



**Bitdefender<sup>®</sup>**

# Rapport sur l'état des e-menaces au 2<sup>nd</sup> semestre 2011

Auteur :

**Bogdan BOTEZATU** – Analyste Senior des e-menaces

Collaborateurs :

- **Loredana BOTEZATU** – Spécialiste en communication (Tendances des malwares)
- **Răzvan BENCHEA** – Analyste Malware
- **Dragoș GAVRILUȚ** – Analyste Malware
- **Alexandru Dan BERBECE** – Administrateur de la base de données
- **Adrian MIRON** - Analyste Spam
- **Tudor FLORESCU** – Administrateur de la base de données SafEgo

# Table des matières

|   |    |
|---|----|
| Table des matières .....  | 3  |
| Table des matières des documents .....  | 4  |
| Introduction .....  | 5  |
| Zoom sur les malwares .....   | 6  |
| L'analyse des malwares .....  | 7  |
| Top 10 des e-menaces du second semestre 2011 .....  | 8  |
| Les malwares du Web 2.0 .....   | 13 |
| Les malwares se diffusant via messagerie instantanée .....                                      | 13 |
| Les menaces sur les réseaux sociaux .....   | 16 |
| L'analyse du spam .....   | 18 |
| Phishing et usurpation d'identité .....   | 21 |
| Vulnérabilités, exploits & brèches de données .....   | 23 |
| Prévisions concernant les e-menaces .....   | 25 |
| L'introduction de HTML5 .....   | 26 |
| IPV6 et la fin d'Internet .....   | 26 |
| Windows 8 et les exploits de type « zero-day » .....  | 27 |
| Les attaques de phishing ciblées basées sur des données partagées sur les réseaux sociaux ..... | 27 |
| Mentions légales .....  | 28 |

# Table des matières des documents

|   |    |
|---|----|
| Document 1 : Les 10 familles de malwares les plus actives.....  | 8  |
| Document 2 : Les différents types de codes malveillants.....  | 12 |
| Document 3 : Des paquets de données spécialement conçus déclenchent « l'exploitation » .....  | 14 |
| Document 4 : Plusieurs messages de spam contenant des liens vers du contenu pornographique .....  | 15 |
| Document 5 : Une conversation de messagerie instantanée contenant un lien vers un service SMS surtaxé.....  | 15 |
| Document 6 : Lien malveillant se faisant passer pour du contenu vidéo et dirigeant l'utilisateur en dehors du site de Facebook™ .....                     | 16 |
| Document 7 : Répartition des scams fournie par SafEgo.....  | 17 |
| Document 8 : Bot promouvant un service pornographique sur Twitter .....   | 18 |
| Document 9 : Répartition du spam par catégories .....   | 19 |
| Document 10 : Message de spam pharmaceutique – modèle d'e-mail simple avec un lien.....   | 19 |
| Document 11 : Offres d'emploi : écouler des produits achetés avec des cartes bancaires volées.....  | 20 |
| Document 12 : Message de spam contenant des malwares et pointant vers des malwares.....   | 21 |
| Document 13 : Incidents de phishing entre janvier et décembre 2011.....   | 22 |
| Document 14 : Campagne de phishing se faisant passer pour PayPal : « Vous découvrirez pourquoi votre compte est bloqué lorsque vous serez connecté »..... | 23 |

# Introduction

Il y a vingt ans naissait un moyen de communication électronique révolutionnaire.

Il a connu un tel succès auprès de personnes de tous âges et professions qu'il constitue aujourd'hui encore le système de communication des données le plus utilisé : il s'agit du SMS, ou *Short Message Service*.

Les téléphones portables sont actuellement bien plus que des gadgets capables de transmettre des messages vocaux et texte d'un endroit à un autre. Ils sont devenus indispensables dans le monde 2.0, si puissants et complexes, ils disposent de leurs propres systèmes d'exploitation, et donc, sont confrontés à leur part de cyber-problèmes.

Si le premier semestre a été marqué par des vulnérabilités logicielles et des brèches de données importantes, le second semestre a mis en lumière une nouvelle famille de malwares ainsi qu'un scandale d'espionnage d'utilisateurs, impliquant apparemment un ensemble d'opérateurs de téléphonie mobile et l'éditeur de logiciels controversé, CarrierIQ.

La paysage des malwares a été dominé par Trojan.Autorun.Inf et Win32.Worm.Downadup, deux rivaux malintentionnés dont l'origine remonte à l'époque de Windows XP mais qui sont parvenus à maintenir leur position alors que la mise à niveau des systèmes d'exploitation ou la mise en place de correctifs aurait permis de mettre un terme aux failles de sécurité qu'ils exploitent. Les principaux concurrents du second semestre 2011 sont Trojan.AutorunInf, Win32.Worm.Downadup, et Exploit.CplLnk.

L'exploitation des brèches de données attribuées au gang des Anonymous et à leurs groupes de hacking satellites se sont poursuivies au cours du second semestre 2011. Citons parmi les principales cibles Mitsubishi Heavy Industries, Adidas, RIM, Tiroler Gebietskrankenkasse, Nexon et même, les Nations Unies.

La confiance que nous avons envers les entreprises a été ébranlée par l'affaire DigiNotar au premier semestre 2011, durant celle-ci des utilisateurs peu méfiants ont été soumis à une attaque de phishing massive utilisant des certificats numériques volés générés pour des institutions et des agences gouvernementales de prestige telles que Google, Tor, la CIA et les services secrets israélien, le Mossad.

Les réseaux sociaux ont également joué un rôle clé dans la diffusion de malwares et de fausses informations concernant le décès de personnalités telles que Mouammar Kadhafi et Steve Jobs. On retiendra en particulier les campagnes de malwares proposant une vidéo de l'exécution de Kadhafi ou un cadeau soit disant offert en l'honneur du regretté Steve Jobs.



**Message mensonger proposant un iPhone gratuit pour commémorer la mort de Steve Jobs.**

## Zoom sur les malwares

- Bien que corrigée en 2008, la fonctionnalité de détournement de l'Autorun continue à être la technologie des systèmes Windows la plus exploitée. La famille Autorun est suivie du ver Downadup (Conficker) qui constitue la deuxième menace la plus destructrice du 2<sup>nd</sup> semestre 2011. Il est intéressant de noter que ces deux malwares continuent à faire des ravages alors que leur code n'a pas été mis à jour depuis des années et que les gangs de cybercriminels les ayant créés ont très probablement disparu.
- Les réseaux sociaux et les sites Web infectés sont deux des principaux vecteurs d'infection. Les utilisateurs de Facebook, dont le nombre atteint presque les 800 millions, sont constamment incités à cliquer sur des vidéos racoleuses (des méthodes d'ingénierie sociale extrêmement virales redirigeant les victimes à l'extérieur du réseau social). Parallèlement, l'augmentation du nombre de services utilisant de nom de domaine de deuxième niveau (tels que co.cc et .co.tv) hébergeant des kits d'exploits Web ont tellement augmentés que le géant des

moteurs de recherche, Google, à été contraint de désindexer l'ensemble des sites en co.cc. La cybercriminalité s'étant alors tournée vers d'autres SLD gratuits, cette mesure s'est révélée inefficace et les noms de domaines de deuxième niveau en co.cc ont retrouvé leur place dans l'index de Google.

- Les messages de spam contenant des malwares, qui avaient gagné du terrain au premier semestre 2011, ont continué à progresser rapidement. Les principales vagues de spam incluant des malwares envoyaient leurs messages au nom de l'Automated Clearing House, un service financier proposé par l'association américaine de paiements électroniques NACHA. À l'ouverture de la pièce jointe, un téléchargeur générique récupérait une variante du bot Zeus sur Internet et l'installait sur la machine locale.
- Les téléphones portables fonctionnant sous Android ont vu l'apparition de nouvelles menaces au cours du second semestre 2011 : des malwares élaborés, comme l'application Android System Message qui enregistre les conversations entrantes et sortantes ou le cheval de Troie jSMShider qui détourne les messages SMS entrants. Fin décembre, Google a également retiré 22 applications différentes de l'Android Market, après avoir confirmé qu'elles exploitaient une vulnérabilité du système d'exploitation pour faire envoyer des SMS vers des numéros surtaxés à l'insu des utilisateurs. Ces applications ont été téléchargées plus de 14 000 fois avant leur retrait de l'Android Market.

