

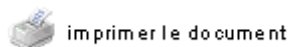
France

- sites globaux
- produits et services
- achats
- support
- partenaires/revendeurs
- security response
- téléchargements
- à propos de Symantec
- recherche
- votre avis

W32.Mydoom.A@mm



Découvert le : 26/01/2004
Dernière mise à jour le : 09/02/2004



évaluation de la menace | détails techniques | recommandations | instructions de suppression

W32.Mydoom.A@mm (également connu sous le nom W32.Novarg.A@mm) est un ver d'envoi en masse de courrier électronique qui se présente sous la forme d'une pièce jointe avec l'extension .bat, .cmd, .exe, .pif, .scr ou .zip. Lorsqu'un ordinateur est infecté, le ver installe une porte dérobée (backdoor) sur le système en ouvrant les ports TCP 3127 à 3198. Ceci permet éventuellement à un pirate de se connecter à l'ordinateur et de l'utiliser comme proxy afin d'accéder à ses ressources réseau. De plus, cette porte dérobée permet de télécharger et d'exécuter des fichiers arbitraires.

Dans 25% des cas, il est probable qu'un ordinateur infecté par le ver réalise une attaque de type Déni de Service (DoS) le 1er février 2004 à 16:09:18 UTC, en fonction de la date/heure système de la machine. Si le ver lance le déni de service, il ne s'expédiera pas en masse. Il contient également une date de déclenchement pour cesser de se propager et suspendre le déni de service le 12 février 2004. Tandis que le ver cessera de se propager le 12 février 2004, le composant de porte dérobée continuera de fonctionner après cette date.

Remarques :

- Les produits "grand public" Symantec prenant en charge la fonctionnalité de blocage des vers détectent cette menace automatiquement lorsqu'elle essaye de se propager.
- Symantec Security Response a créé un [outil de suppression](#) pour nettoyer toutes les infections de W32.Mydoom.A@mm.
- Les définitions de virus antérieures au 04.02.04 détectent ce ver comme W32.Novarg.A@mm.

Egalement connu comme : W32.Novarg.A@mm, W32/Mydoom@MM [McAfee], WORM_MIMAIL.R [Trend], Win32.Mydoom.A [Computer Associates], W32/Mydoom-A [Sophos], I-Worm.Novarg [Kaspersky]

Type: **Worm**

Etendue de l'infection: 22 528 octets

Systèmes affectés: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP

Systèmes non affectés: DOS, Linux, Macintosh, OS/2, UNIX, Windows 3.x

Protection

- | | |
|----------------------------------------------------------------|------------|
| • Définitions de virus (Intelligent Updater) * | 26/01/2004 |
| • Définitions de virus (LiveUpdate™) ** | 26/01/2004 |

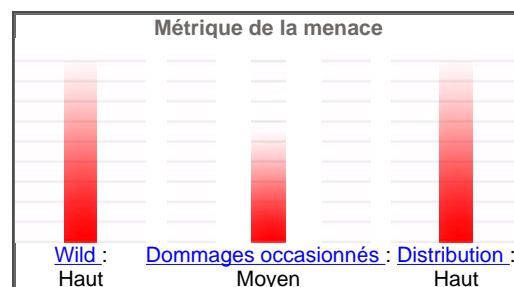
* Les définitions de virus de l'Intelligent Updater sont diffusées quotidiennement, mais requièrent un téléchargement et une installation manuels.
[Cliquez ici](#) pour télécharger manuellement.

