

France

sites globaux

produits et services

achats

support

partenaires/revendeurs

security response

téléchargements

à propos de Symantec

recherche

votre avis

W32.Blaster.Worm

*Découvert le : 11/08/2003**Dernière mise à jour le : 09/02/2004*

imprimer le document

évaluation de la menace

détails techniques

recommandations

instructions de suppression

En raison du nombre décroissant de virus soumis, Symantec Security Response a réévalué cette menace qui passe du Niveau 4 au Niveau 3 à partir du 8 octobre 2003. W32.Blaster.Worm est un ver qui exploite la vulnérabilité DCOM RPC (décrite dans le Bulletin de sécurité de Microsoft MS03-026 en utilisant le port TCP 135. Le ver ne vise que les machines exécutant Windows 2000 et Windows XP. Les machines Windows NT et Windows 2003 Server sont vulnérables à l'exploitation mentionnée plus haut (si le correctif n'a pas été appliqué aux machines), cependant, le ver n'est pas codé pour se dupliquer sur ces systèmes. Ce ver tente de télécharger le fichier msblast.exe dans le répertoire %WinDir%\system32 puis essaie de l'exécuter. Ce ver n'a pas de fonctionnalité d'envoi en masse de courrier électronique.

Des informations complémentaires, ainsi que l'adresse d'un site sur lequel vous pouvez télécharger le correctif Microsoft, sont disponibles dans l'article de Microsoft intitulé [What You Should Know About the Blaster Worm and Its Variants](#).

Nous conseillons aux utilisateurs de bloquer l'accès au port TCP 4444 au niveau du firewall, puis de bloquer les ports suivants, s'ils n'utilisent pas les applications énumérées :

- Port TCP 135, "DCOM RPC"
- Port UDP 69, "TFTP"

Le ver tente également de réaliser une attaque de type déni de service (DoS) sur Windows Update. Cette attaque vise à vous empêcher d'appliquer un correctif sur votre ordinateur afin de vous protéger contre la vulnérabilité DCOM RPC.

Cliquez [ici](#) pour en savoir plus sur la vulnérabilité que ce ver exploite et pour connaître les produits Symantec qui peuvent vous aider à limiter les risques causés par cette vulnérabilité.

Remarque : Cette menace sera détectée par les définitions de virus avec :

- Defs Version: 50811s
- Sequence Number: 24254
- Extended Version: 8/11/2003, rev. 19

Symantec Security Response a créé un [outil de suppression](#) pour nettoyer toutes les infections de W32.Blaster.Worm.

Webcast W32.Blaster.Worm

Ce webcast détaille les stratégies destinées à limiter et à remédier à l'attaque de déni de service et offre également une description complète de l'attaque.

<http://enterprisesecurity.symantec.com/content/webcastinfo.cfm?webcastid=63>

Security Response propose des informations complémentaires destinées aux administrateurs

réseau, afin de les aider à détecter sur leur réseau les machines infectées par W32.Blaster.Worm. Pour en savoir plus, veuillez consulter le document intitulé [Detecting traffic due to RPC worms](#).

Egalement connu comme : W32/Lovsan.worm.a [McAfee], Win32.Poza.A [CA], Lovsan [F-Secure], WORM_MSBLAST.A [Trend], W32/Blaster-A [Sophos], W32/Blaster [Panda], Worm.Win32.Lovesan [KAV]

Type: [Worm](#)

Etendue de l'infection: 6 176 octets

Systèmes affectés: Windows 2000, Windows NT, Windows Server 2003, Windows XP

Systèmes non affectés: Linux, Macintosh, OS/2, UNIX, Windows 95, Windows 98, Windows Me

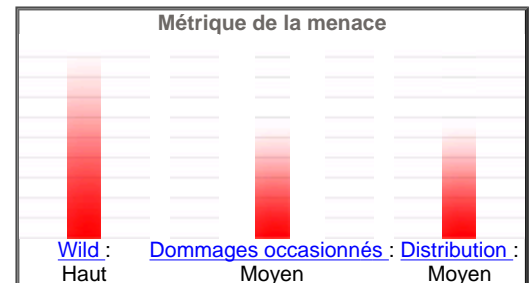
Références CVE : [CAN-2003-0352](#)

