



## La prévention des fuites dans Outpost Firewall Pro 4.0

### Guide des tests de fuite

---

© 2006 Agnitum Ltd. Tous droits réservés. Agnitum® et Outpost Firewall Pro™ sont des marques commerciales ou des marques déposées de Agnitum Ltd. La copie intégrale ou partielle de cette oeuvre est autorisée, à condition que les copies effectuées ou distribuées ne soient pas destinées à la vente, et que la notice Droits d'auteurs et cette notification y figurent.

## Table des matières

|   |    |
|---|----|
| Présentation du document .....  | 3  |
| Structure du document.....  | 3  |
| Une approche multi-niveau de la sécurité.....   | 3  |
| Outils utilisés pour tester la vigilance du pare-feu .....                            | 5  |
| Nouvelle fonctionnalité de protection des données dans Outpost Firewall Pro 4.0 ..... | 6  |
| Présentation des tests de fuite .....   | 6  |
| Méthodes de vol d'informations.....   | 7  |
| Considérons à présent les tests de fuite à proprement parler .....                    | 8  |
| Test de fuite n°1 « Firewall Leakage Tester » .....                                   | 9  |
| Test de fuite n°2 « TooLeaky » .....  | 10 |
| Test de fuite n°3 « WallBreaker » .....   | 11 |
| Test de fuite n°4 « Ghost » .....   | 12 |
| Test de fuite n°5 « YALTA » .....   | 13 |
| Test de fuite n°6 « DNSTester » .....   | 14 |
| Test de fuite n°7 « FireHole » .....  | 15 |
| Test de fuite n°8 « pcAudit » .....   | 16 |
| Test de fuite n°9 « Comodo Parent Injection Leak Test » .....                         | 17 |
| Test de fuite n°10 « Thermite » .....   | 18 |
| Test de fuite n°11 « Copycat » .....  | 19 |
| Test de fuite n°12 « Atelier Web Firewall Tester » .....                              | 20 |
| Test de fuite n°13 « Surfer » .....   | 21 |
| Test de fuite n°14 « Test de fuite PCFlank » .....                                    | 22 |
| Test de fuite n°15 « Breakout » .....   | 23 |
| Test de fuite n°16 « MBtest » .....   | 24 |
| Test de fuite n°17 « OutBound » .....   | 25 |
| Test de fuite n°18 « Jumper » .....   | 26 |
| Quelques mots d'Agnitum.....  | 27 |
| Conclusion .....  | 27 |
| Contacts .....  | 27 |

## Présentation du document

Outpost Firewall Pro 4.0 est le premier pare-feu personnel proposant une technologie anti-fuite spécialement conçue pour empêcher les programmes malveillants de transmettre des informations à partir d'un ordinateur protégé en détournant les autorisations d'accès d'une application sécurisée.

Ce document se concentre sur la protection englobante fournie par Outpost Firewall Pro 4.0 pour éviter la fuite d'informations personnelles et confidentielles depuis votre PC, tombant alors entre les mains de pirates informatiques et de cyber criminels. Des exemples avérés montrent que Outpost Firewall Pro 4.0 passe avec succès tous les tests de fuite tiers reconnus, offrant aux utilisateurs de PC raccordés à Internet une sécurité supplémentaire non négligeable.

## Structure du document

Ce document contient toutes les informations nécessaires aux utilisateurs d'ordinateurs personnels pour comprendre la sécurité système – en particulier les pare-feu – et la façon dont les outils tiers sont utilisés pour évaluer l'efficacité des pare-feu à protéger les utilisateurs contre la fuite d'informations.

Le document est divisé en trois parties :

1. La première partie propose un aperçu de la situation actuelle de la sécurité des ordinateurs basés Windows, le rôle et les fonctionnalités des pare-feu personnels, et les différences de Outpost Firewall Pro par rapport aux autres pare-feu personnels.
2. Vous trouverez au coeur du document les résultats d'une série de tests de fuite appliqués à Outpost Firewall Pro, et destinés à vérifier les capacités de filtrage en sortie du pare-feu. Chaque ensemble de résultats est accompagné d'explications graphiques et d'un bref commentaire rédigé dans un langage de tous les jours, non technique.
3. La partie finale du document est constituée d'une brève interview d'Alexey Belkin, architecte logiciel en chef chez Agnitum, qui explique les raisons qui l'ont décidé à intégrer cette puissante protection anti-fuite dans Outpost Firewall Pro 4.0.

