Rapport F-Secure sur la sécurité informatique – Janvier à juin 2006

Les six premiers mois de l'année 2006 semblaient calmes en apparence. Toutefois, il régnait une grande activité de développement de logiciels malicieux et d'attaques criminelles, malgré l'attention moindre des médias. Les nouvelles menaces étaient souvent plus ciblées et bien mieux cachées, et les criminels réussissent toujours à trouver de nouvelles façons de placer leurs logiciels derrière les lignes de défense.

Le début de l'année 2006 marquait également le 20ème anniversaire du premier virus sur PC, Brain, qui infectait les ordinateurs par disquette. Les choses ont bien changé depuis, comme le démontre ce rapport.

Lisez ce qui suit

Il existe actuellement plus de 185 000 virus, et ce nombre continue d'augmenter rapidement. Le plus gros changement durant ces 20 dernières années ne réside pas dans le type de virus ou la quantité de logiciels malicieux, mais plutôt dans la motivation des programmeurs de virus. Le changement le plus notable est le passage du stade de la programmation d'un virus par hobby au stade de l'activité mafieuse pour détourner de l'argent. Cette tendance se poursuit avec les nouveaux logiciels malicieux qui transforment les ordinateurs infectés en automates d'émission de spam ou de message d'hameçonnage (phishing),ou bien qui subtilisent des données financières et personnelles.

En mars 2005, F-Secure a lancé son moteur d'analyse Blacklight pour détecter les rootkits. Les rootkits sont des mécanismes de masquage, qui permettent à des auteurs de logiciels malicieux de s'introduire sur un ordinateur et de faire ce pourquoi ils sont programmés, sans être détectés. Depuis cette date, nous avons constaté un nombre grandissant de logiciels malicieux utilisant la technologie des rootkits pour se cacher. Il est intéressant de noter que la plupart des éditeurs de logiciels de sécurisation des données ne proposent pas encore de logiciels de détection des rootkits, même après que l'affaire du rootkit de Sony ait fait la une des journaux. Les enjeux deviennent importants : en mai 2006, une porte dérobée utilisant la technologie des rootkits a été découverte dans un utilitaire de calculs de gains téléchargeable sur un site de poker en ligne, dont le but était de glaner des informations sur les joueurs. Heureusement, elle a été détectée par le moteur Blacklight et a été neutralisée avec succès.

Par ailleurs, 2006 est l'année qui a vu le nombre de logiciels malicieux sur téléphones mobiles atteindre et dépasser la barre des 200. Si vous replacez ce nombre dans le contexte des PC, il n'est pas encore alarmant mais indique clairement une tendance à la hausse. Les téléphones mobiles devenant de véritables ordinateurs offrant la possibilité d'effectuer des transactions financières, la communauté des programmeurs de logiciels malicieux s'y intéresse de près.

Un début d'année mouvementé

2006 a débuté de manière très mouvementée, avec un zero-day exploit découvert l'année précédente dans le moteur de rendu de Windows chargé de traiter les images au format WMF. En seulement quelques jours, un grand nombre de fichiers utilisant l'exploit ont été découverts, sans qu'un correctif soit édité. Ilfak Guilfanov de DataRescue a été le premier à créer un correctif temporaire pour contrer cette vulnérabilité. Microsoft a changé ses habitudes de ne fournir des mises à jour qu'une fois par mois en livrant une mise à jour spéciale le 5 janvier. Un des incidents dont nous avons pu être témoins était une attaque très ciblée sur le parlement anglais. Des courriers électroniques tels que celui-ci-dessous ont été envoyés depuis un ordinateur sud-coréen à quelques douzaines de personnalités du monde de la politique.

