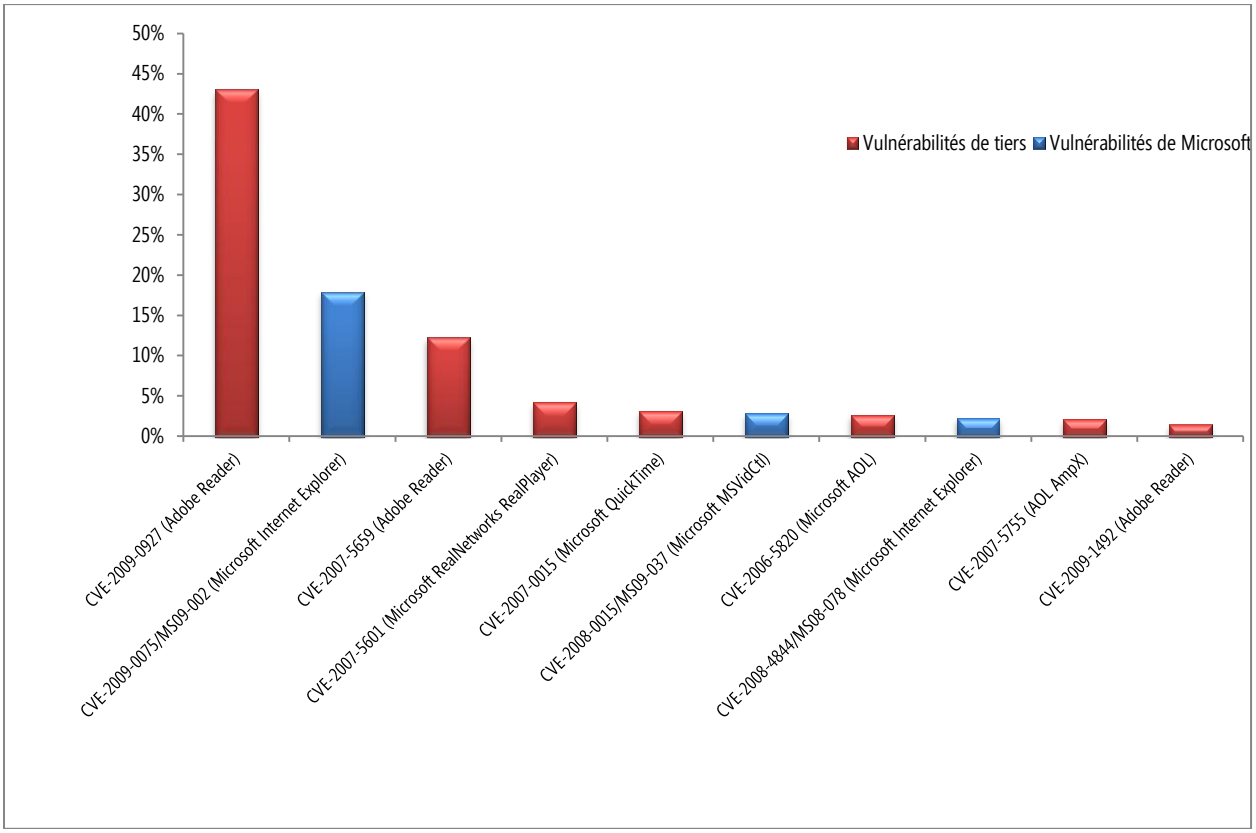


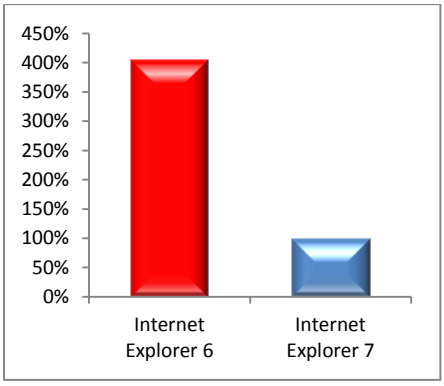
Figure 24 : 10 vulnérabilités de navigateur exploitées le plus souvent sous Windows Vista et Windows 7, par pourcentage d'exploitations pour le 2S09



Les pages de téléchargement en passant sont en général hébergées sur des sites Web légitimes sur lesquels un attaquant a publié un code malveillant. Les attaquants obtiennent l'accès aux sites légitimes par intrusion ou en envoyant un code malveillant à un formulaire Web à faible protection, par exemple via un champ de commentaire sur un blog.

