Rapport sur les e-menaces au 2e semestre 2009

TENDANCES DU MALWARE ET DU SPAM

Avertissement

Les informations et les données exposées dans ce document reflètent le point de vue de BitDefender® sur les sujets abordés à la date de sa publication. Ce document et les informations qu'il contient ne peuvent en aucun cas être interprétés comme un engagement ou un accord de quelque nature que ce soit.

Bien que toutes les précautions aient été prises dans l'élaboration de ce document, l'éditeur, les auteurs et les collaborateurs dénient toute responsabilité pour des erreurs et/ou omissions. Pas plus qu'ils n'assument une responsabilité quelconque pour des dommages consécutifs à l'utilisation des informations qu'il contient. De plus, les informations contenues dans ce document sont susceptibles d'être modifiées sans avertissement préalable. BitDefender, l'éditeur, les auteurs et les collaborateurs ne peuvent garantir que ce document sera repris ultérieurement, ni qu'il sera l'objet de compléments ou de mises à jour.

Ce document et les données qu'il contient sont publiés à titre strictement informatif. BitDefender, l'éditeur, les auteurs et les collaborateurs ne donnent aucune garantie expresse, implicite ou légale relatives aux informations mentionnées dans ce document.

Le contenu de ce document peut ne pas être adapté à toutes les situations. Si une assistance professionnelle est nécessaire, les services d'une personne professionnellement compétente doivent être sollicités. Ni BitDefender, ni les éditeurs du document, ni les auteurs ni les collaborateurs ne peuvent être tenus pour responsables des préjudices pouvant résulter d'une telle consultation.

Le fait qu'une personne ou une organisation, un travail individuel ou collectif, y compris des textes imprimés, des documents électroniques, des sites Web, etc., soient mentionnés dans ce document en tant que référence et/ou source d'information actuelle ou future, ne signifie pas que BitDefender, l'éditeur du document, les auteurs ou les collaborateurs avalisent les informations ou les recommandations que peuvent fournir la personne, l'organisation, les travaux individuels ou collectifs, y compris les textes imprimés, les documents électroniques, les sites Web, etc. Les lecteurs doivent également savoir que BitDefender, l'éditeur du document, les auteurs ou les collaborateurs ne peuvent garantir l'exactitude d'aucune des informations données dans ce document au-delà de sa date de publication, y compris, mais non exclusivement, les adresses Web et les liens Internet indiqués dans ce document qui peuvent avoir changé ou disparu entre le moment où ce travail a été écrit et publié et le moment où il est lu.

Les lecteurs ont la responsabilité pleine et entière de se conformer à toutes les lois internationales applicables au copyright émanant de ce document. Les droits relevant du copyright restant applicables, aucune partie de ce document ne peut être reproduite, mise en mémoire ou introduite dans un système de sauvegarde, ni transmise sous aucune forme ni par aucun moyen (électronique physique, reprographique, d'enregistrement, ou autres procédés), ni pour quelque but que ce soit, sans l'autorisation expresse écrite de BitDefender.

BitDefender peut posséder des brevets, des brevets déposés, des marques, des droits d'auteur, ou d'autres droits de propriété intellectuelle se rapportant au contenu de ce document. Sauf accord express de BitDefender inscrit dans un contrat de licence, ce document ne donne aucun droit sur ces brevets, marques, copyrights, ou autre droit de propriété intellectuelle.

Auteur

Bogdan BOTEZATU, Spécialiste de la communication

Collaborateurs

Răzvan LIVINTZ, Spécialiste de la communication – Menaces WEB 2.0
Daniel CHIPIRIŞTEANU, Analyste Malware
Alexandru MAXIMCIUC, Analyste Malware
Dragoş GAVRILUȚ, Analyste Malware
Ştefan – Cătălin HANU, Analyste Malware
Marius VANȚĂ – Analyste Malware
Alexandru Dan BERBECE - Administrateur de la base de données
Adrian MIRON - Analyste Spam
Irina RANCEA – Analyste Spam

Table des matières

Sommaire

L'année 2009 a été marquée par une large gamme de menaces de sécurité ciblant à la fois les utilisateurs finaux et les réseaux d'entreprise. Le ver Downadrup (connu aussi sous le nom de Conficker ou Kido) a beaucoup progressé et est parvenu à rester l'une des trois principales menaces mondiales en 2009. Bien qu'il ne soit pas réellement dangereux (les variantes A, B, C ne sont pas porteuses de charges malveillantes), ses mécanismes de diffusion et sa résistance à la détection pourraient servir de base à de futurs malwares extrêmement destructeurs.

Au cours des six mois écoulés depuis notre précédent rapport, les auteurs de malware ont poursuivi leurs attaques par email, tout en recherchant activement de nouvelles méthodes de dissémination de leurs produits. De vastes réseaux sociaux, et d'éphémères pages Web stimulées par d'intenses stratégies BlackSEO, sont également devenus des terrains névralgiques propices au téléchargement involontaire et à la diffusion de vers.

Le très populaire iPhone, téléphone mobile d'Apple, a désormais une part de marché suffisamment importante pour constituer une cible intéressante. Son emprise sur le marché, associée au fait que beaucoup d'utilisateurs choisissent de « déverrouiller » (jailbreak) le système, permet aux auteurs de malware de réussir à exploiter le mot de passe par défaut utilisé par l'utilitaire SSH (secure shell) de Unix pour recueillir des coordonnées bancaires sensibles et d'ajouter l'appareil à un botnet.

Le nombre d'attaques de type déni de service distribué est en augmentation en termes de violence et de gravité des dommages causés aux entreprises affectées. Début août, de telles attaques ont visé de nombreux services Web très influents, comme YouTube, Blogger, Twitter et Facebook, et des rumeurs non confirmées, internes aux sociétés ciblées, avançaient que ces attaques soigneusement coordonnées n'étaient pas des tentatives de chantage mais avaient plutôt des objectifs politiques.

Si ces affirmations sont exactes, le champ de bataille s'est déplacé vers le cyber-espace. Si ce n'est pas le cas, ceci veut dire que les cyber-criminels ont atteint un tel niveau d'organisation et de logistique qu'ils sont en train de devenir menaçants à un degré inimaginable pour les fournisseurs de services comme pour leurs utilisateurs. Dans un cas comme dans l'autre, la guerre contre la cyber-criminalité est devenue beaucoup plus âpre.

.

Au cours du deuxième semestre 2009, les auteurs de malware ont concentré leurs efforts sur l'augmentation de leurs revenus. Adware sophistiqué, chevaux de Troie bancaires et une vaste gamme de faux logiciels antivirus (rogues) ont ciblé sans relâche l'utilisateur lambda d'ordinateurs.

Le spam a également pris de l'ampleur pour atteindre un taux de 88,9 %, soit 0,3 % de plus qu'au cours du premier semestre 2009. Le spam concernant les médicaments et l'hameçonnage (phishing) ont été les secteurs d'activité les plus lucratifs, l'éducation et les logiciels OEM gagnant également du terrain.

Win32.Worm.Downadup a pratiquement disparu de la mémoire collective après le 1er avril, mais reste une des trois principales e-menaces. Les laboratoires BitDefender estiment que le nombre d'ordinateurs infectés par toutes les variantes de Downadup dépassent facilement 7 millions. La persistance du ver met en évidence le fait que beaucoup d'utilisateurs refusent encore d'utiliser des correctifs de sécurité, même si elles sont disponibles gratuitement.

Les vedettes du malware

● Des événements internationaux, comme la mort de Michael Jackson et l'émergence de la grippe porcine, ont été exploités au maximum par les auteurs de malware comme tremplins au lancement de leurs dernières contaminations.

● Trojan.Clicker.CM occupe le premier rang des e-menaces du deuxième semestre. Il est utilisé pour imposer des publicités dans les navigateurs des utilisateurs lorsque ces derniers visitent les zones d'ombre du Web (comme les sites pornographiques ou les services proposant des logiciels de type « warez »). Le taux alarmant d'infection fait apparaître que les auteurs de malware sont attirés par le gain et que la fraude de type « pay-per-click » suffit à motiver les cyber-criminels.

● Les attaques de type déni de service distribué deviennent une mode chez les administrateurs de botnet, qui ciblent désormais à la fois les institutions financières et les sites Web en vogue comme Blogger, YouTube, Facebook et Twitter. Plus important encore, les enjeux financiers de la guerre entre les cyber-criminels et les fournisseurs de services légitimes semblent avoir fait place à des enjeux politiques.

● Les plateformes de réseaux sociaux et de services de messagerie instantanée, de même que les réseaux peer-to-peer, sont des vecteurs privilégiés pour la dissémination des vers. Au second semestre 2009 sont apparus Worm.P2p.Palevo.B, Trojan.Agent.Delf.RHO, Win32.Worm.Rimecud.C ainsi que Win32.Worm.Koobface.ALX.