Protection	
• Définitions de virus (Intelligent Updater)*	11/08/2003
• Définitions de virus (LiveUpdate™)**	11/08/2003
* 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](#) : Modéré
- [Suppression](#) : Modéré



[Dommages occasionnés](#)

- [Élément déclencheur](#) : Si la date est le 16 du mois et ce jusqu'à la fin de ce mois si antérieur à août, et chaque jour à partir du 16 août jusqu'au 31 décembre.
- [Résultat d'activation](#) : Réalise une attaque de type déni de service sur windowsupdate.com
 - [Provoque l'instabilité du système](#) : Peut bloquer les machines.
 - [Compromet les paramètres de sécurité](#) : Ouvre un shell distant cmd.exe caché.

[Distribution](#)

- [Ports](#) : TCP 135, TCP 4444, UDP 69
- [Cible de l'infection](#) : Machines exécutant des services DCOM RPC vulnérables.

détails techniques

Lorsque W32.Blaster.Worm s'exécute, il agit ainsi :

1. Il vérifie si un ordinateur est déjà infecté et si le ver s'exécute. Si c'est le cas, le ver n'infectera pas l'ordinateur une seconde fois.
2. Il ajoute la valeur :

```
"windows auto update"="msblast.exe"
```

à la clé de registre :

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

3. Il génère une adresse IP et tente d'infecter l'ordinateur possédant cette adresse. L'adresse IP est générée à partir des algorithmes suivants :

- Dans 40% des cas, l'adresse IP générée prend la forme A.B.C.0, où A et B correspondent aux deux premières parties de l'adresse IP de l'ordinateur infecté.

C est également calculé en fonction de la troisième partie de l'adresse IP du système infecté ; cependant, dans 40% des cas, le ver vérifie si C est supérieur à 20. Si c'est le cas, une valeur aléatoire inférieure à 20 est soustraite à C. Une fois l'adresse IP calculée, le ver tentera de trouver et d'exploiter un ordinateur avec une adresse IP A.B.C.0.

Le ver incrémentera alors de 1 la partie 0 de l'adresse IP, et essaiera de trouver et d'exploiter d'autres ordinateurs en se basant sur la nouvelle adresse IP, et ce jusqu'à atteindre 254.

- Avec une probabilité de 60%, l'adresse IP générée est entièrement aléatoire.
4. Il envoie des données sur le port TCP 135 pouvant exploiter la vulnérabilité DCOM RPC. Il envoie des données sur le port TCP 135 pouvant exploiter la vulnérabilité DCOM RPC. Le ver envoie un seul type de données sur deux pour exploiter soit Windows XP, soit Windows 2000.

Dans 80% des cas, il enverra des données pour Windows XP ; et dans 20% des cas, des données pour Windows 2000.

Remarques :

- Le sous-réseau local sera saturé par des requêtes du port 135.
- W32.Blaster.Worm ne peut pas se propager sur Windows NT ou Windows 2003 Server, cependant, les ordinateurs sur lesquels le correctif n'a pas été appliqué et qui exécutent ces systèmes d'exploitation peuvent être bloqués en raison des tentatives d'exploitation par le ver. Cependant, si le ver est placé et exécuté manuellement sur un ordinateur exécutant ces systèmes d'exploitation, il peut alors s'exécuter et se propager.
- Le ver élabore ses données d'exploitation de façon aléatoire, pouvant provoquer ainsi le blocage du service RPC si celui-ci reçoit des données incorrectes. Ceci peut se traduire par svchost.exe, générant des erreurs provoquées par ces données incorrectes
- Si le service RPC se bloque, la procédure par défaut sous Windows XP et Windows Server 2003 est de redémarrer l'ordinateur. Pour désactiver cette option, reportez-vous à l'étape un des instructions de suppression ci-dessous.

