Virus GPS

Plus besoin de surfer sur Internet ou d'ouvrir un fichier attaché bizarre dans un mail pour être infectés par un virus. Risque potentiel concernant les appareils de navigation par satellite TomTom surtout le modèle GO 910 version 6.51 produits entre septembre et novembre 2006, .
Cet appareil a été vendu suite à une négligence de fabrication avec deux chevaux de Troie nommés selon Daniweb win32.Perlovga.A et TR/Drop.Small.qp.
Ces derniers se mettent à télécharger via Internet du code malicieux ce qui permet à un pirate de récupérer des données sur le PC de l'utilisateur.
Pas de rappel des appareils en cause pour supprimer ledit virus, il suffit de mettre à jour l'antivirus de votre ordinateur

Un Ver dans la Tempête

Attention au mail se rapportant à l'actualité car voici ce qui peut vous arrivé :
La tempête qui secoue le nord de l'Europe ne laisse pas indifférent les pirates qui profitent d'envoyer des mails sur la catastrophe avec une pièce jointe contenant le parasite "Storm Worm" (Ver de la tempête), le but de se ver c'est de s'installer dans le système d'exploitation et donner au pirate le contrôle total à l'ordinateur de sa victime
Ce qui rend ceci exceptionnel, c'est le caractère en temps réel de l'attaque"
En 2005, l'ouragan Katrina, qui a dévasté une bonne partie de la Louisianne, avait aussi fait l'objet de tels courriers contaminés. Une peste qui utilise décidément tout les moyens pour se répandre sur la Toile.

Cheval de Troie : Stom Worm

Ce mois-ci, une technique d'infection inédite est apparue : un parasite de type cheval de troie baptisé Storm Worm infecterait les commentaires sur les blogs,

Les internautes contaminés par ce cheval de troie verraient leurs commentaires postés en ligne, automatiquement affublés d'un lien vers un site Web malveillant.

Storm worm a frappé au mois de janvier en infectant les courriers électroniques (lire la rubrique du mois de Janvier)

Google Adwords utilisé par des virus

Des pirates ont utilisé les liens d'Adwords pour diffuser des virus en dirigeant les internautes vers des sites malveillants en vue de contaminer les PC vulnérables
La faille n'incombe pas la société Google avec ses liens commerciaux mais celle du système Windows avec les ActiveX si le système n'est pas mis à jour
Quid de la sécurisation des liens commerciaux de Google

Virus rançonneur : Gpcode

Un Ransomware (programme malicieux qui rançonne les utilisateurs) fait son apparition Win32.Gpcode.ai, ce programme crypterait les fichiers des ordinateurs infectés, devenant illisible.
Un fichier read_me.txt s'installe dans le système expliquant que les fichiers ont été cryptés, et moyennant l'achat de leur programme pour la somme de 300 dollars, ils pourront récupérer leurs fichiers
Ce parasite serait l'oeuvre d'une équipe de pirate au nom de Glamorous Team,
Ce type de rançonnage n'est pas nouveau, le premier cas est apparu en 1989, ensuite en 2005 avec PGPcoder puis 2006 avec Cryzip

Attention deux parasites circulent sur le Net

- Le ver RegisteredLetter.A utilise le carnet d'adresse pour envoyer un mail contenant un lien qui redirigera l'internaute vers un site mal intentionné pour installer une copie du ver
Ce vers peut causer des dégâts sur votre machine

- ZLFake.A est un cheval de Troie qui s'installe sur votre PC et s'exécute toutes les heures mais sa subtilité c'est qu'il ne reste actif qu'une minute

Parasitage des messageries Gmail et Hotmail

Après les comptes de Yahoo, voici que les messageries Hotmail et Gmail se font exploiter par un cheval de Troie(Trojan.Spammer.HotLan), dont le rôle est de générer et d'utiliser des comptes de messageries dans le but d'envoyer des spams
La diffusion de ce parasite reste relativement rare, mais par précaution faite une analyse de votre ordinateur

Mélodie dans le monde des virus

Des experts en sécurité ont découvert le virus W32.deletemusic, ou W32/deleteMP3.worm
Son effet consiste à détruire les fichiers MP3 sous système Windows
Ce virus crée plusieurs fichiers exécutables et se duplique sur tous les disques de la machine, y compris sur les périphériques amovibles connectés : clé USB, disque dur externe.
Il se met en action dès que l'utilisateur accède à un disque puis à chaque fois qu'il démarre Windows : descriptif fait par Symantec sur son site Internet
Malgré sa faible dangerosité, il est recommandé de se protéger en mettant à jour son antivirus

