Retrouvez-nous sur facebook Suivez-nous twitter

Étude AV-TEST :
les spams dangereux

Spams - plus dangereux que jamais

Les spammeurs envoient des millions de spams tous les jours par le biais de botnets. Durant une étude de 18 mois, l'institut AV-TEST sis à Magdebourg a collecté un demi-million de spams et en a conclu que le danger lié aux spams est plus présent que jamais.

Markus Selinger

Les spams sont tombés dans l'oubli. Ils sont toujours énervants, mais on s'y est habitué. C'est justement cela qui les rend désormais si dangereux. Durant une étude de 18 mois réalisée entre août 2011 et février 2013, le laboratoire d'AV-TEST a collecté plus d'un demi-million d'e-mails classés comme spams et les a analysés. Le résultat fait l'effet d'une douche froide : un tiers des spams à pièce jointe est infecté par un programme malveillant. Les autres e-mails tentent en général d'attirer l'utilisateur sur un site Internet infecté.

Cependant, la découverte bien plus inquiétante est que 25 % des ordinateurs émetteurs de spams se trouvent dans des locaux professionnels- même dans des bureaux allemands !

Plus de 500 000 spams analysés par le laboratoire

En tout, AV-Test a examiné 550 000 e-mails ayant été classés comme étant des spams au préalable. Parmi ceux-ci, 14 000 e-mails étaient infectés, soit env. 2,5 %.

Ces spams ont été collectés grâce à 90 comptes d'e-mail surveillés. Ces adresses électroniques ont pour partie été inscrites dans des forums et des jeux-concours : la première pierre de l'étude était posée. Après une courte durée, les comptes recevaient des douzaines de spams par jour.

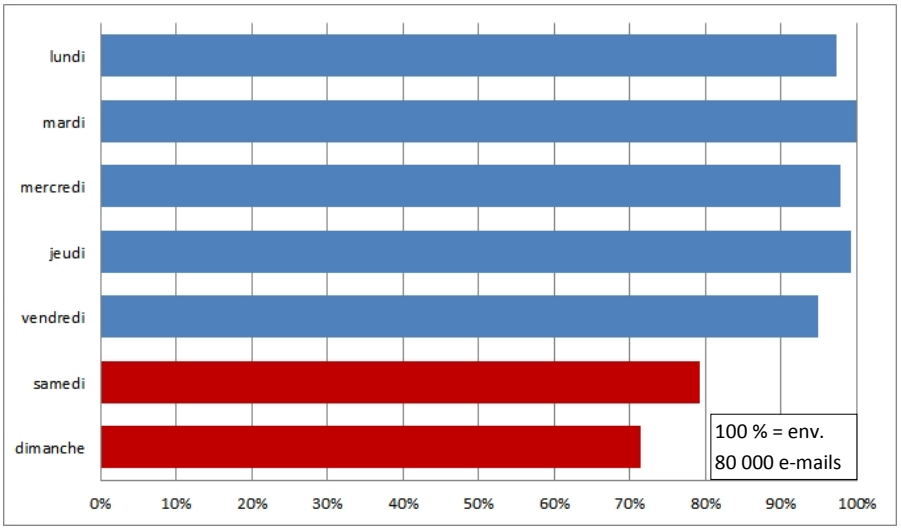
De nombreuses pièces jointes infectées

Plus de 30 000 des 550 000 spams analysés avaient une pièce jointe. 10 000 de ceux-ci, soit plus de 30 %, présentaient un programme malveillant nocif. Outre des textes, 400 000 e-mails comprenaient également des URL, c'est-à-dire des adresses Internet. Dans le cas des e-mails avec des URL, près d'1 % des liens dirigeait l'utilisateur directement sur des sites infectés par des logiciels malveillants. Le reste représentait en général des offres frauduleuses de contrefaçons

Plus d'informations sur www.av-test.org

Sur la page d'accueil d'AV-TEST GmbH, vous pouvez toujours trouver des informations actuelles sur le test, des études supplémentaires et des statistiques actuelles sur les spams et les logiciels malveillants.

25 % des ordinateurs émetteurs de spams se trouvent dans des bureaux !



