Seuls 8,4 % des emails reçus par les entreprises en 2008 n'étaient pas malveillants

- **Sur les 430 millions d'emails analysés, 89,88 % étaient du spam et 1,11 % étaient infectés par des codes malveillants.**

- **Les stimulants sexuels et produits pharmaceutiques sont les sujets les plus fréquents des messages de spam reçus en 2008.**

- **Au cours des trois derniers mois de l'année, 301.000 PC zombies étaient actifs et utilisés principalement pour distribuer du spam.**

Paris, le 5 février 2009

Seuls 8,4 % des courriers électroniques reçus par les entreprises sont légitimes. 89,88 % des emails sont du spam et 1,11 % sont infectés par un virus ou autre malware. Ces données ont été obtenues en compilant les données des 430 millions d'emails analysés en 2008 par TrustLayer Mail, le service de sécurité administrée de la messagerie de Panda Security.

	% spam	% infectés	% dangereux	% suspects	Emails légitimes
Janvier	76,27	1,84	0,59	0,64	20,66
Février	87,83	3,08	0,46	0,62	8,01
Mars	86,51	1,32	0,45	0,53	11,19
Avril	94,75	0,88	0,12	0,12	4,13
Mai	94,71	0,97	0,03	0,07	4,22
Juin	93,35	0,87	0,01	0,16	5,61
Juillet	90,43	0,98	0,11	0,55	7,93
Août	93,01	0,99	1,27	0,18	4,55
Septembre	91,89	2,34	0,19	0,19	5,39
Octobre	90,04	1,92	0,08	0,19	7,77
Novembre	88,36	2,06	0,1	0,33	9,15
Décembre	91,48	1,08	0,05	0,26	7,13
Total	89,88	1,11	0,28	0,32	8,41

La quantité de spam dans les emails des entreprises a fluctué au cours de l'année, avec un pic à 94,27 % au deuxième trimestre. Les taux de spam ne sont passés au-dessous de la barre des 80% qu'en janvier.

Concernant les messages infectés en 2008, le ver Netsky.P est le code malveillant qui a été le plus souvent détecté. Ce type de malware s'active automatiquement lorsque les utilisateurs visualisent le message infecté via le volet de lecture de Microsoft Office Outlook. Le ver exploite une vulnérabilité d'Internet Explorer qui permet l'exécution automatique des pièces jointes des emails. L'exploit de cette vulnérabilité est détecté par PandaLabs sous le nom d'Exploit/iFrame ; il est le troisième type de code malveillant le plus souvent détecté dans les emails par TrustLayer Mail.

« Ces deux codes malveillants sont souvent utilisés ensemble par les pirates, ce qui explique leur grand nombre de détection. Les cybercriminels développent souvent plusieurs variantes de malware couplées à des exploits de vulnérabilités afin d'augmenter leurs chances d'infecter les PC. Ainsi, les utilisateurs dont le PC est à jour peuvent quand même se faire infecter s'ils ouvrent la pièce jointe », explique Luis Corrons, le directeur technique de PandaLabs.

Le cheval de Troie de porte dérobée Rukap.G, conçu pour permettre aux pirates de prendre le contrôle à distance de l'ordinateur, et le cheval de Troie Dadobra.Bl comptent également parmi les codes malveillants les plus fréquemment détectés.