Date: Mon, 02 Jan 2006 13:48:32 +0200
From: tommy@security.state.gov
Subject: Confidential

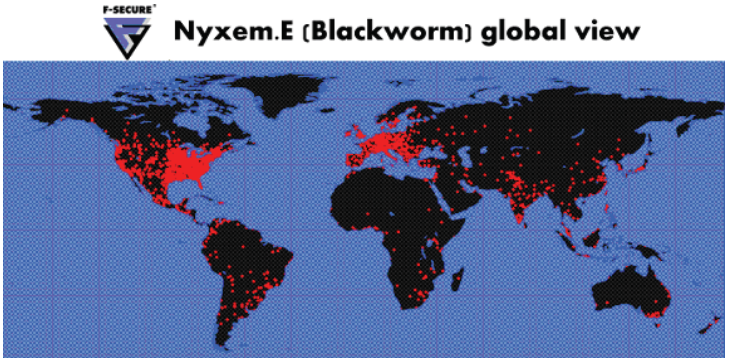
Attached is the digital map for you. You should meet that man at those points seperately. Delete the map thereafter. Good luck.

Tommy

map.wmf

Les messages invitaient les destinataires à ouvrir le ficher MAP.WMF joint qui exploitait la faille et installait une porte dérobée permettant un accès total à toutes les données situées sur leur machine. C'est surtout le texte d'ingénierie sociale utilisé dans ces messages qui rendait ce cas intéressant. Il était rédigé sur un ton mystérieux pour ressembler à un message tiré d'un film d'espionnage, et susciter la curiosité des destinataires pour leur faire ouvrir la pièce-jointe.

Le mois de janvier a continué de débordé d'activité avec l'apparition d'un nouveau ver de messagerie le 17, se propageant de manière agressive. Appelé Nyxem.E (avec des surnoms tels que MyWife, Blackworm et Blackmal), ce nouveau ver est intéressant pour deux raisons : il utilise un compteur web pour mesurer le nombre d'ordinateurs infectés et est programmé pour effacer des fichiers à une date précise de chaque mois. En ces temps de cybercriminalité, il n'est plus très courant de voir des charges destructrices telles que celle-ci. L'utilisation d'un compteur web est un aspect intéressant de ce logiciel malicieux. Il n'est pas le premier à utiliser un compteur web, mais nous avons pu cette fois-ci obtenir les statistiques de la part de son éditeur pour faire le compte des adresses IP qui ont rendu visite au compteur. Nous avons placé les adresses IP sur une carte mondiale à l'aide de notre technologie « Worldmap » pour montrer l'emplacement des machines touchées.



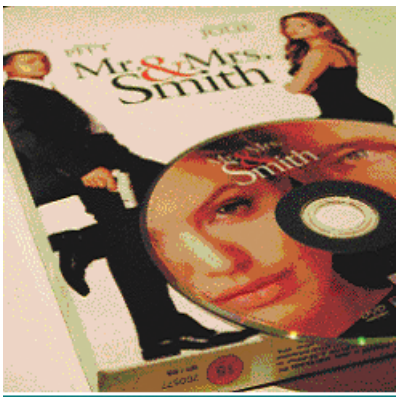
Les pays les plus infectés étaient l'Inde, le Pérou, la Turquie et l'Italie. Heureusement, au moment de l'activation du logiciel malicieux le 3 février, la plupart des utilisateurs avaient déjà nettoyé leur machine, grâce aux alertes publiées dans les médias. Toutefois, des milliers d'utilisateurs ont vu leurs documents Word et Excel réécrits. Un total de 11 formats de fichiers était pris en charge par le ver. Nyxem.E est actif le 3 de chaque mois et continue de réécrire les fichiers des machines infectées. La plupart des machines encore infectées se situent actuellement en Inde.

Virus Macintosh

Les macintosh ne sont désormais plus à l'abri En février, le premier virus sur Mac OSX a été découvert avec l'apparition de Leap.A. Ce logiciel malicieux a été posté à l'origine sur le forum de discussion MacRumors. Se propageant via iChat et infectant les fichiers locaux, le virus a été rapidement suivi par d'autres virus sur la même plate-forme, dont OSX/Inqtana.A qui utilise une vulnérabilité dans la fonctionnalité Bluetooth OBEX Push pour se propager.