Les spams ont été enregistrés lors de chaque jour de la semaine durant l'étude. Le maximum était d'env. 80 000 mails. Du lundi au vendredi, l'envoi de spams est assez régulier. Durant le week-end, il se réduit considérablement. Cela confirme que les ordinateurs se trouvent dans des bureaux et sont éteints lors du week-end. Ainsi, 25 % des ordinateurs qui appartiennent à un botnet et envoient des spams se trouvent dans des bureaux - même en Allemagne !

seuls 15 % de ceux-ci étaient infectés par des logiciels malveillants. Par contre, 78 % des e-mails à pièce jointe venant d'Inde étaient contaminés durant notre étude. Les spams à pièce jointe venant du Viêt-nam viennent juste derrière avec 77 %.

Parmi les 30 000 spams à pièce jointe enregistrés, la moitié était issue des États-Unis, de Chine, d'Inde et même d'Allemagne. Cependant, les spams allemands à pièce jointe n'étaient pas aussi dangereux : 10 % des e-mails présentaient une pièce jointe infectée.

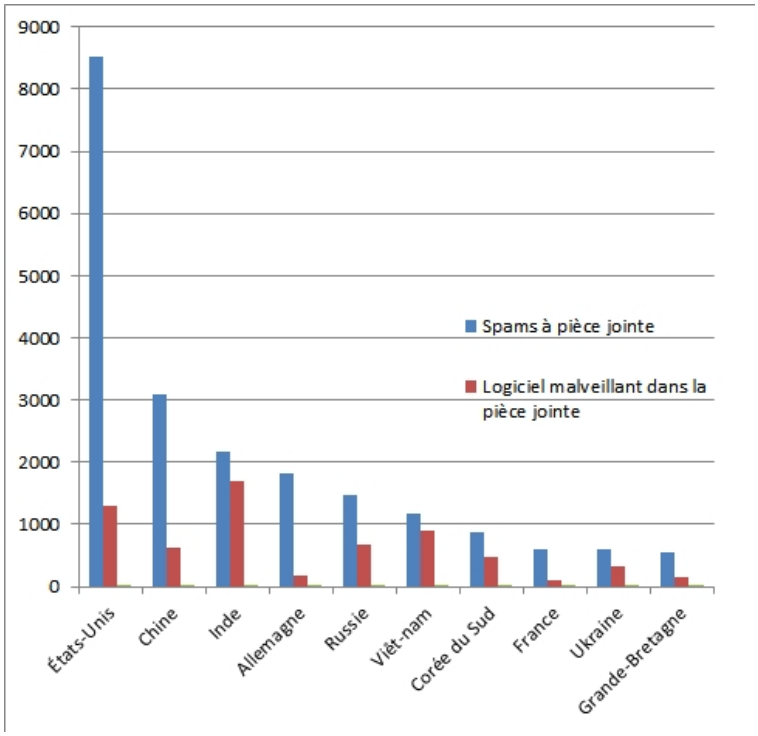
comme par exemple des produits pharmaceutiques.

Concernant les pièces jointes infectées, la plupart était des fichiers de formats classiques : fichiers ZIP, fichiers EXE, COM, SCR, BAT ou PIF exécutables et des documents HTML utilisés dans le but d'une attaque. Mais les fichiers PDF et les images restent très utilisés comme objets infectés. L'étude confirme que lorsqu'un fichier ZIP est attaché à un spam, la chance qu'il soit contaminé est presque de 100 %. Cela est également le cas pour les fichiers exécutables comme les fichiers EXE ou PIF. Dans le cadre de l'étude, plus de 80 % des documents HTML joints aux spams étaient infectés.

Les spams indiens sont toujours dangereux

La plupart des spams à pièce jointe provenait certes des États-Unis mais

Les spams à pièce jointe triés par pays



Durant l'étude, les États-Unis étaient certes le plus grand émetteur de spams à pièce jointe, mais ils contenaient moins de pièces nocives par rapport à d'autres pays. Les e-mails dont l'expéditeur provenait d'Inde ou du Viêt-nam contenaient presque toujours un programme malveillant. 10% des spams à pièce jointe provenant d'Allemagne étaient infectés.

