Date: Jeudi 07 octobre 2004 à 19:46:45
Sujet: 3 Sécurité et Hacking

Toutes les informations sur Sobig.E

Tout sur le virus Sobig.E et comment s'en débarrasser.

Sobig.E est un virus qui se propage par email et via les dossiers partagés comme Sobig.C et Sobig.B (Mankx, Palyh).Ce virus est un Ver. Il se présente sous la forme d'un e-mail dont l'expéditeur, le sujet et le nom de la piece jointe sont aléatoires. Le fichier joint est un fichier .ZIP qui contient soit fichier en .PIF soit un fichier en .SCR, ce qui permet au virus de passer au travers des antivirus de messagerie qui sont parametrés pour ne pas scanner les archives. Il pese seulement 86.528 octets quand c'est un fichier .pif ou .scr et 82.195 octets lorsque c'est un fichier .zip. Si le fichier joint est exécuté, le virus s'envoie aux correspondants présents dans le carnet d'adresses Windows, ainsi qu'aux adresses email collectées dans les fichiers .DBX, .HTM, .HTML, .EML ou .TXT de l'ordinateur infecté.
L'expéditeur du message infecté est support@yahoo.com mais elle peut aussi être une adresse email copiée sur l'ordinateur de la personne infectée par le virus. Le texte de l'e-mail est toujours "Please see the attached file for details.".
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.
Ce virus est deja connu sous les nom de :
- Win32.Sobig.E (CA)
- Worm.Sobig.e (KAV)
- W32/Sobig.e@MM (Mc Afee)
- W32/Sobig-E (Sophos)
- W32.Sobig.E@mm (Symantec)
- WORM_SOBIG.E (Trend Micro) Le titre de l'e-mail est choisi aléatoirement dans la liste ci-dessous : Application Ref: 456003

Your application
Re: Re: Document
Re: Re: Application ref. 003644
Re: Documents
Re: Screensaver
Re: Submited (Ref: 003746)
Re: Movies
Re: Movie
Re: Application
Re: Submitted

Quelques noms de pieces jointes :

- your_details.zip (contient details.pif)
- application.zip (contient application.pif)
- document.zip (contient document.pif)

- screensaver.zip (contient sky.world.scr)
- movie.zip (contient Movie.pif)

Sobig.E est conçu pour ne plus s'activer à compter du 14/07/03 et ne devrait donc plus se propager à partir de cette date.

Dans sa version actuelle, Sobig.E est conçu pour ne plus s'activer à compter du 14/07/03 et ne devrait donc plus se propager à partir de cette date. Mais souvenez vous que Sobig.B et Sobig.C ne devait plus ce propager jusqu'au 31/05/03 et 08/06/03 et que Sobig.E est apparu le 25/06/03 donc une personne a tres legerement ameliorer Sobig.B ou Sobig.C pour propager Sobig.E. Les utilisateurs qui ont executé ce fichier doivent mettre à jour leur antivirus. Et on ne redira jamais assez n'ouvrez pas les e-mails d'utilisateurs inconnus surtout lorsqu'il accompagné d'une piece jointe suspecte, même si le sujet de l'e-mail est attrayant il ne faut pas exécuter un fichier joint sans l'avoir au préalable analysé avec un antivirus mis à jour régulierement.

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=25