

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

## W32.Sasser.B.Worm


Découvert le : 01/05/2004
Dernière mise à jour le : 03/05/2004

imprimer le document
évaluation de la menace
détails techniques
recommandations
instructions de suppression

W32.Sasser.B.Worm est une variante de W32.Sasser.Worm. Il tente d'exploiter la vulnérabilité LSASS décrite dans le Bulletin de sécurité MS04-011 de Microsoft, et se propage en scannant des adresses IP choisies de façon aléatoire, à la recherche de systèmes vulnérables.

© 1995-2004 Symantec Corporation.  
Tous droits réservés.  
[Mentions Légales](#)  
[Politique de Confidentialité](#)

### Remarques :

- L'algorithme hash MD5 de ce ver est 0x1A2C0E6130850F8FD9B9B5309413CD00.
- Symantec Security Response a créé un [outil de suppression](#) pour nettoyer toutes les infections de W32.Sasser.B.Worm.
- Bloquez les ports TCP 5554, 9996 et 445 au niveau du pare-feu et installez le correctif de Microsoft approprié (MS04-011) afin d'empêcher l'exploitation à distance de cette vulnérabilité.

En raison du nombre croissant de virus soumis, Symantec Security Response a réévalué W32.Sasser.B.Worm qui passe du Niveau 3 au Niveau 4.

**Variantes:** W32.Sasser.Worm  
**Type:** **Worm**  
**Etendue de l'infection:** 15872 octets  
**Systèmes affectés:** Windows 2000, Windows Server 2003, Windows XP

### Protection

- |  |            |
|--|------------|
| • <a href="#">Définitions de virus (Intelligent Updater)</a> * | 01/05/2004 |
| • <a href="#">Définitions de virus (LiveUpdate™)</a> **        | 01/05/2004 |

\* 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

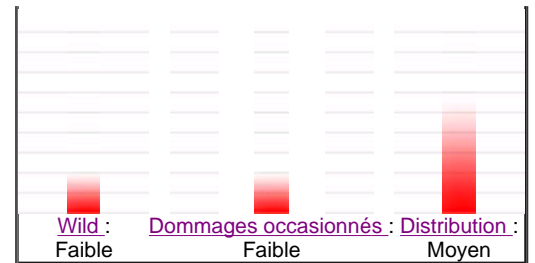
## évaluation de la menace

### Wild :

- [Nombre d'infections](#) : 0 - 49
- [Nombres de sites](#) : Plus de 10
- [Distribution géographique](#) : Moyen
- [Endiguement de la menace](#) : Facile

Métrique de la menace

- Suppression : Facile



### Dommages occasionnés

- Élément déclencheur : Ne s'applique pas
- Résultat d'activation: Ne s'applique pas
  - Distribution par e-mail à grande échelle : Ne s'applique pas
  - Supprime les fichiers : Ne s'applique pas
  - Modifie les fichiers : Ne s'applique pas
  - Dégrade les performances : Dégrade notablement les performances
  - Provoque l'instabilité du système : Ne s'applique pas
  - Divulgue des informations confidentielles : Ne s'applique pas
  - Compromet les paramètres de sécurité: Ne s'applique pas

### Distribution

- Objet de l'e-mail : Ne s'applique pas
- Nom de la pièce jointe : Ne s'applique pas
- Taille de la pièce jointe : Ne s'applique pas
- Date de la pièce jointe : Ne s'applique pas
- Ports : TCP 445, 5554, 9996
- Lecteurs partagés : Ne s'applique pas
- Cible de l'infection : Systèmes sur lesquels le correctif n'a pas été appliqué, vulnérables à l'exploit LSASS - MS04-011

## détails techniques

Lorsque W32.Sasser.B.Worm s'exécute, il agit de la façon suivante :

1. Il tente de créer un mutex nommé Jobaka3 et quitte le système si sa tentative échoue. Ceci permet de garantir qu'une seule instance du ver s'exécute sur l'ordinateur à tout moment.
2. Il se copie comme %Windir%\avserve2.exe.

---

**Remarque** : %Windir% est une variable. Le ver détermine l'emplacement du dossier d'installation de Windows (C:\Windows ou C:\Winnt par défaut) et se copie à cet emplacement.

---

3. Il ajoute la valeur :

```
"avserve2.exe"="%Windir%\avserve2.exe"
```

à la clé de registre :

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

de façon à ce que le ver s'exécute lorsque vous démarrez Windows.

4. Il utilise l'API AbortSystemShutdown afin d'empêcher les tentatives d'arrêt ou de redémarrage de l'ordinateur.
5. Il démarre un serveur FTP sur le port TCP 5554. Ce serveur sert à répandre le ver sur d'autres hôtes.
6. Il tente de se connecter à des adresses IP générées de façon aléatoire sur le port TCP 445. Si une connexion est établie sur un ordinateur, le ver envoie un shellcode à cet ordinateur, ce qui peut provoquer l'exécution d'un shell distant sur le port TCP 9996. Le ver utilise alors le shell pour pousser l'ordinateur à se reconnecter au serveur FTP sur le port

5554 et récupérer une copie du ver. Cette copie portera un nom composé de 4 ou 5 chiffres suivis de \_up.exe (par ex. : 74354\_up.exe).

## recommandations

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 de W32.Sasser

Symantec Security Response a créé un [outil de suppression](#) pour nettoyer toutes les infections de W32.Sasser.B.Worm. Essayez cet outil, il constitue le moyen le plus simple pour éliminer cette menace.

### Suppression manuelle

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

1. Terminer le processus malveillant.
2. Désactiver l'option de restauration du système (Windows Me/XP)
3. Actualiser les définitions de virus.
4. Exécuter une analyse complète du système et éliminez tous les fichiers détectés comme W32.Sasser.B.Worm.
5. Rétablir la modification apportée au registre.

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

### 1. Pour terminer le processus malveillant

Pour terminer le processus malveillant :

- a. Appuyez sur Ctrl+Alt+Suppr une seule fois.
- b. Cliquez sur Gestionnaire des tâches.
- c. Cliquez sur l'onglet Processus.
- d. Cliquez deux fois sur l'en-tête de colonne Nom de l'image pour trier les processus par ordre alphabétique.
- e. Faites défiler la liste pour trouver les processus suivants :

- avserve2.exe
  - tout processus dont le nom est composé de 4 ou 5 chiffres suivis de \_up.exe (par ex. : 74354\_up.exe).
- f. Si vous trouvez un de ces processus, sélectionnez-le puis cliquez sur le bouton Terminer le processus.
  - g. Quittez le Gestionnaire des tâches.

## 2. Pour 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 une méthode alternative pour désactiver la Restauration du système de Windows Me, consultez le document de la base de connaissances de Microsoft intitulé [Les outils antivirus ne peuvent pas nettoyer les fichiers infectés dans le dossier Restore](#) - Numéro de l'article : Q263455.

## 3. Pour 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](#).

#### 4. Pour analyser et supprimer les fichiers infectés

- 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.Sasser.B.Worm, cliquez sur Supprimer.

#### 5. Pour rétablir la modification apportée au 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 à la clé suivante :

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`

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

`"avserve2.exe"="%Windir%\avserve2.exe"`

- e. Quittez l'Editeur du Registre.
- 

#### Historique :

- 02.05.04 :
  - Réévaluation de W32.Sasser.B.Worm au Niveau 4.
  - Ajout d'informations sur les alias.
- 01.05.04 : Ajout du lien vers l'outil de suppression.

#### 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.

---