



G DATA

Livre Blanc - Tendances
2007 et perspectives 2008

Ralf Benzmüller & Thorsten Urbanski

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

Livre Blanc - Tendances 2007 et perspectives 2008

Ralf Benzmüller & Thorsten Urbanski

1. Introduction

Dans notre dernier rapport annuel, nous nous attendions à ce « *que les modèles établis dans le domaine des logiciels publicitaires, des logiciels espions et du phishing, ainsi que l'utilisation de réseaux de bots performants, seraient poursuivis à l'avenir.* ». Cette prévision peu audacieuse s'est, au grand dam de nombreux utilisateurs, bel et bien confirmée, tout comme « *l'augmentation de codes malveillants dans les pages web* » et le faible risque pour les utilisateurs de téléphones mobiles.

En 2007, les auteurs de programmes malveillants nous ont largement tenu en haleine. Au total, le nombre de nouveaux programmes a atteint le record de 133 253 nouveaux parasites ! Ce qui représente une hausse de plus du triple (338,6 %). Les plus nettes augmentations ont été constatées dans le domaine des logiciels publicitaires (570 %), des virus (507 %), des backdoors (499 %) et des logiciels espions (336 %).

Mais si l'on doit dédier l'année 2007 à un groupe particulier de parasites, c'est bien aux chevaux de Troie espions et voleurs de données. Ils arrivent en masse et dérobent désormais bien plus que de simples données d'accès à des banques en ligne. Certains événements majeurs de l'année tournent de ce fait autour du thème du vol de données.

2. Évènements majeurs de l'année 2007

Le vol de données et les réseaux de bots ont aussi fait les grands titres en 2007. Il nous paraît particulièrement intéressant d'évoquer les éléments suivants et leurs conséquences.

2.1 Le « Storm Worm »¹

En janvier, alors qu'une tempête nommée Kyrill s'abat sur l'Europe, engendrant des dégâts considérables dans plusieurs régions, sont envoyés en masse des messages électroniques concernant cette même tempête. Le cheval de Troie dissimulé en pièce jointe faisait de l'ordinateur le zombie d'un réseau de bots. La même source avait par le passé déjà promis des extraits vidéo de l'exécution de Saddam Hussein ou encore les images d'une guerre nucléaire imminente, à quoi suivirent bien d'autres messages électroniques en lien avec l'actualité. Puis de fausses factures furent envoyées entre autres aux clients d'IKEA, de Quelle et d'eBay. Au fil de l'année furent ensuite utilisés des cartes de vœux, des jeux et des logiciels déposés sur des sites web. Ainsi, plusieurs millions d'ordinateurs ont pu être intégrés à ce réseau de bots ravageur, le plus gros jamais créé et qui est utilisé principalement pour l'envoi de spams et pour des attaques de déni de service distribué (DDoS).

2.2 Le vol de données

En janvier, des clients de la banque suédoise Nordea se sont vus proposer, par l'intermédiaire de messages électroniques d'hameçonnage personnalisés, un outil anti-spam à télécharger gratuitement. Cet outil avait cependant pour seul objectif de collecter les données d'accès des clients de la banque. Tout cela avait été précédé du vol d'informations sur la clientèle, lesquelles ont été utilisées pour atteindre les clients de manière ciblée. Une technique qui a porté ses fruits, puisque quelques 900 000 EUR ont pu être dérobés avec les données d'accès volées.

Et d'autres cas de vols de données importants ont été rapportés :

- Plus de 45 millions d'informations sur des cartes de crédit ont pu être dérobées par des attaques ciblées du réseau WLAN de TJX
- En février, quelqu'un a réussi à voler les mots de passe et adresses e-mail des utilisateurs du portail d'études StudiVZ, à la suite de quoi tous les mots de passe ont dû être réinitialisés.
- Des chevaux de Troie ont permis de collecter 1,6 million d'enregistrements concernant les utilisateurs, en grande partie américains, de la bourse de travail Monster.com.
- À cause de ces vols de données et d'autres vols similaires, des millions d'enregistrements contenant des informations personnelles ont atterri entre des mains criminelles.

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.