● Les faux logiciels antivirus (rogues) sont en hausse, propulsés par l'utilisation intensive de stratégies de Black Hat SEO et profitant du manque de connaissances techniques des utilisateurs. Au cours de la seconde moitié de l'année, les créateurs de faux antivirus sont allés encore plus loin dans le franchissement des frontières de la légalité en donnant à leurs œuvres un minimum de fonctionnalités utilitaires destinées à éviter toute conséquence désagréable en cas de procès.

● Les messages de hameçonnage ont rapidement poursuivi leur ascension déjà présagée au premier semestre 2009, et arrivent désormais au deuxième rang, juste derrière les spams pharmaceutiques. Une fois encore, les attaquants ont ciblé les secteurs qui rapportent un maximum de gains dans un minimum de temps.

● De nombreuses vulnérabilités systémiques ont été découvertes dans les produits de Microsoft. La société de Redmond a publié six communiqués de sécurité successifs, de MS09-029 à MS09-035, décrivant les failles d'Internet Explorer qui peuvent permettre qu'un code à distance se déploie sur des ordinateurs lorsque leurs utilisateurs visitent une page Web créée à cette fin. Le plus surprenant est que l'une des vulnérabilités avait été décrite en 2008, mais que Microsoft n'avait pas fourni de correctif.

● Adobe a également signalé au moins 12 points de vulnérabilité susceptibles de permettre l'exécution d'un code illégitime. Ces « exploits » affectent en particulier les versions 9 et 10 d'Adobe Flash Player ainsi qu'Acrobat Reader.

● L'une des vulnérabilités les plus critiques découvertes cette année est le bug SMB 2.0 qui affectent tous les systèmes d'exploitation plus récents que Vista, à l'exception de Windows 7 RTM et Windows Server 2008 R2. Mais la version RC de Windows 7 est concernée.

Les menaces de type malware

Comme les déjà « traditionnelles » infections dues au Trojan.Clicker.CM, Win32.Worm.Downadup s'est révélé être l'une des e-menaces les plus notoires des six derniers mois. Si le Web reste l'un des moyens favoris des auteurs de malware pour disséminer leurs menaces, les techniques fondées sur la fonction Aurorun ont rapidement gagné du terrain. Par défaut, les supports de stockage amovibles contiennent tous un script autorun.ini qui indique à l'ordinateur quel fichier exécuter quand le périphérique est branché. Il est cependant fréquent que les auteurs de malware falsifient le fichier pour qu'il lance diverses applications malveillantes. Bien qu'elle soit extrêmement utile aux utilisateurs d'ordinateur peu expérimentés, la fonctionnalité a été supprimée dans Windows Vista SP2 et Windows 7 pour éviter les contaminations.

Le top 10 du malware mondial

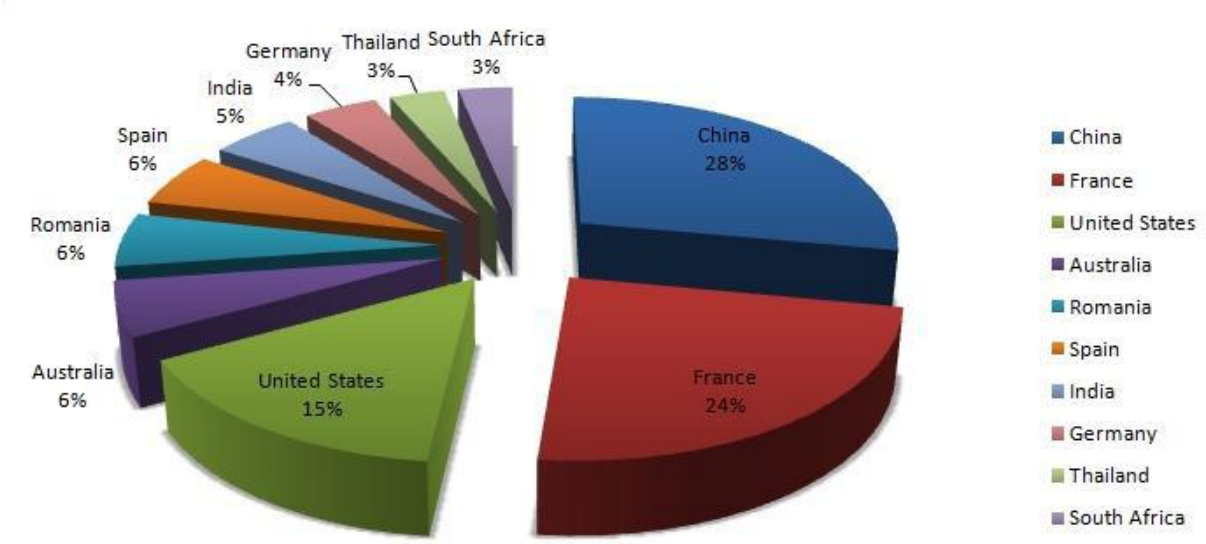


Figure 1: Répartition des malwares par pays

Au cours des six derniers mois, les pays les plus actifs en termes de propagation de logiciels malveillants ont été la Chine, la France et les Etats-Unis, suivis par l'Australie (qui avance d'une place par rapport au premier semestre 2009), la Roumanie (qui avance d'une place également) et l'Espagne (qui recule d'une place).

[1] Sous Windows 7 et Windows Server 2008 R2, seuls les lecteurs de type DRIVE_CDROM lisent et utilisent le fichier autorun.inf. De plus, l'utilisateur ne peut pas annuler cette configuration en modifiant le Registre.

Juillet – Décembre 2009

01.	**TROJAN.CLICKER.CM**	8,97%
02.	Trojan.AutorunINF.Gen	8,41%
03.	**TROJAN.WIMAD.GEN.1**	4,41%
04.	Win32.Worm.Downadup.Gen	4,13%
05.	**EXPLOIT.PDF-JS.GEN**	3,39%
06.	Win32.Sality.OG	2,60%
07.	**TROJAN.AUTORUN.AET**	1,97%
08.	Worm.Autorun.VHG	1,59%
09.	**TROJAN.JS.PYV**	1,50%
10.	Exploit.SWF.Gen	1,47%
11.	Autres	61,57%

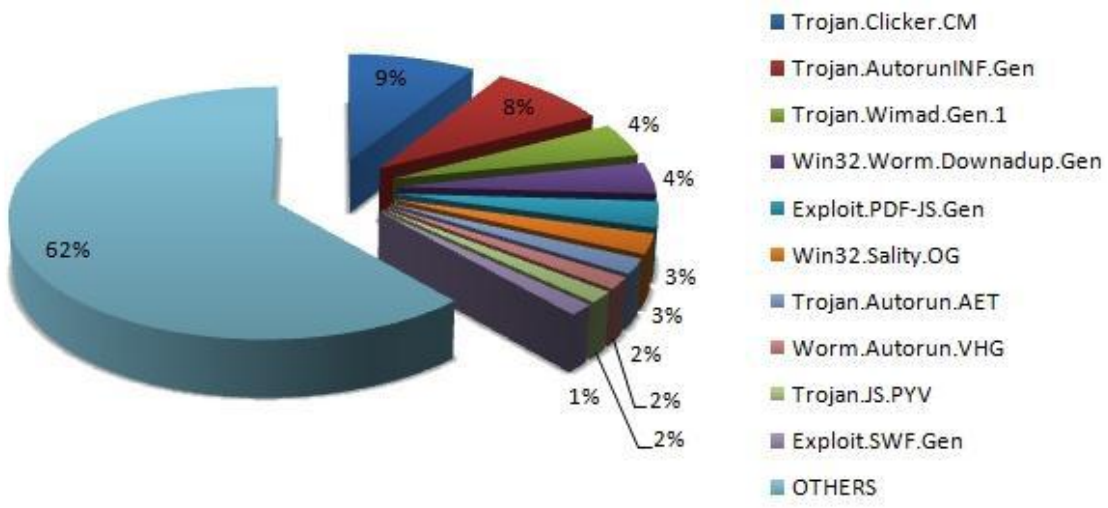


Figure 2 : Top 10 mondial des menaces de type malware au premier semestre 2009

1. Trojan.Clicker.CM

Au premier rang du classement du Top 10 des e-menaces établi par BitDefender pour le deuxième semestre 2009, se trouve **Trojan.Clicker.CM**, principalement présent sur les sites Web hébergeant des applications illégales comme des déverrouilleurs, générateurs de clés et numéros de série pour les logiciels les plus courants. Ce cheval de Troie est utilisé en général pour introduire des publicités dans le navigateur. Trojan.Clicker représente 8,87 % des fichiers infectés.

2. Trojan.AutorunInf.Gen

Au deuxième rang du classement du Top 10 des infections au deuxième semestre 2009, **Trojan.AutorunInf.Gen** est un mécanisme générique de diffusion de malware via des supports amovibles comme des unités de stockage flash, des cartes mémoires ou des disques durs externes. **Win32.Worm.Downadup** et **Win32.TDS** sont deux des plus célèbres familles de malware à utiliser cette approche pour déclencher de nouvelles infections.