Les rootkits restent un problème

Un des problèmes majeurs en 2005 était le cas du rootkit de Sony. Certains CD commercialisés contenaient un mécanisme de protection contre la copie utilisant la technologie des rootkits pour masquer sa présence. Les rootkits continuent d'être un problème au premier trimestre 2006 : de nombreux nouveaux logiciels malicieux utilisent la technologie des rootkits pour masquer les fichiers installés. Par exemple, des variantes du ver Feebs masquent leur présence à l'aide de rootkits. Elles se propagent via des pièces-jointes de courriers électroniques, mais au lieu de générer les messages, attendent que l'utilisateur envoie un courrier pour joindre automatiquement une pièce-jointe sans que l'utilisateur le sache. L'intérêt de cette méthode est que le message semble légitime puisqu'il l'est en réalité ! Le taux de propagation est toutefois bien inférieur à celui des autres vers de messagerie. En février, nous avons reçu des rapports de cas similaires au rootkit Sony BMG. La version allemande du DVD du film « M. et Mme Smith » contenait un mécanisme de protection contre la copie utilisant la technologie rootkit.



Le système de protection Settec Alpha-DISC utilisé sur le DVD masque son processus, mais heureusement, à l'inverse du rootkit de Sony BMG, ne masque pas les fichiers ou les clés de la base de registre, ce qui empêche l'utilisation de ce rootkit pour masquer des fichiers malicieux.

Notre message à l'intention des sociétés produisant des logiciels (pas seulement les produits de protection contre la copie) est clair. Vous devriez toujours éviter de cacher quoi que ce soit aux utilisateurs, en particulier aux administrateurs. Cela n'aide en rien les utilisateurs, et dans de nombreux cas facilite le travail des pirates pour s'introduire dans les systèmes.

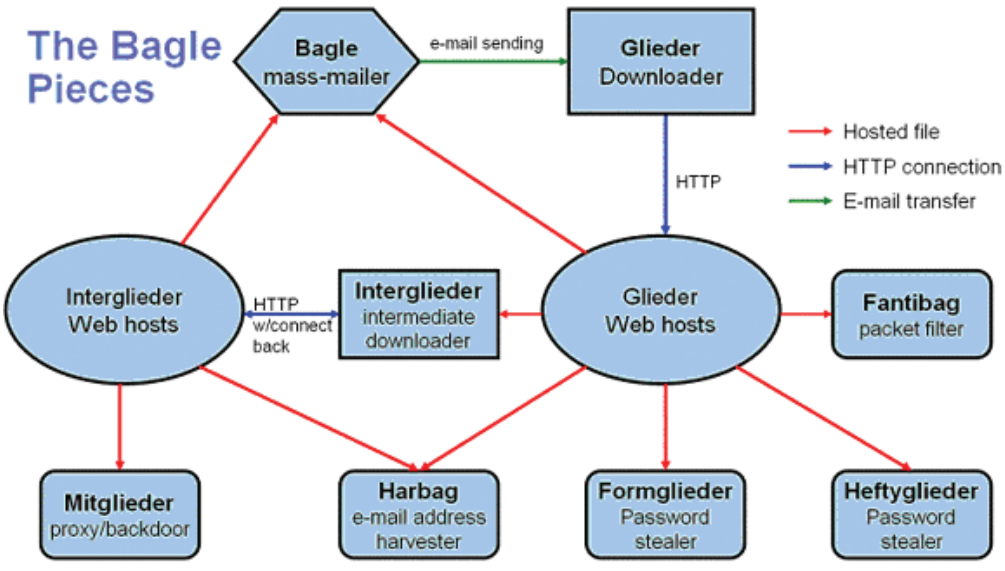
Deux des vers les plus répandus utilisant auparavant des automates clients disposent désormais de rootkits. En mars, des variantes de Bagle et Mydoom utilisant la technologie des rootkits pour masquer leurs fichiers, leurs processus et leurs clés de base de registre, ont été découvertes. Les variantes de Bagle sont les plus intéressantes de par leur démonstration de l'évolution d'un virus et de la collaboration entre les auteurs de virus. Deux ans auparavant, Bagle était un simple virus composé d'un fichier EXE qui se propageait par courrier électronique. Ce n'est plus le cas. Les auteurs de Bagle maintiennent un réseau complexe et ont développé un ensemble de programmes qui fonctionnent ensemble, comme l'illustre le schéma ci-dessous.

