Date: Lundi 04 octobre 2004 à 21:32:27
Sujet: 3 Sécurité et Hacking

Tout sur le virus Bugbear.B

Bugbear.B est un virus qui se propage par email et via les dossiers partagés comme Bugbear.A. Il se présente sous la forme d'un message dont le titre et le nom du fichier joint sont aléatoires.

Bugbear.B est un virus qui se propage par email et via les dossiers partagés comme Bugbear.A. Il se présente sous la forme d'un message dont le titre et le nom du fichier joint sont aléatoires. Si le fichier joint est exécuté, le virus s'envoie à tout votre carnet d'adresse Windows et à un maximum d'adresses email extraites de divers fichiers du disque. Il désactive les antivirus et firewalls personnels les plus populaires (Norton ect..), installe un troyen de type "keylogger" qui espionne les frappes au clavier et infecte un grand nombre de fichiers exécutables présents sur l'ordinateur contaminé.
La piece jointe pèse environ 72.192 octets.
Les utilisateurs concernés doivent mettre à jour leur antivirus. En cas de doute, les utilisateurs d'Internet Explorer 5.01 et 5.5 doivent aussi mettre à jour leur navigateur via le site de Microsoft ou le service WindowsUpdate afin de corriger la faille exploitée par le virus pour s'exécuter automatiquement. Il faut enfin supprimer les partages de ressources inutiles et protéger les autres par mot de passe afin de prévenir toute propagation du virus.

Les utilisateurs ayant executé le fichier joint peuvent telecharger l'utilitaire de desinfection FixBugb pour rechercher et éliminer le virus. En cas de contamination d'un réseau local, les ordinateurs infectés doivent être déconnectés du réseau puis le virus doit etre recherché et éliminer sur chacun des ordinateurs. Les ordinateurs ne devront n'être reconnectés que lorsque tous les ordinateurs auront été désinfectés.

Ce virus est un Ver mais en plus d'etre un ver comme Bugbear.A c'est aussi un infecteur de fichiers car il infecte la plupart des fichiers .exe. Les systémes concernés par ce virus sont Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000 et Windows XP. Vous n'avez pas de soucis avous faire si vous êtes sur Linux ou Mac. Le virus est deja connu sous les noms :
- Win32.Bugbear.B (Computer Associates)
- W32/Bugbear.B@mm (F-Secure)
- I-Worm.Tanatos.B (Kaspersky)
- W32/Bugbear.b@MM (McAfee)
- W32/Bugbear-B (Sophos)
- W32.Bugbear.B@mm (Symantec)
- PE_BUGBEAR.B (Trend Micro)

Le sujet de l'e-mail, le corps et le nom du fichier joint sont aléatoires. Ils sont soit pré-programmés soit tirés d'un ou plusieurs

fichiers choisis au hasard sur le disque dur , ce qui rend le virus impossible à identifier à la seule lecture de l'objet et de l'expéditeur d'un courrier. Vous pouvez très facilement penser que le titre de cette e-mail vous est familier puisque le titre, le corps et le nom de la piece jointe viennent de votre ordinateur. Quelques exemples de titres de messages :

- Your Gift
- Emploi du temps
- profession de foi
- IBM Weekly Update-Canada
- Fw: Note d'infos du site TPE-PME.COM
- Voici une carte virtuelle pour vous
- TR: C'est truculent!...
- Re: cela va tu finir par se rendre!!!
- loto
- Fwd: TR : TR : Joke
- Alcool et grossesse
- DOUAL' AIR
- Fwd: La france que de chouettes noms . . . . Un peut de =
- La revue de presse d'Info-Decideur.com du mercredi 28 mai 2003
- FW: CASS 00-06
- Microsoft Outlook Express 6
- [gti] Explication rapide sur les ACL
- Samedi 18 mai
- we thank you for your quick reply 8894iiytc
- Fw: EXPORT MANAGER
- Renseignement sur
- Re: M/V ARMELLE blk wheat Rouen /Algeria
- boulot
- M.V. "ARMELLE" (02/3535) - C/P D.D. 28.11.02 - WHEAT FROM ROUEN TO
- Information
- Re: Request fax copy of Hawb
- Get 8 FREE issues - no risk!
- Hi!
- Your News Alert
- $150 FREE Bonus!
- Re:
- Your Gift
- New bonus in your cash account
- Tools For Your Online Business
- Daily Email Reminder
- News
- free shipping!
- its easy
- Warning!
- SCAM alert!!!
- Sponsors needed
- new reading
- CALL FOR INFORMATION!
- 25 merchants and rising

- Cows
- My eBay ads
- empty account
- Market Update Report
- click on this!
- fantastic
- wow!
- bad news
- Lost & Found
- New Contests
- Today Only
- Get a FREE gift!
- Membership Confirmation
- Report
- Please Help...
- Stats
- I need help about script!!!
- Interesting...
- Introduction
- various
- Announcement
- history screen
- Correction of errors
- Just a reminder
- Payment notices
- hmm..
- update
- Hello!