3. Trojan.Wimad.Gen.1

Trojan.Wimad.Gen.1 occupe la troisième place, en représentant 4,41 % des infections répandues au cours du second semestre. Il exploite en particulier la capacité des fichiers ASF de télécharger automatiquement à distance le codec voulu pour déployer des fichiers binaires infectés dans le système hôte. Le format ASF est en fait un conteneur de stockage de données au format WMA (Windows Media Audio) ou WMV (Windows Media Video). Ces fichiers WMV sont en général distribués dans le cadre de téléchargements illégaux sur les sites Web Torrent. Les distributeurs de malware profitent couramment du battage médiatique organisé autour de films qui ne sont pas encore sortis pour installer Trojan.Wimad sur leurs torrents. Lorsque le fichier WMV spécialement conçu est lu localement, il demande à télécharger un « codec spécial », qui se trouve être en réalité du code malveillant hébergé sur le site Web d'un tiers.

Figure 3 : Torrent contenant un fichier WMV infecté. Au moment de la rédaction de ce texte, le film Avatar n'était pas encore sorti.

4. Win32.Worm.Downadup

Figurant au 4ème rang dans le rapport de BitDefender sur le paysage des e-menaces, **Win32.Worm.Downadup.Gen** représente 4,13 % de l'ensemble des infections. Ce ver exploite une vulnérabilité dans le service Serveur de Microsoft Windows qui peut permettre l'exécution de code à distance en cas de réception d'une requête RPC spécialement conçue (MS08-67) pour se propager sur d'autres ordinateurs du réseau local et empêcher les utilisateurs d'accéder à Windows Update et aux pages Web des fournisseurs de solutions de sécurité. Les plus récentes variantes du ver installent également de faux logiciels antivirus[2], entre autres.

5. Exploit.PDF-JS.Gen

Exploit.PDF-JS.Gen est un générique de détection de fichiers PDF spécialement conçus pour exploiter les différentes vulnérabilités du moteur Javascript d'Adobe PDF Reader pour exécuter du code malveillant sur l'ordinateur de l'utilisateur. À l'ouverture du fichier PDF infecté, un code Javascript spécialement conçu déclenche à distance le téléchargement de codes malveillants. La menace se situe au 5ème rang, représentant 3,39 % des infections globales.

[2] Pour lire le rapport complet concernant Win32.Worm.Downadup et son évolution au cours de l'année 2009, consultez le livre blanc de BitDefender à l'adresse http://www.bitdefender.fr/NW1262-fr--BitDefender-publie-le-livre-blanc-«-Conficker-—-Un-an-après-».html

6. Win32.Sality.OG

Cette famille de contaminateurs polymorphes de fichiers occupe la sixième place du classement des e-menaces du deuxième semestre 2009, représentant plus de 2,60 % des infections totales. Pour s'auto-propager, le virus ajoute son code crypté à des fichiers exécutables (binaires .exe et .scr). Il fait également figurer un élément rootkit qui se déploie ensuite sur la machine infectée pour dissimuler la contamination. Particulièrement important concernant Win32.Sality.OG est le fait qu'il utilise une liste de mots clés pour trouver et interrompre les procédures et les services associés aux applications antivirus ou de surveillance.

7. Trojan.Autorun.AET

Au septième rang, on trouve **Trojan.Autorun.AET**, un code malveillant se propageant via les dossiers partagés de Windows, aussi bien que sur les supports de stockage amovibles. Ce cheval de Troie exploite la fonction Autorun de Windows destinée à lancer automatiquement des programmes lorsqu'un support de stockage infecté est branché. L'e-menace Trojan.Autorun.AET représente 1,97 % de l'ensemble des infections.

8. Worm.Autorun.VHG

Worm.Autorun.VHG est un ver Internet/réseau qui exploite la vulnérabilité MS08-067 de Windows pour s'exécuter lui-même à distance en utilisant une requête RPC (remote procedure call) spécialement conçue (type d'approche également utilisé par **Win32.Worm.Downadup**). Ce ver occupe la sixième place avec 1,59 % de l'ensemble des infections.

9. Trojan.JS.PYV

La neuvième place du Top du malware de la première moitié de 2009 est occupée par **Trojan. JS.PYV**, un script malveillant qui s'attaque aux utilisateurs naviguant sur des sites Web distributeurs de malware, ou sur des sites légitimes qui ont été compromis. Les sites Web infectés engendrent une fenêtre iframe invisible, capable d'exécuter un code à partir d'un emplacement à distance. Sa présence dans le classement du Top 10 des e-menaces au niveau international est révélatrice du fait qu'un grand nombre de sites légitimes ont été compromis sans même que leurs administrateurs s'en aperçoivent.

10. Exploit.SWF.Gen

Figurant au dernier rang du Top des malwares du deuxième semestre, Exploit.SWF.Gen est une détection générique d'une famille de fichiers Adobe Flash spécialement conçus pour permettre l'exécution à distance d'un fichier en exploitant une vulnérabilité d'Adobe Flash Player. En modifiant la valeur d'enregistrement du fichier SWF, l'attaquant peut placer le programme dans une situation de dépassement de tampon. En général, cet exploit télécharge et installe des chevaux de Troie voleurs de mots de passe.

La montée des Botnets

Les Botnets (également appelés « Réseaux de zombies ») sont des réseaux de PC infectés qui peuvent être contrôlés à distance pour se comporter comme un seul et unique système, extrêmement puissant. Pour prendre le contrôle d'une machine, l'attaquant doit amener par la ruse l'utilisateur à installer un outil d'accès à distance (généralement un cheval de Troie de porte dérobée). Une fois l'infection effective, les cyber-criminels peuvent à distance accéder à l'ordinateur infecté et le contrôler, sans le consentement de l'utilisateur ni interaction avec lui.

Les botnets peuvent servir à différentes manœuvres illégales, allant de l'envoi de spam aux attaques de type déni de service distribué, voire à des vols massifs de données. Leur potentiel lucratif étant pratiquement sans limites, ils sont considérés comme des valeurs marchandes et traités comme telles : les botnets peuvent se vendre, se prêter ou même être utilisés comme outils pour des projets « en interne ».

Comme l'indique le graphique qui suit, les familles de bots les plus actives sont Rustock, Ozdok[3] et Kobcka, équipés tous les trois d'une fonctionnalité rootkit qui leur permet d'agir sans être détectés. Ils sont les principaux responsables, entre autres, de l'énorme quantité de spam concernant les produits pharmaceutiques.

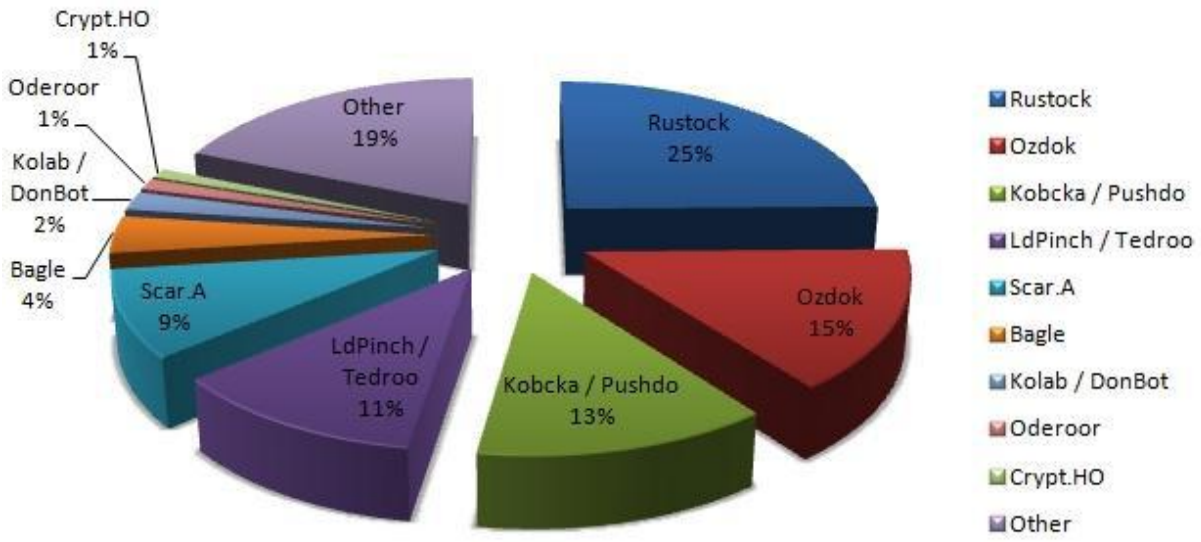


Figure 4 : Activité botnet par type de bots

[3] Le botnet Ozdok avait réussi à surpasser le réseau Storm zombie, mais les efforts coordonnés des autorités et des FAI y ont mis fin début novembre.

