



**G DATA**

Compte rendu des logiciels malveillants

Bulletin semestriel de janvier à juin 2008

Ralf Benzmüller & Thorsten Urbanski

Go safe. Go safer. **G DATA.**

# **Livre Blanc - Tendances Janvier-juin 2008**

Ralf Benzmüller & Thorsten Urbanski

# 1. Résumé :

## Explosion des logiciels malveillants

La phase de consolidation de l'industrie des logiciels espions a en 2008 plus que jamais porté ses fruits dévastateurs. Après une augmentation de 300% de 2006 à 2007, perçue comme l'année du logiciel espion, tous les records sont déjà battus actuellement, en 2008. Comparé à l'année précédente, au cours des seuls 3 premiers mois de cette année, un nombre supérieur de nouveaux programmes nuisibles a été mis en circulation (133 253).

Il ne faut pas s'attendre au cours des prochains mois à une diminution de la propagation de ces logiciels. D'après une estimation des laboratoires de sécurité de G DATA, le seuil de 500 000 nouveaux programmes nuisibles pourrait être dépassé au troisième trimestre 2008, ce qui correspondrait à un taux de croissance nettement supérieur à 400%.

Selon les critères de classification en analyse de codes de malveillance, les buts premiers en fraude informatique sont le vol d'informations et la connexion de PC capturés dans des réseaux bots. Les téléchargeurs (37546) et les portes dérobées (44156) sont les nouveaux phénomènes les plus utilisés de ce premier semestre 2008.

Code malveillant	Nouveaux phénomènes	Part en %
Backdoors	75.027	23,6 %
Downloader/ Dropper	64.482	20,3 %
Spyware	58.872	18,5 %
Chevaux de Troie	52.087	16,4 %
Adware	32.068	10,1 %

Tableau 1 : Top des 5 premiers logiciels malveillants de janvier à juin 2008

### 1.1 Champs de mine du réseau

Les menaces provenant de sites tout préparés ont beaucoup augmenté. Le pronostic de G DATA de 2007 quant à la propagation de codes malveillants sur Internet s'est avéré depuis bien longtemps. Dans ce contexte, les malfaiteurs utilisent des failles de sécurité ou les plug-ins des navigateurs comme Flash, Real Player ou Adobe Reader. Contrairement à ce qui est généralement supposé, ces dangers ne sont pas très présents dans les "quartiers sensibles" d'Internet, mais le plus souvent sur les sites populaires.

### 1.2 Smartphones : explosion de la bulle d'air promotionnelle

La propagation des virus sur smartphones n'apparaît pas dans les chiffres actuels : seuls 41 nouveaux programmes nuisibles ont été mis en circulation jusqu'à la fin juin 2008. D'après les analyses G DATA, la plupart de ces programmes malintentionnés sont des logiciels de surveillance semi-légaux ou des études de réalisation (preuves de concept).

Cette tendance devient plus nette, si l'on tient compte de tous les nouveaux programmes nuisibles apparus depuis janvier 2006 sur smartphones : 145 nouveaux programmes nuisibles sur l'ensemble des systèmes d'exploitation Smartphone. Parler d'un véritable danger pour les possesseurs de smartphone semble, au degré d'évolution actuelle, exagéré.

### **1.3 Conclusion et prévisions**

D'après une estimation de G DATA, aucune pause estivale n'est à prévoir dans l'industrie des logiciels malveillants pour les prochaines semaines et les prochains mois. Le nombre de nouveaux logiciels malveillants continuera d'augmenter et pourrait atteindre d'ici là des proportions jusqu'à présent insoupçonnées.

Les célébrations sportives prévues, comme les Jeux olympiques de Pékin, peuvent engendrer une aggravation de la situation. Les malfaiteurs virtuels se servent d'évènements internationaux comme l'occasion de partir plus activement à la chasse aux données et de faire davantage de profits. Une augmentation des messages malintentionnés est à prévoir sur le court terme.

Les virus de smartphones joueront toutefois un rôle très mineur cette année, la propagation de tels programmes nuisibles étant toujours due à l'interaction de l'utilisateur et limitée dans l'espace lors de la propagation par Bluetooth, et surtout, dernier élément, mais non des moindres, il manque des références de succès solides en Crime électronique, susceptibles d'être imitées. La cyber-délinquance est en fin de compte une industrie spécialisée, vouée à une pratique orientée selon la loi de marché, prédisent les experts en marketing.



## 2. Introduction

Le développement et la propagation des logiciels malveillants est un commerce extrêmement lucratif qui cause chaque année des dommages par milliards. Depuis longtemps les malfaiteurs n'agissent plus par petits groupes de cyber délinquants autonomes, mais par secteurs de travail spécialisé en des réseaux répartis sur toute la terre. Les auteurs de logiciels malveillants, expéditeurs de courrier indésirable et receleurs de données travaillent main dans la main, ce qui les place en situation de monopole sur le secteur de la cyber-délinquance.

Dans ce contexte de trafic de cyber-délinquance, les acteurs ne peuvent pas, d'un point de vue économique, se dispenser de développer et de répandre des nouveaux logiciels malintentionnés afin d'infecter et de dérober le plus d'ordinateurs possible dans le minimum de temps possible et de les intégrer dans l'infrastructure du botnet.

