

13-04-2005

R&T on-line

R&T, Le magazine

CSO Sécurité

Actualités -- Newsletter

Dossiers -- Abonnement

Actu Sécurité -- Newsletter

Chercher

>> sur CSO + Alerte <<



Carnet

Agenda

Contacts

Comparateur de prix



Sécurité & Technologies

Documentation

Pas d'amnésie pour les virus



Page imprimable

Livrez-nous
vos expériences

PUBLICITE

Le Monde
INFORMATIQUE

Toute l'info pour
mieux décider
sur www.
lemondeinformatique
.fr

Le RSS
permet aux
utilisateurs le
téléchargement
XML
de différents
sommaires
thématiques.

S'INFORMER
AVEC
LE MONDE
INFORMATIQUE

Marc OLANIE

09/04/2005

A force de banaliser ses méthodes d'éradication, le virus a presque tendance à devenir anodin, presque inoffensif. S'ajoute également le fait que d'autres menaces, notamment le Spam, le phishing, les spywares, ont un peu trop occupé le devant de la scène... l'infection par pièce jointe était has been, le bubon en paquets Netbios totalement passé de mode. Du coup, la garde se relâche, et les virus frappent de plus belle. « *Ils sont en augmentation de 50 %* » clame le très sérieux **ICSA Lab**. « Ils » frappent en moyenne 392 fois par mois sur un échantillonnage de 1000 machines. Le montant total des infections effectives atteint 166 par mois. Les désastres viraux (plantage de plus de 25 machines par une seule et même attaque) sont en augmentation de 12 % par rapport à l'an passé. Sur 300 entreprises sondées, 192 ont encaissé un tel désastre... elle n'étaient que 92 en 2003. Le chapitre des temps de reprise après sinistres est des plus... sinistres : 7 jours/personne, pour un coût estimé à 130 000 \$, chiffre en progression de 12 % par rapport à l'année précédente. Mais ce qui, durant cet enquête, a le plus marqué les enquêteurs de l'ICSA, c'est le pessimisme dont faisait état les personnes interrogées. « Le problème des programmes nuisibles devient de plus en plus grave » estiment-ils. Et strictement aucun des participants à l'étude n'a déclaré que 2004 avait été meilleur que 2003... Pourtant, précise le rapport, cette année là n'a pas été marquée particulièrement par une infection aussi retentissante que celle de la sinistre troïka Blaster Sobig Nachi.

Et ils s'appellent comment, les virus à la mode en 2005 ? Netsky, netsky, netsky, Netsky, netsky, netsky. On dirait du Malarmé, mais c'est signé **Secuserve**, société spécialisée dans l'externalisation du contrôle de flux smtp. Avec toutes ses variantes, et si l'on excepte une petite quatrième place raflée par un inconnu et une cinquième par une escouade de Zafi D, Netsky est présent sur tous les fronts. La mutation P, à elle seule, représente 40 % des souches détectées début avril. Certes, Secuserve prêche pour sa propre chapelle, mais le quotidien tend à prouver que cette analyse « est dans le vrai ».

- Le Spam = 69,60% des flux mails (+8% par rapport à Février 05);
- Les virus = 5,80% des flux mails (semblable à Février 05);
- Contenu Multimédia (Fichiers audio, vidéo, images fixes) = 1,24% des flux mails.
- Mails non conformes à la norme smtp = 1,6% des flux mails. Ces emails sont généralement utilisés pour contourner les antivirus smtp classiques

Globalement, estime ce prestataire, seul 21% du courrier est authentique, souhaité et légitime. Ceci est, précisons-le, une moyenne. Une adresse smtp qui sert à la rédaction depuis 1987 voit son filtre bayésien « station » expédier ad patres 90% du courrier entrant, sachant qu'au niveau du serveur, déjà 80% des spams « évidents » et des virus les plus connus sont éliminés automatiquement.



ALERTE