Malware Web 2.0

Du fait de leur grande popularité parmi les utilisateurs d'ordinateurs et le nombre d'informations personnelles qu'ils contiennent, les plates-formes de réseaux sociaux sont devenues le terrain de chasse préféré des auteurs de malware. Au moment de la rédaction de ces commentaires, Facebook venait juste de célébrer le chiffre de 350 millions de comptes, chacun d'entre eux contenant des informations personnelles, ou au moins suffisamment pour servir de base à une pêche par hameçonnage. Les plates-formes de messageries instantanées sont également des vecteurs appréciés de dissémination des malwares : de nombreuses familles de vers spéculent sur l'ignorance des utilisateurs pour les attirer vers des liens aboutissant à des applications infectées.

Spam et hameçonnage (phishing)

En tant que l'un des principaux réseaux sociaux du monde, Facebook a depuis longtemps été exploité avec succès pour persuader ses utilisateurs de divulguer leurs informations personnelles. La technique d'hameçonnage est simple, mais efficace : les victimes reçoivent en général un spam annonçant des mises à jour des conditions d'utilisation de Facebook ou même une prétendue fermeture de compte en raison d'une activité suspecte. Pour réactiver son compte, l'utilisateur doit suivre un lien et se connecter à la plateforme. Dès qu'il appuie sur le bouton de connexion, ses authentifiants sont envoyés à un tiers non-autorisé via un script PHP. Les comptes ainsi récupérés seront utilisés pour déclencher des contaminations de vers ou pour rassembler des données utilisables dans d'autres tentatives de hameçonnage.

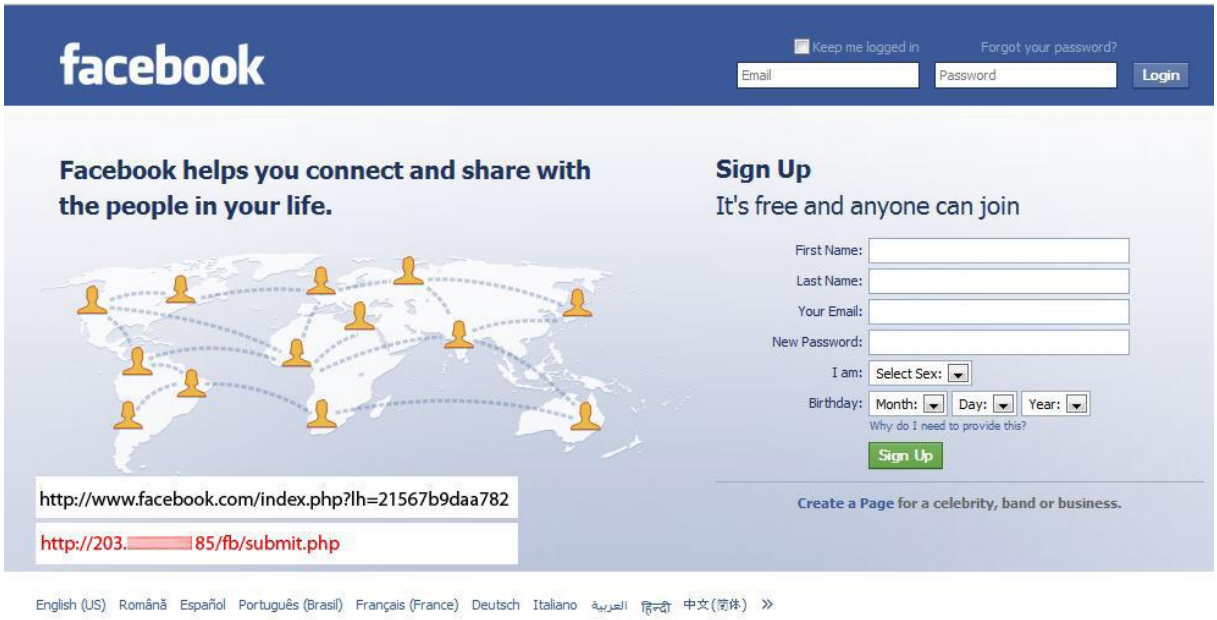


Figure 5 : Page d'hameçonnage sur Facebook

Le spamming est une pratique courante également parmi les utilisateurs des services de réseaux sociaux. Twitter et Facebook ont imposé des politiques strictes à ce sujet, mais d'autres services ont à peine pris en compte ce risque. Par exemple, le réseau professionnel LinkedIn est devenu le terrain de jeux préféré des particuliers et des organisations proposant des services divers. Les spammeurs tentent de pénétrer dans les réseaux professionnels et les bombardent de messages publicitaires vantant leurs produits ou services. Le message ci-dessous représente une offre d'emploi dans une agence de communication. Il est rédigé en roumain et peut être assimilé à du spam car il essaie de vendre des services de communication aux employés de nombreuses sociétés roumaines, bien que LinkedIn demande expressément à ses utilisateurs de ne pas prendre contact avec des gens qu'ils ne connaissent pas, ni directement ni indirectement. Au cours des six derniers mois, BitDefender a identifié de nombreuses variantes du spam LinkedIn – un signe avertisseur du fait que la précarité de la situation économique mondiale incite de plus en plus de gens à proposer leurs services sur les réseaux sociaux.

Figure 6 : Demande de contact pour proposition de services sur LinkedIn

Vers et Bots

Au moment où le spam et le hameçonnage atteignent 80 % des e-menaces sur les réseaux sociaux, on constate une montée rapide des vers exploitant de larges plateformes. Au cours des six derniers mois de 2009, de nombreuses familles de vers ont harcelé les plus importants réseaux sociaux que sont Twitter, MySpace et Facebook.

Apparu en août 2008, le ver Koobface s'est révélé être l'une des e-menaces les plus destructrices pour les réseaux sociaux. Les équipes de cybercriminels à l'origine de ce ver en ont libéré de multiples versions pour augmenter la portée de leur action et atteindre le plus grand nombre possible de ces réseaux[4]. Les infections virales ont pris la plupart des plates-formes par surprise et les dommages infligés aux utilisateurs ont dépassé l'imagination[5], désactivant certains des antivirus et exportant des données sensibles comme des références bancaires et des mots de passe de messagerie instantanée à leur profit. La technique était simple mais efficace : le ver utilisait des comptes compromis pour inciter des amis du réseau à cliquer sur les liens infectés.

[4] Le ver avait à l'origine été créé pour Facebook, mais des variantes de Win32.Worm.Facebook.A ont par la suite pris pour cible des comptes de MySpace et de Twitter. BitDefender a été le premier fournisseur de solutions de sécurité à donner l'alerte et à offrir une protection contre toutes les versions de Koobface. Pour plus d'informations sur Win32.Worm.Koobface.A, une description du ver est disponible à l'adresse http://www.bitdefender.fr/VIRUS-1000362-fr--Win32.Worm.KoobFace.A.html

[5] Win32.Worm.Koobface.ALX contient un composant rootkit qui peut désactiver certains utilitaires antivirus et exporter des données sensibles (coordonnées bancaires électroniques et mots de passe de messageries instantanées) vers un autre ordinateur.

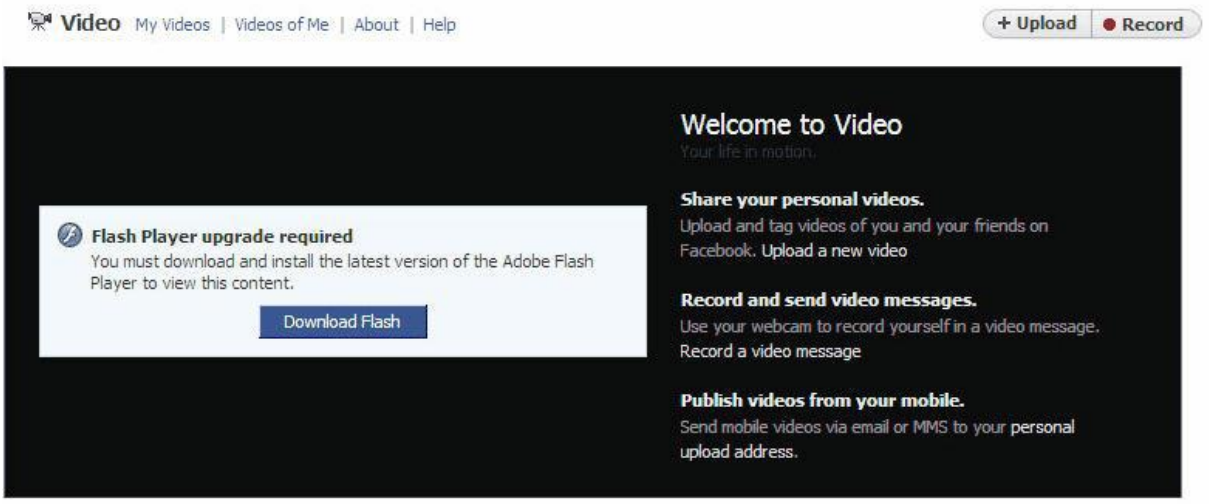


Figure 7 : Le ver Koobface se faisant passer pour une mise à jour de Flash Player

D'autres vers de Facebook associent ingénierie sociale et manipulations d'URL très sophistiquées provoquant des requêtes « cross-site » contrefaites pour que leur message apparaisse à chaque fois que l'utilisateur clique sur un lien infecté. Les attaques de ce type (également connues sous le sigle XSRF) s'effectuent à partir de iframes contenant des scripts tiers qui manipulent Facebook et le font se comporter comme si l'utilisateur du compte avait publié quelque chose sur son mur.