## L'analyse des malwares

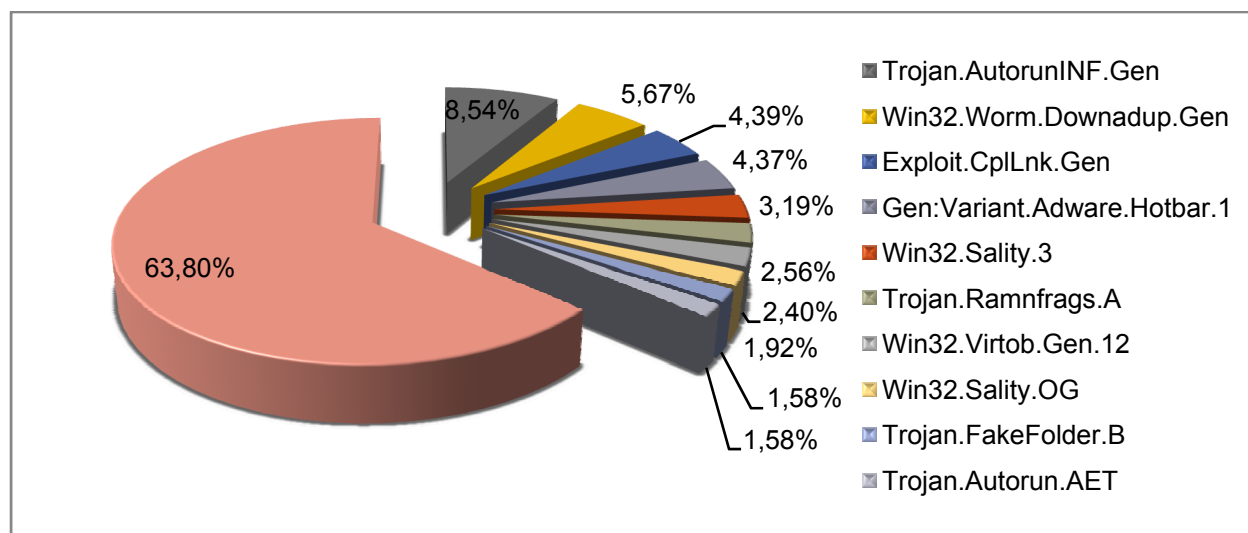
Le classement des malwares du premier semestre 2011 a connu plusieurs modifications, la plus importante étant liée au recul de Downadup au profit de cracks logiciels. Notons également la présence dans ce classement semestriel de la routine générique Exploit.CplLnk.Gen, qui intercepte l'exploit du Panneau de configuration utilisé par les nouvelles variantes du ver Stuxnet.

## Top 10 des e-menaces du second semestre 2011

S'il est vrai que l'état des e-menaces est resté relativement inchangé en comparaison avec le premier semestre de l'année, le 2<sup>nd</sup> semestre a été marqué par l'apparition d'un nouveau malware qui, bien que ne faisant pas partie de ce classement des 10 principales e-menaces, ne peut pas être ignoré en raison de sa complexité et de son importance.

Cette-menace découverte le 1<sup>er</sup> septembre 2011 et nommée Win32.Worm.Duqu.A se situe à un niveau bien supérieur à celui des e-menaces standards : ses composants rootkits ressemblent de façon frappante à un autre malware tristement célèbre, Stuxnet. Bitdefender a ainsi mis en évidence des ressemblances entre Stuxnet et Duqu, notamment le fait qu'ils sont tous les deux basés sur des vulnérabilités du noyau Windows de type Zero-day, et sont signés avec des certificats numériques valides, mais volés.

Cependant, contrairement à Stuxnet, Duqu ne vise pas le sabotage d'installations nucléaires et a une mission plus terre à terre : mettre en place un espace secret pour héberger un keylogger classique.



Document 1 : Les 10 familles de malwares les plus actives

### 1. Trojan.AutorunINF.Gen

Datant de 2009 Trojan.AutorunINF.Gen est une détection générique qui intercepte de faux fichiers autorun.inf, généralement utilisés par les malwares pour permettre de s'auto exécuter à partir de supports amovibles tels que des clés USB et des cartes mémoires.

Actuellement, la plupart des familles de ver ont une routine spécialisée qui infecte les supports amovibles montés avec des copies de la charge utile, avant de créer un fichier autorun.inf dissimulé qui lance le ver dès que le support infecté a été branché. Win32.Worm.Downadup, Stuxnet, et les variantes d'OnlineGames sont quelques exemples des nombreuses familles de malwares exploitant la fonctionnalité Autorun.

## 2. Win32.Worm.Downadup.Gen

L'un des vers les plus tenaces de tous les temps, Win32.Worm.Downadup, est parvenu à rester en place depuis début 2008. Ce malware a été créé par une équipe de professionnels ayant une connaissance approfondie du système d'exploitation Windows, il exploite en effet une vulnérabilité du service serveur RPC de Microsoft Windows (connue sous le nom de [MS08-67](#)) afin de se diffuser. Une fois qu'un PC est infecté, son utilisateur ne peut plus accéder aux sites des éditeurs de sécurité informatique ainsi qu'aux forums consacrés à la désinfection de malwares ou à la résolution de problèmes informatiques. Il est utilisé comme vecteur de diffusion de faux antivirus et d'autres e-menaces en raison de ses capacités de propagation virale.

## 3. Exploit.CplLnk.Gen

Le malware Exploit.CplLnk.Gen n'a plus besoin d'être présenté. La détection identifie le code malveillant utilisé par le tristement célèbre ver Stuxnet, pour se lancer lorsqu'un lecteur USB infecté est branché. Plutôt que d'employer une approche basée sur l'Autorun, le ver utilise des fichiers lnk (raccourcis) qui se servent d'une vulnérabilité présente dans tous les fichiers du système d'exploitation Windows, pour s'exécuter lui-même. En cinquième position dans le classement du premier semestre 2011, Exploit.CplLnk.Gen a progressé de 3 places, et représente 4,93% de l'ensemble des fichiers infectés.

## 4. Gen:Variant.Adware.Hotbar.1

Gen:Variant.Adware.Hotbar.1 est une routine générique qui intercepte une famille d'applications adwares dont l'objectif est d'afficher des publicités sur l'ordinateur des utilisateurs. Ce type d'adwares rapporte de l'argent à ses créateurs en affichant des publicités contextuelles dans le navigateur de l'utilisateur, ou en installant directement ces

adwares dans l'angle supérieur droit de l'écran. Pour augmenter l'intérêt de ces publicités Gen:Variant.Aware.Hotbar.1 surveille et enregistre les habitudes de navigation des utilisateurs et crée les profils de navigation correspondants. Cette e-menace a conservé sa position par rapport au classement précédent.

## 5. Win32.Sality.3

En cinquième position dans ce classement des e-menaces du second semestre 2011, Win32.Sality.3 représente 3,19% de l'ensemble des infections. Cette famille de virus est connue pour l'agressivité de ses attaques : ils commencent par infecter tous les fichiers scr et exe trouvés sur le PC, y compris les fichiers stockés sur des disques distants (disques sur d'autres PC qui sont partagés sur un réseau). Lorsque le virus détecte un fichier scr ou exe, il ajoute son code malveillant fortement chiffré au fichier concerné.

Pour éviter d'être détecté par les logiciels antivirus, le virus installe un composant rootkit qui tente de neutraliser l'antivirus installé localement, ouvrant la voie à un troisième composant : une backdoor permettant à un attaquant de prendre le contrôle du PC infecté.

