Vous Propose ce dossier spécial Mimail,

Le virus qui vole les mots de passe et identifiants d'Internet

La menace Mimail se propage sur Internet :

Ce virus-ver dans sa version c, déguisé en un email de photos de plage, s'installe sur les PC dotés de systèmes Windows puis s'empare des mots de passe et identifiants enregistrés par le navigateur de Microsoft.

Les éditeurs de logiciels antivirus alertent leurs clients sur la dangereuse propagation, un virus-ver qui se fait passer pour un message soi-disant illustré de photos de plages "privées". Il a déjà pris pour cible plusieurs dizaines de machines dans le monde; une forte contamination est attendue en novembre et décembre 2003 ainsi que janvier 2004.

Baptisé "Mimail.c" ("W32.Mimail.c@mm", ou encore "W32.Bics.A" et "I-Worm.WatchNet"), il infecte les ordinateurs qui fonctionnent avec le système d'exploitation Windows (95, 98, ME, NT, 2000, Server 2003 et XP). Les Macintosh et les PC sous GNU/Linux ne sont donc pas concernés. ZDNet lui attribue un indice de dangerosité de 6 sur une échelle de 10.

Ce virus n'est pas inconnu puisqu'il s'agit de la troisième et la plus dangereuse variante du ver Mimail.a, découvert en août dernier. Il se propage sous la forme d'un e-mail facilement reconnaissable car son objet, en anglais, est : "**Re[2]: our private photos ???**", suivi de lettres aléatoires. Il est accompagné d'un message d'un certain James, indiquant que des photos de plages "déshabillées" sont fournies en pièce jointe.

Bien entendu, cliquer sur le fichier joint, compressé au format .Zip, libère le virus et déclanche l'infection. Sans l'ouverture de cette pièce jointe, l'email reste inoffensif; il suffit donc de le supprimer pour s'en protéger.

Les actions de ce virus :

En revanche une fois activé, Mimail.c scanne tout le système à la recherche de fichiers contenant des adresses électroniques, vers lesquelles il va se renvoyer via son propre moteur SMTP. Comme tout "mass-mailer", le premier effet de ce ver est donc de ralentir, voire saturer les réseaux.

Il se duplique également dans les fichiers de démarrage du système afin d'être lancé chaque fois que l'ordinateur est allumé. Mimail.c va, par ailleurs, tenter de voler les informations personnelles que l'utilisateur a demandé à Internet Explorer de retenir. Il cherchera à obtenir mots de passe et identifiants qu'il va transmettra à plusieurs adresses Internet, présumées sous le contrôle de l'auteur du virus. Il détruit ensuite le fichier contenant ces données.

En effet, Le virus s'enregistre sous le nom "newtach.exe", s'envoie à toutes les adresses récupérées dans différents fichiers et fait office de keylogger, c'est-à-dire un enregistreur de touches tapées au clavier qui les envoie ensuite à son créateur.

Les Nouveautés de ce virus :

Après la version C proposant des photos soit disant indiscrètes et la version I armée d'une fausse interface de mise à jour de données Paypal (filiale d'eBay offrant un système de paiement en ligne), Mimail J continue dans la voie.

Mais son impact semble cette fois-ci bien supérieur à celui de son prédécesseur. Selon MessageLabs, quelque 35 000 utilisateurs auraient été touchés dans la seule journée de 18 novembre (la version I n'a, même à son paroxysme, jamais dépassé les 5 200 victimes par jour

Enfin, ce virus lance également une attaque par saturation de type refus de service (DoS, Denial of Service) à l'encontre de quatre sites Internet américains: darkprofits.com, darkprofits.net, darkprofits.com et darkprofits.net. Il s'agit de sites humoristiques, très sarcastiques à l'encontre des "spammeurs" et des "hackers".

Concrètement, chaque PC contaminé envoie des paquets de données aux serveurs hébergeant ces sites afin de les rendre inopérants. Cela semble fonctionner puisque lundi 3 novembre, aucun de ces sites n'était accessible. Les éditeurs de logiciels antivirus recommandent à leurs clients de mettre à jour leur programme; des additifs sont d'ores et déjà disponibles.

Aucune procédure d'éradication manuelle n'a pour l'instant été communiquée, mais Symantec fournit des petits utilitaires à télécharger qui permet de supprimer Mimail du système.

Pour Arrêter les effets du virus Mimail, veuillez cliquez sur le lien ci-dessous :

http://www.symantec.com/avcenter/FxMimail.exe

N'oubliez pas par la suite de mettre à jour votre Anti-Virus et faire un nettoyage complet de votre disque dur et de tous les supports magnétiques (clé USB, Disquettes, etc…)

Les actions préventives contre les infections Mimail : Toutes le variantes de W32.Mimail

Variante A :
http://securityresponse1.symantec.com/sarc/sarc-intl.nsf/html/fr-w32.mimail.a@mm.html

Variante C :
http://securityresponse1.symantec.com/sarc/sarc-intl.nsf/html/fr-w32.mimail.c@mm.html

Variante D :
http://securityresponse1.symantec.com/sarc/sarc-intl.nsf/html/fr-w32.mimail.d@mm.html

Variante E :
http://securityresponse.symantec.com/avcenter/venc/data/w32.mimail.e@mm.html

Variante F :
http://securityresponse.symantec.com/avcenter/venc/data/w32.mimail.f@mm.html

Variante G :
http://securityresponse.symantec.com/avcenter/venc/data/w32.mimail.g@mm.html

Variante I :
http://securityresponse.symantec.com/avcenter/venc/data/w32.mimail.i@mm.html

Variante J :
http://securityresponse1.symantec.com/sarc/sarc-intl.nsf/html/fr-w32.mimail.j@mm.html

Pour accéder à ces liens veuillez les copiés dans la barre d'adresses de votre navigateur web ou cliquez dessus.

Pour Plus télécharger tous les patchs de sécurité liés aux différents virus du moment veuillez cliquez ci-dessous :

http://www.topnet.tn/antivirus.html

Enfin, TOPNET reste à la disposition de ses clients qui n'arrivent pas à éradiquer ce virus ou d'autres virus en contactant le numéro : **73 339 555** ou en envoyant un email à l'adresse suivante : technique@topnet.tn .

Merci