Mais attention si vous recevez un e-mail comportant les caractéristiques cités ne l'ouvrait pas même si sont titre et différents de ceux cités.

Les pièces jointes ont généralement une double extension, la dernière étant toujours EXE, SCR ou PIF. Quelques exemples de noms de fichiers joints :

- antivirus_install.exe.scr
- sauvegarde5janvier03.pxj.scr
- convoc_AG240902.doc.pif
- COMPARATIF IMPRIMANTES.xls.exe
- Anciens documents Excel.lnk.scr
- BD.doc.pif
- Petit Larousse 2000.lnk.pif
- solution de jeux.lnk.scr
- imprimantes.kv3.exe
- advpack.exe.pif
- Mes documents.lnk.scr
- 18 mai 03 10h01 Petit Dijeuner Traditionnel ` l'Apo Logis.JPG.pif

- Classeur1.xls.exe
- 0106515.dxf.exe
- AGENT.lpd.scr
- spider.sav.exe

- ATTESTATION D.doc.pif
- INFORMAGCO.eml.pif
- NOTE.DOC.pif
- Setup.scr
- vie juive.JPG.scr
- Page ENTJTE.doc.scr
- mona lisa.jpg.exe
- J.doc.pif
- cabas.jpg.pif
- attach01.tif.scr

Le message infecté par Bugbear peut-être au format texte ou HTML. Dans le cas du format HTML, le virus utilise une vulnérabilité IFRAME des navigateurs Internet Explorer 5.01 et 5.5 (MS01-020) pour s'exécuter automatiquement à l'ouverture du message ou lors de son affichage dans la fenêtre de prévisualisation avec les logiciels Outlook ou Outlook Express. C'est pour cela qu'il faut mettre a jour internet Explorer le plus souvent possible et appliquer les nombreux patchs. Si le fichier joint est exécuté, le virus se copie dans le répertoire Système de Windows sous un nom aléatoire, modifie la base de registres pour s'exécuter automatiquement au prochain démarrage. Bugbear.B extrait ensuite les adresses emails contenues dans les fichiers INBOX (Mozilla/Netscape) ainsi que ceux comportant l'extension .ODS (Outlook Express), .MMF (Microsoft Mail File), .NCH (Outlook Express News), .MBX (Eudora), .EML (Outlook Express Mail), .TBB (Windows Office Toolbar Button) et .DBX (Outlook Express) pour s'y envoyer automatiquement. Le virus peut s'envoyer avec une fausse adresse d'expéditeur, il est donc le plus souvent impossible de prévenir la personne infectée. Les messages contaminés ne comportent généralement aucun destinataire dans le champ "A:" ou alors simplement l'expression "undisclosed-recipients". Bugbear.B tente ensuite de se propager via les ressources partagées en réseau Microsoft, y compris vers les imprimantes, ce qui provoque des impressions parasites et des gaspillages de papier (les imprimantes ne peuvent pas être infectées mais tentent d'imprimer le code binaire qu'elles reçoivent, le poste contaminé étant celui de la file d'attente à l'origine de l'impression parasite). Le virus tente également de désactiver les antivirus et firewalls les plus populaires (Norton, Panda, ect...), en terminant les processus correspondants :

_AVP32.EXE
_AVPCC.EXE
_AVPM.EXE
ACKWIN32.EXE
ANTI-TROJAN.EXE
APVXDWIN.EXE
AUTODOWN.EXE
AVCONSOL.EXE
AVE32.EXE
AVGCTRL.EXE
AVKSERV.EXE
AVNT.EXE

