Vous propose ce DOSSIER SPECIAL VIRUS SoBig.F

SoBig.F a infecté environ 200 000 est le nombre d'ordinateurs actuellement infectés par SoBig.F. Ces chiffres risquent de s'intensifier. Il faut noter qu'uniquement quelques sites tunisiens ont été affectés pour le moment, mais le risque de prolifération reste réel.

SoBig.F risque de déclencher une attaque mondiale dans les prochains jours. Ainsi, les ordinateurs infectés par SoBig.F qui se propage par e-mail à l'aide d'une pièce jointe vont se connecter à une vingtaine d'ordinateurs situés aux quatre coins de la planète et déclencheront des attaques massives, non encore complètement identifiées.

Les éditeurs d'anti-virus sont parvenus à casser le cryptage du corps du virus, mais l'adresse Web qui y est référencée ne mène nulle part. Elle sera probablement mise à jour "manuellement" quelques instants avant l'attaque par les auteurs du virus, interdisant ainsi de télécharger ce code d'attaque afin d'en connaître les fonctions.

Présentation du virus SoBig.F :

W32.Sobig.F@mm (dit aussi *Sobig.F , W32/Sobig.f@MM , WORM SOBIG.F*) est un virus qui se propage par e-mail et via les dossiers partagés.

Il se présente sous la forme d'un message dont le titre est aléatoire et d'un fichier joint dont l'extension est .PIF ou .SCR. Si ce fichier est exécuté, le virus s'envoie aux correspondants présents dans le carnet d'adresses Windows, ainsi qu'aux adresses e-mail collectées dans les fichiers .DBX, .HLP, .HTM ou ..HTML de l'ordinateur infecté et essaye d'infecter d'autres ordinateurs du réseau local, en exploitant les partages réseau.

Systèmes concernés : Tous les systèmes Microsoft Windows (Windows 95, Windows 98, Windows NT, Windows 2000, Windows Me, Windows XP)

Systèmes Non concernés : Macintosh, OS/2, UNIX, Linux

Moyens de Propagation : E-mail et Partages Réseaux.

L'adresse de l'expéditeur du message infecté est une adresse prise au hasard sur l'ordinateur contaminé ou sinon admin@internet.com. Ne pas ouvrir des messages dont le **titre** est l'un des suivants : **Re: Thank you!, Thank you!, Re: Details, Re: Re: My details, Re: Approved, Re: Your application, Re: Wicked screensaver, Re: That movie**.

Le corps du message est au choix :

See the attached file for details.
Please see the attached file for details.
La pièce jointe possède une extension en .PIF ou .SCR :
your_document.pif
document_all.pif
thank_you.pif
your_details.pif
details.pif
document_9446.pif
application.pif
wicked_scr.scr
movie0045.pif

Serveurs infectés actuellement par SoBig.F :

Les machines serveurs susceptibles de délivrer l'URL des ordinateurs infectés par SoBig.F se connectent au port UDP 8998 de l'un de ces 20 serveurs, afin de télécharger le code nocif utilisé pour l'attaque. La liste des serveurs actuellement identifiés est la suivante :

12.158.102.205
12.232.104.221
218.147.164.29
24.197.143.132
24.202.91.43
24.206.75.137
24.210.182.156
24.33.66.38
61.38.187.59
63.250.82.87
65.177.240.194
65.92.186.145
65.92.80.218
65.93.81.59
65.95.193.138
66.131.207.81
67.73.21.6
67.9.241.67
68.38.159.161
68.50.208.96

Ces serveurs appartiennent à des usagers connectés en permanence sur une ligne à haut débit, qu'il est difficile de déconnecter.

Se protéger du virus SoBig.F :

Configurez votre système (surtout les systèmes windows 95/98) pour permettre l'affichage complet des extensions. Les fichiers ayant une double extension sont nécessairement des fichiers infectés.

Manipuler les pièces jointes avec beaucoup de prudence. Dans certains cas l'émetteur du message n'est pas connu, mais dans de très nombreux cas il l'est. Surtout n'hésitez pas à demander confirmation de l'envoi a l'émetteur. Se méfier des messages incohérents.

Mettre à jour très régulièrement le logiciel anti-virus et sa base de signatures (prendre en compte que de nouvelles menaces apparaissent presque tous les jours).

❖ Recommandations pour les administrateurs

Pour toute précaution, Bloquez au niveau de votre routeur/firewall le port UDP 8998 si vous ne l'exploitez pas et sinon les adresses IP ci-dessus et Appliquez sans tarder les mesures préventives et curatives consignées relatif à ce virus.

❖ MESURES PREVENTIVES

Le virus SoBig.F se présente sous la forme d'un message dont le titre et le nom du fichier joint sont aléatoires. Il est impératif de se méfier des messages contenant des pièces jointes qui vous sont envoyés de façon inattendue, même si vous connaissez l'émetteur supposé de ce message.

❖ MESURES CORRECTIVES

Mettez à jour votre anti-virus. Vous pouvez désinfecter votre PC grâce à l'un des kits gratuits suivants :

http://vil.nai.com/vil/stinger/
http://www.trendmicro.com/ftp/products/tsc/sysclean.com
http://securityresponse.symantec.com/avcenter/FixSbigF.exe
ftp://ftp.f-secure.com/anti-virus/tools/f-sobig.zip
ftp://ftp1.avp.ch/utils/clrav.com
http://www.sophos.com/misc/sobigsfx.exe
http://www.nod32.ch/files/sbfclean.zip

Pour plus d'informations :

http://www.sarc.com/avcenter/venc/data/w32.sobig.f@mm.html
http://www.f-secure.com/v-descs/sobig_f.shtml
http://vil.mcafee.com/dispVirus.asp?virus_k=100561

Merci