** Les définitions de virus de LiveUpdate sont généralement diffusées chaque mercredi.
[Cliquez ici](#) pour obtenir les instructions sur l'utilisation de LiveUpdate

évaluation de la menace

Wild :

- [Nombre d'infections](#) : Plus de 1000
- [Nombres de sites](#) : Plus de 10
- [Distribution géographique](#) : Haut
- [Endiguement de la menace](#) : Facile
- [Suppression](#) : Modéré



Dommages occasionnés

- [Élément déclencheur](#) : ne s'applique pas
- [Résultat d'activation](#) : ne s'applique pas
 - [Distribution par e-mail à grande échelle](#) : S'expédie aux adresses électroniques trouvées dans un ensemble de fichiers spécifiques. Il ignore les adresses électroniques finissant en .edu.
 - [Supprime les fichiers](#) : ne s'applique pas
 - [Modifie les fichiers](#) : ne s'applique pas
 - [Dégrade les performances](#) : Il réalise une attaque Déni de Service (DoS) contre www.sco.com.
 - [Provoque l'instabilité du système](#) : ne s'applique pas
 - [Divulgue des informations confidentielles](#) : ne s'applique pas
 - [Compromet les paramètres de sécurité](#) : Il permet l'accès à distance non autorisé.

Distribution

- [Objet de l'e-mail](#) : Varie
- [Nom de la pièce jointe](#) : Varie avec une extension .pif, .scr, .exe, .cmd, .bat ou .zip.
- [Taille de la pièce jointe](#) : 22 258 octets
- [Date de la pièce jointe](#) : ne s'applique pas
- [Ports](#) : TCP 3127-3198
- [Lecteurs partagés](#) : ne s'applique pas
- [Cible de l'infection](#) : ne s'applique pas

détails techniques

Lorsque W32.Mydoom.A@mm s'exécute, il agit ainsi :

1. Il crée les fichiers suivants :
 - %System%\Shimgapi.dll : Shimgapi.dll agit comme un serveur proxy et ouvre des ports TCP d'écoute de la plage 3127 à 3198. Cette porte dérobée permet également de télécharger et d'exécuter des fichiers arbitraires.
 - %Temp%\Message : Ce fichier contient des lettres aléatoires et il s'affiche via le Bloc-notes.
 - %System%\Taskmon.exe.

Remarques :

- Taskmon.exe est un fichier légitime des systèmes d'exploitation Windows 95/98/Me, mais il se trouve dans le dossier %Windir% et non dans le dossier %System% (par défaut, C:\Windows ou C:\Winnt). *Ne supprimez pas le fichier légitime qui se trouve dans le dossier %Windir%.*
- %System% est une variable. Le ver détermine l'emplacement du dossier System et se copie à cet emplacement. Par défaut, il s'agit de C:\Windows\System (Windows 95/98/Me), C:\Winnt\System32 (Windows NT/2000) ou C:\Windows\System32 (Windows XP).
- %Temp% est une variable. Le ver détermine l'emplacement du dossier temporaire et se copie à cet emplacement. Par défaut, il s'agit de C:\Windows\TEMP (Windows 95/98/Me), ou C:\WINNT\Temp (Windows

2. Il ajoute la valeur :

"(par défaut)" = "%System%\shimgapi.dll"

à la clé de registre :

HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}
\InProcServer32

de sorte que Explorer.exe charge Shimgapi.dll.

3. Il ajoute la valeur :

"TaskMon" = "%System%\taskmon.exe"

aux clés de registre :

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

de sorte que TaskMon s'exécute lorsque vous démarrez Windows.

4. Il vérifie la date système, et si la date est comprise entre le 1er février 2004 et le 12 février 2004, il est probable que dans 25% des cas le ver réalise une attaque de type déni de service contre www.sco.com. Le déni de service est réalisé en créant 63 nouveaux threads qui envoient des requêtes GET et utilisent une connexion directe sur le port 80. Le ver ne s'expédiera pas en masse si le déni de service est déclenché.

Remarques :

- L'attaque de type déni de service sera lancée à 16:09:18 UTC le 1er février 2004. Le ver vérifie l'heure du système local ainsi que la date afin de déterminer s'il doit initialiser le déni de service.
- En raison de la façon dont le ver vérifie la date système, le Déni de Service ne sera exécuté que sur 25% des ordinateurs infectés.
- Le déni de service ne se produira qu'après vérification de la date système, au cours de l'infection initiale ou si l'ordinateur est redémarré.
- Le ver utilisera les paramètres DNS locaux afin de résoudre le nom de domaine utilisé dans l'attaque de déni de service (www.sco.com).