La technique de rootkits utilisée est appelée rootkit en mode noyau, ce qui signifie qu'elle permet l'accès direct à toutes les fonctions du système, rendant sa détection encore plus difficile. Si les auteurs de Bagle ont sérieusement décidé de mettre à jour leur logiciel malicieux en y intégrant un rootkit, cela signifie que cette première étape est à surveiller de près. Heureusement, F-Secure Blacklight, le moteur d'analyse et de suppression des rootkits, est capable de détecter ces menaces.

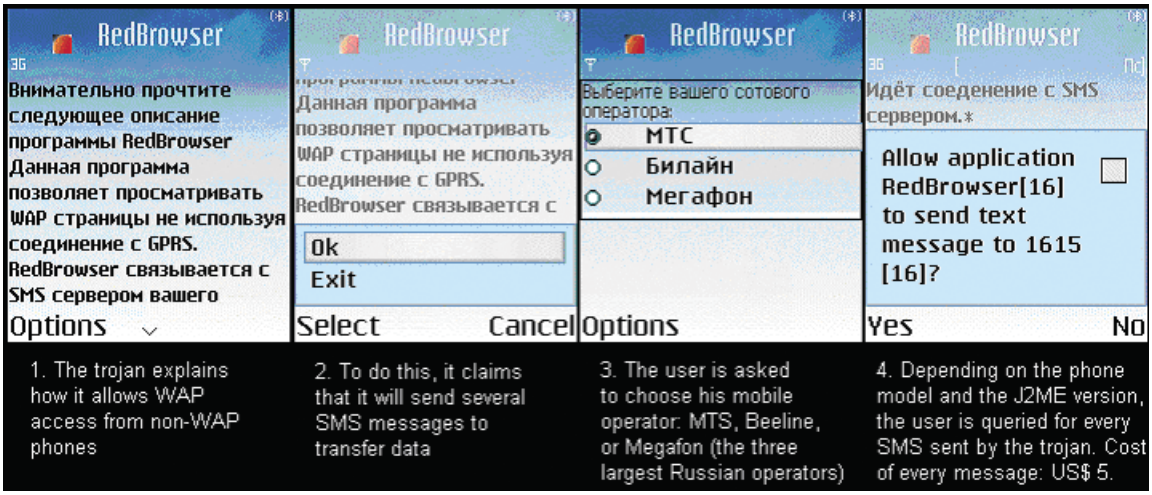
A la mi-mai, nous avons constaté une nouvelle manière d'utiliser les rootkits. Une porte dérobée, stockant des informations sur des joueurs pour éventuellement les escroquer, a été découverte par Blacklight, la technologie de détection de rootkits de F-Secure. L'outil RBCalc.exe, un calculateur de gains, a été distribué par le site de poker en ligne Checkraised.com.

La porte dérobée, une méthode permettant de s'introduire illégalement sur un ordinateur à distance, a été ouverte par l'installation silencieuse de quatre exécutables dans l'ordinateur des utilisateurs à l'aide d'un rootkit pour masquer l'opération. L'auteur de l'outil pouvait accéder aux informations d'accès à différents sites de poker en ligne stockées sur l'ordinateur des utilisateurs. Une fois l'accès aux sites obtenu, le pirate pouvait jouer au poker contre lui-même et faire exprès de perdre pour empocher les gains.

Peu de temps après la découverte, Checkraised.com a retiré le fichier de son site et a publié une déclaration invitant les utilisateurs à changer leurs mots de passe d'accès aux sites de poker, et contenant des instructions pour retirer manuellement le logiciel malicieux.