## 6. Trojan.Ramnfrags.A

Trojan.Ramnfrags.A apparaît pour la première fois dans le classement des malwares Bitdefender. En sixième position avec 2,56% de l'ensemble des infections du 2<sup>nd</sup> semestre 2011, cette e-menace est un fichier dll qui agit comme composant principal du célèbre virus Ramnit. Ce virus infecte les fichiers exécutables Windows et les fichiers HTML, et peut également infecter des lecteurs amovibles. Ramnit peut notamment, entre autres fonctionnalités, dérober des identifiants Facebook et les utiliser pour publier des liens infectés sur les murs des utilisateurs.

## 7. Win32.Virtob.Gen.12

Le virus Virtob est le 2<sup>ème</sup> infecteur de fichiers le plus diffusé après Sality. Contrairement à ce dernier, Virtob est optimisé par sa vitesse et sa taille, puisqu'il est écrit en langage assembleur. Comme Sality, il infecte à la fois les fichiers scr et exe, mais ne modifie pas les fichiers système afin de ne pas endommager le système d'exploitation. Cette méthode lui

permet de ne pas être détecté pendant longtemps, puisque le système d'exploitation ne contient pas d'erreurs. Lorsqu'une connexion à Internet est détectée, le virus utilise le protocole IRC pour se connecter au serveur de son choix, où il attend les instructions de son créateur. Une infection par Virtob entraîne la corruption massive de comptes auxquels l'utilisateur s'est connecté, le virus étant capable de dérober des fichiers, des cookies, des mots de passe ou d'autres informations critiques.

## 8. Win32.Sality.OG

Win32.Sality.OG, variante du virus Win32.Sality, arrive en 8ème position avec 1,92% des infections enregistrées dans le monde au cours du second semestre 2011. Cette e-menace dispose de toutes les fonctionnalités décrites dans le paragraphe sur Win32.Sality.3, mais utilise un algorithme de chiffrement plus ancien.

## 9. Trojan.FakeFolder.B

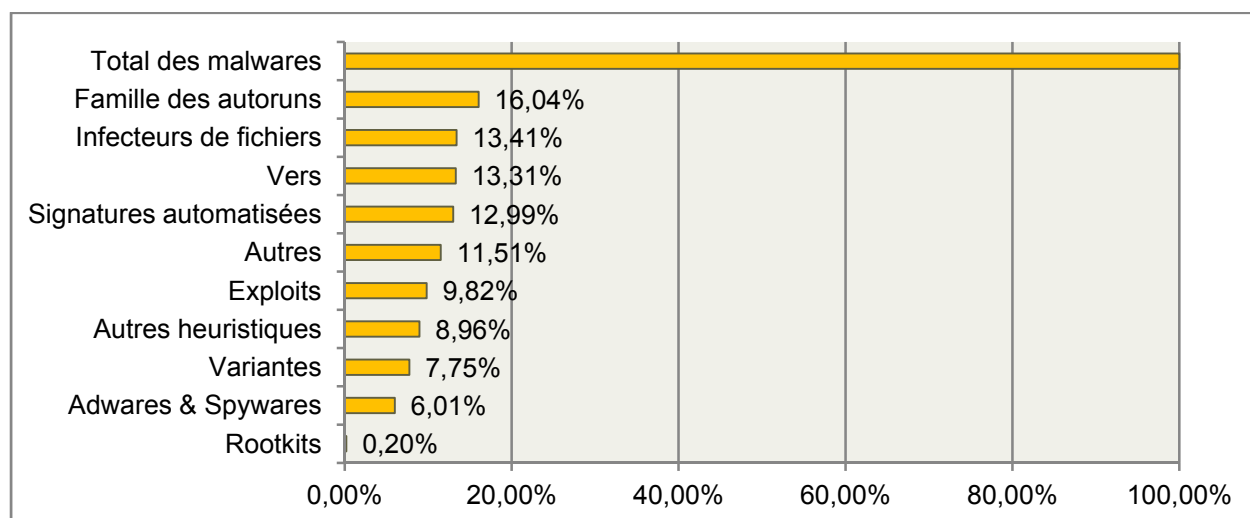
La 9ème position est occupée par Trojan.FakeFolder.B, à l'origine de 1,58% des infections d'ordinateurs dans le monde. Ce nouveau-venu est en fait un fichier de raccourci spécialement conçu appartenant à la famille de malwares Dorkbot. Pour chaque dossier du PC infecté, Dorkbot crée un raccourci et masque le dossier original. Lorsque qu'on clique sur ce dossier, le raccourci ouvre à la fois le dossier original et le composant malveillant situé dans le dossier 'Recycler'.

## 10. Trojan.Autorun.AET

Ce top 10 s'achève avec Trojan.Autorun.AET, qui correspond à 1,583% de l'ensemble des infections mondiales. Il s'agit d'une détection spécifique des fichiers autorun créés par le ver Downadup, qui permet au malware de charger sa charge utile lors de l'accès à ce disque amovible spécifique.

## Classement des malwares de juillet à décembre 2011

|     |                             |   |
|-----|-----------------------------|---|
| 01. | TROJAN.AUTORUNINF.GEN       | 8,54% (1 <sup>er</sup><br>semestre : 6,94%)   |
| 02. | WIN32.WORM.DOWNADUP.GEN     | 6,67% (1 <sup>er</sup><br>semestre : 5,75%)   |
| 03. | EXPLOIT.CPLLNK.GEN          | 4,39% (1 <sup>er</sup><br>semestre : 3,02%)   |
| 04. | Gen:Variant.Adware.Hotbar.1 | 4,37% (1 <sup>er</sup><br>semestre : 5,49%)   |
| 05. | WIN32.SALITY.3              | 3,19% (1 <sup>er</sup><br>semestre : 2,37%)   |
| 06. | TROJAN.RAMNFRAGS.A          | 2,56% (1 <sup>er</sup><br>semestre : -)       |
| 07. | Win32.Virtob.Gen.12         | 2,40% (1 <sup>er</sup><br>semestre : 1,76%)   |
| 08. | Win32.Sality.0G             | 1,92% (1 <sup>er</sup><br>semestre : 2,22%)   |
| 09. | TROJAN.FAKEFOLDER.B         | 1,58% (1 <sup>er</sup><br>semestre : -)       |
| 10. | TROJAN.AUTORUN.AET          | 1,583% (1 <sup>er</sup><br>semestre : 1,78%)  |
| 11. | AUTRES                      | 63,08% (1 <sup>er</sup><br>semestre : 62,16%) |



Document 2 : Les différents types de codes malveillants

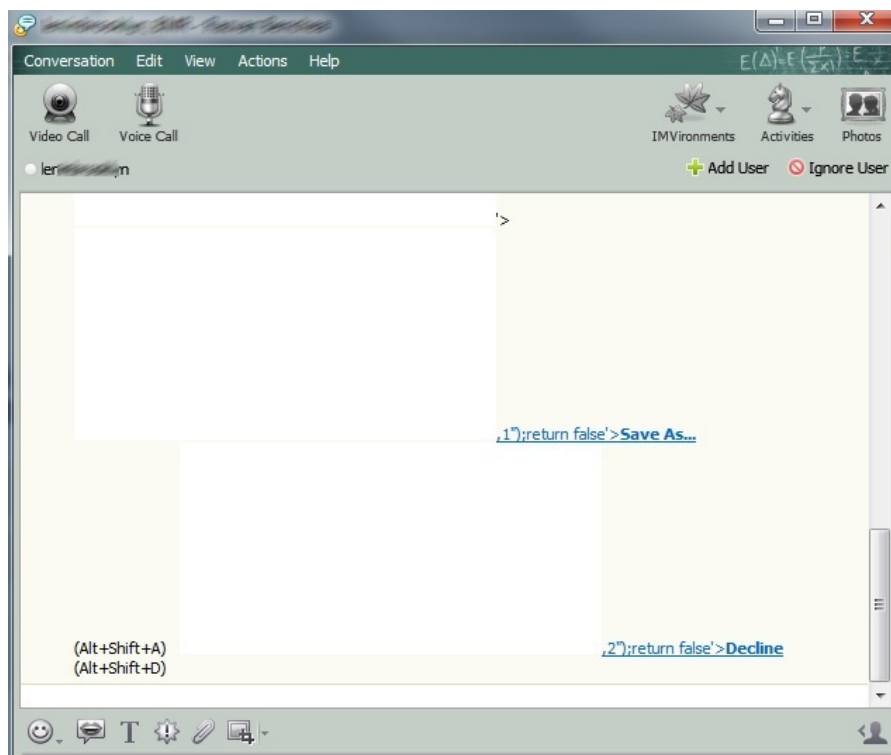
Les malwares exploitant la fonction Autorun constituent le type d'e-menaces le plus présent en décembre 2011, représentant 16,04% des malwares, suivis des infecteurs de fichiers (virus) et des vers. Les rootkits se situent à l'opposé, puisqu'ils représentent seulement 0,2% des malwares au monde.