-
5. Il crée les clés de registre suivantes :

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Explorer\ComDlg32\Version

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Explorer\ComDlg32\Version

6. Il recherche des adresses électroniques dans les fichiers aux extensions précisées ci-dessous.

- .htm
- .sht
- .php
- .asp
- .dbx
- .tbb
- .adb
- .pl
- .wab
- .txt

7. Il tente d'envoyer du courrier électronique en utilisant son propre moteur SMTP. Il émet une requête au serveur de messagerie du destinataire afin de s'expédier. S'il n'y parvient pas, il utilisera le serveur de messagerie local.

Le courrier électronique présente les caractéristiques suivantes :

De : L'adresse de l'expéditeur peut être usurpée

Objet : L'objet sera l'un des suivants

test
hi
hello
Mail Delivery System
Mail Transaction Failed
Server Report
Status
Error

Message : Le message sera l'un des suivants

Mail transaction failed. Partial message is available.

The message contains Unicode characters and has been sent as a binary attachment.

The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.

Pièce jointe : Le nom du fichier joint, sans l'extension, sera l'un des suivants :

document
readme
doc
text
file
data
test
message
body

La pièce jointe peut avoir une ou deux extensions. Si elle en a deux, la première extension sera l'une des suivantes :

.htm
.txt
.doc

La deuxième extension, ou la seule extension si c'est le cas, sera l'une des suivantes :

.pif
.scr
.exe
.cmd
.bat

.zip (Il s'agit d'un fichier .zip qui contient une copie du ver et qui partage le même nom de fichier que le .zip. Par exemple, readme.zip peut contenir readme.exe)

Si le ver a une extension .exe ou .scr, le fichier sera affiché avec l'icône ci-dessous :



Pour les autres extensions de fichiers, il utilisera l'icône pour ce type de fichier.

8. Il se copie dans le répertoire de téléchargement KaZaA sous la forme de l'un des fichiers suivants :

- winamp5
- icq2004-final
- activation_crack
- strip-girl-2.0bdcom_patches
- rootkitXP

- office_crack
- nuke2004

avec l'extension de fichier

- .pif
- .scr
- .bat
- .exe

Symantec Gateway Security 1.0

Une mise à jour du moteur IDS/IPS de Symantec Gateway Security destinée à assurer la protection contre le ver W32.Mydoom.A@mm a été publiée le 30.01.04 à 21:24 PST. Il est conseillé aux administrateurs de Symantec Gateway Security d'exécuter LiveUpdate afin de garantir leur protection contre cette menace.

Symantec Gateway Security 2.0

Une mise à jour du moteur IDS/IPS de Symantec Gateway Security destinée à assurer la protection contre le ver W32.Mydoom.A@mm a été publiée le 29.01.04 à 15:02:00 PST. Il est conseillé aux administrateurs de Symantec Gateway Security d'exécuter LiveUpdate afin de garantir leur protection contre cette menace.

Intruder Alert

Symantec a publié la stratégie [Intruder Alert 3.6 W32_Novarg_Worm Policy](#).

Symantec HIDS 4.1.1

Symantec a publié un package LiveUpdate le 27 janvier 2004 pour les utilisateurs de Symantec HIDS 4.1.1. Veuillez vous reporter à [Symantec Host IDS 4.1.1 Security Update 1](#) pour plus d'informations.

Symantec ManHunt

La mise à jour [Security Update 17](#) a été publiée afin de fournir des signatures spécifiques à l'activité de porte dérobée du ver W32.Mydoom.A@mm.

