Bitdefender mÃ¨ne lâ□□enquÃªteâ□¦ : Que contient votre ration quotidienne de Spam ?
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 1/6/2012 14:00:00

Bitdefender sâ□□est penchÃ© sur le sujet et a trÃ¨s vite dÃ©couvert que le Spam Ã©tait loin de se limiter aux arguments publicitaires des mÃ©dicaments miracles et aux contrefaÃ§ons des produits de luxe.**264,6 milliards de Spams** par jour sont diffusÃ©s dans le monde, soit environ 90 % de lâ□□ensemble du trafic dâ□□e-mails sur Internet.

Outre lâ□□incroyable diversitÃ© de produits ou de services prÃ©sentÃ©s dans ces e-mails non sollicitÃ©s, ceux-ci contiennent Ã©galement tous types de piÃ¨ces jointes, allant de pages HTML avec publicitÃ©s allÃ©chantes pour des contrefaÃ§ons, aux Â« reÃ§us Â» en format PDF exploitant des vulnÃ©rabilitÃ©s de type Â« zero-day Â», ou mÃªme des piÃ¨ces jointes contenant des malwares qui corrompent les systÃ¨mes sur lesquels elles sont tÃ©lÃ©chargÃ©es.

Le nombre de messages de Spam avec des piÃ¨ces jointes malveillantes augmentant de faÃ§on continue, nous avons voulu dÃ©crypter ce que les cyber-escrocs essayaient de mettre en place au travers de ces messages. Nous avons recueilli pendant deux semaines plus de 2 millions dâ□□Ã©chantillons de Spam de divers Â« honeypots Â» situÃ©s dans diffÃ©rentes rÃ©gions, Ã diffÃ©rents moments de la journÃ©e, afin dâ□□Ã©viter les campagnes saisonniÃ¨res et les envois en masse dâ□□une mÃªme campagne. Cela nous a permis de collecter une importante diversitÃ©

de Spams et de rÃ©cupÃ©rer les piÃ¨ces jointes quâ□□ils contenaient.

Deux millions de messages peut sembler Ã©norme aux utilisateurs de messagerie car câ□□est bien plus de spams quâ□□ils nâ□□en recevront jamais, mais cela correspond en fait au nombre de messages de Spam transmis sur Internet toutes les secondes !

Les rÃ©sultats sont les suivants : 1,14% des messages de Spam que nous avons recueillis contenaient des piÃ¨ces jointes. Bien que les messages de Spam soient potentiellement dangereux par nature (ils peuvent conduire les utilisateurs sur des sites de phishing, les impliquer dans des scams ou mÃªme, les arnaquer en leur faisant acheter des objets/mÃ©dicaments de contrefaÃ§on), certaines piÃ¨ces jointes reprÃ©sentent des menaces encore plus importantes pour la sÃ©curitÃ© des utilisateurs.

Une analyse plus approfondie des piÃ¨ces jointes a rÃ©vÃ©lÃ© que 10% dâ□□entre elles contenaient des malwares ou prÃ©sentaient des formes de phishing. Ce nombre nâ□□est peut Ãªtre pas impressionnant au premier abord, mais lâ□□extrapolation Ã lâ□□Ã©chelle du phÃ©nomÃ¨ne - 264,6 milliards de messages de Spam envoyÃ©s par jour â□□ permet dâ□□annoncer quâ□□environ 300 millions de messages de Spam avec piÃ¨ces jointes malveillantes et phishing sont envoyÃ©s tous les jours.