Ce qui a été pronostiqué en 2007 par G DATA s'est avéré en 2008 : le nombre de nouveaux programmes nuisibles a explosé ! Au cours des seuls six premiers mois de l'année en cours, plus de 318 000 nouveaux programmes nuisibles ont été mis en circulation, soit 2,4 fois plus qu'au cours de l'année 2007 dans sa totalité.

La propagation de logiciels malveillants se développe principalement sur des sites Internet, massivement munis d'outils de livraison de téléchargements "Drive-by". Les pièces jointes ont déjà perdu leur première place de porteurs de fichiers nuisibles l'an dernier et servent plutôt à attirer leurs victimes vers des sites de contrefaçon (imités). Actuellement, la majorité des nouvelles infections provient de sites Internet. Internet ressemble donc à un terrain de combat parsemé d'énormes champs de mines !

### 3. Principaux évènements et développements au premier semestre 2008

Au premier semestre 2008, l'activité des cyber-délinquants a augmenté sans relâche. Ainsi, le ver appelé Storm Worm, que beaucoup disaient déjà mort fin 2007, a fêté un anniversaire d'un genre très spécial.

Le gang Storm Worm a réparti les botnets de façon à ce que des ordinateurs derrière des routeurs n'envoient que des Spams. Les ordinateurs sans routeur sont utilisés pour héberger des sites de Spam et d'hameçonnage. La désactivation d'un nom de domaine réfère toujours aux autres ordinateurs du botnet (fast flux). Ainsi il devient nettement plus difficile de distinguer les sites nuisibles du réseau.

Les sites web compromis délivrent de plus en plus de codes malveillants. Il existe des outils spécifiques qui facilitent l'introduction de logiciels malveillants sur des serveurs Internet par les cyber-délinquants. Une ancienne technologie est alors à nouveau réapparue : les virus de secteur d'amorce ne contiennent plus de contamineurs de fichiers mais des rootkits dissimulés.

#### 3.1 Le ver "Storm Worm" fête son anniversaire

Les possesseurs du réseau botnet ont ce premier semestre prouvé les impressionnantes performances de leurs armées de zombies. Parallèlement, les malfaiteurs choisissent les célébrations et jours de commémoration internationale comme marchepieds. Même s'ils ont commencé le jour de la St Valentin (14 février) à la mi-janvier, leur succès n'en a pas été interrompu. De plus, le programme de la bande des Storm a de nouveau affiché des cartes et des sites "humoristiques" le premier avril. Ainsi, de nombreux ordinateurs du monde entier ont été contaminés et transformés en zombies.

Après une phase relativement calme au dernier trimestre 2007, Storm est redevenu actif et, selon les prévisions, le restera !



(1) Du point de vue technique, le ver baptisé « Storm Worm » est en fait un cheval de Troie. Seulement, le terme « Storm Troyen » qui en résulte a beaucoup moins de charme et n'est pas entièrement correct.

### Informations contextuelles du botnet storm :

En janvier 2007, la tempête Kyrill qui s'est abattue sur une grande partie de l'Europe a provoqué des dommages considérables. Sitôt les rafales de vent apaisées, des e-mails avec pièces jointes readmore.exe promettant d'autres informations sur les conséquences de la tempête ont commencé à circuler. C'est de là qu'est venu le nom de Storm Worm (sans tenir compte du fait qu'il s'agisse d'un cheval de Troie et non d'un ver et que le même groupe avait déjà propagé des e-mails avec voeux de fin d'année et autres festivités fin décembre 2006).

L'objectif de ces e-mails reste d'intégrer les ordinateurs infectés dans un réseau botnet, qui sert à expédier des Spam et démarrer des attaques de déni de service distribué. Les mois suivants sont apparues d'autres vagues de messages avec des titres mensongers comme „ Saddam Hussein alive „ ou „ Fidel Castro dead „ ainsi que des alertes contre des virus. Ces e-mails comprenaient également des codes malveillants en pièce jointe.

En juin 2007, la tactique a subi une modification : des cartes électroniques de voeux et de félicitations ont attiré les utilisateurs vers des sites obligeant à installer un fichier (nuisible) pour les visualiser. De plus, il a été tenté, en arrière-plan, de se servir des failles de sécurité du navigateur ou plutôt de ses composants. L'infection se produisait alors durant la visualisation de la carte virtuelle. D'autres pièges comme le téléchargement de codecs pour visionner des vidéos ou des logiciels de transfert de données sécurisés ou de protection des données confidentielles ont suivi. Même l'emploi des betatesteurs a été utilisé comme piège.

L'an dernier, en septembre, des faits d'actualités ont de nouveau donné l'occasion d'attirer les victimes vers des sites dangereux. Tout a commencé lors de la fête du travail, suivie de la nouvelle saison de la ligue nationale de football. C'est à cette occasion qu'a commencé la promotion des téléchargements dangereux „ Free NFL Game tracker „. Il existe d'autres attaques qui se réfèrent comme jeux en ligne, logiciels „ Krackin „, cartes de voeux pour Halloween, Noël et le Nouvel An.