Picture by Scott Molenkamp & Hamish O'Dea / CA



Logiciels malicieux sur téléphones mobiles

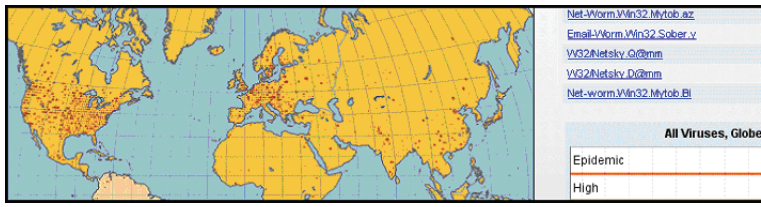
Ils existent depuis juin 2004 et les dommages qu'ils causent sont limités. Le premier logiciel malicieux Java ou J2ME a été découvert en février avec l'apparition du cheval de Troie Redbrowser. Ce cheval de Troie tente de dérober de l'argent en prétendant pouvoir utiliser gratuitement des services WAP, mais envoie un texto surtaxé à un numéro en Russie, ce qui coûte environ 4 euros à l'utilisateur par message. L'utilisation de Redbrowser est heureusement limitée par sa langue, le russe. Nous nous attendons toutefois à voir de futures attaques similaires conduites dans d'autres langues.

En mars 2006, le premier spyware sur téléphone mobile a été découvert : Flexispy. Avec cette application commerciale, le client se connecte à un portail par lequel le logiciel surveille tous les appels et les textos, et les poste sur le portail. Le logiciel est commercialisé à l'attention des épouses et des maris suspicieux pour surveiller les activités de leur conjoint. Pour ceux qui ont un logiciel de sécurisation installé, le logiciel ne fonctionne pas. F-Secure Mobile Anti-Virus détecte et supprime les spywares lorsqu'ils s'installent sans que leur fonctionnalité soit clairement indiquée.

Toujours en mars, le nombre de logiciels malicieux sur téléphone mobile à atteint puis dépassé la barre des 200.

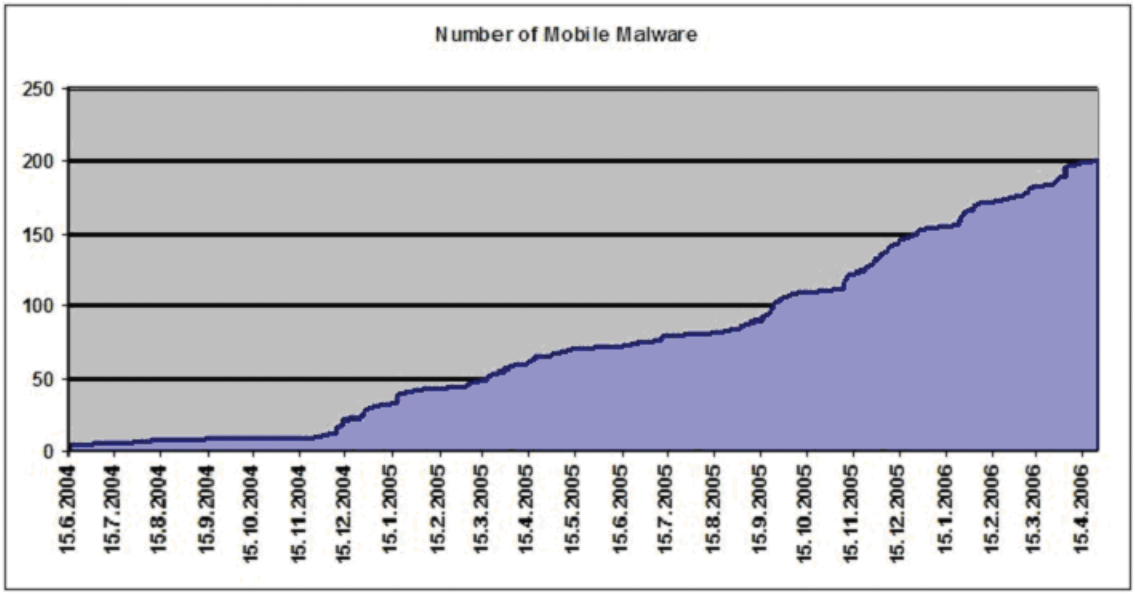
Lancement de F-Secure Worldmap

F-Secure Worldmap est un système utilisé par le laboratoire de recherche F-Secure pour surveiller les épidémies virales en temps réel dans le monde entier. Le système peut également être utilisé pour visualiser des événements passés, par exemple pour comparer une nouvelle épidémie avec une ancienne et déterminer le niveau d'alerte à communiquer à la presse et à d'autres organismes. Une version publique de l'outil a été lancée en mars sur notre site web, pour que chacun puisse voir la propagation des virus dans le monde entier. Les visiteurs peuvent facilement visualiser la situation des virus à n'importe quel moment et à n'importe quel endroit.