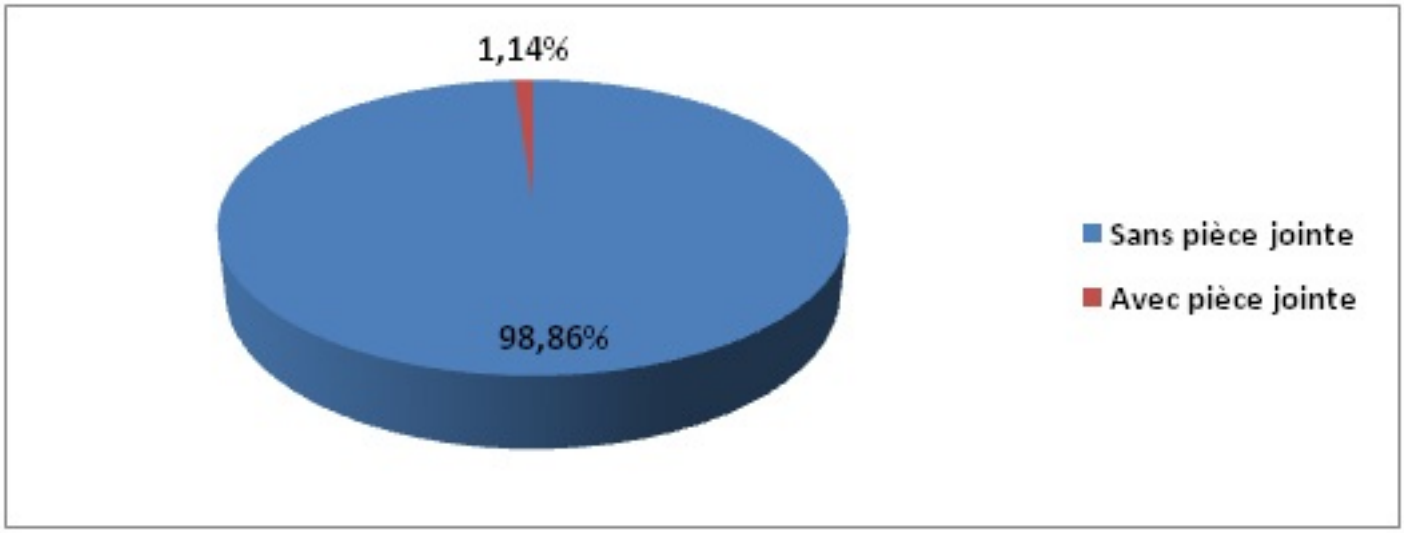


Fig.1 Poids des e-mails de Spam avec piÃ¨ce jointe vs sans piÃ¨ce jointe â□□ Ã©chantillon de 2 millions de spams

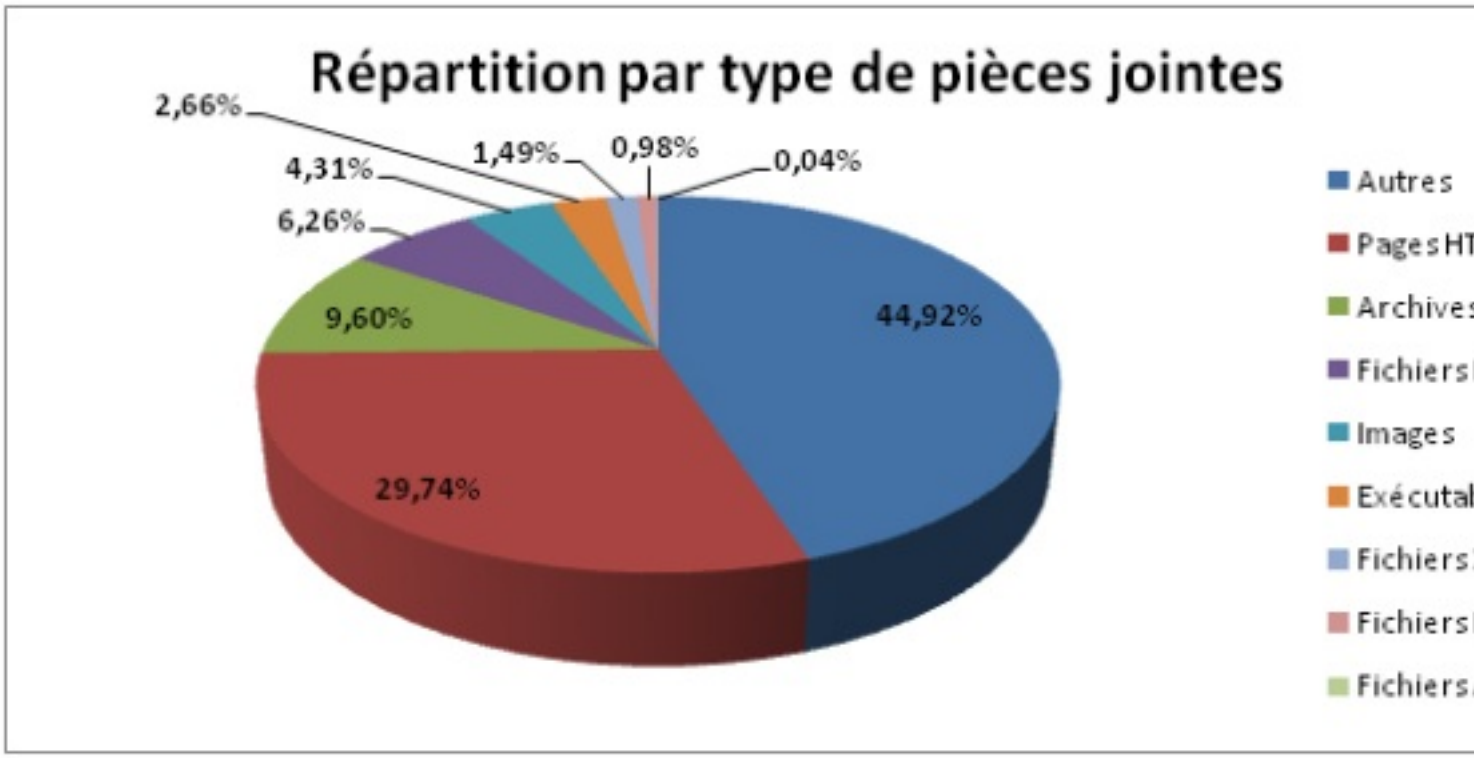
La rÃ©partition des piÃ¨ces jointes par type a rÃ©vÃ©lÃ© que 29,74% dâ□□entre elles sont constituÃ©es de pages HTML (des offres de phishing ou â□□pseudoâ□□ commerciales). Elles sont suivies par les fichiers archives (9,6%) et les fichiers DOC (6,26%). On trouve Ã©galement frÃ©quemment des images, des fichiers exÃ©cutables, des feuilles de calcul XLS. Les fichiers PDF et audio constituent moins de 1% de ces 2 millions de messages de spam.