## Les malwares du Web 2.0

Les réseaux sociaux ont été la cible d'une large gamme d'e-menaces au cours du second semestre 2011. Le vol d'informations personnelles et la diffusion de liens malveillants ont été les préoccupations principales des cybercriminels, mais le spam à des fins lucratives a également connu des développements importants.

### Les malwares se diffusant via messagerie instantanée

Les malwares se diffusant via messagerie instantanée ne sont pas nouveaux : au fil des ans, les cybercriminels ont exploité quasiment toutes les plateformes de messageries instantanées pour diffuser des liens malveillants ou faire connaître leurs produits via le spam dans le cadre de campagnes massives de marketing. De nouveaux dangers sont cependant apparus au cours du second semestre 2011 pour les utilisateurs du client Yahoo! Messenger.

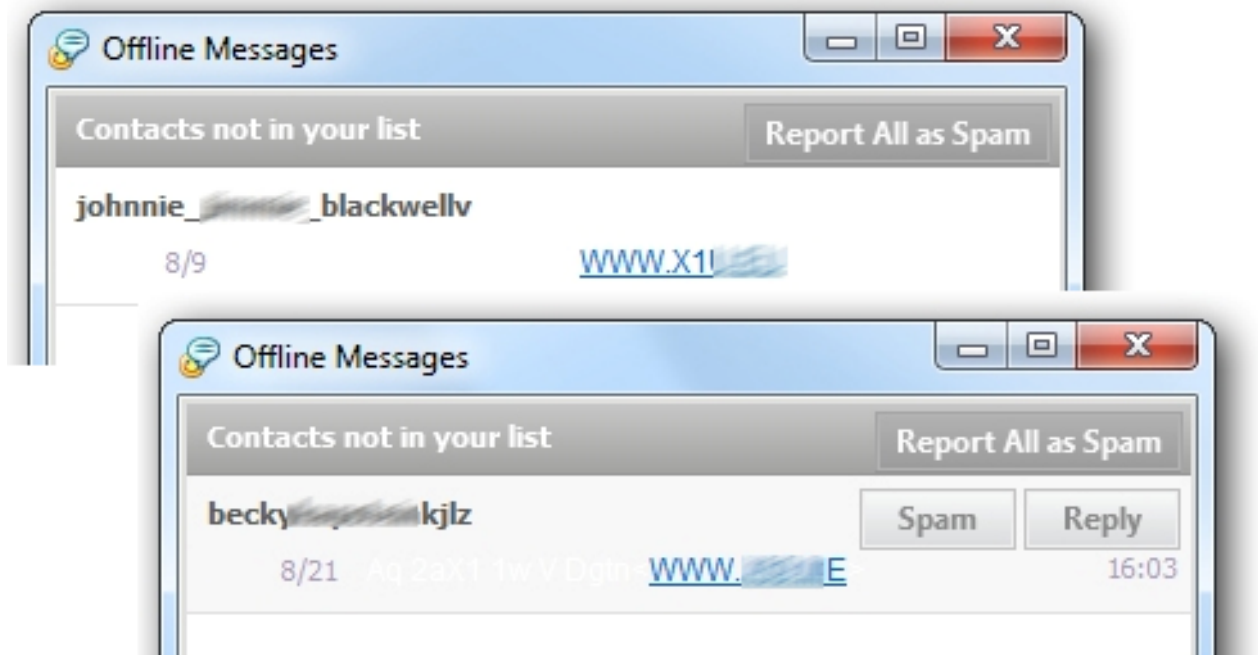


### Document 3 : Des paquets de données spécialement conçus déclenchent l'exploitation

Cet exploit a été détecté en circulation le 5 décembre, il affecte la version 11.x du client de messagerie (y compris la toute récente version 11.5.0.152-us). L'exploitation réussie du client permet à un attaquant de modifier de façon arbitraire et à distance le message de statut de quasiment tout utilisateur de Yahoo! Messenger exécutant la version vulnérable.

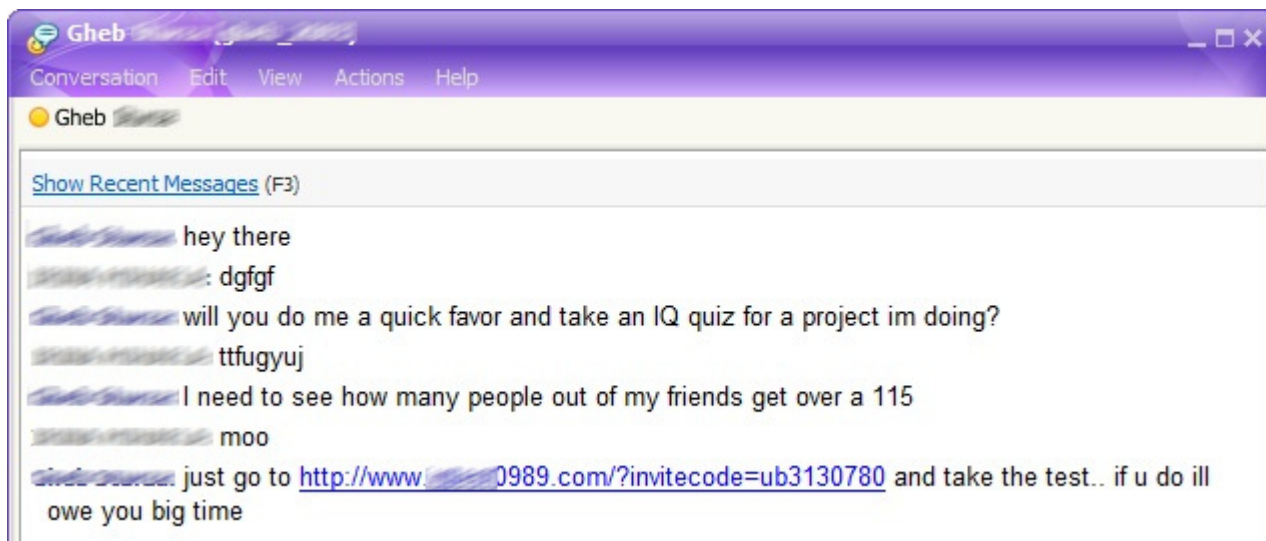
L'exploit fonctionne en s'appuyant sur le fait que l'application de messagerie ne vérifie pas qu'une entrée spécifique est valide ou non, de sorte qu'une requête de transfert de fichier malformée peut déclencher toute action supportée par Yahoo! Messenger, y compris des changements de statut, des exportations d'informations sur les contacts et même, l'accès à un emplacement distant via le navigateur par défaut.

L'envoi de spam au travers d'applications de messagerie instantanée a également augmenté au cours du second semestre 2011. La plupart des liens transmis via messagerie instantanée étaient des publicités pour des services de rencontre en ligne, ou d'autres sites Web avec du contenu pornographique.