2.3 La guerre froide sévit sur Internet

Le déplacement d'un monument russe dédié à la mémoire des soldats à Tallin, la capitale estonienne, a entraîné de violentes protestations de la part de la population russe. Une fois les manifestations réprimées, des attaques de déni de service distribué eurent lieu pendant plusieurs semaines avec des réseaux de bots sur de nombreux sites Internet des ministères, autorités gouvernementales, banques, journaux et entreprises. On ignore les personnes qui se cachent derrière ces attaques. Si l'on soupçonne le Kremlin d'avoir lancé ces attaques, rien n'a pu être confirmé. La manière dont les attaques ont été réalisées porte à penser à des tentatives systématiques d'attaques devant livrer de précieuses données pour les offensives à venir. Sur Internet, on prépare ses armes.

En août, la chancelière allemande Angela Merkel est en visite officielle en Chine. Au même moment, des pirates informatiques pénètrent le système de la chancellerie fédérale avec pour objectif de transférer quelques 160 Go de données sensibles sur un serveur chinois, ce qui sera finalement évité à la dernière minute. Des attaques de ce type ont également eu lieu dans d'autres pays européens. Les services secrets utilisent eux aussi Internet.

3. La tendance 2007 des logiciels malveillants

Certaines évolutions de l'année dernière ont commencé à se dessiner dès 2006. Les attaques basées sur le web ont considérablement augmenté. Les réseaux de bots sont et restent un pivot des cybercriminels. Les logiciels publicitaires s'affirment également comme une source de revenus particulièrement lucrative. De nombreuses nouvelles versions de parasites mettent à profit le temps mis pour créer et livrer de nouvelles signatures de virus au moyen de nombreuses mises à jour. Il se dessine toutefois également de nouvelles évolutions. Les dispositifs d'infection de fichiers classiques (les virus au sens premier du terme) connaissent un regain important et, dans le domaine de l'hameçonnage, des chevaux de Troie spécialisés reviennent au galop sous forme de messages électroniques et sites web falsifiés. Les spammeurs aussi se sont creusés la tête pour contourner les filtres anti-spam. Les paragraphes suivants décrivent cela plus en détail.

3.1 Transfert des logiciels malveillants vers Internet

Cette nouvelle tendance se dessinait déjà en 2006. Au lieu de pièces jointes, les messages électroniques et instantanés ne contiennent plus que des liens vers des fichiers sur Internet. Et les variantes de Storm Worm ne sont pas les seules à s'inspirer de cette nouvelle stratégie. En observant les parasites les plus communs de l'année, on s'aperçoit que la moitié de ceux figurant dans le top 10 est connue depuis plus d'un an. Cela vaut tout particulièrement pour celui qui caracole en tête, apparu pour la première fois en mars 2004.

1	NetSky	31,0
2	Bagle	10,5
3	Mytob	7,8
4	Warezov	6,7
5	Feebs	3,5
6	Mydoom	3,5
7	Bankfraud	3,4
8	Zhelatin	3,1
9	Scano	2,8
10	Small	2,6

Tableau 1 : Logiciels malveillants les plus trouvés en 2007 par famille de virus

Lorsque les URL vers des fichiers malveillants ont commencé à être utilisées pour bloquer des e-mails, un nouveau changement de stratégie a eu lieu et les fichiers exécutables n'ont plus été mis directement en lien, ce sont les pages web qui contenaient les liens vers les programmes malveillants. Sur les pages web, on a également essayé, en alternative ou en complément, d'utiliser les faiblesses du navigateur en termes de sécurité pour infester l'ordinateur des visiteurs avec du code malveillant. Le nombre de parasites agissant par l'intermédiaire de langages de script HTML ou d'autres langages courants sur le web a presque triplé. Les visiteurs de la page ne remarquent rien des attaques. Il suffit d'un simple passage sur la page pour être infecté. On parle ici d'infection par « drive-by download ». Conséquence : les filtres anti-spam sont de plus en plus importants pour détecter les programmes malveillants.

Le transfert des programmes malveillants vers Internet représente de nombreux avantages pour les cybercriminels. 1. le maliciel peut sans cesse être actualisé, 2. après une première analyse de l'ordinateur, les parasites adaptés au système d'exploitation et au navigateur peuvent

être téléchargés ultérieurement, 3. l'accès à la page web peut être refusé à certains utilisateurs. 4. Les experts en matière de virus, qui éveillent les soupçons en visitant régulièrement des sites abritant des programmes malveillants par exemple, doivent s'attendre à recevoir uniquement des fichiers inoffensifs ou à être attaqués.

