Le mardi 25 août 2009

L'étude semestrielle BitDefender sur le spam et les malwares révèle que les menaces s'adaptent aux nouveaux comportements en ligne

L'étude révèle des changements dans le contenu et les moyens de diffusion des menaces

D'après **BitDefender®** la création de malwares est devenue une occupation à part entière, s'inspirant du modèle des entreprises. BitDefender vient de publier les résultats de son étude sur le spam et les malwares réalisée entre janvier et juin 2009, qui révèle que le spam imitant les newsletters et les tentatives de phishing sur le web 2.0 connaissent une forte progression.

Tour d'horizon des malwares

Au cours du premier semestre 2009, les créateurs de malwares ont continué à essayer d'infecter les utilisateurs d'ordinateurs afin de réaliser des profits financiers directs et/ou de prendre le contrôle de leurs machines. Selon le rapport, les chevaux de Troie sont en augmentation et représentent 83 % de l'ensemble des malwares détectés.

Alors que les chevaux de Troie constituaient les menaces les plus actives ces six derniers mois, c'est le célèbre ver Downadup (aussi appelé Conficker ou Kido) qui a causé le plus de dégâts auprès des utilisateurs. Downadup a réussi à infecter un nombre d'ordinateurs record dans le monde entier (environ 11 millions) et a fait la une de la plupart des revues informatique et des médias traditionnels. Ciblant les systèmes n'ayant pas corrigé la vulnérabilité MS08-067, le ver peut s'envoyer depuis tous les ordinateurs précédemment infectés sur le même réseau, et cherche ensuite à accéder aux partages de fichiers. Bien que Microsoft ait publié un patch spécifique pour cette vulnérabilité, l'infection est toujours en circulation et des centaines de systèmes sont compromis chaque jour.

D'après Marc Blanchard, Directeur des Laboratoires BitDefender en France : « Internet est une plateforme de communication incontournable regroupant des personnes de tout âge, de toutes catégories et de tous horizons, mais c'est aussi un vivier pour les criminels et les personnes peu scrupuleuses qui tentent d'accéder à un grand nombre de systèmes, d'informations et de données financières ». « Il est aussi indispensable que chaque internaute prenne conscience que, même si leur ordinateur ne contient aucune données confidentielles ou sensibles, les cyber-délinquants ne sont pas obligatoirement à la recherche de données, mais de l'utilisation potentielle de leur ordinateur de façon télécommandée. C'est pourquoi, il est primordial de bloquer ces délinquants avec des solutions de sécurités efficaces proposant des technologies de protections proactives et prédictives ».

D'après BitDefender, au cours des six derniers mois, les pays les plus actifs pour la diffusion de malwares étaient la Chine, la France et les États-Unis, suivis de la Roumanie, de l'Espagne et de l'Australie.

Classement des 10 principaux malwares au niveau mondial entre janvier et juin 2009

PLACE	Malware	%
1	Trojan.Autorun.Inf	31
2	Win32.Worm.Downadup	13
3	Trojan.Wimad	13
4	Trojan.SkimTrim.HTML.A	11
5	Trojant.Agent.AKXM	10
6	Trojan.Autorun.AET	7

7	Worm.Autorun.WHG	5
8	Packer.Malware.NSAnti.1	4
9	Trojan.Spy.Agent.NXS	3
10	Trojan.JS.PZB	3

Les tendances du spam au premier semestre 2009

Concernant les médias et les techniques, les spécialistes BitDefender ont déterminé une résurgence du spam-texte, qui a atteint 80 % cette année, contre 70% à la même période en 2008.

Le spam-image a quant a lui augmenté de 150% depuis le premier semestre 2008. Les images sont incorporées dans des spam imitant des newsletters au format HTML, ces images téléchargeables font partie de la stratégie développée par les spammeurs pour d'une part inciter les utilisateurs à accepter des images généralement bloquées par les clients de messagerie, et d'autre part contourner autant que possible les filtres antispam en modifiant légèrement la palette de couleurs de l'image.

Les messages de spam promouvant des logiciels piratés/OEM ont également beaucoup augmenté en comparaison avec l'an dernier. D'après les statistiques fournies par le Laboratoire de Recherche Antispam BitDefender, le spam 'logiciel' représente environ 3 % de l'ensemble du spam. En juin 2009, les messages non sollicités liés aux logiciels sont devenus l'une des cinq principales menaces de spam et représentaient 5 % de l'ensemble des messages de spam envoyés dans le monde entier.

Dix principaux contenus du spam au cours du premier semestre 2009 :

1. Spam médical
2. Liens de phishing
3. Emprunts
4. Malwares en pièces jointes
5. Spam produit / Contrefaçons
6. Logiciels/OEM
7. Pornographie
8. Sites de rencontres
9. Emploi
10. Diplômes universitaires et Casinos en ligne

L'état du phishing et des malwares Web 2.0

De janvier à juin 2009, les messages de phishing ont passé le seuil inquiétant de 7% des messages de spam envoyés dans le monde entier. Comme prévu, les pays les plus réceptifs en termes de phishing sont les États-Unis, le Canada et le Royaume-Uni, trois pays anglophones. Mais la Russie est également une source importante de phishing, principalement en raison de sa législation laxiste à l'égard du cyber-crime, et du taux de chômage du pays.

