Vous propose ce DOSSIER SPECIAL VIRUS LovSan/Blaster

Présentation du virus Blaster :

Apparu durant l'été 2003, le virus **Blaster** (qui est connu aussi sous les noms W32/Lovsan.worm, W32/Lovsan.worm.b, W32.Blaster.Worm, W32/Blaster-B, WORM_MSBLAST.A, MSBLASTER, Win32.Poza, Win32.Posa.Worm, Win32.Poza.B) est le premier virus à exploiter la faille RPC/DCOM (Remote Procedure Call, soit en français appel de procédure distante) des systèmes Microsoft Windows permettant à des processus distants de communiquer.

En exploitant la faille grâce à un débordement de tampon, un programme malicieux (tel que le virus LovSan) peut prendre le contrôle de la machine vulnérable.

Les systèmes affectés sont les systèmes Windows NT 4.0, 2000, XP et Windows Server 2003. Le virus Blaster prévoit aussi des attaques mensuelles vers Windows Update, qui est disponible à partir du site de Microsoft.

Le virus LovSan / Blaster est prévu pour effectuer une attaque sur le service *WindowsUpdate* de Microsoft afin de perturber la mise à jour des machines vulnérables !!

Les actions du virus :

Le ver **LovSan / Blaster** est programmé de telle façon à scanner une plage d'adresses IP aléatoire à la recherche de systèmes vulnérables à la faille RPC sur le port 135.

Lorsqu'une machine vulnérable est trouvée, le ver ouvre un shell distant sur le port TCP 4444, et force l'ordinateur distant à télécharger une copie du ver dans le répertoire *%WinDir%\system32* en lançant une commande *TFTP* (port 69 UDP) pour transférer le fichier à partir de la machine infectée.

Une fois le fichier téléchargé, il est exécuté, puis il crée des entrées dans la base de registre de Windows afin de se relancer automatiquement à chaque redémarrage :

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
- Run "windows auto update" = msblast.exe I just want to say LOVE YOU SAN!! Bill

Symptômes de l'infection :

L'exploitation de la faiblesse RPC provoque un certain nombre de dysfonctionnement sur les systèmes des PC affectés, liés à la désactivation du service RPC (processus svchost.exe / rpcss.exe).

Les systèmes vulnérables présentent les symptômes suivants :

- Copier/Coller défectueux ou impossible
- Ouverture d'un lien hypertexte dans une nouvelle fenêtre impossible
- Déplacement d'icônes impossibles
- Fonction recherche de fichier de Windows erratique
- fermeture du port 135/TCP
- Redémarrage de Windows XP : le système est sans cesse relancé par *AUTORITE NT/system* avec le(s) message(s) suivant(s) :

1 - Windows doit maintenant redémarrer car le service appel de procédure distante (RPC) s'est terminé de façon inattendue.
2 - Arrêt du système dans 60 secondes veuillez enregistrer tous les travaux en cours.
3 – Cet arrêt a été initié par AUTORITE NT\SYSTEM Windows doit maintenant démarrer.

Eradiquer le virus :

Pour éradiquer le ver LovSan, la meilleure méthode consiste tout d'abord à désinfecter le système.

Si votre système redémarre continuellement, il faut désactiver le redémarrage automatique :

- Cliquez sur *Poste de travail* avec le bouton droit
- Cliquez sur Propriétés / Avancé / Démarrage et récupération / Paramètres
- Décochez la case "redémarrer automatiquement" !

Vous pourrez rétablir cette option lorsque votre système fonctionnera de nouveau normalement.

Il est indispensable de mettre à jour le système à l'aide du service Windows Update ou bien en mettant à jour votre système avec le patch suivant correspondant à votre système d'exploitation :

- Patch pour Windows 2000 : http://www.microsoft.com/downloads/details.aspx?FamilyId=C8B8A846-F541-4C15-8C9F-220354449117&displaylang=fr
- Patch pour Windows XP : http://www.microsoft.com/downloads/details.aspx?FamilyId=2354406C-C5B6-44AC-9532-3DE40F69C074&displaylang=fr

Les solutions efficaces face au virus Lovsan sont :

Actions correctives : Visitez notre page http://www.topnet.tn/securite.php

Téléchargez un ou tous ces Kits de désinfection contre le vers Blaster :

http://www.topnet.tn/PatchsAntivirus/AntiBlaster/blastsfx.exe
http://www.topnet.tn/PatchsAntivirus/AntiBlaster/FixBlast.exe
http://www.topnet.tn/PatchsAntivirus/AntiBlaster/Antimsblast-%28A,B,C,F%29.exe
http://www.topnet.tn/PatchsAntivirus/AntiBlaster/f-lovsan.zip

D'autre part, dans la mesure où le virus se propage par l'intermédiaire du réseau Microsoft Windows, il est fortement conseillé d'installer un pare-feu personnel sur vos machines connectées à Internet et de filtrer les ports tcp/69, tcp/135 à tcp/139 et tcp/444.

Plus d'informations sur le virus :

- **Nai :** http://vil.nai.com/vil/content/v_100547.htm
- **Microsoft :** http://www.microsoft.com/isapi/CTRedir.asp?type=CT&source=WWW&sPage=WP_S2_Topic6|Virus%20Alerts||W32.Blaster.Worm&tPage=http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/virus/alerts/msblaster.asp
- **Sophos :** http://www.sophos.fr/virusinfo/analyses/w32blastera.html
- **Symantec :** http://www.symantec.fr/techsupp/ssi/virus_alerts/fr/fr_w32_blaster_worm.html
- **Symantec :** http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.removal.tool.html

Enfin, il faut noter que Microsoft a mis hors de service l'url http://www.windowsupdate.com afin d'éviter les milliers d'attaques de Blaster, via les PC infectés par ce virus.

Vous pouvez contacter notre service technique au **73 33 95 55** en cas de problème.

Veuillez visiter notre site web pour nous contacter par email et découvrir nos dossiers de sécurité et précisément les adresses suivantes :

http://www.topnet.tn/
http://www.topnet.tn/securite.php
http://www.topnet.tn/historique.php

En cas d'urgence veuillez utiliser un de ces Kits pour nettoyer votre PC des virus qui circulent maintenant sur Internet : MyDoom, Blaster, Sobig, Sircam, Klez, etc.…

http://www.topnet.tn/PatchsAntivirus/KitAntivir/stinger.exe
http://www.topnet.tn/PatchsAntivirus/KitAntivir/aswclnr.exe
http://www.topnet.tn/PatchsAntivirus/KitAntivir/tsc.zip
http://www.topnet.tn/PatchsAntivirus/KitAntivir/clrav.zip

Avec Mes Sincères Salutations

BOUBAKER Nobel El Houssine
Directeur Relation Client
TOPNET