3.2 Le recyclage de programmes malveillants.

Le nombre de nouveaux parasites informatiques a battu tous les records en 2007. Avec 133 253 nouveaux parasites, leur chiffre a plus que triplé par rapport à l'année précédente.

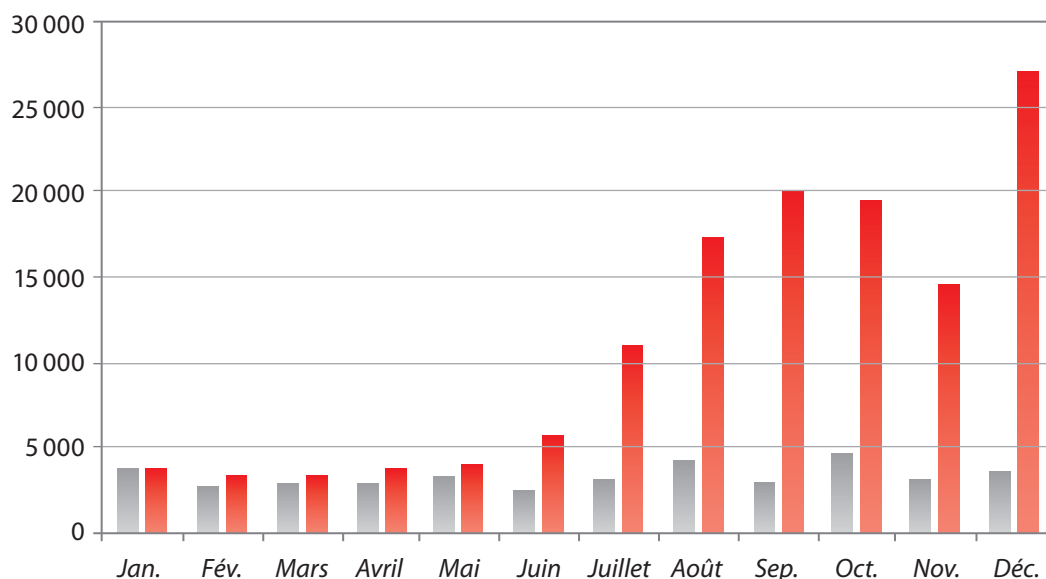


Diagramme 1 : Comparaison 2006 - 2007 du nombre total de nouveaux programmes malveillants

Une des raisons pour lesquelles le nombre de parasites a connu une telle augmentation réside dans la manière dont les droppers et téléchargeurs de chevaux de Troie sont utilisés et recyclés. Ces deux types de programmes malveillants sont conçus pour un usage unique ; c'est ce que l'on pourrait appeler des chevaux de Troie jetables. Lorsqu'une signature est établie pour le parasite, le programme malveillant est alors considéré comme brûlé (« burned »). Ce que l'on appelle les runtime-packers permettent cependant de recycler le même code malveillant. Pour cela, on a utilisé dans un premier temps des packers standard avec des paramètres inhabituels. À présent, il existe des centaines de packers spécialement développés qui disposent de mécanismes polymorphes et incluent ainsi toute copie du code source dans un autre habit. Les auteurs de programmes malveillants font cela jusqu'à ce que le nouveau code ne puisse plus être reconnu par les scanners anti-virus courants. La boucle du recyclage est ainsi refermée. Ce procédé fonctionne apparemment tellement bien que, si le nombre de téléchargeurs et de droppers a certes presque doublé, il est, avec 263,7 %, bien au-dessous de la croissance totale de 338,6 %.

3.3 Les e-criminels s'appuient toujours principalement sur les réseaux de bots.

Les réseaux de bots ne servent pas seulement à envoyer des spams ou à exécuter des attaques de déni de service. Les ordinateurs zombies sont également utilisés pour héberger des pages de maliciels et d'hameçonnage et pour explorer les adresses des serveurs de messagerie électronique. Il n'est donc pas étonnant que le nombre d'ordinateurs zombies ait augmenté en 2007. Le nombre de réseaux de bots a également beaucoup augmenté car ceux-ci ont été segmentés en plus petites unités. Ils sont désormais loués à des conditions de plus en plus avantageuses.

