

France

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

## W32.Korgo.F

Découvert le : 01/06/2004  
Dernière mise à jour le : 22/06/2004



imprimer le document

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

En raison du nombre croissant de virus soumis, Symantec Security Response a réévalué cette menace et passe du Niveau 2 au Niveau 3 à compter du 02.06.04.

W32.Korgo.F est une variante mineure de [W32.Korgo.E](#). Il s'agit d'un ver qui tente de se propager en exploitant la vulnérabilité de saturation de mémoire tampon LSASS de Microsoft Windows (SID 10108) le port TCP 445. Il écoute également sur les ports TCP 113 et 3067, ainsi que des ports aléatoires.

### Remarques :

- Les définitions de virus Rapid Release, version 2/06/04 rév. 17 (numéro de séquence 31552) ou supérieures, identifient cette menace comme W32.Korgo.F.
- Les définitions de virus Version 60408w (version étendue du 08/04/2004 rév. 23) détectent cette menace comme Bloodhound.Packed.

Symantec Security Response a publié un [outil de suppression](#) pour nettoyer toutes les infections de W32.Korgo.F.

**Egalement connu comme :** Worm.Win32.Padobot.e [Kaspersky], W32/Korgo.worm.g [McAfee], WORM\_KORGO.F [Trend]  
**Variantes:** W32.Korgo.A, W32.Korgo.B, W32.Korgo.C, W32.Korgo.D, W32.Korgo.E  
**Type:** **Worm**  
**Etendue de l'infection:** 10 752 octets  
**Systèmes affectés:** Windows 2000, Windows XP  
**Systèmes non affectés:** DOS, Linux, Macintosh, Novell Netware, OS/2, UNIX, Windows 3.x, Windows 95, Windows 98, Windows Me, Windows NT

### Protection

- |  |            |
|--|------------|
| • <a href="#">Définitions de virus (Intelligent Updater) *</a> | 02/06/2004 |
| • <a href="#">Définitions de virus (LiveUpdate™) **</a>        | 02/06/2004 |

\* 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

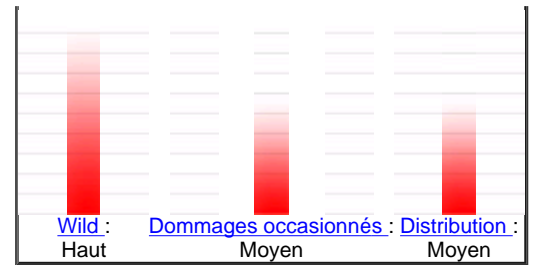
## évaluation de la menace

### Wild :

- [Nombre d'infections](#) : 50 - 999

Métrique de la menace

- [Nombres de sites](#) : Plus de 10
- [Distribution géographique](#) : Faible
- [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](#) : Ne s'applique pas
  - [Supprime les fichiers](#) : Ne s'applique pas
  - [Modifie les fichiers](#) : Ne s'applique pas
  - [Dégrade les performances](#) : Les routines de propagation par le réseau peuvent dégrader la performance générale du réseau.
  - [Provoque l'instabilité du système](#) : Ne s'applique pas
  - [Divulgue des informations confidentielles](#) : La fonction de porte dérobée permet l'accès non autorisé.
  - [Compromet les paramètres de sécurité](#): La fonction de porte dérobée peut compromettre les paramètres de sécurité.

### 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, 113, 3067 et 6667. Peut écouter sur des ports aléatoires également..
- [Lecteurs partagés](#) : Ne s'applique pas
- [Cible de l'infection](#) : Systèmes sur lesquels le correctif n'a pas été appliqué, vulnérables à l'exploitation de LSASS Windows de Microsoft.

## détails techniques

Lorsque W32.Korgo.F s'exécute, il réalise les opérations suivantes :

1. Il supprime le fichier Ftpupd.exe dans le dossier à partir duquel le ver a été exécuté.
2. Il supprime les valeurs :

```
"System Service Manager"
"System Restore Service"
"Bot Loader"
"Windows Update Service"
"WinUpdate"
"Windows Security Manager"
"avserve.exe"
"avserve2.exe"
"avserve2.exe"
```

de la clé de registre :

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

3. Il recherche la valeur :

```
"Disk Defragmenter"
```

dans la clé de registre :

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

- Si la valeur "Disk Defragmenter" n'existe pas, le ver ajoute la valeur :

"Client"="1"

à la clé de registre :

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Wireless

- Si la valeur "Disk Defragmenter" existe, mais que le chemin d'accès au fichier est différent, le ver réalise alors les opérations suivantes :
  - a. Il se copie comme %System%\<nom de fichier aléatoire>.exe.