En automne, le botnet Storm connaît un moment de calme. Manifestement, les malfaiteurs ont déplacé leurs activités de St Pétersbourg vers la Chine et la Turquie, pour pouvoir agir de façon plus virulente.

## 3.2 Rootkits du secteur d'amorce

Lors de l'activation de l'ordinateur commence la course entre les logiciels malveillants et les logiciels de sécurité. Plus tôt le contrôle du système réussit, mieux le logiciel de sécurité peut assurer sa protection ou au contraire, le logiciel malveillant peut éluder les fonctionnalités de protection.

### Anciennes tactiques redevenues usuelles

Début janvier, Backdoor.Win32.Sinowal a mis en circulation un programme nuisible qui réécrit le MBR pour ancrer les fonctions de cache de Windows XP Kernel. Cette nouvelle technologie de cache sert à inhiber les fonctions de vol lors de la gestion des comptes en banque en ligne. Au premier semestre 2008, 97 variantes de cette espèce sont apparues. Le verrouillage des codes malveillants dans le secteur d'amorce est toutefois un module indépendant de la fonction de dommages. Cette dernière pourrait bientôt être intégrée à d'autres logiciels malveillants.

Le logiciel malveillant a la partie belle car sous XP, l'apporteur par défaut peut réécrire le MBR. Pour Vista, la procédure est plus compliquée.

Il existe toutefois des mécanismes de protection : le système BIOS permet souvent de protéger le MBR de toute réécriture. C'est peut être maintenant le moment opportun d'y procéder. Les premiers virus de secteur d'amorce ont été découverts lorsque l'on démarrait les ordinateurs avec une disquette désinfectée.

**Le CD de démarrage de solutions de protection antivirus de G DATA permet de détecter les rootkits de MBR actuels avec fiabilité.**

D'après une estimation du laboratoire de sécurité de G DATA, ce n'est plus qu'une question de temps avant que de nouveaux programmes nuisibles recourent à cette technologie de camouflage.

### Fonctionnement

Lors du processus de démarrage, le premier emplacement où se déroule le contrôle des programmes modifiables, est le Master Boot Record (MBR) d'un disque dur, c'est-à-dire le secteur d'amorce d'autres périphériques de démarrage, comme des disquettes. Le MBR est le premier secteur d'un disque dur. Entre autre, le chargeur d'amorçage et le tableau de partition y sont transférés. Le chargeur d'amorçage contient des codes exécutables et examine la partition d'amorçage et charge les composants importants du système d'exploitation (par exemple le noyau).

Le secteur d'amorce étant le premier emplacement possible à isoler dans un système en code étranger, les premiers virus comme Brain, Stoned et Michelangelo ont été nommés virus de secteur d'amorce. Il n'est nouveau pour personne que les codes malveillants réécrivent le secteur d'amorce, pour prendre en main le contrôle de l'ordinateur dès que possible.

Malheureusement, Windows XP permet toujours de réécrire le MBR. Toutefois, un nombre limité de logiciels nuisibles en a fait l'usage ces dernières années. En 2005, Derek Soeder d'Eye Digital Security a constaté avec BootRoot, qu'il était possible d'activer un rootkit dans le MBR. Les fonctions de camouflage s'activent ensuite, avant le chargement complet du système d'exploitation. En 2007, Nitin et Vipin Kumar d'NV Labs ont publié le VBootkit, permettant d'installer la fonction de camouflage de Vista. BootRoot comme VBootkit sont des preuves de concept techniques sans fonction de dommage réelle. Elles n'ont jamais été associées à des logiciels malveillants. Sinowal a maintenant changé la donne.

## 3.3 Champs de mines d'Internet : cliquer - infecter - dérober

Les menaces des sites infectés et imités ont beaucoup augmenté en présence au premier semestre 2008, ce qui a transformé Internet en champ de bataille.

Actuellement, plus de 70% des contaminations proviennent de consultations d'offres sur sites Internet. Au cours des célébrations sportives comme les J.O de Pékin, une nouvelle augmentation est à envisager. Les plateformes de fans mal surveillées et endommagées représentent une mine d'or pour les malfaiteurs.

### Procédure des gangs en ligne :

Seul un nombre minimal d'e-mails propagateurs de programmes nuisibles comportent encore des pièces jointes. La plupart d'entre eux réfèrent soit directement à un fichier nuisible par lien, soit invitent au téléchargement de ce fichier nuisible sur un site. Le plus souvent il est fait

recours à des manoeuvres de diversion comme des informations actuelles, des cartes électroniques de voeux, des prélèvements abusifs ou des Codecs pour des films intéressants.

Le code malveillant, qui a été introduit clandestinement sur des sites Internet, essaie d'utiliser les failles du navigateur ou de ses composants (comme Adobe Reader ou Flash) pour mettre discrètement la main sur l'ordinateur lors du téléchargement de la page internet. Contrairement à ce que pensent beaucoup d'utilisateurs, ces **Drive-by Downloads** agissent rarement depuis les zones rouges, dites sensibles, d'Internet.

La majorité écrasante des infections provient de sites normaux et bien fréquentés. De nombreux pièges publicitaires y sont posés ou des serveurs Web y sont eux-même crackés. Cela peut se produire grâce à des mots de passe FTP peu efficaces ou volés ou lorsque des failles de sécurité sont utilisées dans les applications en cours comme les systèmes de gestion de contenu ou BBS.