Si, l'année dernière, la commande avait lieu presque exclusivement par IRC, en 2007, plus de réseaux de bots utilisant d'autres protocoles de commande ont été créés. Le réseau de bots Storm est construit comme un réseau P2P. Le réseau de bots Zunker, également très puissant, communique par HTTP. Les mécanismes de camouflage sont eux aussi de plus en plus finagolés. Très souvent, les backdoors se cachent derrière des mises à jour et des rootkits. Les programmes et données pour un ordre sont transmis immédiatement puis effacés.

	# 2007	%	# 2006	%	% 2006 - 07
Backdoors	41 477	31,1	8 321	21,1	498,5
Logiciels espions	29 887	22,4	8 889	22,7	336,2
Téléchargeurs / droppers	28 060	21,1	10 640	27,2	263,7
Chevaux de Troie	13 787	10,3	5 230	13,4	263,6
Logiciels publicitaires	7 654	5,7	1 343	3,4	569,9
Vers	4 647	3,5	1 751	4,5	265,4
Virus	2 127	1,6	419	1,1	507,6
Outils	1 366	1,0	526	1,3	259,7
Rootkits	559	0,4	229	0,6	244,3
Autres	3 688	2,8	1 776	4,5	207,7
Total	133 253	100,0	39 124	100,0	338,6

Tableau 2 : Nombre et part de nouveaux logiciels malveillants en 2007 par type et modification par rapport à 2006

On constate en observant l'évolution des types de programmes malveillants que les réseaux de bots formaient (et forment encore) le pilier central des activités cybercriminelles. Les PC infectés peuvent être actualisés et coordonnés à distance par l'intermédiaire de programmes à portes dérobées. Ces portes dérobées (backdoors) non pas seulement été multipliées quasiment par cinq par rapport à 2006 mais ont également augmenté la part qu'elles représentent, avec environ 3 portes dérobées pour 10 nouvelles variantes et laissent ainsi derrière elles même les téléchargeurs et les logiciels espions. Les autres types de programmes malveillants atteignant les meilleures places utilisent la procédure habituelle lors d'une infection. L'ordinateur est tout d'abord infecté par un téléchargeur ou un dropper qui, outre le chargement et le démarrage d'un fichier, diminue les paramètres de sécurité du système. Une fois affaibli, la porte dérobée fait en sorte que l'ordinateur puisse être commandé à distance et pourvu d'autres logiciels mal-

veillants. Il s'agit ici souvent de logiciels espions ou autres chevaux de Troie qui transforment l'ordinateur en producteur de spams ou serveur de fichiers et web.

3.4 Le logiciel publicitaire est à la mode

Outre les réseaux de bots, il y a une autre possibilité d'utiliser les ordinateurs infectés de manière assez lucrative : les logiciels publicitaires. Si ces programmes ne volent aucune donnée, ils enregistrent cependant par moment les actions de l'utilisateur sur Internet et affichent de la publicité à l'ouverture de certaines pages ou manipulent des requêtes. Le paiement de ces publiciels a lieu soit après un certain nombre de clics (la page d'accueil de l'ordinateur infecté est par exemple manipulée), soit par version installée. Des programmes affiliés correspondants peuvent être trouvés dans des forums en ligne spécialisés.

Bien que l'année dernière de très grandes entreprises de la branche aient elles aussi eu à faire face à des défaites juridiques, le nombre de logiciels publicitaires malveillants et de programmes potentiellement non souhaités a été multiplié par plus de cinq (voir tableau 2).

3.5 La résurrection des infections de fichiers

Les virus classiques joints aux fichiers ont perdu en importance ces dernières années. Cependant, l'utilisation répandue de lecteurs amovibles tels que les clés USB ou les disques durs externes remet ce mécanisme de propagation au goût du jour. Le nombre de virus au sens premier du terme a ainsi été presque multiplié par cinq.

3.6 Les spams

Les envois en masse de messages électroniques non souhaités ont, cette année encore, inondés chaque jour des millions de boîtes de messagerie. En novembre, 95 % des e-mails échangés étaient des spams. Les spammeurs usent sans cesse de nouvelles techniques pour faire passer leurs envois en masse à travers les filtres. Ce sont tout d'abord les spams images qui ont envahi les boîtes de messagerie. Ici, le véritable message publicitaire était caché dans l'image. Les textes compris dans le message électronique servaient alors simplement à contourner les filtres de Bayes. De nombreuses astuces telles que le découpage d'images ou les variations au hasard de police et de couleurs ont permis de contourner même les méthodes d'analyse les plus développées tels que la reconnaissance optique des caractères et les procédés basés sur des bases de données. Lorsqu'au milieu de l'année, les filtres anti-spam se sont attaqués aux fichiers image, les spammeurs ont changé de stratégie et envoyé des e-mails au format Excel, PDF, MP3 et vidéo. À la fin de l'année, le pourcentage de ces formats inhabituels avait cependant à nouveau diminué.