Détection du déni de service à l'aide des règles d'alerte de flux de ManHunt - l'équipe Symantec Network IDS recommande aux administrateurs d'utiliser la fonctionnalité règle d'alerte de flux pour consigner les événements détectant tout trafic suspect sur le site web de SCO le 01.02.04 et sur le site web de Microsoft le 03.02.04. Des instructions détaillées sont disponibles dans l'article suivant de la base de données de Symantec :

<http://service1.symantec.com/SUPPORT/intrusiondetectkb.nsf/docid/2004012813061253>

De plus, les clients de Symantec ManHunt 2.2/3.0/3.01 peuvent appliquer la signature suivante afin de détecter la tentative de Déni de Service contre www.sco.com. Le Déni de Service commencera le 1er février 2004. Le ver cessera de se propager le 12 février 2004. Cette signature permettra de déterminer à partir de quels ordinateurs est émise la requête.

```
*****start file*****
```

```
alert tcp any any -> any 80 (msg:"W32_Novarg_SCO_DOS"; content:"GET / HTTP/1.1|0d0a|Host: www.sco.com|0d0a0d0a|"; offset:0; dsize:37;)
```

```
*****EOF*****
```

Pour en savoir plus sur la façon de créer des signatures personnalisées, reportez-vous au guide administrateur de Symantec ManHunt "Symantec ManHunt Administrative Guide: Appendix A Custom Signatures for HYBRID Mode".

recommandations

Symantec Security Response vous propose des suggestions de configuration des produits Symantec afin de minimiser votre exposition aux menaces.

passerelle

Symantec Gateway Security

- Activez l'analyse AV pour smtpd.
- Assurez-vous qu'aucun port TCP de la plage 3127-3198 n'est ouvert (ils ne sont pas ouverts par défaut). Ceci empêchera la propagation.
- Configurez un filtre ou une règle de refus pour www.sco.com et/ou 216.250.128.12
- Configurez le mécanisme de filtrage de contenu pour bloquer www.sco.com et/ou 216.250.128.12.

Symantec Enterprise Firewall

- Déchargez l'analyse AV pour tout le trafic SMTP.
- Assurez-vous qu'aucun port TCP de la plage 3127-3198 n'est ouvert (ils ne sont pas ouverts par défaut). Ceci empêchera la propagation.
- Configurez un filtre ou un règle de refus pour www.sco.com et/ou 216.250.128.12
- Configurez le mécanisme de filtrage de contenu pour bloquer www.sco.com et/ou 216.250.128.12

client

Norton Internet Security

- Exécutez LiveUpdate afin de télécharger les dernières définitions de virus.
- Assurez-vous que la fonction AutoProtect est activée et si elle ne l'est pas, activez-la. La fonction AutoProtect est activée par défaut.
- Utilisez Norton AntiVirus pour effectuer l'analyse antivirus.
- Créez une règle de cheval de Troie pour bloquer les communications TCP entrantes des ports 3127 à 3198. Ceci empêchera la propagation.
- Configurez une règle générale pour refuser les communications TCP sortantes avec www.sco.com et/ou 216.250.128.12 Notez qu'avec cette règle, les utilisateurs ne pourront pas accéder à www.sco.com. Les utilisateurs devront désactiver ces règles pour pouvoir communiquer avec www.sco.com.

Norton Personal Firewall

- Créez une règle de cheval de Troie pour bloquer les communications TCP entrantes des ports 3127 à 3198. Ceci empêchera la propagation.
- Configurez une règle générale pour refuser les communications TCP sortantes avec www.sco.com et/ou 216.250.128.12 Notez qu'avec cette règle, les utilisateurs ne pourront pas accéder à www.sco.com. Les utilisateurs devront désactiver ces règles pour pouvoir communiquer avec www.sco.com.

Symantec Security Response invite utilisateurs et administrateurs à adopter les mesures de base les plus efficaces en matière de sécurité :