AVP.EXE
AVP32.EXE
AVPCC.EXE
AVPDOS32.EXE
AVPM.EXE
AVPTC32.EXE
AVPUPD.EXE
AVSCHED32.EXE
AVWIN95.EXE
AVWUPD32.EXE
BLACKD.EXE
BLACKICE.EXE
CFIADMIN.EXE
CFIAUDIT.EXE
CFINET.EXE
CFINET32.EXE
CLAW95.EXE
CLAW95CF.EXE
CLEANER.EXE
CLEANER3.EXE
DVP95.EXE
DVP95_0.EXE
ECENGINE.EXE
ESAFE.EXE
ESPWATCH.EXE
F-AGNT95.EXE
FINDVIRU.EXE
FPROT.EXE
F-PROT.EXE
F-PROT95.EXE
FP-WIN.EXE
FRW.EXE
F-STOPW.EXE
IAMAPP.EXE
IAMSERV.EXE
IBMASN.EXE
IBMAVSP.EXE
ICLOAD95.EXE
ICLOADNT.EXE
ICMON.EXE
ICSUPP95.EXE
ICSUPPNT.EXE
IFACE.EXE
IOMON98.EXE
JEDI.EXE
LOCKDOWN2000.EXE
LOOKOUT.EXE
LUALL.EXE
MOOLIVE.EXE
MPFTRAY.EXE
N32SCANW.EXE

NAVAPW32.EXE
NAVLU32.EXE
NAVNT.EXE
NAVW32.EXE
NAVWNT.EXE
NISUM.EXE
NMAIN.EXE
NORMIST.EXE
NUPGRADE.EXE
NVC95.EXE
OUTPOST.EXE
PADMIN.EXE
PAVCL.EXE
PAVSCHED.EXE
PAVW.EXE
PCCWIN98.EXE
PCFWALLICON.EXE
PERSFW.EXE
RAV7.EXE
RAV7WIN.EXE
RESCUE.EXE
SAFEWEB.EXE
SCAN32.EXE
SCAN95.EXE
SCANPM.EXE
SCRSCAN.EXE
SERV95.EXE
SMC.EXE
SPHINX.EXE
SWEEP95.EXE
TBSCAN.EXE
TCA.EXE
TDS2-98.EXE
TDS2-NT.EXE
VET95.EXE
VETTRAY.EXE
VSCAN40.EXE
VSECOMR.EXE
VSHWIN32.EXE
VSSTAT.EXE
WEBSCANX.EXE
WFINDV32.EXE
ZONEALARM.EXE

Bugbear.B comporte une backdoor qui ouvre le port 1080 de l'ordinateur afin de permettre à une personne distante de se connecter à l'ordinateur de la victime pour dérober, exécuter ou supprimer des fichiers et comme il desactive votre firewall vous ne pouvez pas vous en apercevoir. Il est aussi composé d'un composant keylogger qui espionne les frappes au clavier et envoie périodiquement le résultat à plusieurs adresses emails pré-programmées. Le virus tente enfin d'infecter les fichiers exécutables suivants :

%windows%scandskw.exe
%windows% egedit.exe
%windows%mplayer.exe
%windows%hh.exe
%windows% otepad.exe
%windows%winhelp.exe
%ProgramFilesDir%Internet Exploreriexplore.exe
%ProgramFilesDir%adobeacrobat 5.0 eaderacrord32.exe
%ProgramFilesDir%WinRARWinRAR.exe
%ProgramFilesDir%Windows Media Playermplayer2.exe
%ProgramFilesDir%RealRealPlayer ealplay.exe
%ProgramFilesDir%Outlook Expressmsimn.exe
%ProgramFilesDir%FarFar.exe
%ProgramFilesDir%CuteFTPcutftp32.exe
%ProgramFilesDir%AdobeAcrobat
%ProgramFilesDir%4.0ReaderAcroRd32.exe
%ProgramFilesDir%ACDSee32ACDSee32.exe
%ProgramFilesDir%MSN Messengermsnmsgr.exe
%ProgramFilesDir%WS_FTPWS_FTP95.exe
%ProgramFilesDir%QuickTimeQuickTimePlayer.exe
%ProgramFilesDir%StreamCastMorpheusMorpheus.exe
%ProgramFilesDir% one Labs oneAlarm oneAlarm.exe
%ProgramFilesDir%TrillianTrillian.exe
%ProgramFilesDir%LavasoftAd-aware 6Ad-aware.exe
%ProgramFilesDir%AIM95aim.exe
%ProgramFilesDir%Winampwinamp.exe
%ProgramFilesDir%DAPDAP.exe
%ProgramFilesDir%ICQIcq.exe
%ProgramFilesDir%kazaakazaa.exe
%ProgramFilesDir%winzipwinzip32.exe
%Windows% = C:Windows ou C:Winnt (selon la version de Windows)
%ProgramFilesDir% = C:Program Files (par défaut)

Publication de Tout sur l'informatique - Programmation C#, Sécurité, Divx, P2P:
http://www.zmaster.fr

URL de cette publication
http://www.zmaster.fr/modules.php?name=News&file=article&sid=14