Alerte imminente de tempête avec Storm

Depuis Janvier sévit sur le net, un parasite de type vers au nom de Storm
Comme d'habitude, cette technique utilise les mails pour infecter les ordinateurs, jusqu'à présent Storm aurait infectés environ un millions de PC, il les utiliseraient comme "PC Zombies"
D'où l'inquiétude des sociétés en sécurité informatique, qui anticipe sur l'étendue du phénomène face aux dégâts que pourrait causer Storm
La solution face à cet ouragan, reste la prudence face aux pièces jointes, aux liens ou sites web douteux

Faille dans Norton

L'éditeur Symantec a publier un correctif en vue de colmater une faille dans ses logiciels de sécurité grand public édition 2006 :
antivirus Norton, Norton Internet Security, Norton System Works, mais aussi le logiciel antiespiogiciel de Symantec
La faille détectée se situait dans un composant ActiveX, si elle était exploitée par un pirate, ce dernier pourrait prendre à distance le contrôle de l'ordinateur
Pour installer le correctif, utilisez l'outil de mise à jour automatique Live update.

Septembre

Les portables Médion victime d'un virus

Des ordinateurs portables Médion (MD 96290), vendu par le hard discount ALDI en Allemagne et au Danemark seraient infectés par le virus Stoned.Angelina, le paradoxe c'est que ce virus de boot date tous de même de 1994
Ces portables sont vendus avec le dernier système d'exploitation Windows Vista et de l'anti-virus Bullguard, ce dernier averti l'utilisateur de la présence du virus mais il est incapable de le supprimer
L'éditeur Bullguard propose un outil de désinfection pour supprimer ce virus

Un virus piège un anti-virus

Alerte de l'éditeur Spamfighter car un malware tente de se faire passer pour le logiciel antiviral : VirusFighter.
Si vous êtes infecté un pop-up apparaît pour prévenir les utilisateurs de la présence d'un virus et moyennant rémunération ce virus sera éliminé.
En réalité, il s'agit de Malware.AMCC qui se fait passer pour Virusfighter via des éléments graphiques copiés sur le site Web officiel, afin d'induire en erreur les victimes.
Spamfighter met donc en garde les internautes contre ce type d'arnaque.
Le logiciel Virusfighter peut-être téléchargé et acheté directement depuis le site légitime

Une banque en déroute

La banque indienne Bank of India fut victime d'acte de pirates informatiques
Ces derniers ont utilisés du code malicieux pour que les clients de la banque puissent télécharger et installer sur leurs machines un cheval de Troie
Du coup la banque a du stopper le site pendant quelques jours
Bonne nouvelle pour les clients, selon un communiqué aucune information bancaire n'aurait été affectée

Google secoué par la tempête

Revoilà le ver Storm, accompagné de ses variantes, qui s'attaque au blog vidéo de Google
Une des variante est transmise par e-mail
Pour mieux attirer l'internaute, le sujet du mail incite à regarder des vidéos people Américaines
Une fois installé le virus télécharge d'autres parasites

Un ver au bout de la ligne (téléphonique)

Le ver au nom de W32/Ramex.a - W32/Skipi.A. ou W32.Pykspa.D, selon les éditeurs d'antivirus, infecte le logiciel de téléphonie Skype
A partir de la messagerie instantanée, l'internaute peut recevoir un message contenant un lien, si ce dernier clique dessus, une fenêtre Windows s'ouvre pour enregistrer un fichier image .jpg ou .scr (extension des économiseurs d'écran) ces derniers contiennent un fichier exécutable qui va installer le parasite
Une fois sur votre machine, le parasite enverra un message instantané à d'autres contacts de Skype pour les contaminer
Si vous utilisez Skype, mettez à jour votre anti-virus puis faites une analyse de votre ordinateur
Ce parasite fait suite à un cas précédent au mois d'avril : «Pykse.A»

Des bannières publicitaires infectées

Les sites communautaires, du type MySpace, Bebo, seraient touchés par un cheval de Troie : le trojan Downloader.VBS.Agent.n
Ce parasite se cacherait dans des bannières de publicité, en provenance du réseau publicitaire Right Media Online, infectées par ce parasite.
Ce trojan est considéré par les experts comme dangereux car l'infection se déclenche sans interaction au préalable.