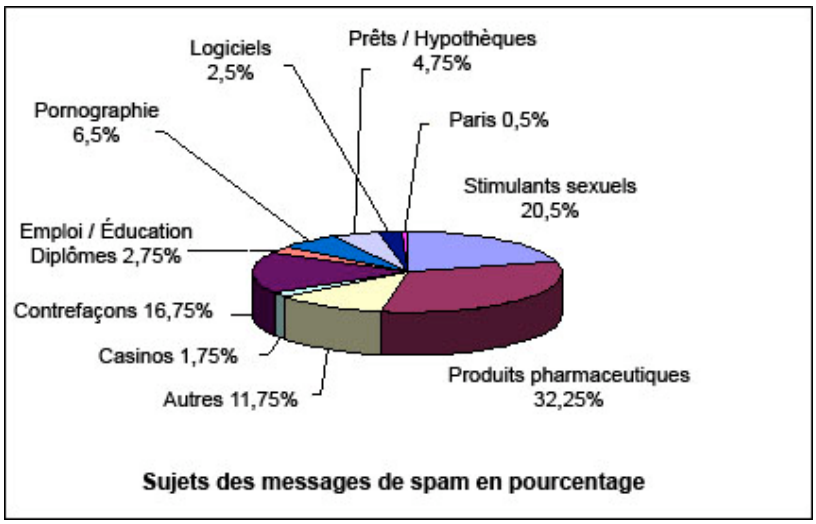
Top malwares dans les emails
Netsky.P.worm
Bck/Rukap.G
Exploit/iFrame
Trj/Dadobra.BL
Generic Malware
Trj/Downloader.PSJ
Trj/SpamtaLoad.DO
Trj/Downloader.PWR
Bck/Haxdoor.PL
Trj/Spamtaload.DZ

« Pour les entreprises, le spam représente bien plus qu'une nuisance. Ces messages indésirables consomment inutilement la bande passante, font perdre du temps aux salariés et peuvent également entraîner des disfonctionnements du système. Au final, le spam entraine des pertes de productivité pour l'entreprise. », précise Luis Corrons.

La majeure partie des emails indésirables sont transmis par l'intermédiaire de réseaux de PC zombies contrôlés par les pirates. Les PC zombies sont des ordinateurs infectés par des codes malveillants appelés des « bots » qui permettent aux pirates de les contrôler à distance. Ces ordinateurs sont généralement organisés en réseaux qui sont utilisés pour des actions malveillantes telles que l'envoi de spam. Au cours du dernier trimestre 2008, ce sont 301.000 ordinateurs zombies qui étaient en activité chaque jour.

Sujets des spams en 2008

Concernant les types de spam reçus en 2008, 32,25 % de ces emails indésirables faisaient la promotion de produits pharmaceutiques et 20,5 % étaient en rapport avec les stimulants sexuels.



Sujets des messages de spam en pourcentage

L'impact de la crise économique s'est également ressenti dans les messages de spam. Les fausses offres d'emploi et les diplômes falsifiés ont constitué 2,75 % des emails indésirables reçus en 2008. Les messages promouvant de faux prêts et hypothèques ont quant à eux représenté 4,75 %.

Les publicités pour des produits de contrefaçons (montres...) constituaient 16,75 % du spam. Cette dernière catégorie de spam a cependant chuté de 21 % au premier semestre à 12,5 % au deuxième semestre.

A propos de PandaLabs

Depuis 1990, la mission de PandaLabs est d'analyser les nouvelles menaces le plus rapidement possible pour assurer une totale sécurité à nos clients. Pour cela, PandaLabs a développé un système automatisé et innovant qui analyse et traite les milliers de nouveaux échantillons reçus chaque jour et renvoie automatiquement un verdict (logiciel malveillant ou inoffensif). Ce système repose sur l'Intelligence Collective Antimalware, le nouveau modèle de sécurité de Panda Security, qui détecte même les codes malveillants capables de passer au travers des autres solutions de sécurité.

Actuellement, 94 % des malwares détectés par PandaLabs sont analysés par l'Intelligence Collective Antimalware. Cette analyse automatique est complétée par le travail de plusieurs équipes spécialisées dans chaque type spécifique de malware (virus, vers, chevaux de Troie, logiciels espions, phishing, spam, rootkits, etc.) qui travaillent 24 heures sur 24 et 7 jours sur 7 pour offrir une garantie maximale. Grâce à ce système, Panda peut offrir à ses clients des solutions plus sûres, plus simples et consommant moins de ressources.

Pour plus d'informations, visitez le blog de PandaLabs : http://www.pandalabs.com

	CONTACTS PRESSE : ÉMILIE SACKSICK **SACKSICK@ELIOTROPE.FR** LIGNE DIRECTE : **01 53 17 16 43**	**ELIOTROPE** 151, rue du Faubourg Saint Antoine 75011 Paris France **www.eliotrope.fr** TEL : + 33 (0)1 53 17 16 40 FAX : + 33 (0)1 53 17 16 41