

GLOSSAIRE*

Pour vous aider à vous familiariser avec le thème de ce [séminaire], nous vous proposons quelques définitions de termes liés aux sujets abordés cet après-midi.

Adware : Logiciel dont l'auteur se rémunère par l'affichage de bannières publicitaires, sans pour autant recueillir de données personnelles sur ses utilisateurs.

Backdoor : Programmes qui détournent des fonctionnalités systèmes dans le but d'ouvrir des accès utiles aux pirates pour contrôler à distance les machines ciblées. Ces programmes, très dangereux, sont la plupart du temps installés par le biais d'un "cheval de Troie".

Bulk mail : Voir Spam

Cheval de Troie : Un cheval de Troie est un programme d'aspect anodin, masquant un code exécutable malicieux déclenchant ou servant à déclencher une attaque. Un cheval de Troie est en général utilisé pour ouvrir une porte dérobée (Backdoor) sur un système et donc permettre l'accès à distance de son ordinateur à un pirate informatique.

Dialer : Programme permettant de composer un numéro de téléphone. Certains dialers sont fournis par les fournisseurs d'accès pour créer ou simplifier la connexion Internet de leurs clients, alors que d'autres sont des logiciels douteux ou malveillants qui se présentent à l'internaute de manière plus ou moins trompeuse lors de l'accès à un service payant (notamment comme moyen d'accéder à des sites de charme « sans carte

bancaire ») voire qui s'installent à son insu pour se substituer au numéroteur de Windows et se connecter à Internet via un numéro surtaxé.

Firewall : Système logiciel ou serveur dédié situé entre deux réseaux informatiques, dont la tâche est de contrôler aussi bien les communications entrantes que sortantes, dans le but de sécuriser les échanges d'informations.

Hoax : En français, "canular". Il s'agit de rumeurs et fausses informations qu'une personne cherche à répandre le plus largement possible en utilisant comme support les autres internautes, qui relaieront l'information généralement par E-Mail.

Liste de diffusion : Ces listes se composent d'un ensemble d'adresses électroniques ayant un dénominateur commun (centre d'intérêt, profession, etc.). Elles permettent d'adresser régulièrement des informations ou des promotions et contribuent à la fidélisation des abonnés.

Macro : Petit programme qui permet l'exécution d'une série de commandes prédéfinies. On l'utilise pour automatiser les tâches répétitives dans les logiciels et notamment dans les applications Microsoft Office (Word, Excel, etc.).

Mailbombing : Attaque basique qui consiste à envoyer des centaines, des milliers voire des dizaines de milliers de messages appelés "mailbomb" à un

unique destinataire dans un but évidemment malveillant. Ce dernier va du simple encombrement de boîte aux lettres, avec possibilité de perte de données en cas de saturation de la capacité de stockage, jusqu'au crash machine ou déni de service.

Mailing-list : Voir **liste de diffusion**.

Malware : Contraction de "malicious software", le terme malware désigne les programmes spécifiquement conçus pour endommager ou entraver le fonctionnement normal d'un système, tels que les virus, les vers, les chevaux de Troie, ainsi que certains javascripts ou applets java hostiles. Cette famille ne doit pas être confondue avec les spywares, autre famille de logiciels dont le fonctionnement est également contestable mais dont le but premier n'est pas de nuire à l'intégrité d'un système.

Opt-in : Mécanisme par lequel un internaute sollicite de manière préalable l'envoi de messages, souvent publicitaires, provenant d'un expéditeur particulier.

Opt-out : Système sous lequel l'envoi d'E-Mails publicitaires est autorisé sans l'accord préalable du destinataire, mais en lui laissant, en théorie, la possibilité de s'opposer à de futurs envois.

Pollupostage : Voir **Spam**

Spyware : Programme ou un sous-programme conçu dans le but de collecter des données personnelles sur ses utilisateurs et de les envoyer à son concepteur ou à un tiers via internet ou tout autre réseau informatique, sans avoir obtenu au préalable une autorisation explicite et éclairée desdits utilisateurs.

Spam : Message publicitaire envoyé par E-Mail à de nombreuses personnes, sans que celles-ci n'aient au préalable donné leur accord.

Trojan ou Trojan horse : Voir **cheval de Troie**.

Unsolicited Commercial Email (UCE) : voir **spam**.

Ver : Un Ver est un programme indépendant, qui se copie d'ordinateur en ordinateur. La différence entre un ver et un virus est que le ver ne peut pas se greffer à un autre programme et donc l'infecter, il va simplement se copier via un réseau ou Internet, d'ordinateur en ordinateur. Ce type de réplique peut donc non seulement affecter un ordinateur, mais aussi dégrader les performances du réseau dans une entreprise. Comme un virus, ce ver peut contenir une action nuisible du type destruction de données ou envoi d'informations confidentielles.

Worm : Voir **Ver**

* Ce glossaire a été réalisé sur base des sources suivantes :

- Glossaire du FORUM TELECOM
- http://www.hp-expo.com/be/fire/products/glossary_c.html
- <http://www.commercial-database.fr/fr/glossaire>
- <http://www.cimbat.com/ressources/glossaire.html>
- http://www.emailingbooster.com/emarketing_glossaire.asp
- <http://aidaindustrie-demo.ineris.fr/glossaire/glossaire.htm>
- <http://www.secuser.com/glossaire>