

PAGE ANIMÉE PAR NACER AOUADI

SECURITE

Les attaques sur Internet

Je vous propose un tour d'horizon des principales attaques que vous pourrez subir sur Internet et les techniques pour les prévenir et s'en défendre... Virus, Bombmailing, Nuke et chevaux de Troie.

De nombreux internautes et entreprises sont connectés chaque jour à Internet et sont alors des cibles potentielles pour des personnes malfaisantes. La sécurisation de votre système est particulièrement importante. Elle permet de protéger votre ordinateur et vos données contre les différentes attaques qu'ils peuvent subir.

En effet, nul n'est à l'abri d'une intrusion indésirable ou d'un virus. Ces attaques se révèlent souvent dangereuses pour vos données et votre système.

Heureusement, les solutions existent. L'application de certaines règles de prudence et l'installation de logiciels pare-feux et d'antivirus, vous permettent de préserver votre système de ces attaques.

Cependant rien ne vous assurera une protection infaillible. Les virus évoluent vite, mutent parfois, devenant de plus en plus furtifs, de plus en plus pervers. Ils exploitent les failles du système, tout comme les chevaux de Troie.

Etre connecté à Internet vous rend vulnérable aux attaques directes (Nukes) et posséder une boîte aux lettres vous expose au Bombmailing.

LE BOMBMAILING

Cette attaque consiste à envoyer un très grand nombre de messages identiques (pouvant atteindre des milliers) dans votre boîte aux lettres électronique afin de saturer celle-ci.

En général, ces messages sont générés par un logiciel qui masque la véritable adresse de l'expéditeur. Il est donc difficile de remonter jusqu'à lui. L'auteur de ces messages est souvent quelqu'un rencontré sur un forum ou une connaissance qui cherche à vous nuire.

Si vous êtes connectés à Internet via un modem, le téléchargement de tous ces messages inutiles sera long et coûteux.

Si l'attaque est ponctuelle et ne se reproduit pas, inutile de chercher à connaître l'identité du mauvais plaisant.

Utilisez le freeware **Ermov** qui permet de ne télécharger que l'entête des messages qui vous ont été envoyés. Vous pouvez alors choisir les messages que vous souhaitez conserver et ceux que vous souhaitez supprimer.

Si l'attaque se reproduit fréquemment, il vous faudra alors employer un logiciel de filtrage d'email afin de rejeter les messages indésirables.

Le logiciel **SpamBuster** filtre les messages selon certains critères comme l'objet, l'entête, la taille ou l'expéditeur. Il vérifie par ailleurs si l'adresse de l'expéditeur est valide.

LES CHEVAUX DE TROIE

Le cheval de Troie (ou Trojan Horse) est un programme qui effectue certaines actions à votre insu comme ouvrir une porte dérobée, permettant alors à n'importe qui de prendre le contrôle de votre ordinateur. Il peut également collecter des informations comme les mots de passe.

Les premières versions des chevaux de Troie n'étaient que de petits exécutable, qui une fois lancés, affichaient des messages d'erreurs du type : "Un fichier DLL requis, XXXXX.DLL n'a pas été trouvé." La détection de ceux-ci était assez aisée. Mais les versions plus récentes des chevaux de Troie sont plus insidieuses car elles peuvent désormais être contenues dans un programme courant qui fonctionne parfaitement.

L'utilisateur ne soupçonne alors pas qu'il vient d'être infecté par un cheval de Troie.

La présence d'un cheval de Troie se traduit par une activité anormale de votre

ordinateur. Si lorsque vous êtes connecté à Internet, votre disque dur "travaille" alors que vous ne faites rien ou si des fenêtres s'ouvrent et se ferment sur votre bureau, il est fort probable que vous soyez infectés.