Le phishing évolue et se transforme constamment, ce qui inclut une augmentation des techniques de phishing Web 2.0. Les comptes utilisateurs de réseaux sociaux sont des éléments clés permettant de réaliser des attaques ciblant d'autres utilisateurs de ces réseaux. Cependant, les fournisseurs de services ayant renforcé leur niveau de sécurité afin de protéger les informations personnelles de leurs utilisateurs, les attaquants ont conçu de fausses pages d'accueil afin de tenter d'obtenir les véritables informations de connexion des utilisateurs.

Les Laboratoires BitDefender ont découvert que la plupart des tentatives de phishing du web 2.0 au cours du premier semestre 2009 reposaient sur des techniques d'ingénierie sociale et exploitaient la naïveté des utilisateurs. L'arnaque du « Twitter Porn Name » en est un bon exemple. Les utilisateurs étaient invités à révéler le nom de leur premier animal de compagnie, ainsi que celui de la première

rue dans laquelle ils ont habité. Ces noms sont généralement utilisés comme questions de sécurité. Un pirate en possession d'un nom d'utilisateur et de ces éléments peut facilement retrouver un mot de passe qu'il peut par la suite utiliser pour accéder à un compte et envoyer du spam, accéder à des transactions ou utiliser les données du compte quelle qu'en soit la manière pour réaliser du profit (ce qui peut même aller jusqu'à la demande d'une rançon pour restituer le compte piraté à son propriétaire).

Cependant, les cibles les plus visées par les phishers sont relativement constantes. Il s'agit en général d'usurper l'identité d'organismes du secteur financier, en particulier les banques et les institutions permettant de réaliser des transferts d'argent.

Les trois entreprises dont les identités ont le plus souvent été usurpées au cours du premier semestre 2009 :

1. Bank of America
2. Paypal
3. Abbey

BitDefender estime que plus de 55 000 utilisateurs sont victimes d'arnaques de phishing tous les mois, pour un total de 330 000 victimes entre janvier et juin 2009. Afin de parvenir à tromper leurs victimes, les phishers doivent imiter (ou « spoofer ») une véritable page Web aussi précisément que possible. Cependant, si copier une page Web consiste en un simple copier/coller, le message de spam contient généralement des fautes d'orthographe et/ou une mise en page peu soignée.

Ce n'est pas le cas de la plupart des attaques ciblant la Bank of America. Non seulement le texte est disposé de façon irréprochable mais la page de phishing a été réalisée avec le plus grand soin, ce qui laisse penser que les personnes à l'origine de ces attaques de phishing sont un gang de cybercriminels très bien organisés.

Vlad Vâlceanu Directeur de la Recherche Antispam des laboratoires BitDefender explique que « contrairement aux malwares, le phishing et le spam sont des menaces universelles, qui fonctionnent avec tous les ordinateurs, quels que soient les systèmes d'exploitation et les patches de sécurité installés. » « La prudence et une solution antimalware de qualité comprenant des modules antispam, antiphishing et antimalware sont indispensables pour tout utilisateur d'Internet. »

Pour plus d'informations sur cette étude, veuillez consulter le rapport BitDefender sur les e-menaces.

À propos de BitDefender®

*BitDefender est la société créatrice de l'une des gammes de **solutions de sécurité** la plus complète et la plus certifiée au niveau international reconnues comme étant parmi les plus rapides et les plus efficaces du marché. Depuis sa création en 2001, BitDefender n'a cessé d'élever le niveau et d'établir de nouveaux standards en matière de protection proactive des menaces. Chaque jour, BitDefender protège des dizaines de millions de particuliers et de professionnels à travers le monde – en leur garantissant une utilisation sereine et sécurisée de l'univers informatique. Les **solutions de sécurité** BitDefender sont distribuées dans plus de 100 pays via des partenaires revendeurs et distributeurs hautement qualifiés. Dans les pays francophones, BitDefender est édité en exclusivité par Éditions Profil. Plus d'informations sur BitDefender et ses solutions sont disponibles via le **Centre de presse**. Retrouvez également sur le site **www.malwarecity.fr** les dernières actualités au sujet des menaces de sécurité qui permettent aux utilisateurs de rester informés des dernières évolutions de la lutte contre les malwares.*

À propos des Editions Profil

Editions Profil, société indépendante créée en 1989, développe, édite et diffuse des logiciels sur différents secteurs d'activités, professionnel et grand public. L'éditeur a constitué un large catalogue de solutions dans de nombreux domaines, par exemple sur les segments de la bureautique et de la productivité. Editions Profil s'est plus particulièrement spécialisée ces dernières années dans l'édition et la distribution d'outils de sécurité informatique et la protection des données en général. Editions Profil édite notamment les solutions de sécurité BitDefender et Parental Filter, ainsi que les solutions Farstone et diffuse les solutions de récupération de données et de gestion de serveurs MS Exchange de Kroll-Ontrack.