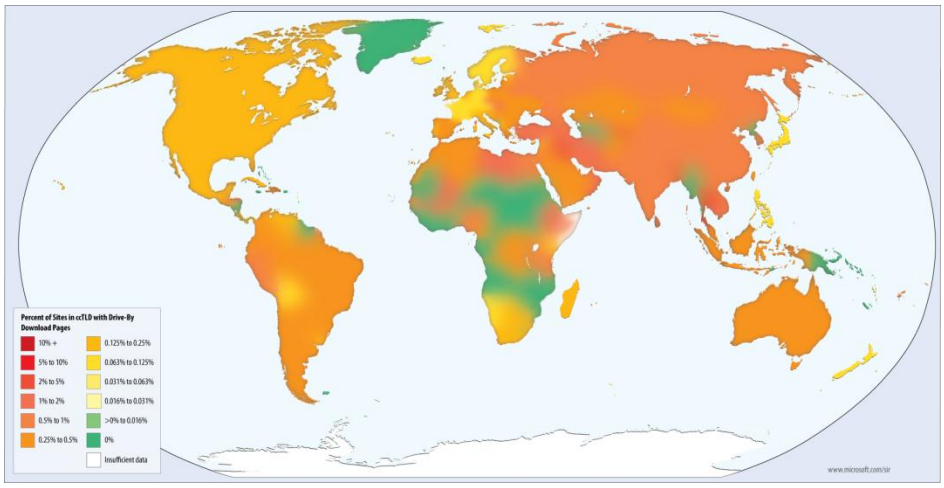
- Une analyse des vulnérabilités spécifiques ciblées sur les sites de téléchargement en passant indique que la plupart des exploitations utilisées par ce type de sites malveillants ciblent des navigateurs plus anciens et sont inefficaces sur les navigateurs plus récents. Comme l'indique la figure suivante, les exploitations qui affectent Internet Explorer 6 sont apparues sur quatre fois plus de sites de téléchargement en passant au 2S09 que ceux qui affectent Internet Explorer 7, navigateur plus récent.

Figure 25 : Sites de téléchargement en passant ciblant Internet Explorer 6 et Internet Explorer 7, indexés sur le total pour Internet Explorer 7, au 2S09



- Lorsque Bing indexe le Web, les pages sont évaluées pour détecter une éventuelle présence d'éléments ou de comportements malveillants.
  - Bing détecte un grand nombre de pages de téléchargement en passant chaque mois, avec plusieurs centaines de milliers de sites qui hébergent des pages de téléchargement en passant contrôlés à un moment donné.
  - Les propriétaires des sites compromis étant généralement des victimes eux-mêmes, les sites ne sont pas retirés de l'index Bing. Au lieu de cela, le fait de cliquer sur les résultats de la recherche permet d'afficher un avertissement évident signalant que la page pourrait contenir des logiciels malveillants.
    - Au 2S09, environ 0,3 % des pages de résultats fournies aux utilisateurs par Bing contenaient des avertissements sur les sites malveillants.
  - Dans l'ensemble, le nombre de sites Web affectés contrôlés par Bing a augmenté au 2S09, avec 0,24 % de l'ensemble des sites Web qui hébergent au moins une page malveillante, une augmentation par rapport au 0,16 % du 1S09. Cette augmentation est probablement due en partie à un certain nombre de nouveaux mécanismes de détection améliorés déployés par Bing dans la seconde moitié de 2009.
- Bien que Bing ait détecté des sites de téléchargement en passant dans le monde entier, le risque n'est pas le même pour tous les internautes du monde. Les utilisateurs de certains pays du monde encourent davantage de risques que les autres. La figure qui suit montre la proportion de sites Web de domaine de niveau supérieur de code de pays (ccTLD) ayant été détectés comme hébergeant des pages de téléchargement en passant au cours du 2S09.
  - Les pages de téléchargement en passant ont été détectées sur plus de 2,1 % des sites en .th (associé à la Thaïlande) et presque 1 % sur .cn (Chine).