Heureusement, ce vers ne véhiculait pas de charge malveillante et n'avait aucun effet sur les utilisateurs piégés en dehors de l'embarras probablement provoqué par la photo ci-dessous.

Figure 8: Résultat d'une contrefaçon « cross-site » sur Facebook

Les services de messageries instantanées ont également été bien exploités par les auteurs de malware à cause de la popularité dont ils jouissent auprès des utilisateurs d'ordinateurs. Skype a connu de mauvais moments depuis début 2008 avec les vers de messagerie instantanée mais, au moment où nous écrivons, les messageries actuellement visées sont Yahoo Messenger et MSN Messenger.

Détecté pour la première fois cette année à la fin du mois de juin, Worm.P2P.Palevo.B est une e-menace extrêmement agressive, ciblant essentiellement les utilisateurs de services peer-to-peer. Un des premiers symptômes de l'infection est l'augmentation de l'activité réseau sur les ports UDP provenant de explorer.exe et la présence d'un fichier caché, nommé sysdate.exe, dans le dossier "%systemdrive%\RECYCLER\S-1-5-21-[groupes de chiffres aléatoires]".

Le ver a été conçu afin de se diffuser de diverses manières. Il peut ajouter son code à la liste des partages P2P d'applications de partages de fichiers connues telles qu'Ares, BearShare, iMesh, Shareza, Kazaa, DC++, eMule et LimeWire, mais il peut également infecter tout support amovible USB branché sur une machine déjà infectée ou même des lecteurs réseau connectés en local.

Worm.P2P.Palevo.B peut aussi envoyer des liens à des sites Web infectés s'il détecte la présence de MSN Messenger sur le système compromis, trompant ainsi la vigilance des contacts pour qu'ils téléchargent et installent le vers à leur insu.

Le ver ne limite pas ses habitudes destructrices à infecter d'autres hôtes et à laisser l'utilisateur devant un système à peine utilisable du fait de l'activité accrue. Il peut également intercepter des mots de passe et d'autres données sensibles saisies dans les navigateurs Mozilla Firefox et Microsoft Internet Explorer, ce qui le rend extrêmement dangereux pour les utilisateurs de services bancaires ou les personnes effectuant des d'achats en ligne.

Worm.P2P.Palevo.B contient un composant backdoor qui permet aux attaquants de prendre à distance le contrôle de la machine infectée et de s'en servir comme ils l'entendent (par exemple pour installer d'autres logiciels, exporter des documents enregistrés en local, falsifier les scrutins en ligne à partir de plusieurs IP, ou même lancer des attaques TCP/UDP massives contre des serveurs Internet.

Un autre cheval de Troie agressif exploitant Yahoo Messenger est Trojan.Agent.Delf.RHO, un malware qui se propage par l'intermédiaire de liens dans les messages instantanés envoyés par des utilisateurs infectés. Pour inciter l'utilisateur à accéder aux liens malveillants, le cheval de Troie les place dans un contexte acceptable. Par exemple, certains messages avertissent la victime qu'elle est infectée et devrait immédiatement télécharger un outil de désinfection en utilisant le lien fourni, alors que d'autres proposent un outil permettant de gérer les contacts. Trojan.Agent.Delf.RHO semble avoir pour origine la Roumanie car les messages qu'il envoie sont rédigés en roumain.

Le lien dirige l'utilisateur vers un site Web ou un blog contenant une vidéo demandant à l'utilisateur de télécharger un codec qui se révèle être le cheval de Troie lui-même. Une fois exécuté, le fichier installe : *%WINDIR%\system32\yahooui.exe, %WINDIR%\system32\yahooauth2.dll, %WINDIR%\system32\ssleay32.dll, et %WINDIR%\system32\libeay32.dll.*

Ce cheval de Troie attend que l'utilisateur se connecte à son compte et ensuite commence à envoyer des messages spam aux contacts figurant dans sa liste.
Trojan.Agent.Delf.RHO est moins anodin qu'il n'en a l'air : en dehors d'être agaçant, il invite des amis à la fête, comme le très dangereux **Trojan.Spy.Banker.ACFQ**, qui tente de séduire l'utilisateur en lui donnant accès à des sites de hameçonnage visant des services bancaires en ligne.

Les menaces de type spam

Au cours de la seconde moitié de 2009, le paysage du spam est resté à peu près le même, avec les Produits pharmaceutiques canadiens occupant le rang le plus élevé à l'échelle mondiale. La plupart des messages contenaient de la publicité pour des produits augmentant la vigueur sexuelle, alternatifs au Cialis, Viagra et Levitra. Cette catégorie de spam est extrêmement lucrative, car les produits commandés aux boutiques en ligne de produits pharmaceutiques canadiens ne sont en général jamais livrés au client, qui a souvent honte de le signaler aux autorités. Plus grave encore est le fait que ces paiements en ligne sont extrêmement risqués, le spammer ayant accès à toutes les données de la carte de crédit utilisée et pouvant retirer autant d'argent qu'il le souhaite.

Taux de distribution du spam par pays

Les pays les plus actifs en termes de spam figurent dans le tableau qui suit.

Distribution du spam par zone d'origine
Juillet – Décembre 2009

POURCENTAGE de SPAM	
Etats-Unis	27
VIETNAM	9,63
COREE	5,77
CHINE	5,28
BRESIL	4,91
COLOMBIE	4,1
RUSSIE	3,9
ARGENTINE	3
ESPAGNE	2,7
POLOGNE	0,5
AUTRES	33,21

Tandis que les Etats-Unis et le Vietnam comptent pour un tiers du nombre de messages distribués dans le monde, l'Argentine, l'Espagne et la Pologne arrivent en fin de classement avec un pourcentage d'environ 6 %. La Russie enregistre une petite diminution par rapport au premier semestre de l'année (passant de 4,2 à 3,9 %), sans doute liée aux initiatives des FAI de restreindre les activités des botnets et d'interdire les serveurs de messagerie illicites sur leur territoire.

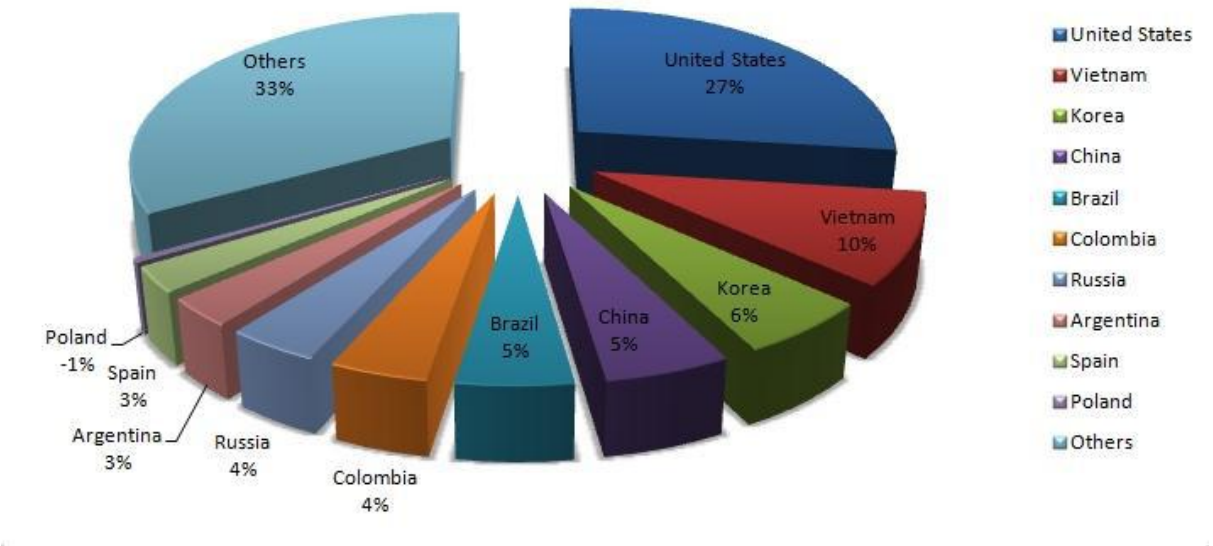
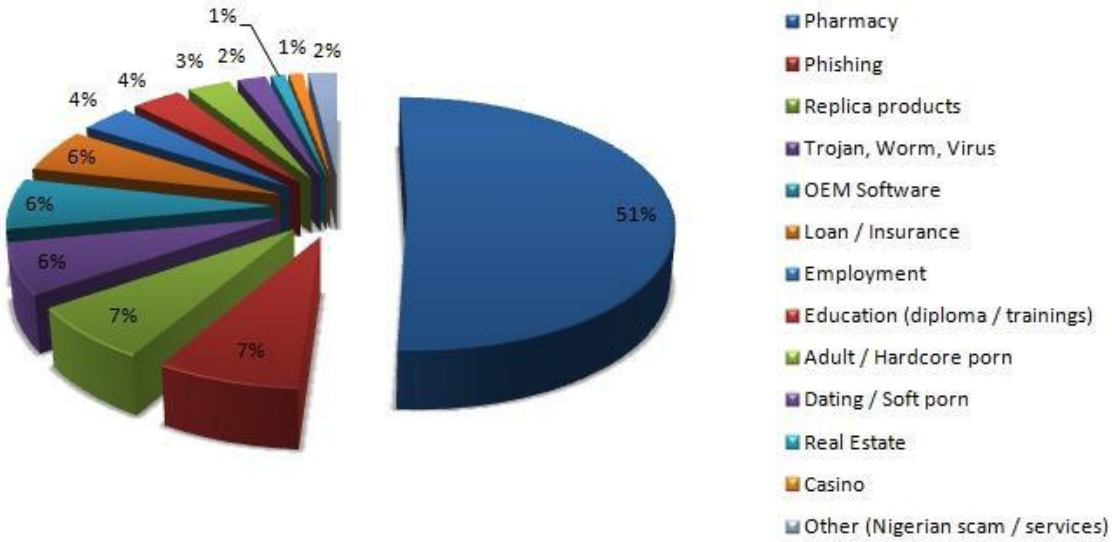