Document 4 : Plusieurs messages de spam contenant des liens vers du contenu pornographique

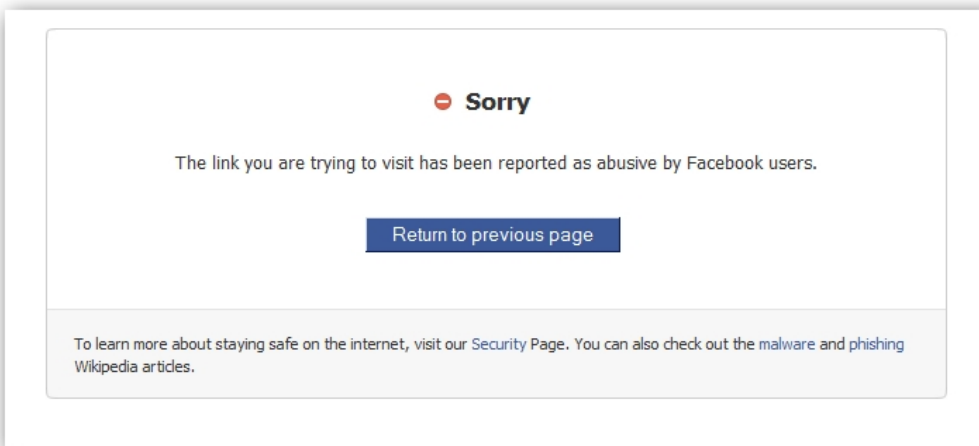
D'autres vagues de spam importantes transmises sur Yahoo! Messenger présentaient des propositions commerciales douteuses et des jeux concours, des propositions pour prendre part à des sondages, des offres d'« emplois à domicile » pour écouler des biens dérobés ou des recrutements pour obtenir des services de résolution de CAPTCHA « humainement assistés ».



Document 5 : Une conversation de messagerie instantanée contenant un lien vers un service SMS surtaxé

## Les menaces sur les réseaux sociaux

Le second semestre 2011 a été marqué par de nouvelles e-menaces ciblant l'importante base de données de plus de 800 millions d'utilisateurs de Facebook, ainsi que par la remise en circulation d'anciens scams optimisés par leurs créateurs, dans le but d'obtenir de meilleurs résultats. Les techniques d'ingénierie sociale sont de loin la façon la plus efficace de convaincre les utilisateurs de partager des contenus malveillants. Les cyber-escrocs ont également tiré profit de la mort de Mouammar Kadhafi et de Steve Jobs, les deux principaux événements de ce semestre.



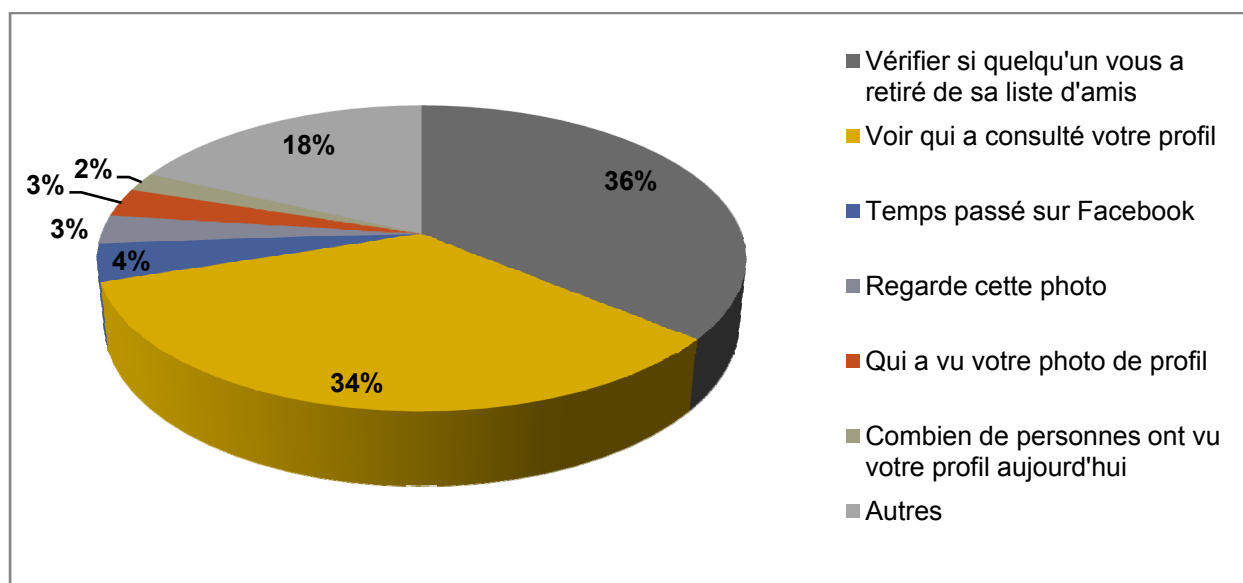
### **Document 6 : Lien malveillant se faisant passer pour du contenu vidéo et redirigeant l'utilisateur en dehors du site de Facebook**

Une attaque sur Facebook se compose de trois étapes distinctes. La première consiste à convaincre les utilisateurs de se rendre sur un site malveillant qui promet de visualiser une vidéo racoleuse ou d'obtenir un cadeau. Les stars et les événements nationaux sont également utilisés, mais plus irrégulièrement.

En combinant ingénierie sociale, vulnérabilités des applications ou clickjacking (détournement de clic), le contenu malveillant est partagé de nouveau et devient accessible à de plus en plus de contacts.

La troisième étape de l'attaque est la monétisation, par des sondages ou des ventes de programmes d'affiliation essentiellement. D'autres méthodes pour tirer profit d'une attaque

consistent à recueillir des informations personnelles ou des identifiants qui serviront à d'autres campagnes ou seront vendus sur le marché noir.



Document 7 : Répartition des scams, chiffres fournis par SafEgo

La plupart des applications rogues apparues au cours des six premiers mois de l'année 2011 visent à recueillir des informations personnelles. La publicité de ces applications est assurée par des « vers de murs » qui dirigent les utilisateurs vers une page sur laquelle l'application recherchée leur demande l'accès à des informations telles que le nom complet, l'adresse e-mail, les réseaux, les loisirs et toutes les autres informations publiques. Ces informations sont recueillies dans une grande base de données qui peut être filtrée par habitudes, régions, préférences, langues, etc. Dès que ces données ont été recueillies, l'application poste sur le mur de l'utilisateur lui-même le message racoleur sur lequel il avait cliqué au départ, le rendant ainsi visible aux amis de la victime.

Bien que Facebook attire la plus grosse partie de l'attention des cybercriminels, ce n'est pas le seul réseau social infesté de spam et de malwares.

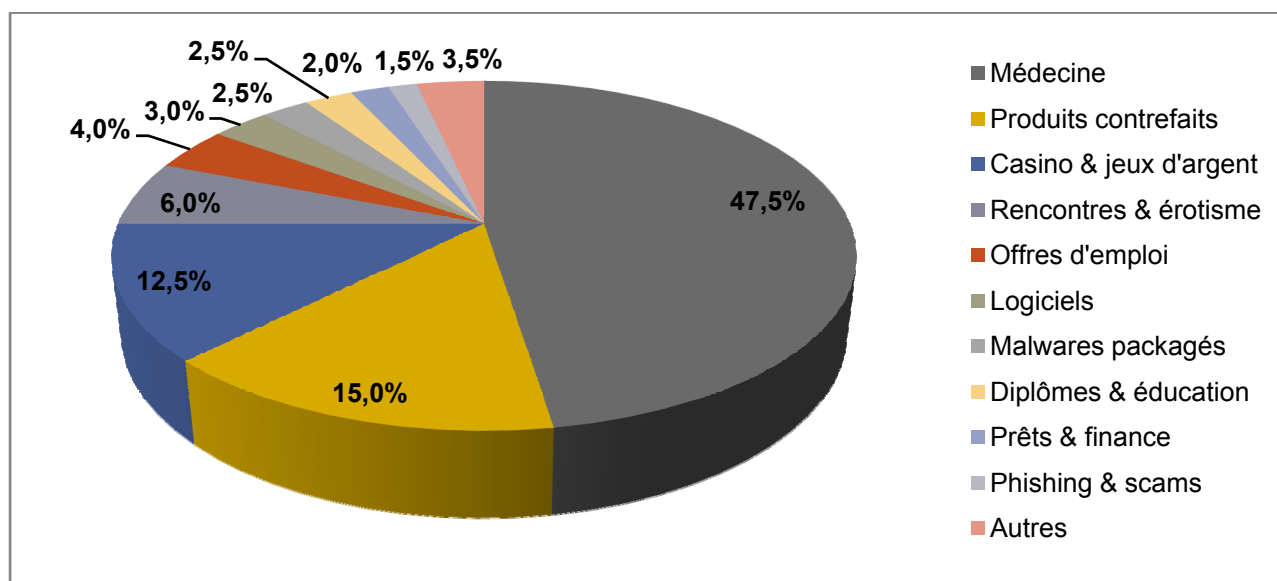
De par sa nature, **Twitter** offre un accès gratuit aux timelines des utilisateurs, à moins que ceux-ci ne verrouillent explicitement leurs comptes. Cette technique permet à des tiers de suivre n'importe qui sans son accord, travail également réalisés par des bots Twitter automatisés qui surveillent étroitement les conversations et envoient des réponses en fonction de mots-clés.