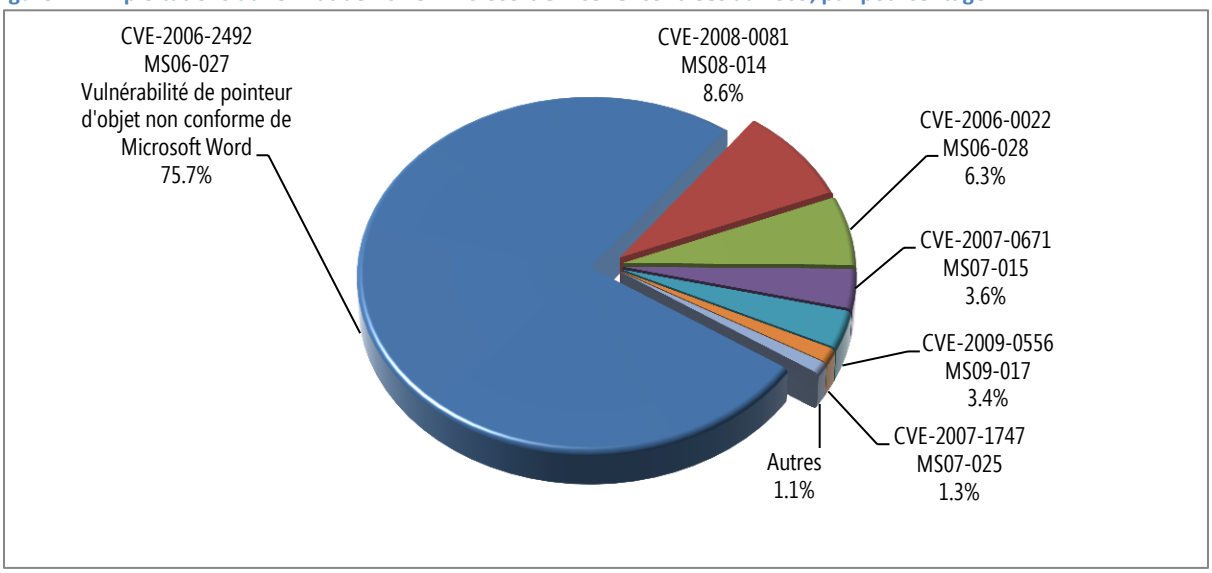
Figure26 : [BingGeo_Heatmap] Pourcentage de sites Web dans chaque domaine de niveau supérieur de code pays (ccTLD) qui hébergent des pages de téléchargement en passant au semestre 2S09



- Par comparaison, les domaines de niveau supérieur génériques et sponsorisés qui ne desservent pas des régions ou des pays particuliers n'affichent pas le même niveau de variation que les ccTLDs.
    - Le domaine de premier niveau .biz, destiné aux entreprises contient le plus haut pourcentage de sites qui hébergent des pages de téléchargement en passant ; 0,76 % de tous les sites .biz actifs ont été détectés comme contenant ce type de pages.
- Bien que les pages de téléchargement en passant se trouvent en quantité dans la plupart des domaines de premier niveau génériques, sponsorisés et codes pays, les serveurs d'exploitation se concentrent sur un nombre de domaines de premier niveau plus petits, avec en tête les .com (33,2 %) et .cn (19,0 %).
    - Au 2S08, le serveur d'exploitation le plus utilisé a affecté environ 100 000 pages. Ce chiffre a été porté à plus de 450 000 au 1S09 et à environ 750 000 pages au 2S09.
        - Malgré cette augmentation, un nombre infime des serveurs figurant en tête de liste au 1S09 y sont restés au 2S09.
- Les réseaux de distribution de logiciels malveillants ont tendance à être des cibles mouvantes, avec des serveurs qui apparaissent et disparaissent constamment à divers endroits.