-
5. Il utilise Cmd.exe pour créer un processus de shell distant caché qui écoutera sur le port TCP 4444, permettant alors à un attaquant d'envoyer des commandes à distance sur le système infecté.
 6. Il écoute sur le port UDP 69. Lorsque le ver reçoit une requête d'un ordinateur auquel il a pu se connecter en utilisant l'exploit DCOM RPC, il enverra alors le fichier msblast.exe à cet ordinateur et lui demandera d'exécuter le ver.
 7. Si la date en cours est comprise entre le 16 et le dernier jour du mois pour les mois de janvier à août, ou si le mois courant est entre septembre et décembre, le ver tentera de réaliser une attaque de type déni de service sur Windows Update. Cependant, la tentative d'attaque de type déni de service ne réussira que si l'une des conditions suivantes est remplie :
 - Le ver s'exécute sur un ordinateur Windows XP qui a été infecté ou réinitialisé au cours de la période de résultat d'activation.
 - Le ver s'exécute sur un ordinateur Windows 2000 qui a été infecté au cours de la période de résultat d'activation et qui n'a pas été redémarré depuis son infection.
 - Le ver s'exécute sur un ordinateur Windows 2000 qui a été redémarré depuis son infection, au cours de la période de résultat d'activation, et sur lequel l'utilisateur connecté est l'Administrateur.
 8. Le trafic de l'attaque de déni de service présente les caractéristiques suivantes :
 - Il s'agit d'un flux SYN sur le port 80 de windowsupdate.com.

- Il tente d'envoyer 50 paquets HTTP toutes les secondes.
- Chaque paquet a une longueur de 40 octets.
- Si le ver ne trouve pas d'entrée DNS pour windowsupdate.com, il utilise une adresse de destination de 255.255.255.255.

Voici certaines caractéristiques fixes des en-têtes TCP et IP :

- Identification IP = 256
- Durée de vie = 128
- Adresse IP source = a.b.x.y, où a.b proviennent de l'IP hôte et x.y sont aléatoires. Dans certains cas, a.b sont aléatoires.
- Adresse IP de destination = résolution dns de "windowsupdate.com"
- Le port source TCP est entre 1000 et 1999
- Port de destination TCP = 80
- Les deux octets bas du numéro de séquence TCP sont toujours définis sur 0 ; quant aux deux octets hauts, ils sont aléatoires.
- Taille de la fenêtre TCP = 16384

Le ver contient le texte suivant, qui n'apparaît jamais :

```
I just want to say LOVE YOU SAN!!
billy gates why do you make this possible ? Stop making money and fix
your software!!
```

Comment limiter le résultat d'activation du déni de service

A compter du 15 août 2003, Microsoft a retiré l'enregistrement DNS pour windowsupdate.com. La portion DoS du ver n'affectera pas la fonction Windows Update de Microsoft, cependant, les administrateurs réseau peuvent utiliser les recommandations suivantes afin de limiter le résultat d'activation du déni de service :

- Reroutez windowsupdate.com sur une adresse IP interne spécifique. Vous saurez ainsi quelles machines sont infectées si vous disposez d'un serveur qui écoute afin d'intercepter le flux SYN.
- Configurez des règles anti-spoofing sur les routeurs si ce n'est déjà fait. Vous éviterez ainsi qu'un pourcentage élevé de paquets ne quittent le réseau. L'utilisation de uRPF ou de ACL sortants serait efficace.

Symantec Gateway Security

- Le 12 août 2003, Symantec a publié une mise à jour pour Symantec Gateway Security 1.0.
- La technologie de vérification d'applications des firewalls Symantec vous protège contre cette vulnérabilité de Microsoft, bloquant par défaut tous les ports TCP énumérés ici. Pour une sécurité optimale, la technologie de vérification d'applications de troisième génération bloque intelligemment la mise sous tunnel du trafic DCOM sur des canaux HTTP, fournissant ainsi une couche supplémentaire de protection qui n'est généralement pas disponible dans les firewalls de filtrage réseau les plus courants.

Symantec Host IDS

Le 12 août 2003, Symantec a publié une mise à jour pour Symantec Host IDS 4.1.