Fig.2 RÃ©partition des piÃ¨ces jointes par type sur un Ã©chantillon de 2 millions de messages

Une attention particuliÃ¨re doit Ãªtre portÃ©e Ã la prÃ©sence de fichiers PDF intÃ©grant des attaques de type Java scripts (JSs) et Ã la catÃ©gorie des fichiers DOC / DOCX. Il sâ□□agit en effet

dâ□□un vecteur dâ□□infections connu au niveau des entreprises puisque ces formats de fichiers sont frÃ©quemment utilisÃ©s dans le cadre du travail en entreprise et ne sont pas bloquÃ©s par dÃ©faut par le pare-feu de lâ□□entreprise.

La plupart des piÃ¨ces jointes avec des fichiers exÃ©cutables contenaient des vers gÃ©nÃ©riques de messagerie (Worm.Generic.24461 et Worm.Generic.23834), ainsi que des virus gÃ©nÃ©riques (Win32.Generic.497472 et Win32.Generic.494775). Parmi les autres menaces â□□originalesâ□□ identifiÃ©es comme piÃ¨ces jointes, on trouve des invitations Ã des rÃ©unions commerciales en tÃªte-Ã -tÃªte avec le spammeur, des publicitÃ©s audio mais Ã©galement des fichiers exÃ©cutables infectÃ©s par Win32.Worm.Mytob.C@mm, un Mass Mailer existant depuis 7 ans et tristement cÃ©lÃ¨bre pour avoir interrompu en direct les services de CNN le 16 aoÃ»t 2005.



En conclusion, ils sont partout, ils se prÃ©sentent sous toutes les formes, pour les Ã©viter, il y a quelques prÃ©cautions de base Ã prendre en permanence :

â□¢ VÃ©rifier lâ□□adresse de lâ□□expÃ©diteur : si vous avez un doute, faites une recherche sur Internet pour Ãªtre certain que des utilisateurs nâ□□ont pas rencontrÃ© de problÃ¨mes avec ce type dâ□□email/expÃ©diteur

â□¢ Lire entiÃ¨rement le contenu de lâ□□e-mail afin de dÃ©tecter dâ□□Ã©ventuelles fautes dâ□□orthographe, des formats de dates inhabituels, des tournures de phrases improbables

â□¢ Se mÃ©fier de toutes notions dâ□□urgence souvent utilisÃ©es par les spammeurs : Â« DÃ©pÃªchez-vous Â», Â« Vite Â», Â« Sans tarder Â» ou de forme dâ□□intimidation Â« vous Ãªtes dans lâ□□illÃ©galitÃ© Â» Â« vous utilisez des programmes sans licence Â»â□¦

â¢ Installer une suite de sÃ©curitÃ© performante, intÃ©grant une fonctionnalitÃ© Antispam

Pour retrouver Bitdefender en ligne