Les attaquants utilisent les formats de fichiers communs comme vecteurs de transmission des exploitations (formats tels que .doc, .pdf, .ppt et .xls, par exemple). Les *vulnérabilités d'analyseur* sont un type de vulnérabilité pour lequel l'attaquant crée un document sur mesure pour tirer avantage d'une erreur dans la façon dont le code traite ou analyse le format de fichier. Nombre de ces formats sont complexes et conçus pour la performance, et un attaquant peut créer un fichier comportant une section non conforme exploitant la vulnérabilité du programme.

Figure 27 : Exploitations du format de fichier Microsoft Office rencontrées au 2S09, par pourcentage



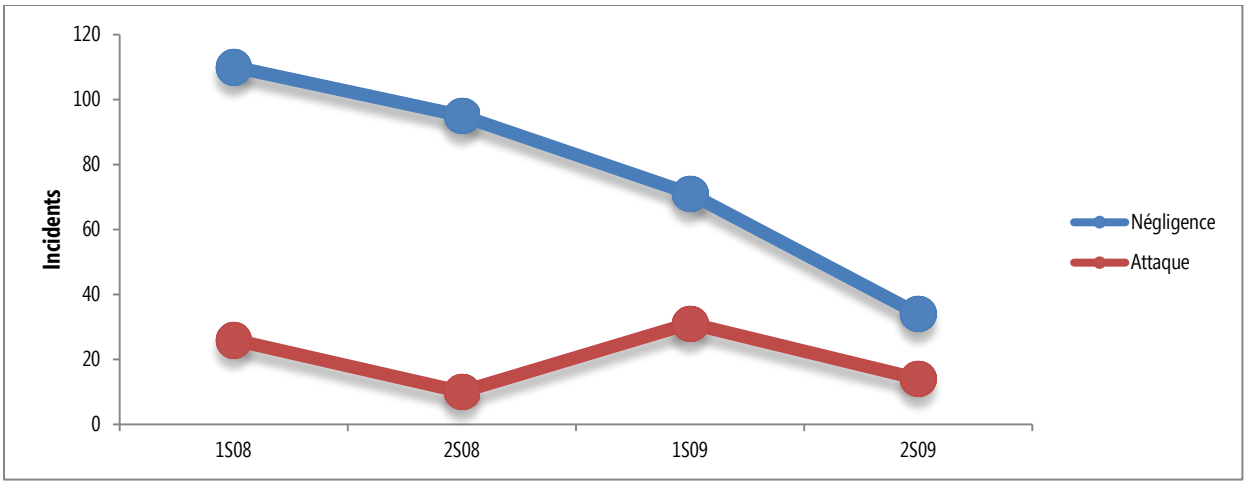
- La plupart des vulnérabilités exploitées dans l'échantillon de données dataient de plusieurs années, et toutes disposaient de mises à jour de sécurité capables de les protéger contre l'exploitation. Un tiers d'entre elles ont été identifiées pour la première fois dès 2006.
- 75,7 % des attaques ont mis à profit une vulnérabilité (CVE-2006-2492, Vulnérabilité de pointeur d'objet non conforme) pour laquelle une mise à jour de sécurité était disponible depuis trois ans à la fin de 2009.
- Les utilisateurs qui ne mettent pas à jour leurs installations de programme Office et leurs systèmes d'exploitation Windows à l'aide des Services Packs et des mises à jour de sécurité sont davantage exposés aux attaques. La plupart des attaques concernaient des ordinateurs dont les installations Office étaient très dépassées.
  - Plus de la moitié des attaques (56,2 %) ont affecté des installations logicielles Office qui n'avaient pas été mises à jour depuis 2003.
  - La plupart de ces attaques ont touché des utilisateurs Office 2003 qui n'avaient pas appliqué de Service Pack ou autre mise à jour de sécurité depuis la version originale d'Office 2003 d'octobre 2003.
  - Il n'est pas rare que les victimes subissant une exploitation d'Officedisposent d'installations Windows plus récentes. Presque deux tiers (62,7 %) des attaques Office observées au 2S09 ont affecté des versions de Windows mises à jour au cours des 12 mois précédents.
  - Le délai moyen depuis la dernière mise à jour du système d'exploitation pour les ordinateurs de l'échantillon était de 8,5 mois, par rapport aux 6,1 années pour la mise à jour de programme Office, soit un délai quasiment 9 fois plus long.
    - Ces données illustrent le fait que les utilisateurs peuvent garder Windows à jour de façon très rigoureuse et avoir à faire face à des risques d'exploitation, à moins de mettre à jour leurs autres programmes régulièrement.