Figure 9 : Taux de distribution du spam par pays

Taux de spam par catégories

Les laboratoires Antispam de BitDefender ont calculé que les produits ayant fait l'objet du maximum de publicités au cours des six derniers mois de l'année 2009 sont les produits pharmaceutiques canadiens qui représentent 51 % de la totalité du spam envoyé à l'échelle mondiale.
Les tentatives de hameçonnage envoyées par courrier électronique ont conservé le même taux que celui observé au cours du premier semestre, bien que les institutions visées ne soient plus tout à fait les mêmes.



Les produits contrefaits se situent au troisième rang au cours de ces six derniers mois, mais la quantité de messages faisant de la publicité pour les contrefaçons augmente rapidement au moment des fêtes, lorsque les utilisateurs les achètent probablement pour les offrir en cadeau. Le spam contenant du malware attaché représente 6 % du montant total des courriers électroniques non sollicités. Si les chiffres sont restés les mêmes qu'au premier semestre 2009, les documents attachés envoyés au cours du second ont eux spectaculairement changés, comme décrit dans la rubrique suivante.

Tendances du spam

Le spam représente 88,9 % du montant total des messages électroniques envoyés dans le monde entier. Les messages textuels constituent la forme la plus fréquente du spam, tandis que le spam image est extrêmement rare, avec un pourcentage se situant entre 2,3 et 2,5. La taille moyenne d'un message spam est de 3,5 Ko, mais peut s'échelonner entre 2 et 9 Ko en fonction de son type.

Au cours de ce deuxième semestre, les spammeurs se sont particulièrement servi des événements internationaux ou nationaux pour inciter leurs victimes à ouvrir leurs messages. L'une des plus importantes vagues de spam a été lancée après la mort controversée de Michael Jackson. En juillet dernier, BitDefender a identifié de multiples courants de spam prétendant dévoiler plus d'informations sur l'assassin de Michael Jackson, mais véhiculant en fait de la publicité pour des produits améliorant la performance sexuelle et des malwares[6].

Figure 10 : Message spam avec malware embarqué exploitant la mort de Michael Jackson

Dans le cas présent, le fichier joint est une variante de Trojan.Spy.Zbot.UI qui, une fois installée, ajoute l'ordinateur compromis au Botnet Zeus, le transforme ensuite en relais de spam, envoyant des centaines de messages à l'insu de l'utilisateur et consommant de précieuses ressources informatiques.

[6] Pour plus d'informations sur la façon dont la mort de Michael Jackson a été exploitée par les auteurs de malware et les spammeurs, visitez http://www.malwarecity.com/blog/michael-jacksons-unknown-killer-481.html.

Les abus sexuels subis par Samantha Geimer et l'arrestation de Roman Polanski en septembre ont donné aux escrocs une nouvelle occasion d'envoyer des spams de leurs produits et d'attirer l'attention sur les faux logiciels antivirus. Pour convaincre les utilisateurs de visiter leurs sites Web malveillants, les spammeurs ont non seulement envoyé des millions de messages électroniques, mais ont utilisé des sites Web parfaitement optimisés (BlackSEO) pour disséminer de faux logiciels antivirus.

Figure 11 : Pages Web malveillantes optimisées pour ces mots-clés

Ces liens redirigent le navigateur vers plusieurs sites Web enregistrés sur des domaines .cn contenant le plus récent membre de la famille des faux antivirus : **Total Security Rogue,** identifié par BitDefender comme étant Trojan.FakeAV.SQ.

Hameçonnage et usurpation d'identité

Par rapport à la première moitié de 2009, le nombre de messages de hameçonnage est resté relativement stable, bien que leurs auteurs aient choisi pour victimes des institutions susceptibles de leur apporter un maximum de gain dans un minimum de temps.

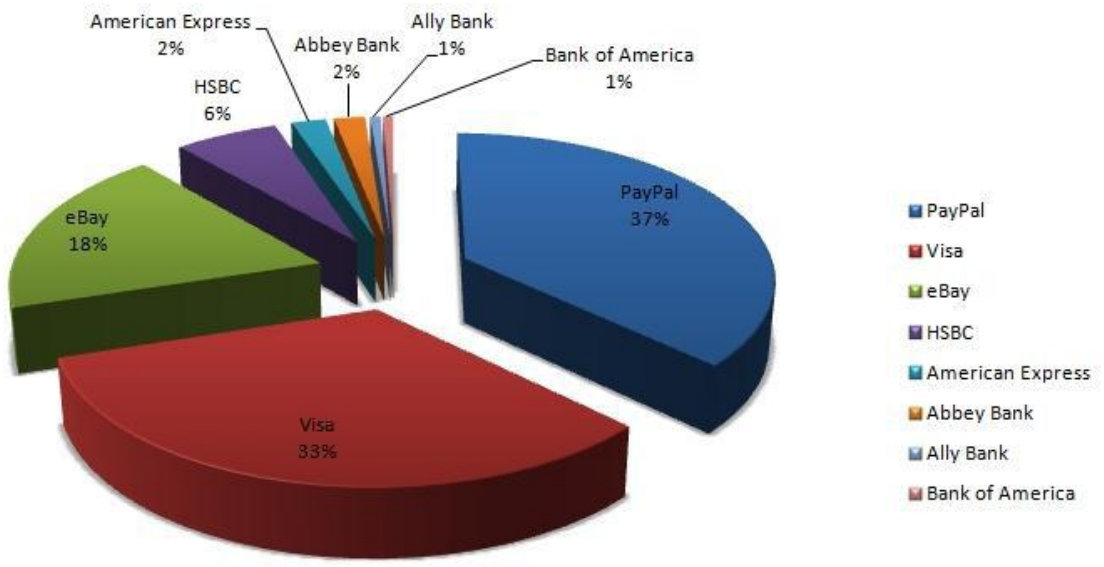


Figure 12 : Top des institutions les plus visées par le hameçonnage au cours du deuxième semestre 2009

Comme le montre le camembert ci-dessus, les cibles principales des hameçonneurs sont PayPal, Visa et eBay, suivis par HSBC, American Express et Abbey Bank. Ally Bank et Bank of America figurent en dernier avec un peu plus de 1% seulement du nombre total de messages d'hameçonnage.

Ces messages visent pour la plupart des utilisateurs anglophones utilisant les services d'au moins une des institutions citées.

Par exemple, les clients de eBay ont eu affaire à une campagne de hameçonnage de moyenne ampleur. Il leur était demandé de remplir un nouveau « formulaire de confirmation » obligatoire, en cliquant sur le lien fourni dans le spam. Les utilisateurs confiants suivant ces liens se voyaient présenter un formulaire qui n'avait rien à voir avec eBay, mais recueillaient au contraire des informations personnelles et financières susceptibles d'être utilisées pour des fraudes à la carte bancaire, voire des vols d'identité.