- Eteignez et supprimez tous les services inutiles. Par défaut, de nombreux systèmes d'exploitation installent des services auxiliaires qui ne sont pas primordiaux, tels qu'un client FTP, telnet, et un serveur Web. Ces services sont la porte ouverte aux attaques. S'ils sont supprimés, les attaques ont moins de chances de parvenir et vous avez moins de services à entretenir au moyen de correctifs.
- Si une attaque multiple exploite un ou plusieurs services réseau, désactivez ou bloquez l'accès à ces services jusqu'à ce qu'un correctif soit appliqué.
- Maintenez toujours le niveau de vos correctifs à jour, en particulier sur les ordinateurs qui hébergent des services publics et qui sont accessibles via un firewall, tels que HTTP, FTP, messagerie, et services DNS.
- Appliquez une stratégie un mot de passe. Sur les ordinateurs compromis, il est plus difficile de violer les fichiers de mots de passe si ceux-ci sont complexes. Ceci vous permet d'éviter ou de limiter les dommages potentiels encourus par un ordinateur compromis.
- Configurez votre serveur de messagerie afin de bloquer ou de supprimer les e-mails qui contiennent des annexes couramment utilisées pour propager des virus, comme par exemple les fichiers .vbs, .bat, .exe, .pif et .scr.
- Isolez rapidement les ordinateurs infectés afin d'éviter de compromettre d'avantage votre organisation. Effectuez une analyse complète et restaurez les ordinateurs utilisant des médias approuvés.
- Exhorte les employés à n'ouvrir que les pièces jointes attendues. Aussi, n'exécutez aucun logiciel téléchargé depuis Internet qui n'a pas subi de recherche de virus. Le simple fait de visiter un site Internet compromis peut provoquer une infection si certaines vulnérabilités du navigateur ne sont pas corrigées.

instructions de suppression

Suppression à l'aide de l'outil de suppression

Symantec Security Response a créé un [outil de suppression](#) pour nettoyer toutes les infections de W32.Mydoom.A@mm. Il s'agit de la méthode recommandée dans la plupart des cas.

Suppression manuelle

Procédez à une suppression manuelle si vous ne pouvez obtenir l'outil.

Les instructions suivantes sont valables pour tous les derniers produits anti-virus Symantec, y compris les gammes Symantec AntiVirus et Norton AntiVirus.

1. Désactivez l'option de restauration du système (Windows Me/XP)
2. Actualisez les définitions de virus.
3. Redémarrez l'ordinateur en mode sans échec ou en mode VGA.
4. Exécutez une analyse complète du système et éliminez tous les fichiers détectés comme W32.Mydoom.A@mm.
5. Supprimez et modifiez la valeur ajoutée au registre.
6. Enregistrez de nouveau le fichier webcheck.dll. (Ceci permettra de supprimer les modifications apportées au Registre et responsables du chargement de Shimgapi.dll)

Pour plus de détails sur chacune des étapes, lisez les instructions suivantes.

1. Désactiver l'option de restauration du système (Windows Me/XP)

Si vous utilisez Windows Me ou Windows XP, nous vous conseillons de désactiver temporairement la restauration du système. Windows Me et XP utilisent cette fonctionnalité, activée par défaut afin de pouvoir restaurer des fichiers sur votre ordinateur, s'ils venaient à être endommagés. Si un ordinateur a été infecté par un virus, un ver ou un cheval de Troie, il est possible que ce virus, ver ou cheval de Troie soit sauvegardé par la Restauration du système.

Windows empêche des programmes tiers, y compris les programmes anti-virus, de modifier la Restauration du système. Par conséquent, les programmes ou outils anti-virus ne peuvent pas éradiquer les menaces dans le dossier de Restauration du système. Par conséquent, la Restauration du système peut restaurer un fichier infecté sur votre ordinateur même après avoir nettoyé les fichiers infectés sur tous les autres emplacements.

Une analyse des virus peut également détecter une menace dans le dossier de restauration du système même si vous avez supprimé la menace.

Pour savoir comment désactiver la Restauration du système, consultez la documentation de Windows ou l'un des articles suivants :

- [Comment désactiver ou activer la restauration automatique de Windows Me](#)
- [Comment désactiver ou activer la restauration automatique de Windows XP](#)

Remarque : Lorsque vous avez terminé la procédure de suppression, et que vous pensez que la menace est éliminée, vous devriez réactiver System Restore en suivant les instructions détaillées dans les documents cités ci-dessus.