L'hameçonnage est populaire

F-Secure a recherché parmi les domaines com/net/org/us/biz/info des noms de banques et autres organismes financiers. Les résultats montrent que certains noms correspondent bien aux organismes légitimes, mais que la plupart existent pour tenter de détourner l'argent des utilisateurs.



Mot clé	Nombre de domaines
citibank*	497
bankofamerica*	407
lloyds*	994
bnpparibas*	41
egold*	691
hsbc*	1258
chase*	6470
paypal*	1634
ebay*	8057

Malheureusement, l'hameçonnage fonctionne. Dans une étude récente examinant les techniques d'hameçonnage, il ressort que les sites les plus réussis sont capables de tromper 90% des participants. Ce chiffre inclus des utilisateurs expérimentés parmi les participants. Il s'avère que c'est l'aspect et non la méthode d'hameçonnage qui présente les meilleurs résultats. Pour résumer cet article publié l'année dernière dans le magazine Neuron : si vous ne voyez pas régulièrement quelque chose, vous ne le verrez pas souvent. Vous pourriez également dire : si vous ne voyez pas régulièrement des faux, alors vous ne verrez pas souvent de faux. De ce fait, de nombreux pirates qui conçoivent des sites d'hameçonnage ressemblants comptent moins sur les subterfuges techniques que sur les défauts de perception du cerveau humain. Si cela ressemble à ce que le cerveau attend, alors le cerveau ne voit pas ce que cela n'est pas.

Nos experts se demandent pourquoi les banques ne permettent pas à leurs utilisateurs de personnaliser leur interface client avec une photo ou des préférences, par exemple une photo d'identité, la photo d'un animal domestique ou d'un autre membre de la famille, quelque chose qui indiquerait l'authenticité et qui viendrait à manquer si cet élément n'y était pas. Des entreprises travaillent actuellement sur des technologies de personnalisation visuelle, et les chercheurs de F-Secure pensent c'est une idée pouvant réduire de manière significative les tentatives d'hameçonnage.

Ce n'est pas un poisson d'avril

Le premier avril est traditionnellement le jour de l'année où il ne faut pas croire tout ce que l'on entend. Pour cette raison, un nombre étonnant de gens ont pensé que notre nouveau produit de sécurisation Internet Security 2006, revêtant l'interface Moomin, était un poisson d'avril, ce qui est normal quand on fait des annonces un jour pareil !

Le produit est pourtant bien réel et sera disponible en Europe plus tard cette année. Il est déjà en vente au Japon pour une bonne raison. La popularité et le succès de Moomin a considérablement augmenté au Japon dans les années 90 lorsqu'un studio de production japonais a réalisé une série animée.

Vols de voitures

Les voleurs de voitures n'ont aujourd'hui plus besoin de pieds de biche ou de portemanteaux pour subtiliser des véhicules : ils utilisent leur portable. Si votre voiture utilise un système de démarrage sans clé de contact avec un chiffrage sur 40 octets, vous pourriez bien voir votre voiture disparaître en moins d'une minute.

Robert Vamosi a rédigé un article sur les systèmes de démarrage sans clé de contact, basé sur une étude menée par l'université John Hopkins et RSA. Vamosi a noté en conclusion que les fabricants de systèmes RFID ne semblent pas penser qu'il existe un problème. Ils devraient s'inspirer de David Beckham, à qui on a volé sa BMW X5 en Espagne par cette méthode. Jusqu'à ce que la situation change, notre avis si vous disposez d'un tel système de démarrage est de recouvrir l'émetteur de papier d'aluminium. L'article est intéressant et vous pouvez le lire à l'adresse http://reviews.cnet.com/4520-3513_7-6516433.html?tag=txt.

Déboires de Word

Fin mai, une vulnérabilité zero-day de Word a fait couler beaucoup d'encre. Selon plusieurs sources, une société américaine a été la cible de messages électroniques envoyés depuis l'extérieur mais qui semblaient provenir de l'intérieur.