Document 8 : Bot promouvant un service pornographique sur Twitter

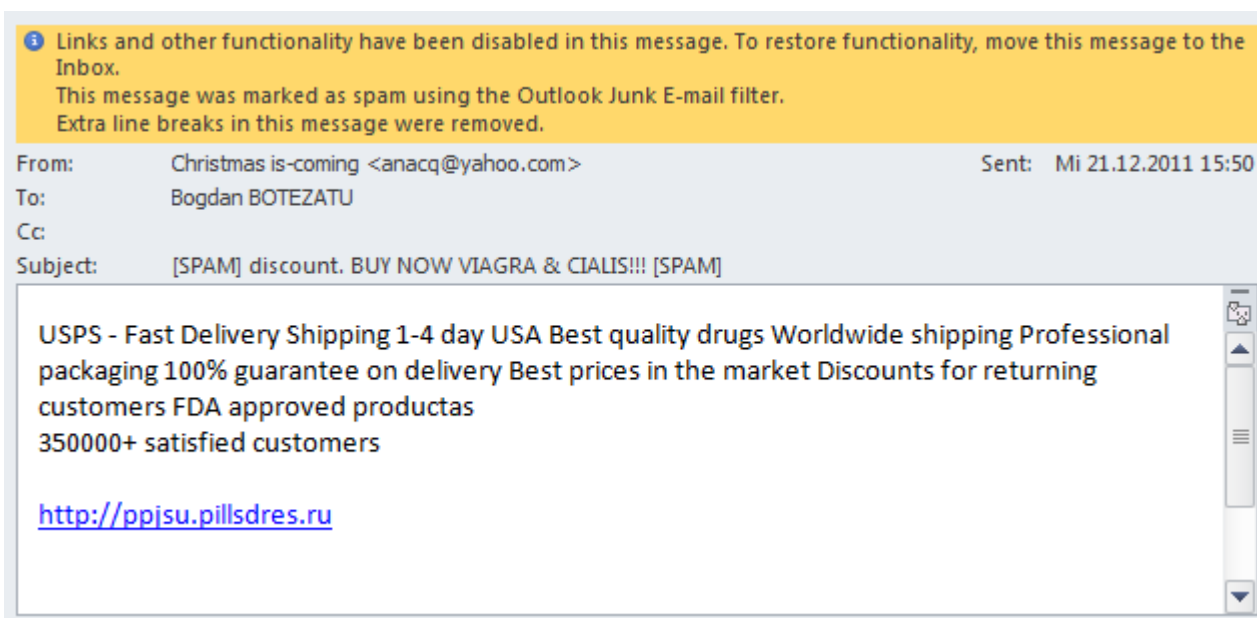
# L'analyse du spam

Bien que l'industrie du spam ait été affectée à de nombreuses reprises en 2011, notamment par la fermeture du plus grand service de spam affilié au monde (SpamIt) et par le démantèlement de Rustock, le botnet le plus puissant et le plus efficace au monde, le spam a réussi à maintenir un rythme relativement soutenu. Au second semestre 2011, l'indice du spam atteignait 75,1% du nombre total d'e-mails envoyés dans le monde. Le spam se répartit entre les catégories suivantes :



## Document 9 : Répartition du spam par catégories

Le spam pharmaceutique se taille la part du lion avec 47,4% des messages de spam envoyés dans le monde. Les offres 'médicales' vont de l'amélioration des performances sexuelles, qui fait partie de l'offre proposée par Canadian Pharmacy depuis ses débuts, aux substances réglementées telles que le Prozac et le Zoloft.



Links and other functionality have been disabled in this message. To restore functionality, move this message to the Inbox.  
This message was marked as spam using the Outlook Junk E-mail filter.  
Extra line breaks in this message were removed.













From: Christmas is-coming <anacq@yahoo.com> Sent: Mi 21.12.2011 15:50  
To: Bogdan BOTEZATU  
Cc:  
Subject: [SPAM] discount. BUY NOW VIAGRA & CIALIS!!! [SPAM]

USPS - Fast Delivery Shipping 1-4 day USA Best quality drugs Worldwide shipping Professional packaging 100% guarantee on delivery Best prices in the market Discounts for returning customers FDA approved productas 350000+ satisfied customers

<http://ppjsu.pillsdres.ru>

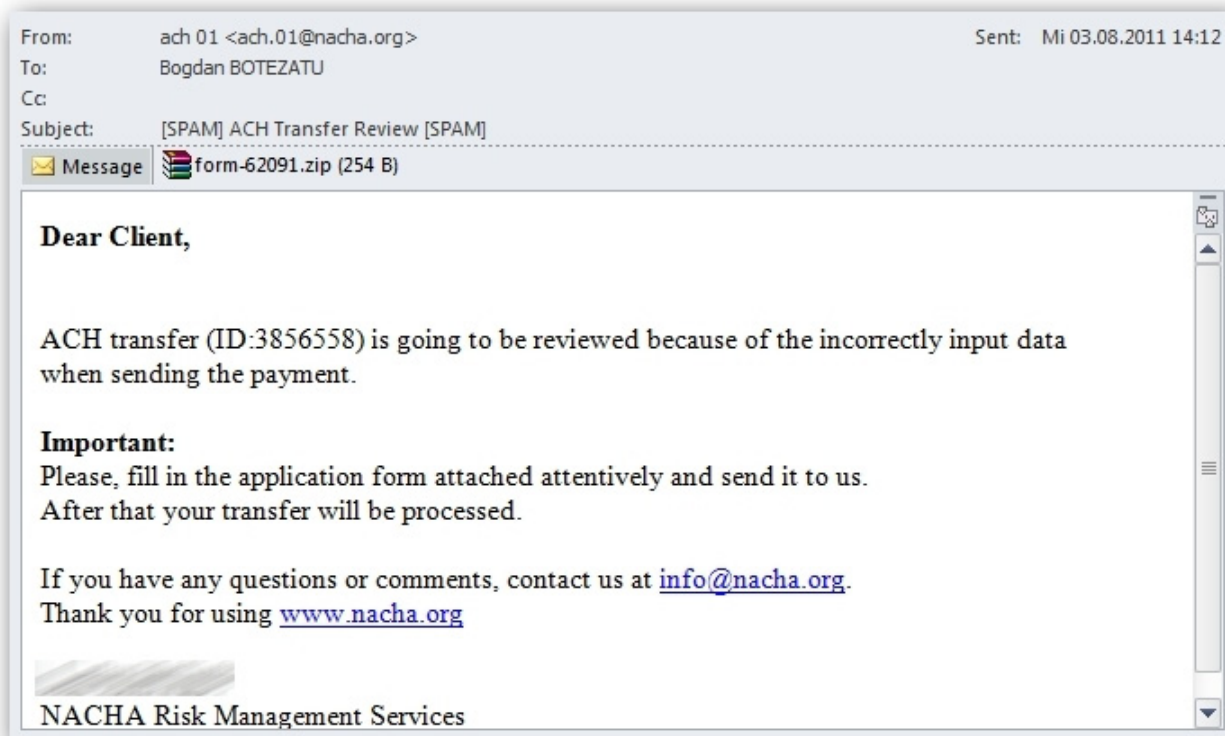
## Document 10 : Message de spam pharmaceutique – modèle d'e-mail simple avec un lien