Tendances pour les violations de la sécurité

Incidents liés à la violation de la sécurité ayant entraîné des conséquences pour la confidentialité

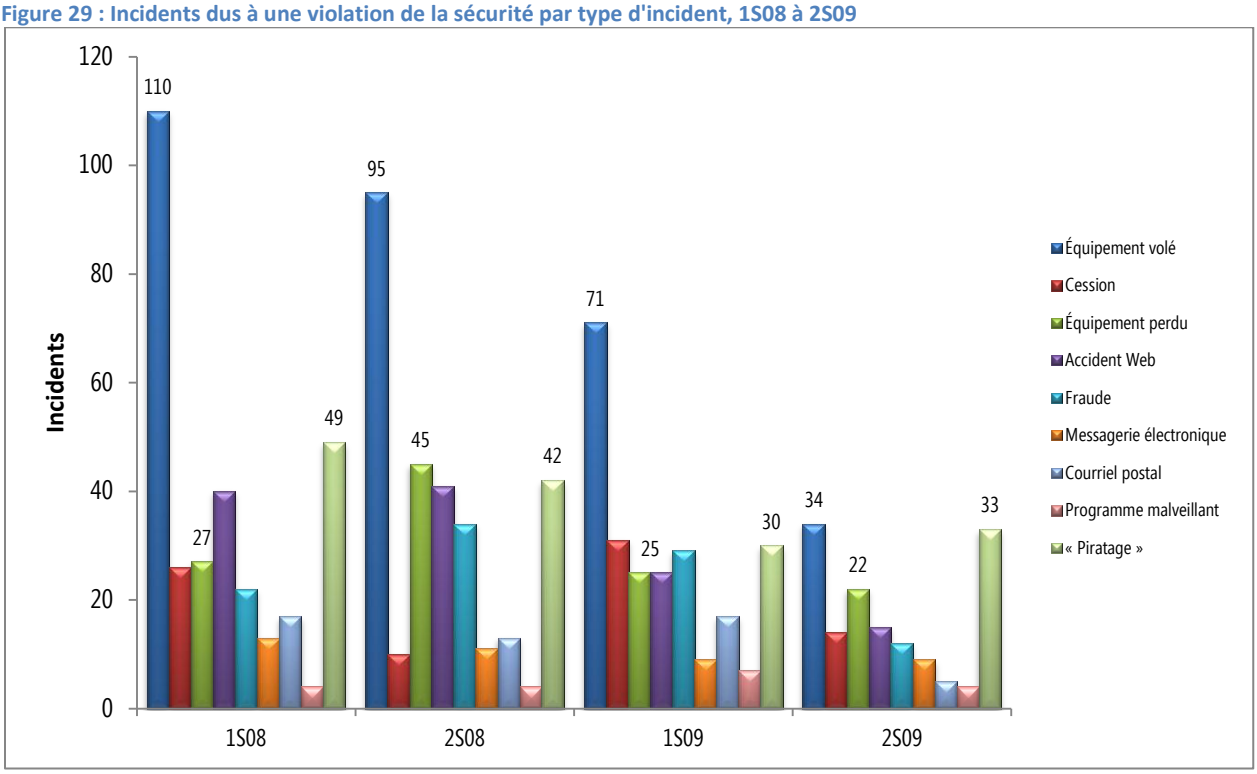
Au cours des dernières années, des lois ont été passées dans un certain nombre de juridictions dans le monde imposant aux organisations d'avertir les personnes affectées en cas de perte de contrôle d'informations qui leur ont été confiées et qui permettent leur identification (PII). Ces notifications obligatoires proposent un point de vue unique sur la façon dont les efforts de sécurité doivent porter sur les problèmes de négligence et de technologie[4].