Intruder Alert

Le 12 août 2003, Symantec a publié une stratégie [Intruder Alert 3.6 W32_Blaster_Worm Policy](#).

Symantec Enterprise Firewall

La technologie de vérification d'applications des firewalls Symantec vous protège contre le ver W32.Blaster.worm, bloquant par défaut tous les ports TCP énumérés ici.

Symantec ManHunt

- Les technologies de détection des anomalies de protocole de Symantec ManHunt identifient l'activité générée par cette exploitation comme "Portsweep". Bien que ManHunt détecte l'activité générée par cette exploitation grâce à sa technologie de détection des anomalies

de protocole, vous pouvez utiliser la signature personnalisée "Microsoft DCOM RPC Buffer Overflow", publiée dans la [Mise à jour de sécurité 4](#), afin d'identifier précisément l'exploitation envoyée.

- La [Mise à jour de sécurité 5](#) a été publiée afin de fournir des signatures spécifiques à W32.Blaster.Worm, et permettre la détection de davantage d'attributs de W32.Blaster.Worm.
- Les technologies de détection des anomalies de protocole de Symantec ManHunt détectent l'activité associée au flux SYN de l'attaque de déni de service. Security Response a créé une signature personnalisée pour ManHunt 3.0, publiée dans la [Mise à jour de sécurité 6](#), afin de détecter cette attaque spécifique comme Blaster DDoS Request.

Enterprise Security Manager

Symantec Security Response a publié une [Stratégie de réponse](#) pour cette vulnérabilité le 17 juillet 2003.

Symantec Vulnerability Assessment

Symantec Security Response a publié le 17 juillet 2003 une version qui détecte et signale cette vulnérabilité. Cliquez [ici](#) pour plus d'informations.

Symantec NetRecon

Symantec NetRecon peut identifier les machines sensibles à W32.Blaster.Worm en identifiant la vulnérabilité "Microsoft DCOM RPC Buffer Overflow". Reportez-vous à [SU6](#) de Symantec NetRecon pour des informations détaillées.

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.Blaster.Worm

Symantec Security Response a créé un [outil de suppression](#) pour nettoyer toutes les infections de W32.Blaster.Worm. Essayez cet outil, il constitue le moyen le plus simple pour éliminer cette menace. Pour obtenir l'outil de suppression de W32.Blaster.Worm, veuillez cliquer sur le lien suivant : [Outil de suppression de W32.Blaster.Worm](#).

Suppression manuelle

Si vous n'utilisez pas l'outil de suppression, vous pouvez éradiquer cette menace manuellement. Les instructions suivantes sont valables pour tous les derniers produits anti-virus Symantec, y compris les gammes Symantec AntiVirus et Norton AntiVirus.

1. Restaurer la connectivité Internet.
2. Terminer le processus du ver.
3. Obtenir les dernières définitions de virus.
4. Rechercher et supprimer les fichiers infectés.
5. Rétablir les modifications apportées au registre.
6. Obtenir le HotFix de Microsoft afin de corriger la vulnérabilité DCOM RPC.

Pour des instructions détaillées, lisez les sections suivantes :

1. Pour restaurer la connectivité Internet

Dans de nombreux cas, sous Windows 2000 et XP, la modification des paramètres du service d'appel de procédure distante (RPC) peut vous permettre de vous connecter à Internet et éviter que l'ordinateur ne s'arrête. Pour restaurer la connectivité Internet sur votre PC, procédez comme suit :

- a. Cliquez sur Démarrer > Exécuter. La boîte de dialogue Exécuter apparaît.
- b. Saisissez :

```
SERVICES.MSC /S
```

dans le champ Ouvrir puis cliquez sur OK. La fenêtre Services apparaît.

- c. Dans le volet de droite, localisez le service Appel de procédure distante (RPC).

ATTENTION : Il existe également un service nommé Localisateur d'appels de procédure distante (RPC). Ne confondez pas ces deux services.