---

**Remarque :** %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).

---

- b. Il ajoute la valeur :

"Disk Defragmenter"="%System%\<nom de fichier aléatoire>.exe

à la clé de registre :

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion

- c. Il lance <nom de fichier aléatoire>.exe, puis termine le processus en cours.
- Si la valeur "Disk Defragmenter" existe et cette valeur correspond au chemin du ver, supprimera la valeur suivante :

"Client"

de la clé de registre :

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Wireless

4. Il tente d'injecter une fonction dans Explorer.exe comme thread.

S'il y parvient, il continuera de s'exécuter dans le processus Explorer.exe. Toutes les actions détaillées dans l'étape suivante sembleront avoir été effectuées par Explorer.exe, et le ver n'apparaîtra pas dans la liste de processus du gestionnaire des tâches de Windows.

S'il n'y parvient pas, il continuera de s'exécuter comme son propre processus.

5. Il crée des threads supplémentaires et effectue les opérations suivantes :

---

**Remarque :** Tandis que le ver crée ces threads, il empêche l'arrêt ou le redémarrage de l'ordinateur.

---

- Il ouvre les ports TCP 113, 3067 et d'autres ports aléatoires. Le ver écoute sur ces ports dès qu'il reçoit un message particulier, il enverra une copie de lui-même à l'ordinateur distant.
- Il tente d'exploiter la vulnérabilité LSASS de Windows sur le port TCP 445 (décrite dans [Bulletin de sécurité Microsoft MS04-011](#)) sur des adresses IP aléatoires. Si le ver parvient à trouver un ordinateur vulnérable, cet ordinateur tentera de se reconnecter à l'ordinateur infecté sur l'un des ports TCP ouverts par le ver.
- Il tente de se connecter à l'un des serveurs IRC suivants sur le port TCP 6667 et de recevoir des commandes :
  - gaspode.zanet.org.za
  - lia.zanet.net
  - irc.tsk.ru
  - london.uk.eu.undernet.org
  - washington.dc.us.undernet.org
  - los-angeles.ca.us.undernet.org
  - brussels.be.eu.undernet.org
  - caen.fr.eu.undernet.org
  - flanders.be.eu.undernet.org

- graz.at.eu.undernet.org
- moscow-advocat.ru
- gaz-prom.ru

## **Symantec Gateway Security 5400 Series et Symantec Gateway Security version 1.0**

- *Composant antivirus* : Une mise à jour du moteur antivirus de Symantec Gateway Security est désormais disponible afin d'assurer la protection contre le ver W32.Korgo.F.Worm. Les utilisateurs de Symantec Gateway Security 5000 sont invités à exécuter LiveUpdate.
- *Composant IDS/IPS* : Une signature pour Symantec Gateway Security 5400 Series détectant les attaques contre la vulnérabilité LSASS de Microsoft a été ajoutée à SU 8, publié le 14 avril. Une signature détectant les attaques contre la vulnérabilité LSASS de Microsoft sur SGS v1.0 a été publiée. Les utilisateurs de Symantec Gateway Security 5000 sont invités à exécuter LiveUpdate.
- *Composant d'inspection de la sémantique des données des pare-feu* : Par défaut, la technologie d'inspection de la sémantique des données des pare-feu assure la protection contre la propagation de W32.Korgo.F.Worm en empêchant les attaquants d'accéder au port TCP/445, et les portes dérobées sur les systèmes infectés (TCP/113, TCP/3067). Nous conseillons vivement aux administrateurs de vérifier que leurs stratégies de sécurité n'autorisent pas les connexions entrantes sur ces ports. Les administrateurs doivent analyser leurs fichiers journaux afin de détecter toute tentative de tentative par des systèmes internes d'établir d'une session IRC sur le port TCP 6667 vers une destination. Ceci serait un signe éventuel d'un système compromis.

## **Symantec Enterprise Firewall 8.0**

Par défaut, la technologie d'inspection de la sémantique des données des pare-feu assure la protection contre la propagation de W32.Korgo.F.Worm en empêchant les attaquants d'accéder au port TCP/445 et les portes dérobées sur les systèmes infectés (TCP/113, TCP/3067). Nous conseillons vivement aux administrateurs de vérifier que leurs stratégies de sécurité n'autorisent pas les connexions entrantes sur ces ports.

## **Symantec Enterprise Firewall 7.0.x et Symantec VelociRaptor 1.5**

Par défaut, la technologie d'inspection de la sémantique des données des pare-feu assure la protection contre la propagation de W32.Korgo.F.Worm en empêchant les attaquants d'accéder au port TCP/445 et les portes dérobées sur les systèmes infectés (TCP/113, TCP/3067). Nous conseillons vivement aux administrateurs de vérifier que leurs stratégies de sécurité n'autorisent pas les connexions entrantes sur ces ports.

## **Symantec Clientless VPN Gateway 4400 Series**

Symantec Clientless VPN Gateway v5.0 n'est pas affecté par cette menace.

## **Symantec Gateway Security 300 Series**

Par défaut, la technologie du pare-feu "stateful inspection" de Symantec empêche un attaquant d'accéder au port TCP/445 sur les systèmes internes et aux portes dérobées sur les systèmes infectés (TCP/113, TCP/3067, ou tout autre port aléatoire). Nous conseillons vivement aux administrateurs de vérifier que leurs stratégies de sécurité n'autorisent pas les connexions entrantes sur TCP/445, TCP/113, TCP/3067. Nous conseillons également d'utiliser la fonctionnalité AVpe de SGS 300 Series pour vérifier que les clients AV disposent des dernières définitions de virus.