La meilleure solution consiste à ne pas télécharger de programmes à partir de sites douteux ou non officiels et ne pas ouvrir les pièces jointes des mails suspects. Mais si malgré tout, vous soupçonnez la présence d'un cheval de Troie sur votre disque dur, il est recommandé d'utiliser un programme de désinfection comme The Cleaner.

Il recherche la présence de chevaux de Troie sur les différents lecteurs et les supprime. Il peut également intercepter les chevaux de Troie avant qu'ils n'infectent votre système et l'endommagent.

Par ailleurs, l'utilisation d'un antivirus mis à jour régulièrement et d'un Firewall est fortement conseillée.

LES ATTAQUES DIRECTES (NUKE)

Les attaques directes se produisent uniquement lorsque votre ordinateur est connecté à Internet ou à un réseau local.

Ces attaques sont l'œuvre de gens souvent malintentionnés qui cherchent à s'introduire dans votre ordinateur. A la différence des chevaux de Troie, les attaques directes ne nécessitent pas qu'un programme soit installé sur la machine cible. L'adresse IP seule suffit. Elle peut facilement être récupérée sur un chat tel ICQ ou IRC.

Les utilisateurs bénéficiant d'une adresse IP fixe (type Câble ou ADSL) et qui sont connectés en permanence sont des cibles parfaites pour les Nukes.

Les attaques directes sont souvent destructives pour votre système car elles peuvent déclencher le redémarrage de votre ordinateur ou pire encore, le formatage de votre disque si l'attaquant utilise un logiciel de prise de contrôle.

Pour détecter une intrusion, il faut être vigilant. Elle se caractérise par un ralentissement de votre ordinateur et une activité anormale ou par l'apparition d'un écran bleu (du type erreur fatale).

Pour se défendre face à ce type d'attaque, il vous faut utiliser un Firewall mis à jour.

Vous pouvez également y adjoindre **NukeNabber 2.9** qui surveille les ports de votre ordinateur et redémarre la machine de l'intrus après avoir mémorisé son adresse IP.

Vous êtes alors en mesure de porter plainte auprès de son fournisseur d'accès en indiquant cette adresse IP et l'heure approximative de l'intrusion.

LES VIRUS

Un virus est un programme informatique introduit dans un système à l'insu de l'utilisateur. Le virus a pour mission première de se propager en infectant les cibles désignées par son concepteur. Après cette période d'incubation, il se manifeste de façon plus ou moins agressive. Les actions des virus sont très diverses. Cela peut aller de l'affichage d'un message humoristique accompagné d'une musique au formatage complet du disque dur.

Les virus sont une menace réelle. De petite taille et souvent furtifs, ils se propagent facilement via la messagerie électronique et tout ordinateur connecté à Internet devient une cible potentielle.

Les virus sont nombreux et de types différents (comme nous l'avons vu dans de précédents papiers) :

Virus de fichiers : ces virus se greffent sur une application en ajoutant leur code à celui des exécutables. Ils s'installent en mémoire centrale.

Virus compagnons : ces virus se contentent de copier un EXE et ajoute l'extension .COM à la copie infectée qu'ils placent dans le même répertoire. L'EXE lui, reste sain et on ne peut déceler dans celui-ci aucune trace du passage d'un virus. Lorsque l'EXE sera appelé, c'est la copie en .COM qui aura

priorité et donc qui sera lancée.

Virus d'amorce de disque : ces virus remplacent le code de l'amorce d'un disque par leur propre code. De là, ils peuvent contaminer d'autres lecteurs de la même manière. Ces virus sont moins nombreux mais très répandus car ils se propagent facilement.

Virus des tables de partition : assez semblables aux virus d'amorce de disque, ces virus se chargent dans les tables de partitions. Un formatage du disque ne modifie pas la table de partitions et ne supprime donc pas ce type de virus.

Virus furtifs : ce type de virus échappe à la plupart des moyens de détection en se camouflant. Il soustrait, en effet, sa longueur à la longueur du fichier infecté. La taille de celui-ci ne semble donc pas avoir été modifiée et il n'y a alors aucune raison de soupçonner que le fichier abrite un virus.