Pour plus d'informations, et pour obtenir une méthode différente afin de désactiver la Restauration du système de Windows Me, consultez le document de la base de connaissances de Microsoft : [Les outils antivirus ne peuvent pas nettoyer les fichiers infectés dans le dossier Restore](#), numéro d'article : 263455.

2. Mettre à jour les définitions de virus

Symantec Security Response réalise des tests complets de qualité pour toutes les définitions de virus avant leur publication sur nos serveurs. Il y a deux façons de se procurer les dernières définitions de virus :

- La méthode la plus simple pour obtenir les dernières définitions de virus est d'exécuter LiveUpdate : Celles-ci sont publiées chaque semaine sur les serveurs LiveUpdate (en principe tous les mercredis) sauf en cas d'attaque virale critique. Pour savoir si des

définitions de LiveUpdate sont disponibles pour cette menace, reportez-vous à la ligne **Définitions de virus (LiveUpdate)** de l'encadré Protection de cet article.

- L'autre consiste à télécharger les définitions de virus en utilisant Intelligent Updater. Les définitions de virus d'Intelligent Updater sont publiées les jours ouvrés aux Etats-Unis (du lundi au vendredi). Elles doivent être téléchargées sur le site Web de [Symantec Security Response](#) puis installées manuellement. Pour savoir si des définitions d'Intelligent Updater sont disponibles pour cette menace, reportez-vous à la ligne **Définitions de virus (Intelligent Updater)** de l'encadré Protection de cet article.

Les définitions de virus d'Intelligent Updater sont disponibles : Pour des instructions détaillées, consultez le document intitulé Comment mettre à jour les définitions de virus en utilisant l'Intelligent Updater.

3. Pour redémarrer l'ordinateur en mode sans échec ou en mode VGA

Arrêtez l'ordinateur puis éteignez-le. Attendez au moins 30 secondes puis redémarrez l'ordinateur en mode sans échec ou en mode VGA.

- Si vous exécutez Windows 95, 98, Me, 2000 ou XP, redémarrez votre ordinateur en mode sans échec. Pour connaître les instructions, consultez le document [Comment démarrer l'ordinateur en mode sans échec](#).
- Si vous exécutez Windows NT 4 redémarrez votre ordinateur en mode VGA.

4. Rechercher les fichiers infectés et les supprimer

- a. Démarrez votre programme anti-virus Symantec et assurez-vous que ce dernier a été configuré pour analyser tous les fichiers.
 - Pour les **produits grand public Norton AntiVirus** : Lisez le document [Comment configurer Norton AntiVirus afin qu'il analyse tous les fichiers](#).
 - Pour les **produits anti-virus Enterprise Symantec** : Lisez le document [Comment vérifier qu'un produit antivirus Corporate Edition de Symantec est configuré de façon à analyser tous les fichiers](#).
- b. Exécutez une analyse complète du système.
- c. Si un fichier est détecté comme infecté par W32.Mydoom.A@mm, cliquez sur Supprimer.

5. Supprimer et modifier la valeur du registre

ATTENTION : Nous vous recommandons vivement d'effectuer une sauvegarde du registre avant d'y apporter des modifications. Une modification incorrecte du registre peut provoquer la perte définitive de données ou la corruption de fichiers. Ne modifiez que les clés indiquées. Pour des instructions détaillées, consultez le document [Comment faire une copie de sauvegarde du Registre de Windows](#).

- a. Cliquez sur Démarrer > Exécuter. (La boîte de dialogue Exécuter apparaît.)
- b. Tapez `regedit`

Puis cliquez sur OK. (L'Editeur du Registre apparaît.)