Les messages contenaient un fichier Word en pièce-jointe. Une fois lancé, le fichier ouvrait une porte dérobée masquée par un rootkit, permettant un accès sans restriction aux pirates qui opéraient depuis un hôte enregistré sous le domaine chinois 3322.org.

Les fichiers DOC sont un dangereux vecteur d'attaque pour plusieurs raisons. Quelques années auparavant, lorsque les virus de macro étaient le problème numéro un, de nombreuses entreprises bloquaient les fichiers DOC au niveau de leurs passerelles de messagerie. Aujourd'hui, les fichiers DOC sont généralement admis. La plus importante raison est que Word a des vulnérabilités et que les utilisateurs n'installent typiquement pas les correctifs Word aussi souvent que ceux de Windows. 3322.org est un service gratuit de redirection pour la Chine. N'importe qui peut enregistrer un hôte avec 3322.org et le service pointera l'hôte sur l'adresse IP spécifiée. Il existe plusieurs services de ce type, dont 8866.org, 2288.org, 6600.org, 8800.org et 9966.org. Si vous avez des doutes sur l'origine d'un fichier Word arrivant dans votre boîte de messagerie, nous vous recommandons de vérifier le journal de la passerelle de votre entreprise pour voir si des contacts ont eu lieux avec ce type de service.

Virus Da Vinci sur téléphones mobiles - vérité ou fiction ?

En fin mai également, une rumeur provenant d'une publication indienne en ligne a provoqué des remous à propos d'un nouveau virus sur téléphone mobile, appelé « Da Vinci » pour profiter apparemment de l'engouement lié à la sortie du film Da Vinci Code.

Le laboratoire F-Secure n'a reçu ni rapport d'infection ni exemplaire du virus. Est-ce un mythe ou une réalité ? Le temps nous le dira… L'article qui a débuté la rumeur est disponible à l'adresse http://ww1.mid-day.com/news/city/2006/may/137895.htm

Coupe du monde ou jeu personnel ?

Les fans de football allemands pourraient bien déchanter s'ils répondent à un ver de messagerie appelé Banwarum (ou encore Zasran et Ranchneg) qui utilise des messages sur le thème de la coupe du monde.

Le ver s'envoie sous forme d'archive protégée par mot de passe et inclut le mot de passe dans le message. Les messages sont envoyés en allemand et certains proposent des billets pour les matchs de football en Allemagne pour le mois de juin. Il existe déjà trois variantes similaires de ce ver. FSAV détecte les variantes .A et .B avec la mise à jour numéro 2006-05-24, et la variante .C avec la version numéro 2006-05-25_01. Un des messages envoyés pourrait se traduire comme suit :

« Salut,

J'ai vu que tu voulais participer à la Coupe du monde. Ne me demande pas qui je suis et pourquoi je le fais. Voici 5 billets. Ce sont des versions électroniques spéciales, imprime-les et signe-les. Le mot de passe de l'archive est : mot de passe

Amicalement,

Personne ;-) »

Nous recommandons à tous les fans de football de rechercher des informations sur la Coupe du monde et les billets sur le site officiel de la FIFA.

Statistiques sur les virus pour le premier semestre 2006

Top 10 des virus classés par F-Secure Worldmap :

1.	Email-Worm.Win32.Nyxem.e	17,3 %
2.	Net-Worm.Win32.Mytob.x	11,2 %
3.	Email-Worm.Win32.NetSky.q	11,2 %
4.	Net-Worm.Win32.Mytob.az	11 %
5.	Email-Worm.Win32.Sober.y	5,7 %
6.	Email-Worm.Win32.Bagle.fj	4,3 %
7.	Email-Worm.Win32.Mydoom.m	3,3 %
8.	Email-Worm.Win32.Doombot.g	2,4 %
9.	Net-Worm.Win32.Mytob.c	2,2 %
10.	Net-Worm.Win32.Mytob.bi	2,2 %

En juin 2006, tous justes 20 ans après la détection de Brain, le premier virus, on dénombre plus de 185 000 virus.

Auteurs : Patrik Runald, Spécialiste sécurité senior, et Mark Woods, Responsable communication.