Virus polymorphes (ou mutants) : ces virus ont la capacité de modifier leur aspect à chaque nouvelle contamination d'un fichier. L'élimination de tels virus est ardue car ils sont présents sous différentes identités.

Virus piégés : ce type de virus associe deux virus : l'un connu et l'autre inconnu. L'utilisateur détecte le premier et le supprime pensant avoir écarté la menace. Le second virus se propage alors et infecte le système.

Rétrovirus : ces virus ont été conçus pour déjouer l'action d'un logiciel antivirus spécifique. Ils restent détectables par d'autres antivirus.

Les formats des fichiers infectés sont eux aussi variés. Ainsi les fichiers .EXE, .COM, .DLL, et .SYS peuvent être la cible des virus. Certains virus s'attaquent même aux fichiers de données .DOC créés par Word.

Les symptômes d'une infection virale ne sont pas toujours évidents. Le ralentissement général de l'ordinateur, les messages d'erreurs inattendus, le plantage de l'ordinateur, la modification de fichiers et en règle générale le comportement anormal de votre système, sont tout autant de signes d'infection.

La prévention reste la meilleure arme contre les virus. Ne téléchargez rien à partir de sites douteux et n'ouvrez en aucun cas les pièces jointes aux emails suspects ou avec une accroche grossière du genre : "Vous avez gagné un million... !"

Un bon antivirus mis à jour régulièrement reste la meilleure solution pour éradiquer les virus.

Il est également conseillé de mettre fréquemment son système d'exploitation à jour en téléchargeant les updates.

POUR VOS QUESTIONS :

Email: microsatdz@yahoo.fr

Fax: 038 86 61 76

Adresse: 19, rue du CNRA 23000, Annaba

News

UIF : le nouvel ultra-portable d'Asus

Asus a récemment annoncé l'UIF, une ordinateur ultra-portable de seulement 1 kg. Equipé d'un Core Duo basse consommation U2400 et d'un disque dur de 80 Go, l'UIF possèdera également, et c'est ici tout son intérêt, un écran à rétro éclairage par LED de 11,1 pouces (1 360 x 768). En plus d'offrir une meilleure luminosité, ce type de technologie permet d'avoir un écran plus fin et une consommation plus faible qu'un système classique. En contrepartie, le prix de ce type d'écran est deux fois plus élevé...

Les autres caractéristiques de cet ordinateur sont un chipset Intel 945GM Express, un adaptateur Wifi Intel PRO/Wireless 3945ABG, une webcam intégrée, un contrôleur Bluetooth 2.0, 4 ports USB 2.0, un port FireWire et un slot ExpressCard. Asus a également intégré au UIF un scanner d'empreinte digitale ainsi qu'un module TPM. Le graveur Blu-ray est en revanche externe. Pour arriver à 1 kg, Asus a certainement doté son UIF d'une petite batterie, ce qui se ressent sur l'autonomie annoncée à 2 heures. Cet Asus UIF devrait arriver en mars, mais le fabricant n'a pas encore indiqué de prix...

Attaque pirate massive en Corée, 92 000 PC infectés

La Corée du Sud vient d'être victime d'une attaque massive de pirates informatiques sur tout son territoire. Le bilan est lourd : 1000 sites web touchés, et 92 000 PC infectés. Les 1000 sites Internet attaqués ont été modifiés pour infecter le PC de leurs visiteurs à l'aide d'un virus inséré sur la page Web consultée. Les autorités du KISA (Korea Information Security Agency) estiment que ces sites ont infecté 92 000 ordinateurs dans le pays, avec un malware destiné à voler des données personnelles, et pas n'importe lesquelles... En effet, l'attaque a tout spécialement ciblé les Coréens adeptes de jeux en ligne, et le virus en question consistait à dérober comptes de jeu et mots de passe. L'attaque a pris une telle envergure que le KISA a publiquement averti les potentiels victimes, leur conseillant vivement de supprimer ce malware.