Il y a quatre ans, la plupart des offres d'emploi présentées par spam appâtaient les victimes en leur faisant payer un droit d'entrée, mais la crise économique mondiale a modifié cette approche : vous pouvez désormais travailler pour des cybercriminels sans avoir à verser un centime. Ils cherchent en effet des « money mules » permettant de blanchir de l'argent et des personnes écoulant des biens volés, pour empêcher les autorités de remonter jusqu'à eux.

|   |   |                |      |
|---|---|----------------|------|
|  | bogdan.b... New job vacancy - see details     | Mi 12.10.20... | 8 KB |
|  | bogdan.b... Position opening in your area     | Mi 12.10.20... | 8 KB |
|  | bogdan.b... Employment you've been searching! | Mi 12.10.20... | 8 KB |
|  | bogdan.b... Vacancy - apply online            | Mi 12.10.20... | 7 KB |
|  | bogdan.b... Employment you've been searching! | Mi 12.10.20... | 8 KB |
|  | bogdan.b... Work offer inside                 | Mi 12.10.20... | 7 KB |
|  | bogdan.b... New job vacancy - see details     | Mi 12.10.20... | 7 KB |
|  | bogdan.b... New job vacancy - see details     | Mi 12.10.20... | 7 KB |
|  | bogdan.b... Job opportunity - hurry to apply! | Mi 12.10.20... | 8 KB |
|  | bogdan.b... Job offer match, respond to apply | Ma 11.10.2...  | 7 KB |
|  | bogdan.b... Work offer inside                 | Ma 11.10.2...  | 7 KB |
|  | bogdan.b... Position opening in your area     | Ma 11.10.2...  | 7 KB |

#### Document 11 : Offres d'emploi : écouler des produits achetés avec des cartes bancaires volées

Bien que relativement peu nombreux en comparaison avec le spam médical ou les contrefaçons, les messages contenant des malwares compensent leur quantité moindre par un potentiel destructeur supérieur. Certaines des principales campagnes de spam contenant des malwares ont usurpé l'identité de services de paiements connus (tels que NACHA ou PayPal) ou d'entreprises de livraison de colis (UPS). La plupart de ces messages sont accompagnés de fichiers exécutables en pièces jointes, dissimulés sous forme de fichier PDF. Une fois qu'ils sont ouverts, l'ordinateur est infecté par une variante du cheval de Troie bancaire Zeus.



Document 12 : Message de spam contenant des malwares et pointant vers des malwares

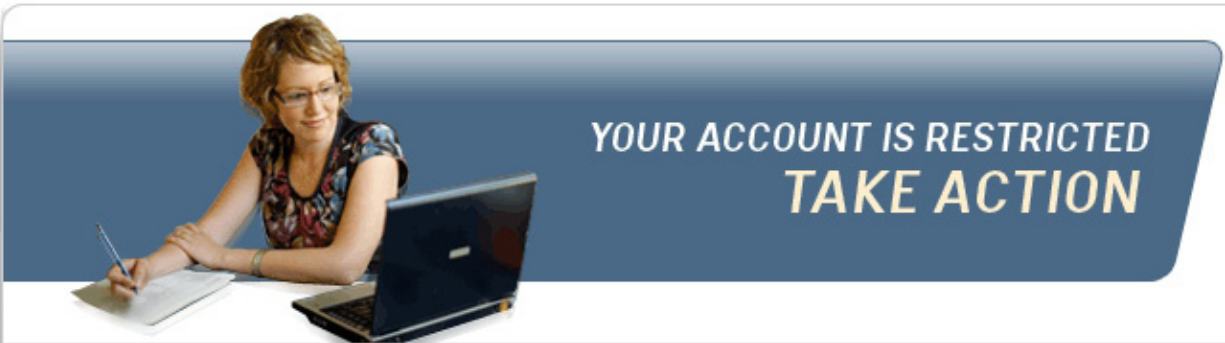
## Phishing et usurpation d'identité

Au cours du second semestre 2011, l'évolution des messages de phishing a suivi une courbe légèrement descendante, proportionnelle au niveau de spam envoyé au cours des deux semestres. Si les messages de phishing sont restés stables entre juillet et septembre, leur nombre a commencé à diminuer début octobre alors que le botnet Kelihos (aussi connu sous le nom de Waledac 2.0) était démantelé grâce à la collaboration de Microsoft avec des fournisseurs d'accès Internet tchèques. La fermeture de Kelihos a libéré environ 41 000 ordinateurs infectés, qui étaient responsables de l'envoi d'environ 3,8 milliards de spam par jour.



**Document 13 : Incidents de phishing entre janvier et décembre 2011**

Au second semestre 2011, l'intérêt des phishers pour les institutions financières n'a pas changé, PayPal et eBay demeurant les cibles principales, suivies par les jeux en ligne et les réseaux sociaux. La plupart des identifiants de réseaux sociaux ayant été obtenus par phishing sont diffusés sur des sites de partages publics (comme les 10 000 noms d'utilisateurs et mots de passe révélés par l'équipe de TeamSwaStika en octobre).



**Dear Value Member,**

You may have noticed that some limitations have been placed on your PayPal account. As a valued PayPal customer, we want to let you know what this means and how to resolve the situation.

**What does it mean to have limited access?**

Your account may be restricted for a number of reasons; you'll find out when you next log in to PayPal. As a result, you'll notice that some of the following options are now unavailable:

- â€¢ Send money to other PayPal users
- â€¢ Request or receive money from other users
- â€¢ Edit or remove account details
- â€¢ Close your PayPal account

**Document 14 : Campagne de phishing se faisant passer pour PayPal : « Connectez vous pour savoir pourquoi votre compte est bloqué »**

# Vulnérabilités, exploits & brèches de données

La série de brèches de données initiée début 2011 sous la supervision du groupe de hackers Anonymous s'est poursuivie au cours du second semestre. Parmi les victimes les plus importantes se trouvaient à la fois des entreprises et des agences gouvernementales, et les informations obtenues par le piratage ont toutes été rendues publiques.

Début juillet, l'on assistait au piratage d'un organisme chargé de l'application de la loi en Arizona, suivi de la diffusion de données personnelles de 1 200 officiers de police. Deux

jours plus tard, l'un des serveurs d'Apple était corrompu et une liste de 27 noms d'utilisateurs et mots de passe étaient publiés en ligne. La base de données d'Apple contenait uniquement une liste d'utilisateurs ayant participé à des enquêtes, ce qui a considérablement diminué la portée de l'attaque.

La situation s'est aggravée le 11 juillet, avec la publication par le groupe Anonymous de 90 000 adresses e-mail de militaires et du hash MD5 correspondant après la réalisation d'une brèche dans le réseau du sous-traitant du ministère de la défense américain Booz Allen Hamilton. L'incident, surnommé « Military Meltdown Monday » (« la débâcle militaire du lundi »), a été le premier d'une série d'attaques de haut niveau contre des objectifs militaires.

L'édition en ligne du journal britannique The Sun a été piratée une semaine après l'incident Booz Allen Hamilton et ses visiteurs redirigés vers une page annonçant, de façon mensongère, la mort de Rupert Murdoch.