### Programmes de forums, points d'accès

Dans les quatre premiers mois de 2008, les attaques de masse sur les failles des applications Web se sont renforcées. C'est ainsi que par exemple des erreurs du programme phpBB furent responsables de milliers de sites infectés. En avril, des centaines de milliers de sites attaqués par injection SQL ont infligé un IFRAME dangereux à leurs visiteurs. Le nombre de programmes nuisibles provenant de Flash a également augmenté considérablement.

Pour ces serveurs ainsi attaqués, des outils encore plus efficaces sont parus. Ils permettent de dissimuler un code malveillant sur un site capturé, attaquant à son tour les utilisateurs le consultant.

Au début de l'année, FirePack, qui existe déjà sous sa version chinoise, est apparu. En février, un nouvel outil Multi-Exploit est né. En revanche MPack, IcePack, TrafficPro, Nuclear Malware Kit, Web-Attacker, SmartPack et bien d'autres sont également commercialisés sur Internet à des prix de 40 à 3 000 \$.

Il est évident que chacun des ces sites peut comporter des codes nuisibles. La protection antivirus doit alors être paramétrée pour la vérification du flux de données HTTP avant que le navigateur ne s'en charge.

Pour vérifier cela, essayez de télécharger la version texte brut du fichier test EICAR. Il s'agit d'un programme DOS affichant le texte : „EICAR-STANDARD-ANTIVIRUS-TEST-FILE!“ Ce programme, en lui-même inoffensif, sera toutefois considéré comme espèce nuisible par tout logiciel antivirus.

En téléchargeant la version texte brut de ce fichier à partir de <http://www.eicar.org/download/eicar.com.txt>, vous recevrez soit un message d'alerte bloquant l'accès au site, soit une ligne en texte codé apparaîtra dans le navigateur, énonçant le message indiqué ci-dessus. Dans ce dernier cas, votre ordinateur reste dépourvu de toute protection contre les attaques sur Internet. Des codes scripts semblables à ce message affiché peuvent se charger sur votre navigateur. Ils s'exécuteront d'abord puis la protection anti-virus constatera qu'un programme nuisible a été activé uniquement après leur enregistrement sur Temporary Internet Files par le navigateur, l'alerte est alors trop tardive.

## 4. Tendances et statistiques des logiciels malveillants au premier semestre 2008

Le nombre de nouveaux logiciels malveillants a de nouveau considérablement augmenté. Il ne faut pas oublier que les packers font partie des coupables. La présence des réseaux botnet, logiciels espions et publicitaires est toujours certaine. La quantité de Spams a atteint un niveau élevé et les expéditeurs de courrier indésirable ont acquis deux nouvelles tactiques. Les paragraphes suivants décrivent cela plus en détail.

### 4.1 Le déluge des logiciels malveillants en 2008

L'année 2008 est déjà gravée dans l'histoire des logiciels malveillants. En l'espace de trois mois, les agresseurs ont réussi, grâce à une tactique jusqu'à présent unique, à renvoyer l'année 2007 dans l'ombre de l'histoire des records. Fin mars 2008, les experts des laboratoires de G DATA Security avaient déjà recensé un nombre de nouveaux codes malveillants supérieur à celui de l'ensemble de l'année 2007. Pour la fin de cette année, G DATA estime une multiplication par quatre au minimum du nombre de nouveaux programmes nuisibles. Cela est dû au fait que les analyseurs de signatures ne détectent que les logiciels malveillants déjà connus. Les auteurs de logiciels malveillants en profitent. Comme cela est décrit dans la rubrique Recyclage du dernier rapport des logiciels malveillants, les codes malveillants sont déformés jusqu'à être indétectables par les signatures antivirus, à l'aide des emballeurs et autres outils de camouflage. Le fonctionnement du code malveillant reste inchangé. Le code modifié, non reconnu, est alors livré.

Un autre système, créateur également de nombreuses autres versions, est souvent introduit par les portes dérobées. La plupart d'entre elles disposent d'une fonction de mise à jour. Cette fonction est fréquemment utilisée en tant que système de camouflage. Les portes dérobées sont actualisées si souvent, que le logiciel d'analyse antivirus détecte toujours une variante qu'il ne connaissait pas. C'est parce, dans ce cas également, il est d'avance certain qu'une nouvelle version ne sera pas reconnue par le logiciel. Le temps de réflexion entre l'apparition du virus et la préparation de la signature correspondante joue alors un rôle déterminant.