Mais les spams restent un sujet de premier ordre. Non seulement en raison des recettes qu'ils génèrent, mais aussi parce que les spammeurs et auteurs de logiciels malveillants collaborent de plus en plus étroitement. Environ 90 % de tous les spams sont envoyés par réseau de bots. Mais la nouvelle stratégie consistant à envoyer des messages électroniques avec un lien vers des pages malveillantes renforce aussi l'importance des filtres anti-spam dans la protection contre les programmes malveillants.

3.7 Hameçonnage, pharming, chevaux de Troie bancaire et vol d'identité

Le hameçonnage classique ne progresse pas. Les tentatives d'arnaques à l'aide de messages électroniques prétendument envoyés par des banques ou des boutiques en ligne, lesquels renvoient à des pages web désormais bien imitées, ne jouent plus qu'un rôle minime grâce aux barres d'outils d'hameçonnage omniprésentes et aux filtres anti-spam améliorés. Cette régression a plus que profité aux chevaux de Troie spécialisés, en particulier aux chevaux de Troie bancaires. Les versions les plus récentes ne se contentent cependant pas seulement de voler les données d'accès aux comptes en ligne et les informations sur les cartes de crédit. Certains programmes espions dérobent toutes les données d'accès enregistrées dans la zone de stockage protégée. D'autres, tels que Bzub, envoient tous les contenus des formulaires web à des auteurs d'attaques. De cette manière, les victimes de chevaux de Troie peuvent perdre toute leur identité en ligne. Et de plus en plus d'innocents sont ainsi victimes des machinations de cybercriminels.

Voici un bref aperçu des principales caractéristiques techniques des logiciels espions

- Le **PHARMING** dirige l'utilisateur vers de fausses pages web sans qu'il ne s'en aperçoive et ce même s'il a entré un nom de domaine correct dans le navigateur. Ce type d'attaques est basé sur la détermination de l'adresse IP du nom de domaine. Pour cela, le système DNS même peut être attaqué, mais l'ordinateur client offre lui aussi certains points d'attaque. Les représentants de la famille de virus Qhosts, par exemple, modifient les entrées du fichier HOSTS pour certaines pages web ou enregistrent un serveur DNS contrôlé par l'auteur de l'attaque.
- **LES ENREGISTREURS DE FRAPPE** enregistrent comme leur nom l'indique les frappes du clavier et les envoient à un tiers non autorisé. Très souvent, ils ne sont actifs que lorsque certaines conditions sont remplies. Par exemple, lorsque la page web ouverte à ce moment-là fait partie d'une liste souvent très longue de noms de domaine ou lorsque des fenêtres avec des noms bien particuliers sont ouvertes. Des claviers sur écran tactile ont été développés pour aller à l'encontre de ces enregistreurs de frappe. Suite à quoi sont apparus les **SCREENLOGGERS**. Ils font soit des captures d'écran de tout le contenu affiché à intervalles réguliers (par exemple **RBOT**), soit un graphique de l'environnement de la souris à chaque clic. Quelques fois, des séquences d'images sont même instantanément transformées en film AVI.

Certains outils d'espionnage (par exemple **RBOT**) utilisent les webcams et micros d'ordinateurs infectés

- Certains parasites (par exemple **TORPIG**) modifient l'apparence et le contenu du navigateur. Ils sont en mesure de représenter la ligne supérieure contenant la bonne adresse bien que le contenu vienne d'un autre domaine trafiqué. Même le cadenas signalant une liaison sécurisée peut être affiché de façon tout à fait injustifiée. D'autres parasites (par exemple certaines versions de **BANCOS** ou **NURECH**) insèrent soit d'autres champs de formulaire sur une page, soit des pages web supplémentaires dans le dialogue. Ce faisant, les certificats SSL existants restent actifs. Sans outils spéciaux, il est impossible de savoir si ces données sont falsifiées ou non.
- **LES HIJACKERS** reprennent la session de telle manière que l'auteur de l'attaque change les montants et les coordonnées bancaires en sa faveur (Bancos par exemple). La victime voit, elle, ses propres informations. Même le montant total du compte est falsifié en conséquence. Ici aussi, l'arnaque ne peut être constatée que sur les relevés bancaires.
- Les redirecteurs dévient le flux de données de manière à rendre possible une attaque de