Juillet s'est achevé avec deux importantes brèches supplémentaires. La première, réalisée le 28 juillet, a abouti à la publication de plus de 500 Mo de données de l'OTAN. La seconde attaque a été lancée un jour plus tard contre le sous-traitant du FBI, ManTech, ainsi que contre l'infrastructure du Département de la Sécurité intérieure des États-Unis. Le groupe de hackers a divulgué des dossiers confidentiels détaillant la création d'un logiciel de gestion personnelle censé être capable de manipuler et d'espionner l'opinion publique sur les réseaux sociaux.

En août, les Anonymous ont également publié plus de 10 Go de données recueillies dans 76 bureaux de shérifs américains. Ces informations ont été récupérées après l'accès frauduleux du groupe dans le système du prestataire hébergeant les bases de données des shérifs.

Vanguard Defense Industries, entreprise de défense et d'aéronautique basée au Texas, a été frappé par une attaque DDoS massive fin août. Pendant l'attaque, les Anonymous ont pu copier 1 Go d'informations personnelles des employés de l'entreprise, qui ont été par la suite divulguées sur les trackers de torrents.

L'année s'est achevée par une attaque sur l'infrastructure de Stratfor, autre grand fournisseur militaire, un cabinet-conseil basé au Texas fournissant au gouvernement américain des services militaires dans le domaine de la sécurité et des affaires

étrangères. Le groupe de hackers est parvenu à obtenir la liste des clients de l'entreprise, des informations bancaires, l'identité de 221 militaires britanniques et de 242 employés de l'OTAN ainsi que d'autres données confidentielles.

## Prévisions concernant les e-menaces

L'année 2011 a été particulièrement riche en activités malveillantes. Elle a débuté sous le signe des détournements de données et des fuites d'informations en entreprises avec l'émergence de bots extrêmement sophistiqués tels que ZeroAccess et TDL4, et s'est achevée avec Duqu, « le fils de Stuxnet ».

Le nombre de malwares continuera à augmenter de façon endémique en 2012 pour atteindre le nombre de 90 millions d'échantillons recensés, soit presque 17 millions de malwares de plus qu'à la fin de l'année 2011. Ils apparaîtront essentiellement sous la forme d'anciens malwares repackagés pour éviter la détection et de menaces exploitant des vulnérabilités de type « zero-day » présentes dans les systèmes d'exploitation et les logiciels additionnels.

Les réseaux sociaux seront la cible prioritaire des créateurs de malwares en 2012. Avec plus de 800 millions d'utilisateurs actifs, Facebook est devenu la plus grande communauté du Web. Bien que l'entreprise ait amélioré significativement la protection des interactions entre les utilisateurs et ait réduit le temps de réponse entre l'apparition d'une menace et sa suppression, plus de 400 millions d'utilisateurs sont exposés en permanence à de nouvelles menaces ayant une durée de vie très courte. Nous prévoyons pour 2012 une intensification des scams sur Facebook et Twitter, ainsi que l'apparition d'une famille importante de malwares se diffusant via des liens infectés postés directement sur les murs des utilisateurs.

Le système d'exploitation Android est également devenu un acteur majeur des attaques en 2011 à mesure que de plus en plus de constructeurs de tablettes et de smartphones intègrent leur version de l'OS dans leurs matériels. Depuis son introduction en 2008, la part de marché d'Android n'a cessé d'augmenter de façon exponentielle, passant à 25% aux États-Unis et même à 50% au Royaume-Uni (pays dans lesquels la pénétration des smartphones est la plus

forte). Parallèlement, le nombre de menaces ciblant le système d'exploitation Android a considérablement augmenté, de même que le risque de fuite de données personnelles.

Bitdefender estime que le nombre de menaces spécifiquement conçues pour Android augmentera de façon phénoménale en 2012, à mesure que le système d'exploitation progressera sur le marché des appareils entrée et moyen de gamme.

Les nouvelles technologies joueront également un rôle essentiel dans les incidents liés à des malwares. Parmi ces technologies, on dénombre :

## L'introduction de HTML5

Ce nouveau langage est actuellement pris en charge par les principaux navigateurs et offre de nouveaux niveaux d'interaction entre l'utilisateur et les sites Web. Si l'amélioration de l'interaction est le principal objectif du lancement d'une version majeure du populaire langage de balisage, les nouvelles fonctionnalités permettront aux cyber-escrocs de concevoir des scams plus efficaces contre les utilisateurs d'Internet via les « Notifications Web », de suivre les victimes avec les données de géolocalisation (en particulier si elles utilisent HTML5 sur leur smartphone) ou même, de lancer des attaques contre d'autres sites directement à partir du navigateur de la victime.

## IPV6 et la fin d'Internet

On devrait, au dernier trimestre 2012, assister à l'épuisement des adresses IP du système IPv4. Cette sérieuse limitation qui pourrait empêcher tout nouvel abonné d'accéder à Internet, a été anticipée depuis quelques temps avec le début de la mise en place du protocole IPv6. Ce nouveau protocole est supporté par la plupart des systèmes d'exploitation tels que Windows Vista, Windows 7, Mac OS/X, tous les matériels Linux et BSD. Les appareils compatibles IPv6 supportent par défaut la configuration automatique sans état ('Stateless') qui leur permet de communiquer avec d'autres appareils et services du réseau IPv6 sur le même segment du réseau en signalant leur présence via le protocole Neighbor Discovery Protocol (NDP). Ce processus automatisé peut cependant exposer les appareils du réseau aux attaquants ou, dans

des situations extrêmes, permettre à un attaquant de prendre le contrôle complet du matériel d'un réseau.

Le trafic IPv6 supporte également IPSec, un mécanisme qui permet au trafic de circuler de façon chiffrée entre la source et la destination. Bien que cette fonctionnalité protège contre le sniffing du trafic, elle sera probablement exploitée par les cybercriminels pour masquer le trafic de botnets depuis et vers le centre de commande.

## Windows 8 et les exploits de type « zero-day »

Le nouveau système d'exploitation de Microsoft, Windows 8, sortira prochainement. Les versions sorties en avant-première sur les services Web de partage de torrents et de peer-to-peer sont en général des versions « repackagées » du système d'exploitation avec de nombreux malwares qui corrompent le système avant que celui-ci ne soit complètement chargé, compliquant ainsi la détection et la désinfection. Les vulnérabilités de logiciels tiers constitueront également un important vecteur d'infection car les « packs d'exploits » en tirent constamment profit.

## Les attaques de phishing ciblées basées sur des données partagées sur les réseaux sociaux

Les 800 millions d'utilisateurs actifs sur Facebook publient de nombreuses informations personnelles et professionnelles en ligne sur le réseau social et souvent, ces informations sont accessibles à des personnes qui ne font pas partie de leurs amis en raison de paramètres de confidentialité insuffisants. Ces informations feront augmenter le risque d'attaques de phishing ciblées en 2012.

# Mentions légales

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 lors de l'élaboration de ce document, l'éditeur, les auteurs et les collaborateurs se dégagent de toute responsabilité en cas d'erreurs et/ou d'omissions. Ils ne sauraient être tenus pour responsables 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 fera 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 fournissent 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'un professionnel compétent 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 de la consultation du document.

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 fournies 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 réalisé et publié et celui où il est lu.

Le respect de l'ensemble des lois internationales applicables au copyright émanant de ce document relève de la pleine et entière responsabilité des lecteurs. Les droits relevant du

copyright restant applicables, aucune partie de ce document ne peut être reproduite, stockée ou introduite dans un système de récupération des données, ou transmise à quelque fin ou par quelque moyen que ce soit (électronique, mécanique, photocopies, enregistrement ou autres), ou dans quelque but que ce soit, sans l'autorisation expresse et 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 indication expresse figurant dans un contrat de licence écrit émanant de Bitdefender ce document ne concède aucune licence sur ces brevets, marques, droits d'auteur ou autres droits de propriété intellectuelle.

Tous les autres noms de produits ou d'entreprises mentionnés dans ce document le sont à titre purement informatif et sont la propriété, et éventuellement les marques, de leurs propriétaires respectifs.

*Copyright © 2012 Bitdefender. Tous droits réservés.*