

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Propagation du ver/virus NIMDA (Concept Virus)

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2001-ALE-013>

Gestion du document

Référence	CERTA-2001-ALE-013
Titre	Propagation du ver/virus NIMDA (Concept Virus)
Date de la première version	19 septembre 2001
Date de la dernière version	-
Source(s)	Avis CA-2001-26 du Cert CC FIRST Sophos
Pièce(s) jointe(s)	Aucune

TAB. 1 – gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Exécution de code arbitraire ;
- Accès aux données ;
- Virus ;
- Déni de service ;
- Compromission ;
- Installation de portes dérobées.

2 Systèmes affectés

Microsoft Windows 95, 98, ME, NT, et 2000.

3 Résumé

Un nouveau ver se propage en exploitant des vulnérabilités connues sous Microsoft Windows.

4 Description

Le ver NIMDA s'attaque aux serveurs IIS ainsi qu'aux postes clients utilisant Internet Explorer et/ou Outlook.

Il s'installe sur les serveurs par le biais des vulnérabilités suivantes :

- Failles des serveurs IIS décrites dans les avis CERTA-2000-AVI-028, CERTA-2001-AVI-053 et CERTA-2000-AVI-061 ;
- Réutilisation d'une porte dérobée préalablement installée par le ver Code Red II ou le ver sadmind (Réf : CERTA-2001-ALE-008-003 et CERTA-2001-ALE-007)

Une fois installé, le ver modifie tous les fichiers web (HTML et ASP) en y incorporant un script « javascript » dans le but d'infecter les visiteurs du site contaminé (Exploitation d'une vulnérabilité de Windows Média Player, Réf : CERTA-2001-AVI-041).

Sur les postes clients, le ver se transmet par la messagerie en expédiant aux destinataires du carnet d'adresses Outlook un message accompagné d'une pièce jointe README.EXE ou lors de la consultation d'une page Web infectée par le code javascript précédemment cité.

Lors de l'infection, le ver active le partage masqué des disques (exemple : partage de C sous C\$).

- Sous Windows 9x et Me : partage total sans mot de passe ;
- Sous Windows NT et 2000 : création d'un compte guest dans le groupe admin.

Ce partage ne devient effectif qu'en cas de redémarrage de la machine infectée.

5 Détection

- Vérifier les extraits des logs au niveau des serveurs IIS.

Exemples de log :

```
GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir
GET /scripts/root.exe?/c+dir
GET /MSADC/root.exe?/c+dir
GET /c/winnt/system32/cmd.exe?/c+dir
GET /d/winnt/system32/cmd.exe?/c+dir
GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir
GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir
GET /scripts/root.exe?/c+dir
GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir
GET /MSADC/root.exe?/c+dir
GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt
/system32/cmd.exe?/c+dir
```

- Vérifier le contenu des pages mises en ligne et notamment la présence de la ligne javascript suivante :
windows.open("readme.eml",null,"resizable=no,top=6000,left=6000")

- Vérifier l'état des partages réseau et la présence d'un compte guest sous Windows NT et 2000 ;

- Le ver ajoute à la ligne shell=, dans le fichier system.ini, l'entrée load.exe :
shell=explorer.exe load.exe -dontrunold

- Les clés suivantes sont également ajoutées ou modifiées dans la base de registre :

- HKEY_CURRENT_USER\Software\Microsoft\Windows\currentVersion\Explorer\advanced\HideFileExt
- HKEY_CURRENT_USER\Software\Microsoft\Windows\currentVersion\Explorer\advanced\Hidden

- HKEY_CURRENT_USER\Software\Microsoft\Windows\currentVersion\Explorer\advanced\SuperHidden
- Sous Windows NT et 2000 la clé suivante est supprimée :
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lanmanserver\Share\Security
- Vérifier la présence du fichier admin.dll à la racine des disques ;
- Le virus modifie des fichiers légitimes ou ajoute des exécutables :
 - ADMIN.DLL
 - LOAD.EXE
 - MMC.EXE
 - README.EXE
 - RICHED20.DLL
 - MEP*.TMP.EXE

6 Contournement provisoire

- Placer les paramètres de sécurité de Internet Explorer en mode élevé et désactiver les javascripts et le téléchargement automatique de fichiers ;
- Filtrer le port 69/UDP (TFTP) au niveau du garde barrière ;
- Filtrer les ports 135 à 139/TCP-UDP (Partage NETBIOS) au niveau du garde barrière ;
- Désactiver les serveurs IIS (installé par défaut) s'ils ne sont pas indispensables.

7 Solution

- Mettre à jour vos antivirus :
 - Sophos :
<http://www.sophos.com/virusinfo/analyses/w32nimdaa.html>
 - NAI :
http://www.vil.nai.com/vil/virusSummary.asp?virus_k=99209
 - F-Secure :
<http://www.f-secure.com/v-descs/nimda.shtml>
 - Symantec :
<http://www.sarc.com/avcenter/venc/data/w32.nimda.a@mm.html>
 - Les éditeurs proposent également des outils (non testés) afin de détecter et d'éradiquer ce ver. Exemple :
<http://download.nai.com/products/mcafee-avert/nimda2.exe>
- Mettre à jour vos serveurs IIS :
<http://www.microsoft.com/technet/security/bulletin/MS01-044.asp>
- Mettre à jour Internet Explorer :
<http://www.microsoft.com/technet/security/bulletin/MS01-020.asp>

8 Documentation

Bulletin du Cert CC :
http://www.cert.org/body/advisories/CA200126_FA200126.html

Gestion détaillée du document

19 septembre 2001 version initiale.