l'HOMME DU MILIEU (MAN-IN-THE-MIDDLE). Il peut s'agir d'un mandataire local ou d'un serveur mandataire contrôlé par l'auteur de l'attaque. Il est ainsi possible d'épier l'ensemble de la communication en réseau de la victime, ce qui permet de surveiller les messages électroniques, chats, pages web visitées, données de formulaire et les téléchargements de fichiers.

- **LES RENIFLEURS** observent le transfert de données sur le réseau de la victime. Le nombre de nouveaux renifleurs a considérablement diminué.
- **LES CHEVAUX DE TROIE PSW** recherchent des informations utiles dans tout le PC. Il peut s'agir d'adresses e-mail ou de fichiers au contenu particulier ou d'un certain type de fichier. Ces données sont rassemblées et transmises à l'auteur des attaques. Les informations de connexion, clés d'enregistrements et mots de passe (ou leurs caractères de substitution) enregistrés dans le système sont une cible privilégiée de ce genre de programme. Les mots de passe pour l'accès à certaines pages web et aux boîtes de messagerie sont enregistrés dans la zone de stockage protégée lorsque l'utilisateur accepte la possibilité d'enregistrer le mot de passe. Cette proposition souvent utilisé est affiché par le navigateur ou le fournisseur de boîte de messagerie. Il est donc judicieux de renoncer à l'enregistrement automatique des mots de passe et informations de connexion. Un des plus grands représentants de cette catégorie s'appelle LdPinch.

Comme on le voit, les méthodes sont de plus en plus raffinées et efficaces. Cela explique qu'en 2007 aussi, le nombre de victimes et de dommages ait augmenté.

3.8 Les joueurs en ligne dans le collimateur

Les backdoors ne sont pas les seules à se distinguer dans ce tableau. L'ancien et nouveau numéro un, Backdoor Hupigon, est 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. Rbot s'attaque avec agressivité aux programmes de protection des ordinateurs.

	#2006	Famille de virus	#2007	Famille de virus
1	2.549	Hupigon	16.983	Hupigon
2	1.474	Zlob	8.692	OnLineGames
3	1.420	Banload	3.002	Rbot
4	1.147	Banker	2.973	Banker
5	869	LdPinch	2.848	Banload
6	848	Rbot	2.627	Zlob
7	562	Horst	2.533	Virtumonde
8	555	Lineage	1.922	Magania
9	497	SdBot	1.882	LdPinch
10	489	QQHelper	1.751	BZub

Tableau 3 : Le top 10 des familles de virus 2007

Il est particulièrement intéressant de constater qu'avec «OnLineGames» et «Magania», deux dérobeurs de mots de passe se sont fait une place dans le top 10, deux programmes se concentrant sur les mots de passe de jeux en ligne. En 2006 déjà, on constatait avec Lineage qu'un tel programme atteignait les premières places. Les deux représentants de cette année ont cependant atteint de bien meilleurs résultats par rapport à l'année précédente. Cela montre que les joueurs en ligne sont de plus en plus attaqués. Le nombre d'espions de mots de passe se concentrant sur les joueurs en ligne dépasse désormais le nombre de chevaux de Troie bancaires.

3.9 Du code malveillant sur différentes plateformes mais aucun risque pour les téléphones mobiles

Au niveau des plateformes pour lesquelles les parasites informatiques ont été développés, Windows occupe très largement la scène. Aux places suivantes, les attaques basées sur le web dans Javascript, HTML, VBSkript, PHP et Perl ont plus que triplé. En revanche, seuls 119 parasites ont été découverts pour Linux.

En 2007, il ne nous a cependant pas été possible d'établir le risque maintes fois évoqué dans ce domaine pour les téléphones mobiles. Avec tout juste 26 nouveaux parasites, parmi lesquels la majorité sont des outils espions semi-légitimes s'adressant aux époux jaloux et parents inquiets, le nombre de parasites pour Symbian a été réduit au tiers de sa valeur de 2006 et, occupant la 14ème place, n'est plus représenté dans le top 10.