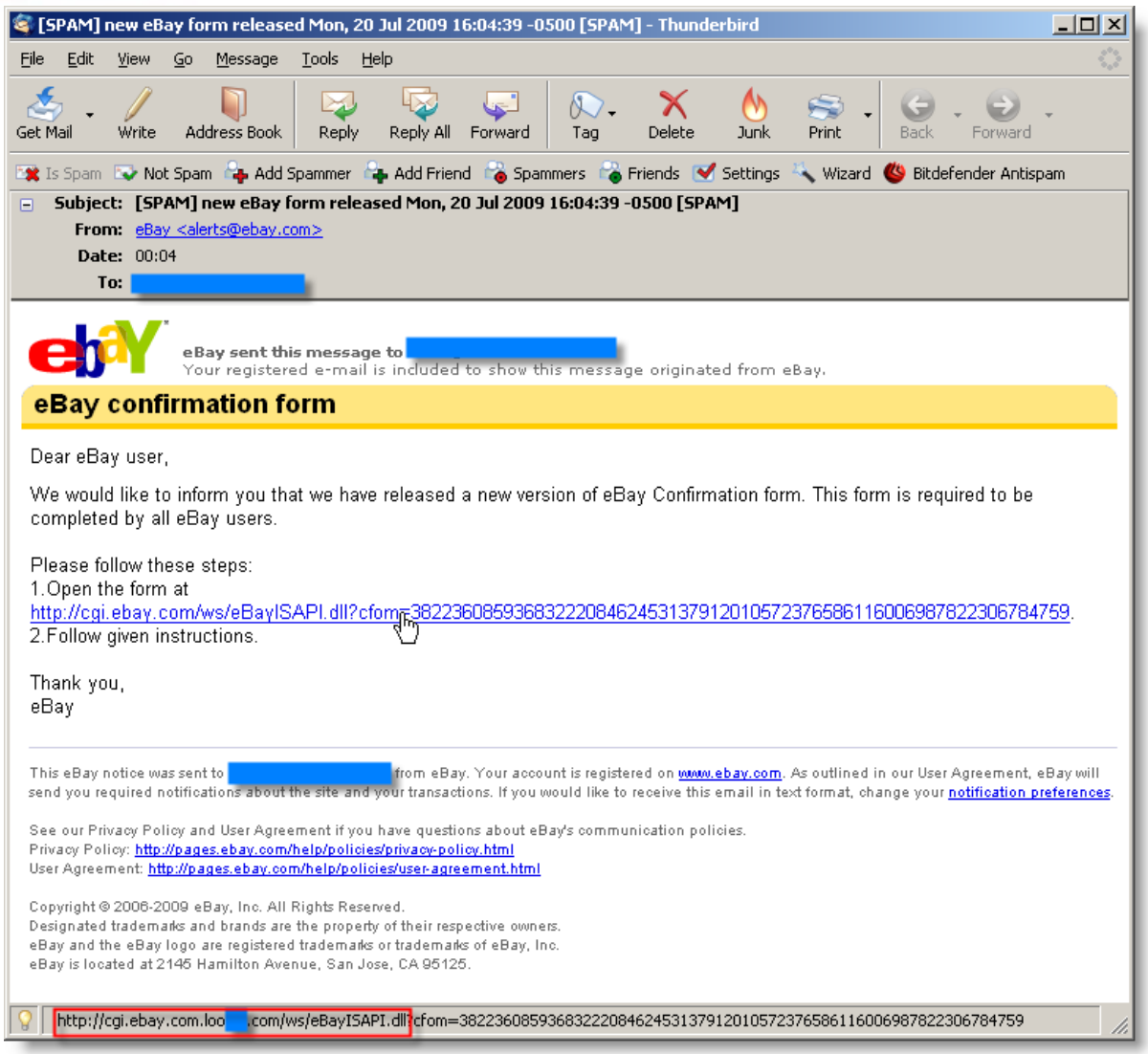
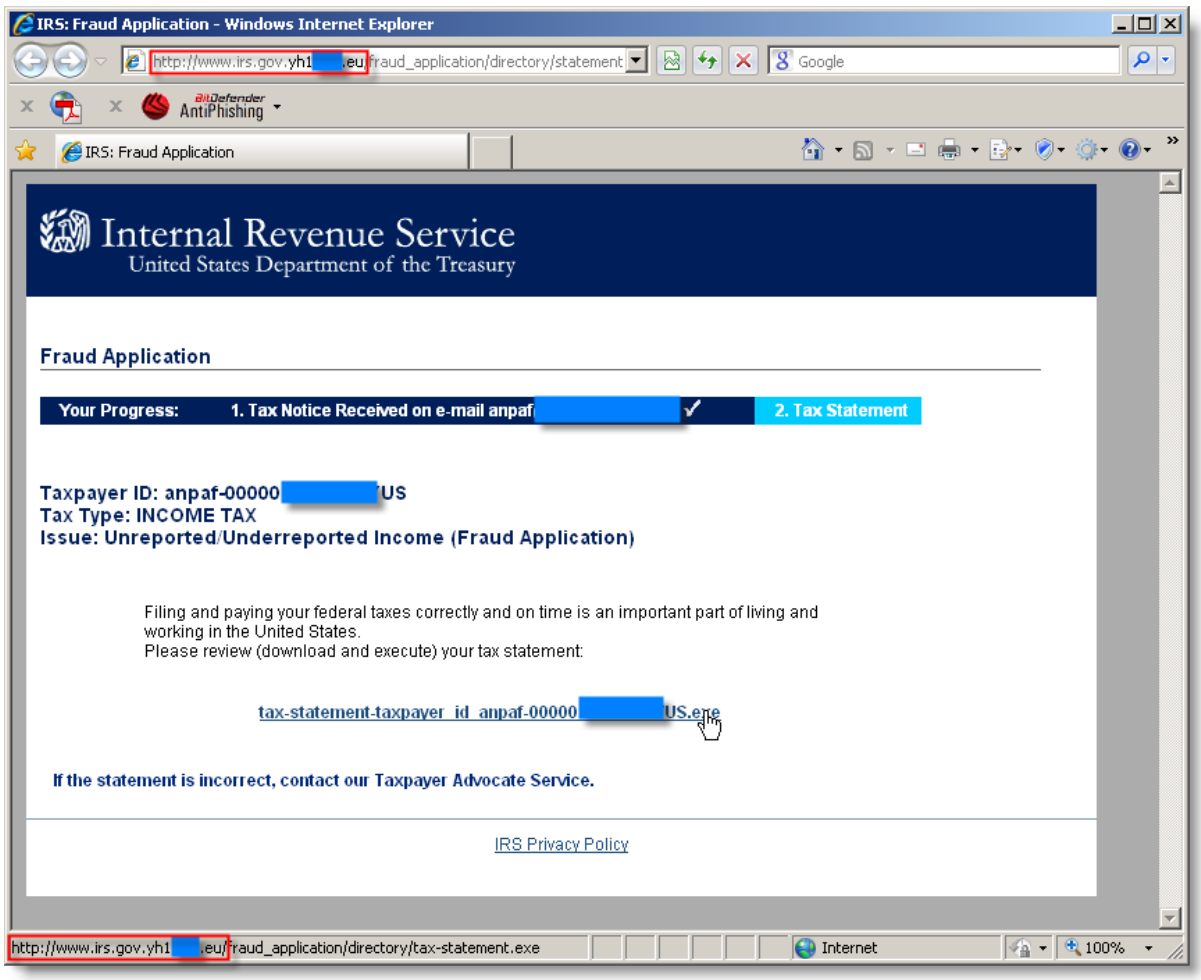


Figure 13 : Message de hameçonnage visant les utilisateurs de eBay

Le 15 septembre constituait un autre événement impatiemment attendu par les spammers, car c'est la date limite à laquelle les contribuables américains sont censés fournir leur déclaration de revenus. Le spam utilisé se présentait sous la forme d'un formulaire de déclaration, et leur fournissait un lien présumé direct vers le site Web du fisc.

Le lien n'aboutissait pas au portail du fisc mais sur une page Web (enregistrée sous le nom de domaine .eu) qui imitait un formulaire en ligne, comportant plusieurs éléments visuels du véritable site Web du fisc (à savoir son logo et des éléments de son formatage).

La page fournissait également un lien vers une prétendue déclaration que l'utilisateur devait télécharger et exécuter. Mais, en cliquant sur le lien, l'utilisateur ne téléchargeait pas un formulaire électronique, mais recevait un code malveillant que BitDefender a identifié comme étant Trojan.Generic.2436384, qui est en réalité une autre variante du tristement célèbre Zbot.



Vulnérabilités, « exploits » et brèches de sécurité

Bien qu'ils ne soient pas le vecteur principal de dissémination de malwares, les vulnérabilités et les exploits contribuent de manière significative à compromettre avec succès l'infrastructure informatique pour obtenir un bénéfice financier. Au cours du premier semestre 2009, les e-menaces les plus importantes étaient liées à l'émergence et la prolifération du ver Downadup, qui exploite une vulnérabilité dans le service Serveur de Microsoft Windows qui peut permettre l'exécution de code à distance en cas de réception d'une requête RPC spécialement conçue (MS08-67) pour se propager sur d'autres ordinateurs du réseau local. La réussite des attaques MD5 au début de janvier a également soulevé de multiples questions sur la sécurité des données et les méthodes d'authentification sur le Web.