Les 1000 sites visés étaient presque tous des sites officiels d'éditeurs de jeux en ligne coréens. Il suffisait alors que le joueur se connecte au site infecté pour que le malware se transfère discrètement sur son PC. Les autorités affirment que 620 000 PC ont ainsi été exposés à l'attaque, qui utilisait une faille de sécurité de Windows. 92 000 de ces ordinateurs n'avaient pas Windows mis à jour correctement et sont maintenant infectés, selon les premières estimations. La police coréenne pense que l'attaque vient encore de pirates chinois, qui se sont fait une spécialité de s'attaquer aux données personnelles des internautes coréens.

Une faille hautement critique pour les produits Trend Micro

La société de sécurité iDefense Labs a découvert une faille de sécurité affectant une grande partie des logiciels de protection de Trend Micro, dans leurs versions Windows et Linux. La faille peut être utilisée pour provoquer un dépassement de mémoire tampon puis pour gagner le contrôle total du système et/ou des attaques par déni de service (DoS).

Parmi les produits touchés, on trouvera particulièrement :

Trend Micro's PC-Cillin Internet Security 2007

VsapiNL.sys (scan engine) version 3.320.0.1003

ServerProtect for Linux v2.5 on RHEL 4.x

vsapiapp version 8.310

La faille a également été publiée chez Secunia qui la recense comme hautement critique. La solution est assez simple car il suffit de lancer une mise à jour du logiciel si celle-ci n'est pas paramétrée pour être automatique.

Astuces...

Empêcher l'envoi d'informations à Microsoft

Lorsqu'Internet Explorer provoque une erreur système, il envoie à Microsoft des informations concernant cette erreur. Pour des raisons de confidentialité, vous ne souhaitez peut-être pas informer Microsoft de votre configuration logicielle et matérielle.

Pour cela, éditez la base des registres puis rendez-vous à la clé HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main. Si la valeur IEWatsonDisabled n'existe pas, créez-la.

Cliquez sur le menu Edition, sur Nouveau, Valeur DWORD. Nommez cette valeur IEWatsonDisabled. Double cliquez dessus, puis saisissez 0 dans le champ Données de la valeur. Fermez la base des registres pour valider les changements.

Fini les www. et .com

Sous Internet Explorer vous voulez aller sur <http://www.lesoiridalgérie.com> mais vous êtes fatigué de taper www. et .com!

Tapez juste [lesoiridalgérie](http://www.lesoiridalgérie.com) et au lieu d'appuyer sur la touche Entrée appuyez simultanément sur la touche Ctrl et sur la touche Entrée, le navigateur ajoutera automatiquement <http://www. et .com>

Utiliser Internet Explorer comme client FTP

En plus de visiter des sites Web, Internet Explorer permet également de faire du FTP. Il suffit simplement de taper l'adresse d'un site FTP sous la forme <ftp://ftp.nomdusite.com> dans la barre d'adresse puis de valider.

Si vous avez besoin d'entrer un nom et un mot de passe, cliquez sur le menu Fichier puis sur la commande Se connecter en tant que.

Une fois connecté, vous pouvez utiliser le glisser/déposer pour télécharger ou envoyer des fichiers.

Alléger Windows XP

Si votre configuration est un peu juste pour exploiter confortablement Windows XP, vous pouvez désactiver les effets de transitions des menus pour l'alléger.

Pour cela, cliquez avec le bouton droit de la souris sur le bureau puis cliquez sur Propriétés.

Dans la fenêtre de propriétés de l'affichage, cliquez sur l'onglet Apparence puis sur le bouton Effets. Décochez ensuite la case Utiliser l'effet de transition suivant pour les menus et les infos bulle. Validez par OK.