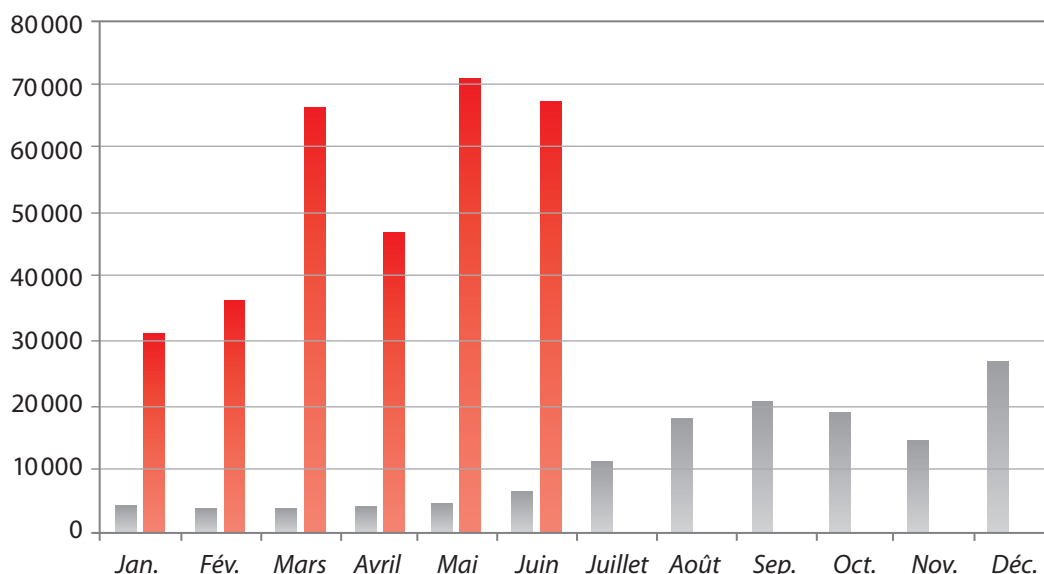


Diagramme 1 : comparaison du nombre total de nouveaux programmes malveillants ■ en 2007 par rapport au ■ premier semestre 2008

## 4.2 Virus de smartphones : publicité ou danger réel ?

Le danger assuré à de multiples reprises pour les possesseurs de Smartphones au premier semestre cette année n'était pas à prendre au sérieux, selon les laboratoires de sécurité de G DATA. Les 41 nouvelles espèces nuisibles attaquant les Smartphones étaient presque toutes des preuves de concept permettant de tester de nouvelles possibilités techniques ou des logiciels de surveillance pour les parents inquiets ou les époux possessifs.

La stagnation de ce type de logiciels malveillants qui dure depuis des années ne suscite aucune admiration : La propagation échoue d'une part à cause de la minime autonomie de Bluetooth, d'autre part du nombre insuffisant de smartphones accessibles avec fonctionnalité MMS, sans oublier que la connexion et l'installation doivent être confirmées par l'utilisateur.

La principale cause, souvent ignorée, est à trouver sur le plan économique : la cyber-délinquance est un marché florissant, donc soumis aux règles du marché. Le principal objectif est de réaliser le plus de bénéfices avec le moins d'activité possible. Le développement de logiciels malveillants sur smartphones coûte énormément à ses auteurs, et pas seulement financièrement. Un bénéfice par rapport aux investissements est jusqu'à présent utopique pour l'industrie des logiciels malveillants. Jusqu'à présent, dans d'autres secteurs, il est possible de réaliser plus en agissant moins.

Il manque alors d'une part des modèles commerciaux rentables, d'autre part, tous les moyens de réaliser des bénéfices dissimulent un risque de se faire arrêter. Par ailleurs, le danger souvent évoqué paraît plutôt trouver son origine dans une politique publicitaire et manque de toute preuve à l'heure actuelle.

Mois	Quantité
Janvier 2008	6
Février 2008	2
Mars 2008	9
Avril 2008	1
Mai 2008	15
Juin 2008	8

Tableau 2 : nombre de nouveaux logiciels espions sur smartphones

## 4.3 Botnets et logiciels espions en tête

Les logiciels malveillants sont répartis en différents types sur le tableau 3. Dans chaque catégorie, à l'exception des virus classiques, le nombre de nouvelles variantes apparues au premier semestre 2008 excède le nombre total de l'année 2007. Les portes dérobées maintiennent leur première position avec tout juste un quart des nouveaux logiciels malveillants, bien que leur part ait nettement diminué depuis 2007. Elles constituent la base de constitution des botnets, qui représentent désormais les armes les plus dangereuses des cyber-délinquants. Un bon cinquième des nouvelles espèces sont des téléchargeurs ou dropers.

Les malfaiteurs se servent de cette famille de logiciels malveillants pour installer des portes dérobées et autres programmes nuisibles sur les ordinateurs. Avec leurs 20%, ils occupent la seconde place du classement des nouveaux programmes nuisibles au premier semestre. Le nombre de logiciels espions a beaucoup diminué, mais peut défendre la troisième place.

	# 2008 T1	Part	# 2007	Part en 2007	Différence
Portes dérobées	75.027	23,6 %	41.477	31,0 %	362 %
Téléchargeurs / droppers	64.482	20,3 %	28.060	21,0 %	460 %
Logiciels espions	58.872	18,5 %	29.887	22,4 %	394 %
Chevaux de Troie	52.087	16,4 %	13.787	10,3 %	756 %
Logiciels publicitaires	32.068	10,1 %	7.654	5,7 %	838 %
Outils	12.203	3,8 %	1.731	1,3 %	1.410 %
Vers	10.227	3,2 %	4.647	3,5 %	440 %
Composeurs	4.760	1,5 %		n.a.	
Exploit	1.613	0,5 %		n.a.	
Rootkits	1.425	0,4 %	559	0,4 %	510 %
Virus	327	0,1%	2.127	1,6 %	31 %
Autres	5.170	1,6 %	3.688	2,8 %	280 %
Total	318.261	100,0 %	133.617	100	476 %

Tableau 3 : nombre et part des nouveaux types de logiciels malveillants au premier semestre 2008 et en 2007, et différence

## 4.4 Explosions des logiciels publicitaires

En 2007, le nombre de nouveaux logiciels publicitaires avait déjà été multiplié par cinq. Il a encore beaucoup augmenté depuis. Début 2008, plus de huit fois plus de logiciels publicitaires ont été découverts qu'en 2007 en moyenne. Sans compter les outils soutenant la croissance la plus robuste.