Figure 28 : Incidents dus à une violation de la sécurité résultant d'attaques et de négligence, 1S08 à 2S09



[4] Depuis 2005, des chercheurs bénévoles étudiant la sécurité se penchent sur les données relatives aux rapports internationaux sur les violations de la sécurité et les enregistrent dans la base de données des données perdues (DataLossDB) à l'adresse http://datalossdb.org

Figure 29 : Incidents dus à une violation de la sécurité par type d'incident, 1S08 à 2S09



- La tendance est clairement à la baisse pour le nombre absolu des incidents de chaque catégorie, excepté les attaques par logiciels malveillants, dont le nombre reste inchangé.
- Les équipements et les supports volés et les pertes accidentelles sur le Web sont les catégories qui enregistrent les baisses les plus importantes.
- La destruction inappropriée des enregistrements professionnels est à l'origine de peu d'incidents. Les organisations peuvent pallier ce type de violations assez facilement, grâce à des stratégies efficaces en matière de destruction d'enregistrements papier et électroniques contenant des informations sensibles.
- Bien que de nombreuses personnes lient les brèches de sécurité à des personnes malveillantes cherchant à accéder illégalement à des données sensibles, les incidents impliquant des attaques (piratage, logiciels malveillants et fraudes) ont été dépassés de façon significative ces dernières années par des incidents impliquant la négligence (perte, vol ou équipement manquant, divulgation accidentelle ou destruction inappropriée).
- Les incidents dus à la négligence ont énormément décliné au cours des deux dernières années (de 110 au 1S08, à 34 au 2S09).
    - Les entreprises prennent davantage de mesures pour sécuriser leurs équipements sensibles, par exemple grâce à des contrôles de sécurité aux entrées des bâtiments ou à des programmes de formation des employés aux meilleures pratiques.
    - L'adoption de solutions de chiffrement puissantes comme le chiffrement de lecteur Windows BitLocker® affectent également ce déclin. Les lois sur la divulgation dans de nombreuses juridictions ne requièrent aucune notification lorsque des données chiffrées sont perdues ou volées, car il est beaucoup plus difficile pour le voleur ou celui qui les a trouvées de les extraire.

Stratégies de prévention

Comment Microsoft IT gère les risques chez Microsoft

Microsoft IT est responsable du fonctionnement quotidien et de la sécurité du réseau global chez Microsoft. Dans cette nouvelle section du Rapport Microsoft sur les données de sécurité, Microsoft IT partage de nombreuses stratégies de prévention spécifiques qu'il utilise pour gérer les risques dans cet environnement très complexe, et fournit des conseils pratiques que les professionnels de l'informatique et de la sécurité peuvent utiliser pour sécuriser leurs propres environnements. Les sujets abordés concernent les différentes façons de protéger l'infrastructure réseau d'une organisation, ainsi que la façon de promouvoir la prise de conscience et des comportements informatiques sûrs dans l'entreprise.

Microsoft a également mis en place une aide très complète pour aider les professionnels de l'informatique à gérer les processus d'évaluation, d'établissement des priorités et de déploiement de mises à jour de sécurité pour les produits Microsoft. Le Guide Microsoft des mises à jour de sécurité est disponible au téléchargement gratuitement, sur le site www.microsoft.com/securityupdateguide.

Le *Rapport complet Microsoft sur les données de sécurité* contient également des stratégies de prévention et des informations sur les meilleures pratiques pour aider les organisations à prévenir les nombreux risques de la sécurité identifiés dans le *Rapport Microsoft sur les données de sécurité*.

Le *Rapport complet Microsoft sur les données de sécurité* peut être téléchargé à partir de www.microsoft.com/france/sir.

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 souhaitons nous assurer qu'il reste aussi fonctionnel et pertinent que possible pour nos clients. Pour tout commentaire sur ce volume ou pour toute suggestion visant à améliorer les prochains, envoyez un message électronique à l'adresse sirfb@microsoft.com.

Merci, bien cordialement,

Microsoft Trustworthy Computing