	#2007	Plateforme	#2006	Plateforme
1	126.854	Win32	37.397	Win32
2	2.463	JS	487	HTML
3	1.106	HTML	334	JS
4	1.007	VBS	323	VBS
5	707	BAT	287	BAT
6	197	PHP	145	Linux
7	166	MSWord	123	MSWord
8	139	Perl	101	DOS
9	137	Linux	73	SymbOS
10	90	ASP	70	Perl

Tableau 4 : Top 10 des plateformes en 2006 et 2007

4. Perspectives 2008

Nous escomptons pour 2008 un maintien et une sophistication des méthodes éprouvées, avec en particulier les points suivants :

- **Encore plus de logiciels malveillants basés sur Internet.** Les nouvelles possibilités offertes par le web 2.0 vont être encore plus exploitées par les cybercriminels en ligne. Nous soulignons en particulier les faiblesses en matière de sécurité que présentent les applications web à cause desquelles du code malveillant peut être introduit dans les pages web résultantes. De même, les bases de données à la source de ces applications web vont être de plus en plus attaquées. Les (versions d') outils à venir vont fortement simplifier ces processus.
- **Des envois en masse de messages électroniques personnalisés.** Les informations récupérées au travers de vols de données seront utilisées l'année prochaine pour envoyer des spams et des messages d'hameçonnage de façon ciblée à des groupes de personnes. Ces messages électroniques seront adressés personnellement à leurs destinataires et l'adresse de l'expéditeur sera une personne connue par le destinataire.
- **Encore plus de spams ?** Dans l'ensemble, le nombre de spams augmentera à peine. Ils seront pourtant considérablement plus ciblés et donc plus efficaces. Les spams dans les blogs et forums poseront l'année prochaine un problème massif.
- **L'hameçonnage par l'intermédiaire de messages électroniques et de sites web va considérablement diminuer, même dans le secteur bancaire.** Les nouvelles cibles sont les boutiques en lignes, les plateformes de réseaux sociaux (MySpace, Facebook, LinkedIn etc.), les bourses de travail et les jeux en ligne. Prévision : le nombre de types va sensiblement augmenter l'année prochaine
- **Une année difficile pour les chercheurs anti-maliciels.** La masse de logiciels malveillants ne diminuera pas. En revanche, leur complexité va, elle, augmenter. Le cryptage, les Runtime-packer spéciaux, les outils de camouflage du code, les programmes malveillants ciblés ne sont que quelques-uns des défis à venir

Nous nous attendons cependant aussi à quelques nouveautés :

- **Plus de chantage.** En 2007, le rançongiciel était très rare. Nous prévoyons pour l'année à venir des améliorations dans l'infrastructure des réseaux de bots et dans le domaine du Bullet Proof Hosting (le plus connu étant le Russian Business Network RBN). Si l'anonymat du malfaiteur peut ainsi être assurée, le nombre de chantages basés sur des fichiers image et Office cryptés devrait augmenter. Le remède : la protection des données
- **La virtualisation.** Depuis plusieurs mois, tous les nouveaux processeurs livrés comportent des fonctions permettant une utilisation simple et efficace de machines virtuelles. Ces fonctions de virtualisation peuvent entre autres être utilisées pour la création de nouveaux rootkits (mot-clé : Bluepill). D'un autre côté, la virtualisation offre de nombreuses possibilités pour la réalisation de modèles de protection efficaces. Dans ce domaine, aussi bien les auteurs d'attaques que les défenseurs renforcent leurs recherches
- **Des technologies nouvelles et évolutives.** Vista et MacOSX sont sur le point de franchir la barre critique des 10 % de part de marché. Cela les rend encore plus intéressants pour les cybercriminels, ce qui entraînera une augmentation des attaques sur ces systèmes. Les gadgets proposés par Vista pourraient être à l'origine d'une nouvelle créativité. La paisible oasis des utilisateurs d'Apple devra elle aussi faire face à quelques bouleversements en 2008.
- Il est très difficile de prévoir quelles nouvelles technologies vont focaliser l'attention des

pirates informatiques. Pour l'instant, nous n'escomptons pas d'attaques de plus grande ampleur mais nous nous attendons à des attaques test dans le domaine de la VoIP et des consoles de jeux compatibles avec Internet.

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