Vulnérabilités SSL et imitation de sites Web

Début juillet, deux chercheurs indépendants ont découvert un nombre important de vulnérabilités dans l'implémentation du protocole SSL, permettant à un pirate d'imiter n'importe quel site Web avec protection SLL et de réussir à mettre au point une attaque de hameçonnage parfaite.

D'après les résultats de ces chercheurs, la vulnérabilité repose sur l'implémentation de la technologie SSL dans tous les navigateurs du commerce. Ces certificats sont quelquefois l'ultime élément de sécurité permettant à l'utilisateur de s'assurer qu'il est bien sur la page Web correcte. Ils peuvent être achetés auprès d'Autorités de certification comme VeriSign et Thawte. Lorsqu'une demande de certificat SSL est effectuée pour un domaine de premier niveau, l'Autorité de certification contacte le propriétaire du nom de domaine à l'adresse électronique de la base de données Whois pour valider la propriété du domaine.

Cependant, si le pirate réussit à enregistrer un domaine, il peut par la suite demander un certificat pour le sous-domaine de son site, par exemple bankofamerica\0.somesite.com, simplement en ajoutant le caractère nul ('\0'). Étant donné qu'il est propriétaire du domaine principal, l'Autorité de certification lui fournira un certificat, même si le sous-domaine contient des noms déposés tels que BankOfAmerica.

Récemment mise à jour, cette vulnérabilité dans l'implémentation SSL des navigateurs se traduit par le fait que le certificat du pirate est interprété comme étant attribué à BankOfAmerica. Cette erreur est provoquée par le caractère nul ('\0') qui interrompt immédiatement la lecture par le navigateur du nom du sous-domaine.

Autres vulnérabilités logicielles

Au cours du mois de juillet, Microsoft a publié pas moins de six bulletins concernant la sécurité (MS09-029 à MS09-035), qui décrivent des failles de sécurité dans Internet Explorer permettant l'exécution de code malveillant téléchargé à partir de sites Web spécialement conçus. Etant donnée la gravité de ces bogues, Microsoft a publié deux mises à jour (MS09-34 et MS09-035) pour corriger les vulnérabilités dans la bibliothèque Active Template.

C'est également au mois de juillet que d'autres vulnérabilités ont été détectées dans les applications d'autres vendeurs. Par exemple, Adobe a publié un bulletin de sécurité mettant à jour pas moins de 12 vulnérabilités exploitables à distance, touchant des programmes comme Adobe Flash Player versions 9 et 10, ainsi que Adobe Reader.

Un mois plus tard, en août, la vulnérabilité CVE- 2009-2675 permettant l'exécution de code à distance à partir de sites spécialement conçus a été détectée dans la machine virtuelle de Java (JVM). Ce même mois, d'autres correctifs pour le Flash Player d'Adobe ont été publiés pour contrer l'exécution arbitraire de code. Cependant, la vulnérabilité la plus spectaculaire est le bogue SMB 2.0 qui affect tous les systèmes d'exploitation depuis Vista, à l'exception de Windows 7 RTM et Server 2008 R2. SMB 2.0 est la plus récente version du protocole utilisé pour le partage de fichiers et d'imprimantes sur un réseau. Bien que le bogue ne soit pas présent dans Windows 7, ce n'est pas le cas pour sa version Release Candidate (RC).

Les prévisions pour la sécurité informatique en 2010

L'année 2009 a été marquée par une large gamme de menaces de sécurité ciblant à la fois les utilisateurs finaux et les réseaux d'entreprise. Le ver Downadrup (connu aussi sous le nom de Conficker ou Kido) a beaucoup progressé et est parvenu à rester l'une des trois principales menaces mondiales en 2009. Bien qu'il ne soit pas réellement dangereux (les variantes A, B, C ne sont pas porteuses de charges malveillantes), ses mécanismes de diffusion et sa résistance à la détection pourraient servir de base à de futurs malwares extrêmement destructeurs.

L'activité des botnets

Les botnets sont au cœur des activités impliquant le malware. Ils sont relativement facile à maintenir et fournissent à des organisations criminelles le moyen d'exercer une emprise informatique inégalée, avec des objectifs multiples, par exemple envoyer du spam, lancer des attaques par déni de service ou pratiquer des extorsions de fonds de type « pay-per-click ».

- Le spam envoyé par les botnets continuera sur la lancée observée en 2009.

- Le spam envoyé par les botnets sera au cœur des e-menaces en 2010. Des attaques par déni de service distribué serviront d'« exemple » à de futurs ou potentiels acheteurs de botnets. Si un client souhaite louer un botnet, mais n'est pas sûr des capacités du réseau qu'il veut louer, il peut souhaiter assister à une « démonstration de force ».

Les applications malveillantes

La plupart des applications malveillantes ont pour objectif de générer des gains financiers illicites. BitDefender estime que les malwares augmenteront significativement en 2010, en particulier les applications adwares et les faux logiciels antivirus (Rogue). Les malwares plus complexes, tels que les infecteurs de fichiers rootkits et les vers utilisant de multiples vecteurs d'infection (les protocoles peer-to-peer, de messagerie et de messagerie instantanée) devraient également progresser.

Les réseaux sociaux

Les sites de réseaux sociaux seront sans doute parmi les principaux vecteurs d'infection en 2010. Exploitant leur expérience de ces réseaux sociaux, les auteurs de malwares devraient poursuivre sur cette voie avec la « Google wave » au fur et à mesure que le service de messagerie instantanée du moteur de recherche gagnera en popularité. Les sites Internet de réseaux sociaux demeureront également les cibles spécifiques de certaines menaces. Le spam et les tentatives de phishing ciblant les utilisateurs de ces réseaux devraient également augmenter.

En dehors du fait qu'il est prévisible que les sites Web des réseaux sociaux vont devenir l'un des plus importants vecteurs des infections, il est également probable qu'ils seront le théâtre d'autres problèmes de sécurité, par exemple la divulgation involontaire d'informations sensibles.

Les systèmes d'exploitation

Le récent système d'exploitation Windows® 7 de Microsoft s'est avéré être bien plus sûr que ses prédécesseurs. Cependant, plus les utilisateurs passeront de Vista et XP à Windows 7, plus les créateurs de malwares rechercheront à tirer profit des vulnérabilités logicielles et des brèches de sécurité dans le système d'exploitation.

Nous recommandons vivement aux utilisateurs de Mac OS X d'Apple d'adopter une suite antimalware afin d'éviter les infections. Outre les tentatives de phishing et de spam qui concernent tous les systèmes d'exploitation et qui ciblent tous les utilisateurs d'ordinateurs connectés à Internet, la transition d'Apple vers la plateforme Intel s'accompagnera de nouvelles opportunités pour les pirates qui créent actuellement des malwares pour Windows.

Les systèmes d'exploitation mobiles

La dernière version de l'iPhone 3G a considérablement fait augmenter le parc d'utilisateurs d'iPhones en 2009. Beaucoup d'entre eux ont décidé de « jail-breacker » (débloquer) le système d'exploitation afin d'installer des applications tierces. Cette opération nécessite l'activation du service SSH avec un accès « root » et un mot de passe par défaut. BitDefender pense que de nouvelles e-menaces apparaîtront en 2010, exploitant les plateformes mobiles à la mode, en particulier des vers et des chevaux de Troie voleurs de mots de passe.

Les utilisateurs d'Android et de Maemo, seront, à priori, épargnés. Leur part de marché étant modeste comparée à Windows Mobile, Symbian et iPhone OS, les auteurs de malwares n'essaieront pas de trouver des vulnérabilités, mais se consacreront plutôt à des attaques de type « ingénierie sociale ».

Les menaces pour les entreprises

Les technologies de virtualisation de VMWare vSphere et Windows Server 2008 R2 Hyper-V de Microsoft ont offert de nouvelles possibilités aux petites et moyennes entreprises. Faire fonctionner plusieurs serveurs sur une seule machine grâce à la virtualisation contribuera à réduire considérablement les coûts. En 2010, on s'attend à ce que des pirates recherchent des vulnérabilités logicielles leur permettant de prendre le contrôle de l'hyperviseur et de toutes les machines virtuelles déployées sur le système.

Les services de « cloud computing » connaissent aussi de beaux jours. Qu'ils soient utilisés pour l'envoi d'e-mails ou pour la sauvegarde et le stockage de données, les technologies « cloud » contiennent et traitent de grandes quantités de données sensibles. BitDefender prévoit qu'en 2010, les attaquants se tourneront vers ces infrastructures, afin de prendre le contrôle de ces ressources « in the cloud » ou d'en limiter l'accès.

Enfin, les netbooks et les assistants numériques personnels (PDA) sont suseptible de représenter un risque sécuritaire croissant pour les entreprises alors que leur usage gagne en popularité. Les netbooks ne comprenant pas de puce TPM ou d'autres solutions de cryptage matériel/logiciel pouvant être administrés à distance (afin d'effacer le contenu du disque dur en cas de perte ou vol), des données sensibles pourraient se retrouver entre de mauvaises mains.

Table des figures