- c. Accédez aux clés suivantes :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run  
et
```

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

- d. Dans le volet de droite, supprimez la valeur :

```
"Taskmon"="%System%\taskmon.exe"
```

Remarque : %System% est une variable qui indique l'emplacement du dossier System. Par

défaut, il s'agit de C:\Windows\System (Windows 95/98/Me), C:\Winnt\System32 (Windows NT/2000) ou C:\Windows\System32 (Windows XP).

- e. Quittez l'Editeur du Registre.

6. Réenregistrer le fichier Webcheck.dll

(Ceci permettra de supprimer les modifications apportées au Registre et responsables du chargement de Shimgapi.dll)

- a. Cliquez sur Démarrer puis sur Exécuter (la boîte de dialogue Exécuter apparaît.)
- b. Saisissez, ou copiez/collez, le texte suivant :

```
regsvr32 webcheck.dll
```

- c. Cliquez sur OK. Lorsque ce message apparaît : "DllRegisterServer in webcheck.dll succeeded," cliquez sur OK.

Informations complémentaires :

Lorsque W32.Mydoom.A@mm envoie du courrier électronique, il évitera d'en envoyer aux domaines contenant l'une des chaînes suivantes :

- avp
- syma
- icrosof
- msn.
- hotmail
- panda
- sopho
- borlan
- inpris
- example
- mydomai
- nodomai
- ruslis
- .gov
- gov.
- .mil
- foo.
- berkeley
- unix
- math
- bsd
- mit.e
- gnu
- fsf.
- ibm.com
- google
- kernel
- linux
- fido
- usenet
- iana
- ietf
- rfc-ed
- sendmail
- arin.
- ripe.

- isi.e
- isc.o
- secur
- acketst
- pgp
- tanford.e
- utgers.ed
- mozilla

Ou aux comptes qui correspondent aux chaînes suivantes :

- root
- info
- samples
- postmaster
- webmaster
- noone
- nobody
- nothing
- anyone
- someone
- your
- you
- me
- bugs
- rating
- site
- contact
- soft
- no
- somebody
- privacy
- service
- help
- not
- submit
- feste
- ca
- gold-certs
- the.bat
- page

Ou aux comptes qui contiennent les chaînes suivantes :

- admin
- icrosoft
- support
- ntivi
- unix
- bsd
- linux
- listserv
- certific
- google
- accoun

Il fait suivre l'un des noms suivants au nom de domaine obtenu :

- adam
- alex

- alice
- andrew
- anna
- bill
- bob
- brenda
- brent
- brian
- claudia
- dan
- dave
- david
- debby
- fred
- george
- helen
- jack
- james
- jane
- jerry
- jim
- jimmy
- joe
- john
- jose
- julie
- kevin
- leo
- linda
- maria
- mary
- matt
- michael
- mike
- peter
- ray
- robert
- sam
- sandra
- serg
- smith
- stan
- steve
- ted
- tom

Historique :

- 3 février 2004 :
 - Changement du nom de W32.Novarg.A@mm à W32.Mydoom.A@mm.
 - Ajout des mises à jour Norton Internet Security et Norton Personal Firewall
- 31 janvier 2004 :
 - Ajout d'informations concernant les threads supplémentaires pour réaliser l'attaque de déni de service.
 - Ajout d'informations concernant l'heure à laquelle l'attaque débute.
 - Ajout d'informations concernant la probabilité de 25% d'attaque de déni de service par le ver.
 - Ajout des mises à jour Symantec ManHunt et SGS.
- 30 janvier 2004 : Modification de la suppression manuelle afin d'utiliser la commande regsvr32 pour réenregistrer le fichier webcheck.dll plutôt que de procéder ainsi dans le Registre.
- 27 janvier 2004 :
 - Mise à jour du lien vers l'outil de suppression de W32.Novarg.A@mm
 - Mise à jour des informations concernant les alias.

- Ajout de la référence à la mise à jour de Symantec HIDS.
- January 30, 2004. Changed manual removal to use regsvr32 command to reregister the webcheck.dll file rather than do this in the registry.

Version anglaise de ce document

[Cliquez ici pour lire ce document en anglais](#)

Remarque : En raison du temps nécessaire à la traduction, il est possible que le contenu des documents traduits diffère du contenu original, si celui-ci a été mis à jour alors que la traduction était en cours. Le document en anglais contient toujours les dernières mises à jour.

Article rédigé par : Peter Ferrie & Tony Lee