Logiciels publicitaires : WinFixer prétend être un logiciel antivirus. Après son installation, il détourne toutes les pages de démarrage du navigateur et affiche continuellement des fenêtres publicitaires pop-up.

Les pages d'accueil et fichiers détournés avec contenu potentiellement non désiré, comme des pièges publicitaires ou résultats de recherche manipulés, bénéficient désormais d'une grande popularité sur le marché de la cyber-délinquance.

Le leader de cette branche est Virtumonde. Le programme nuisible s'intègre comme objet d'aide du navigateur dans Internet Explorer, puis affiche des publicités dans des fenêtres contextuelles pop-up. Les clics artificiels massifs créés ainsi enrichissent les auteurs de logiciels publicitaires.

L'installation de programmes permet la création d'un autre mode de paiements. En effet, chaque installation génère le règlement de quelques centimes. Cela se rentabilise ici aussi par la quantité massive. L'augmentation considérable de nouveaux logiciels malveillants montre que ce commerce fonctionne.

## 4.5 Nouvelle augmentation des Spams

En janvier, le nombre de Spams avait diminué d'environ 60%, mais il est ensuite remonté à 70%. Depuis le mois de mars, la part du courrier indésirable s'élève à nouveau à plus de 80%, avec une valeur record de 94% en avril, et un niveau de 87% en juin dernier.

Les sujets les plus fréquents sont listés par catégories sur le tableau suivant :

Thème	Part en %
Performance sexuelle	30 %
Médicaments	22 %
Copies	21 %
Titre académique :	5 %
Logiciels	3 %

Tableau 3 : Les 5 meilleurs thèmes de courrier indésirable au premier semestre 2008

Le botnet sert toujours pour l'envoi d'une grande partie du courrier indésirable. Au premier semestre 2008, une moyenne de 85% a été calculée. Chaque jour, 5 à 10 millions de zombies sont impliqués dans l'expédition de courrier indésirable. De 200 000 à 500 000 (360 000 en moyenne) ordinateurs sont transformés en zombies quotidiennement. La plupart d'entre eux sont en Allemagne, en Italie et au Brésil (voir tableau 4). Ainsi, près de 130 milliards de messages de Spam, d'hameçonnage ou d'autres logiciels malveillants sont envoyés chaque jour.

Pays	Part en %
Brésil	10,2%
Allemagne	9,3%
Italie	8,9%
Turquie	8,3 %
Chine	6,6 %

Tableau 4 : 5 meilleurs pays où le plus d'ordinateurs se sont transformés en zombies

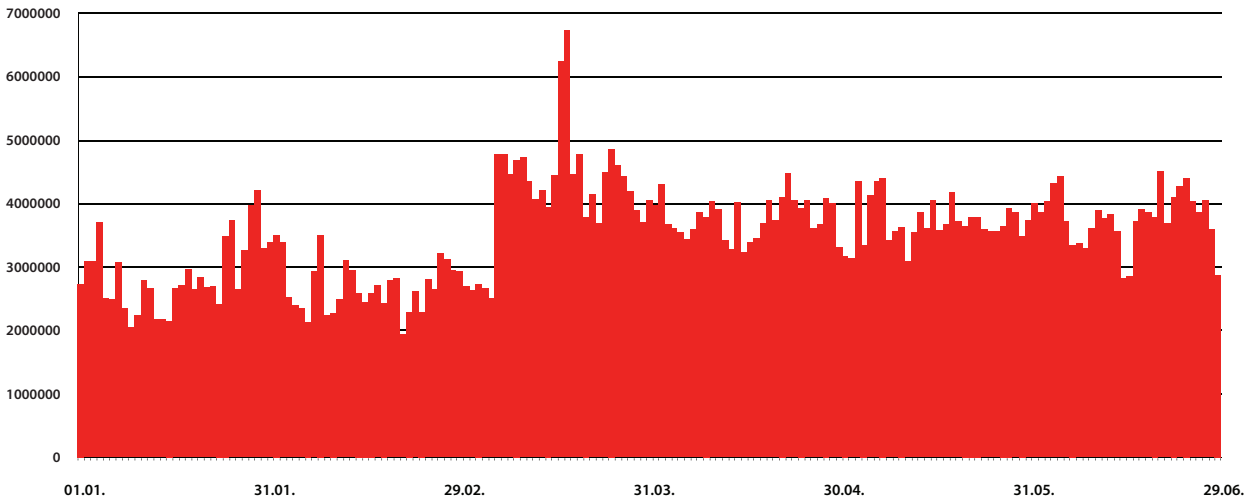
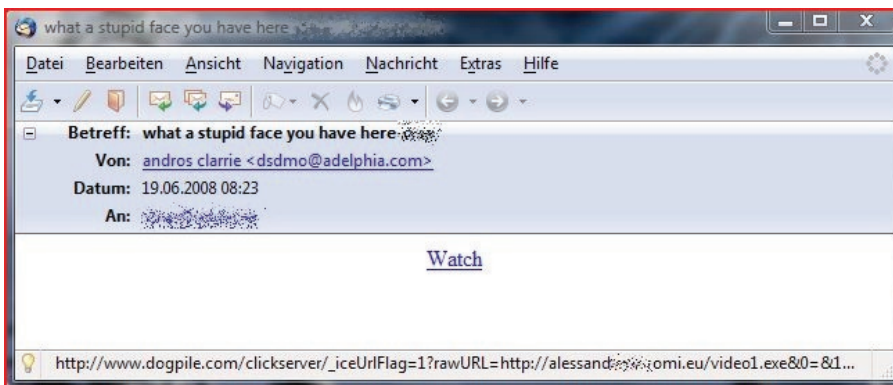