## **Symantec Firewall/VPN 100/200 Series**

Par défaut, la technologie du pare-feu "stateful inspection" de Symantec empêche un attaquant d'accéder au port TCP/445 sur les systèmes internes et aux portes dérobées sur les systèmes infectés (TCP/113, TCP/3067 ou tout autre port aléatoire).

## **Symantec ManHunt**

Le 13 avril 2004, la [Mise à jour de sécurité 22](#) a été publiée afin de détecter toutes les tentatives d'exploitation de la vulnérabilité LSASS, portant la signature "Microsoft RPC LSASS DS Request". Dès l'apparition de W32.Korgo.F worm, les clients disposant de Symantec ManHunt bénéficiaient déjà d'une protection contre cette vulnérabilité.

recommandations

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

#### passerelle

##### Symantec Enterprise Firewall

- Assurez-vous que votre stratégie de sécurité ne permette pas les connexions entrantes sur les ports TCP 445, 113 et 3067.

##### Symantec Gateway Security

- Exécutez LiveUpdate sur le boîtier afin d'obtenir les dernières définitions de virus et IDS/IPS.
- Assurez-vous que votre stratégie de sécurité ne permette pas les connexions entrantes sur les ports TCP 445, 113 et 3067.
- Si votre stratégie de sécurité exige que vous autorisiez l'accès au port TCP/445 (Microsoft Networking), assurez-vous d'activer GATING (IPS) pour la signature contre l'attaque LSASS de MS.

##### Symantec Clientless VPN

- Assurez-vous de ne pas disposer d'une règle autorisant TCP 445, 113 ou 3067 sur les systèmes internes.
- Assurez-vous que vos utilisateurs exécutent bien LiveUpdate sur tous les périphériques des utilisateurs finaux.

##### Symantec Gateway Security 300 Appliance

- Assurez-vous que votre stratégie de sécurité NE PERMETTE PAS les connexions entrantes sur les ports TCP 445, 113, 3067 (ceci est bloqué par défaut).
- Configurez la fonctionnalité de mise en application des stratégies AV sur vos passerelles afin de vous assurer que vos postes Symantec Antivirus Corporate Edition et Symantec Client Security disposent bien des dernières définitions de virus.
- Exécutez LiveUpdate sur vos clients AV de bureau et invitez tous vos utilisateurs à effectuer une analyse complète de leurs postes.

##### Symantec Firewall / VPN Appliance

- Assurez-vous que votre stratégie de sécurité NE PERMETTE PAS les connexions entrantes sur les ports TCP 445, 113, 3067 (ceci est bloqué par défaut).
- Exécutez LiveUpdate sur vos clients AV de bureau et invitez tous vos utilisateurs à effectuer une analyse complète de leurs postes.

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 attaqués 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 de mot de passe. Sur les ordinateurs compromis, il est plus difficile de récupérer 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 .v, .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.
- Exhortez les employés à n'ouvrir que les pièces jointes attendues. Aussi, n'exécutez aucun log 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.Korgo

Symantec Security Response a créé un [outil de suppression](#) pour nettoyer toutes les infections de W32.Korgo.F. Essayez cet outil en premier lieu, il représente le moyen le plus simple pour éliminer ce menace.

## Suppression manuelle

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

1. Désactiver l'option de restauration du système (Windows Me/XP)
2. Actualiser les définitions de virus.
3. Redémarrez l'ordinateur en mode sans échec ou en mode VGA.
4. Exécuter une analyse complète du système et éliminez tous les fichiers détectés comme W32.Korgo.F.
5. Rétablir les modifications apportées au registre.

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

### 1. 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 pc restaurer des fichiers sur votre ordinateur, s'ils venaient à être endommagés. Si un ordinateur a été in 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 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 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 anti-virus ne peuvent pas nettoyer les fichiers infectés dans le dossier \\_Restore](#) - Numéro de l'article : Q263455

### 2. 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 Protégé 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. 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.Korgo.F, 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 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 :  
  
`"Disk Defragmenter"="%System%\<nom de fichier aléatoire>.exe"`
- e. Accédez à la clé suivante :  
  
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wireless`
- f. Dans le volet de droite, supprimez la valeur :  
  
`"Client"="1"`
- g. Quittez l'Editeur du Registre.
- h. Redémarrez l'ordinateur en Mode normal. Pour obtenir des instructions détaillées, reportez-vous à la section concernant le mode normal dans le document intitulé [Comment démarrer l'ordinateur en mode sans échec](#).

---

**Historique :**

- 2 juin 2004 :
  - Réévaluation du Niveau 2 au Niveau 3 en raison du nombre croissant de virus soumis.
  - Ajout du lien vers l'outil de suppression.
  - Ajout d'actions et de recommandations spécifiques aux produits Symantec.

**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 : Maryl Magee & Neal Hindocha