- d. Cliquez avec le bouton droit de la souris sur le service Appel de procédure distante (RPC) puis cliquez sur Propriétés.
- e. Cliquez sur l'onglet Récupération.
- f. Dans les listes déroulantes des champs "Première défaillance", "Deuxième défaillance" et "Défaillances suivantes", sélectionnez "Redémarrer le service."
- g. Cliquez sur Appliquer puis sur OK.

ATTENTION : Assurez-vous de rétablir les paramètres initiaux une fois que vous avez supprimé le ver.

2. Pour terminer le processus du ver

- 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 jusqu'à trouver Msblast.exe.
- f. Si vous trouvez le fichier, sélectionnez-le puis cliquez sur le bouton Terminer le processus.
- g. Quittez le Gestionnaire des tâches.

3. Pour obtenir les dernières 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 :

Pour les utilisateurs débutants

La méthode la plus simple pour obtenir les dernières définitions de virus est d'exécuter LiveUpdate : Les définitions de virus pour W32.Blaster.worm sont disponibles sur le serveur LiveUpdate depuis le 11 août 2003. Pour obtenir les dernières définitions de virus, cliquez sur le bouton LiveUpdate qui se trouve sur l'interface utilisateur principale de votre produit Symantec. Lorsque vous exécutez LiveUpdate, assurez-vous que seules les "Définitions de virus de Norton AntiVirus" sont sélectionnées. Vous pourrez vous procurer les mises à jour des produits plus tard.

Pour les administrateurs système et les utilisateurs avancés

L'autre méthode 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 à partir du 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 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.Blaster.Worm, cliquez sur Supprimer.

5. Pour rétablir les modifications apportées 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 sauvegarder le Registre de Windows](#).

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

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

- c. Naviguez vers la clé suivante :

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

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

`"windows auto update"="msblast.exe"`

- e. Quittez l'Editeur du Registre.

6. Pour obtenir le HotFix de Microsoft afin de corriger la vulnérabilité DCOM RPC

W32.Blaster.Worm est un ver qui exploite la vulnérabilité DCOM RPC en utilisant le port TCP 135 pour infecter votre PC. W32.Blaster.Worm tente également de réaliser une attaque de type déni de service sur le serveur Web Windows Update de Microsoft (windowsupdate.com) en utilisant votre PC. Pour remédier à cela, vous devez impérativement vous procurer le HotFix de Microsoft.

Cliquez ici : [Microsoft Security Bulletin MS03-026](#).

Informations complémentaires :

Des informations complémentaires, ainsi que l'adresse d'un site sur lequel vous pouvez télécharger le correctif Microsoft, sont disponibles dans l'article de Microsoft intitulé [What You Should Know About the Blaster Worm and Its Variants](#).

Historique :

8 octobre 2003 :

- Passé du Niveau 4 au Niveau 3 en raison du nombre décroissant de virus soumis.

28 août 2003 :

- Ajout d'un lien à un document contenant des informations sur le trafic réseau lié à Blaster.

20 août 2003 :

- Ajout de la référence à Symantec Client Security.

15 août 2003 :

- Ajout de recommandations complémentaires pour limiter l'attaque de déni de service.
- Ajout de références à des mises à jour pour Symantec NetRecon et Symantec Vulnerability Assessment.
- Ajout du lien à Symantec webcast.
- Informations complémentaires sur les mises à jour de Symantec ManHunt.

14 août 2003 :

- Recommandations pour limiter l'attaque de déni de service.
- Mise à jour des informations de résultat d'activation du déni de service.
- Ajout d'informations sur le trafic du déni de service.

13 août 2003 :

- Réorganisation des étapes principales dans les instructions de suppression.
- Ajout de l'emplacement du téléchargement.
- Léger reformatage.
- Retrait des instructions de restauration système Windows de la section suppression

12 août 2003 :

- Mise à niveau : le ver passe du Niveau 3 au Niveau 4, dû au nombre croissant de virus soumis.
- Ajout d'alias supplémentaires.
- Mise à jour de la description technique.
- Ajout d'informations de suppression sur la modification des paramètres RPC.

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 : Douglas Knowles, Frederic Perriot & Peter Szor