Diagramme 2 : messages indésirables au premier semestre 2008

Pour glisser à travers les filtres anti-Spam, les expéditeurs de courrier indésirable recourent à des sites fiables et connus. Ils utilisent pour cela les fonctions de détournement de Google, Yahoo et autres sites. Les utilisateurs comme les filtres anti-Spam sont malmenés par le recours à un site de confiance.



Une approche semblable peut démarrer des images et sites Internet. Elles sont hébergées par des portails populaires comme Flickr ou Blogpost. La barrière des technologies de détection basées sur la réputation est alors franchie.

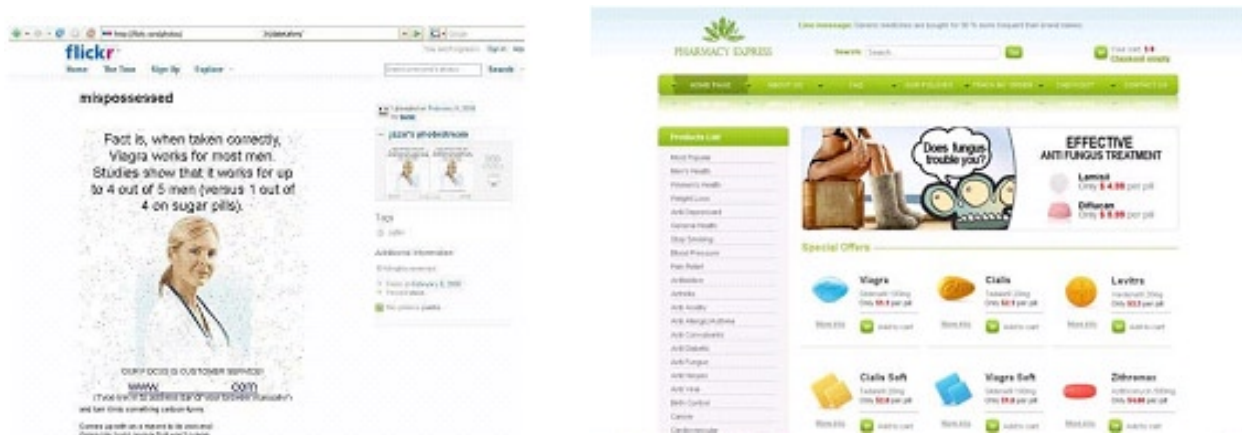


Diagramme 3 : images et Spam hébergés par Flickr et Blogspot

## 4.6 Les joueurs en ligne dans le collimateur

Les portes dérobées Hupigon et Bifrose ne sont pas les seules à se distinguer dans ce tableau 5. L'ancien et nouveau numéro un, Hupigon, est l'une des familles de programmes malveillants faisant le plus usage des packers. Les nouvelles versions peuvent être attrapées rapidement et efficacement avec un utilitaire. Certaines variantes utilisent jusqu'à 11 packers différents.

Les chevaux de Troie comme Online Games et Magania (GameMania) permettant le vol de codes d'accès des jeux en ligne ont acquis une certaine position parmi les familles les plus actives. Les joueurs sont donc toujours dans le collimateur des voleurs de données. Les codes d'accès des jeux en ligne, comme les personnages et objets des jeux sont commercialisés pour de l'argent réel dans de nombreux forums. Cela attire également les fraudeurs de la vie de tous les jours dans Internet.