25 % des ordinateurs émetteurs de spam se trouvent dans des bureaux

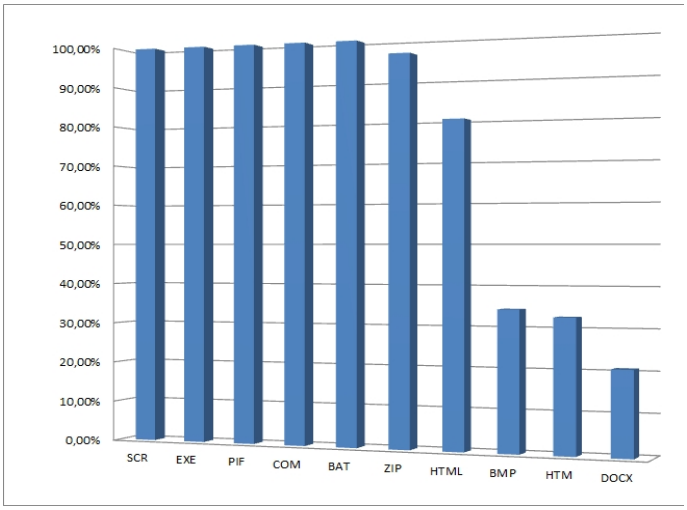
L'envoi de spams a été enregistré chaque jour de la semaine durant l'étude et il a ensuite été analysé après 18 mois. Résultat : du lundi au vendredi, le niveau de spams envoyés restait assez constant. Lors du week-end, c.-à-d. le samedi et dimanche, l'envoi diminuait de 25 %. Ainsi, l'étude confirme que 25 % des ordinateurs émetteurs de spam se trouvent dans des bureaux où ils sont éteints durant le week-end. Le lundi venu, le niveau de spams remontait invariablement.

Après des mois, nous n'avons pas constaté de pics. Il a seulement été possible de constater que juillet et août étaient les mois présentant les e-mails avec le taux d'infection le plus élevé. Ce faisant, un motif récurrent n'a cependant pas pu être identifié.

Les botnets - actifs et sournois

L'envoi de spams se fait presque toujours par le biais d'ordinateurs qui sont discrètement commandés à distance par des botnets. Ainsi, les e-mails possèdent toujours des IP d'envoi différentes. Cela rend difficile aux fournisseurs d'accès Internet d'identifier rapidement les e-mails problématiques grâce à leur adresse IP.

Top 10 des pièces jointes d'e-mail infectées



Durant l'étude, 30 types de fichiers différents de pièce jointe ont été dénombrés au total. Le top 5 montre que dès qu'un spam présente un fichier exécutable, celui-ci est toujours infecté par un programme malveillant.

Les ordinateurs infectés et commandés par un cheval de Troie se comportent de manière vicieusement discrète pour l'utilisateur. En effet, celui-ci ne doit pas remarquer que quelqu'un utilise son ordinateur pour envoyer des e-mails. Les botnets présentent également des tailles très différentes. Les botnets démantelés durant les dernières années comptaient 1 à 10 millions d'ordinateurs contrôlés. Ils n'étaient certes jamais tous en ligne en même temps, mais quelques centaines de milliers d'ordinateurs suffisent à envoyer de nombreux spams en très peu de temps.

« Est-ce que je fais partie d'un botnet ? » Testez votre ordinateur en ligne !

En collaboration avec l'Association de l'économie Internet allemande, l'Office fédéral allemand pour la sécurité met le site Internet www.botfrei.de à votre disposition. Vous y trouverez de nombreux liens de fabricants qui vous permettent de vérifier si votre ordinateur fait partie d'un botnet.

Les logiciels antivirus protègent

Si une suite de protection actualisée est installée sur un ordinateur, il est presque exclu qu'il soit compromis par un botnet. En effet, les suites de protection possèdent également un scanner pour les rootkits et les chevaux de Troie qui sont les outils préférés des exploitants de botnets. Vous pouvez à tout moment consulter gratuitement les tests actuels des meilleures suites de protection sur www.av-test.org

Retrouvez-nous sur facebook

Suivez-nous twitter

À Magdebourg, le 11 avril 2013
Auteur : Markus Selinger

Veuillez vous adresser à l'équipe d'AV-TEST GmbH si vous avez des questions supplémentaires.
E-mail : presse@av-test.de
Tél. : +49 391 6075460
Internet : www.av-test.org