	#2006	Famille de virus	#2007	Famille de virus
1	32.383	Hupigon	16.983	Hupigon
2	19.415	OnLineGames	8.692	OnLineGames
3	13.922	Virtumonde	3.002	Rbot
4	11.933	Magania	2.973	Banker
5	7.370	FenomenGame	2.848	Banload
6	7.151	Buzus	2.627	Zlob
7	6.779	Zlob	2.533	Virtumonde
8	6.247	Cinmus	1.922	Magania
9	6.194	Banload	1.882	LdPinch
10	5.433	Bifrose	1.751	BZub

Tableau 3 : Les 10 meilleures familles les plus actives en 2007 et au premier semestre 2008

Dans le tableau 5, les rubriques suivantes sont touchées par les programmes nuisibles suivants :

- **Virtumonde** : logiciels publicitaires intégrant Internet Explorer et affichant des fenêtres de pop-up.
- **FenomenGame** : détection d'erreurs à cause de la création automatique de signatures
- **Buzus** : chevaux de Troie, logiciels espions et enregistreurs de frappe avec portes dérobées
- **Zlob** : téléchargeur populaire de chevaux de Troie, qui modifie les paramètres d'Internet Explorer pour afficher des sites pornographiques ou installer des roguewares
- **Cinmus** est un logiciel publicitaire, qui s'intègre à Internet Explorer et affiche des fenêtres de pop-up.
- **Banload** : téléchargeur de chevaux de Troie pour la gestion des comptes en banque ciblant essentiellement les banques portugaises et brésiliennes

## 4.7 Codes malveillants sur différentes plates-formes - Concentration sur Windows

Au premier semestre 2008, la part des codes nuisibles attaquant Windows a de nouveau augmenté de 95,2% à 98,2%. Cela démontre que les auteurs de logiciels malveillants se concentrent sur le pôle des ordinateurs Windows. Manifestement, c'est ici qu'ils réalisent le plus de bénéfices.

	#2008 H1	Plateforme	#2007	Plateforme
1	312.668	Win32	126.854	Win32
2	2.650	JS	2.463	JS
3	845	HTML	1.106	HTML
4	572	VBS	1.007	VBS
5	545	BAT	707	BAT
6	252	MSIL	197	PHP
7	231	SWF	166	MSWord
8	92	MSWord	139	Perl
9	91	PHP	137	Linux
10	33	MSExcel	70	ASP

Tableau 4 : Les 10 meilleurs des plateformes en 2007 et au premier semestre 2008

Les attaques web de Javascript, HTML, VBScript, Flash (SWF), PHP et Perl ont bien vu une réduction de leur part de 2,5% à 1,4%. Toutefois, pour l'année 2008, d'après une estimation brute, le nombre d'attaques Web devrait plus que doubler. Cela démontre qu'en dehors des logiciels malveillants de Windows, cachés sur sites Internet, un nombre grandissant d'attaques ciblées sur des plateformes Web sont actuellement exécutées. Les systèmes de protection contre ces attaques étant très récents, ils n'ont pas besoin d'être actualisés très fréquemment.



Pour Linux, seules 21 nouveaux programmes nuisibles ont été découverts contre 41, au maximum, pour les smartphones (20 pour Symbian, 19 pour J2ME et 2 pour Win CE. en 2007). Pour cette raison, le danger si souvent évoqué reste peu inquiétant pour le premier semestre 2008, concernant les téléphones mobiles.

## 5. Prévisions pour le second semestre 2008

**G DATA prévoit les développements suivants pour les semaines et les mois à venir :**

- **Logiciels malveillants dans les sites Web :**

La propagation de logiciels malveillants par les sites Internet est depuis peu épuisée. Du côté des visiteurs, certaines failles restent néanmoins à combler. Non seulement le navigateur, mais aussi tous ses plug-ins doivent être isolés. Toutefois, du côté des fournisseurs de services Internet, il reste du pain sur la planche. Les applications Web couvent de nombreuses failles de sécurité comme le Cross-Site Scripting, le Cross Site Request Forgery et les injections qui peuvent profiter à la mise en écluse de contenus inconnus des sites Internet. Il faudra attendre quelques temps avant que des développeurs d'applications Web prennent en compte et mettent en place les mesures de sécurité nécessaires. En attendant, les visiteurs de sites Internet restent exposés à un risque d'infection plus élevé. Seule une protection antivirus vérifiant également les données HTTP et les codes malveillants assure une protection fiable. Cela concerne en particulier les utilisateurs assidus de sites Web 2.0 comme MySpace, Flickr, Facebook etc.

- **Modèles de rentabilité :**

Les Spam, vols de données, et logiciels publicitaires constituent des entreprises multimilliardaires, que les cyber-délinquants ne sont pas prêts d'abandonner dans l'immédiat, malgré les efforts des procureurs. Ce sont les botnets tout puissants qui forment désormais le pilier de cette industrie. Ainsi, dans les mois qui suivront, les téléchargeurs et portes dérobées transformant les ordinateurs en zombies inonderont les réseaux.

- **Commerce de données florissant**

Les logiciels espions peuvent, en attendant, démasquer bien plus que les codes d'accès des utilisateurs de sites bancaires. Quiconque est victime d'un enregistreur de frappe peut perdre toute son identité en ligne.

- **Les logiciels publicitaires, le secteur le plus croissant.**

Les clics extorqués et l'installation de logiciels publicitaires rapportent énormément de bénéfices.

- **Nouveaux systèmes de cache :**

Il est possible que les rootkits et programmes malintentionnés, ancrés dans le secteur d'amorce comme MasterBootRecord se renforcent dans les mois qui suivront.

- **Marchepieds :**

Les grandes manifestations prévues comme les Jeux olympiques serviront certainement d'opportunités pour les actes frauduleux.

Go safe. Go safer. **G DATA.**