## Une approche multi-niveau de la sécurité

Nous avons tous des informations importantes stockées sur nos PC, il est donc important de réfléchir à la façon de les protéger de manière sûre. Internet est infesté de logiciels malveillants conçus pour voler des informations personnelles – comme des mots de passe, des informations de compte bancaire ainsi que d'autres données confidentielles sans que l'utilisateur en ait conscience. Les données sont ensuite transmises par téléphone aux pirates informatiques et autres cyber criminels.

La vulnérabilité de ces informations signifie qu'il est vital aux utilisateurs d'ordinateurs de pouvoir contrôler comment et quelles informations sont autorisées à quitter l'ordinateur ; ils doivent pouvoir surveiller les connexions vers l'extérieur, de façon à empêcher tout transfert de données non autorisé.

Tandis que les programmes anti-virus et anti-logiciels espions peuvent détecter et supprimer des programmes malveillants téléchargés sur un PC depuis Internet, le rôle d'un pare-feu est plus vaste. Les pare-feu empêchent la connexion des programmes malveillants à Internet, servent de point de contrôle virtuel pour les données en transit et acceptent uniquement les connexions autorisées. Même si un virus ou un logiciel espion parvient à se frayer un chemin dans l'ordinateur de l'utilisateur, le pare-feu peut empêcher ce dernier de communiquer ou de se propager en dehors de la machine infectée. L'efficacité de la reconnaissance des nouveaux types de menaces par les anti-virus et anti-logiciels espions dépend de la régularité des mises à jours des signatures : les créateurs de logiciels malveillants sont donc toujours aux commandes. Le pare-feu sert à protéger les ordinateurs des risques de dommages générés par les nouvelles menaces des logiciels malveillants, tandis que les vendeurs d'anti-virus et d'anti-logiciels espions préparent leurs mises à jour.

Windows XP, en particulier avec le Service Pack 2, fournit une protection relativement efficace – la mise à jour de la sécurité a aidé à éliminer la plupart des brèches précédemment utilisées par les logiciels malveillants pour compromettre le système, et son pare-feu intégré a été amélioré afin de mieux riposter

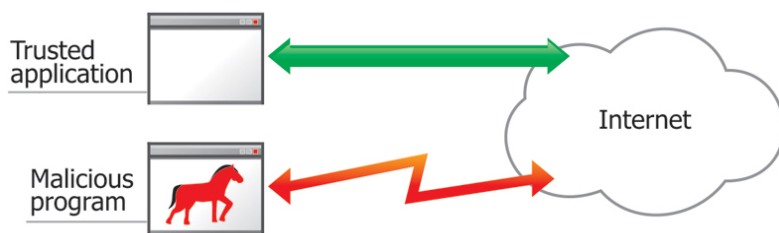
face aux nouvelles menaces. Ces réalisations sont malheureusement insuffisantes pour contrer les failles de sécurité présentes dans le système d'exploitation lui-même.

Tout d'abord, le pare-feu intégré de Windows XP néglige la protection des connexions vers l'extérieur. Tout transfert de données vers l'extérieur est présumé sûr et autorisé par défaut – ce qui n'est pas toujours un bon postulat, comme en témoigne la récente recrudescence du nombre de logiciels espions, de programmes de porte dérobée, de l'activité des machines zombies, et d'autres menaces à l'encontre de la sécurité des informations stockées sur les systèmes Windows XP.

En second lieu, Windows XP est conçu de telle sorte qu'il autorise un programme installé sur l'ordinateur à communiquer sans restriction, échanger des données et partager des composants internes avec d'autres programmes, leur donnant une légitimité totale. En cliquant par exemple sur un lien hypertexte dans un email, le navigateur par défaut est démarré et le lien spécifié est ouvert. Cela s'effectue automatiquement sans avoir besoin de lancer manuellement le navigateur et de saisir l'URL. D'un côté, cela simplifie la tâche, mais d'un autre, la sécurité du système s'en trouve amoindrie – un programme malveillant peut invoquer et exécuter une application légitime de façon rigoureusement identique, sans qu'aucune question ne soit posée. De nombreux pare-feu tiers, y compris le pare-feu intégré à Windows XP, sont incapables de détecter de tels agissements furtifs et permettent aux logiciels malveillants d'utiliser la connexion Internet de l'ordinateur.

Ci-dessous, trois scénarios présentant le niveau de protection d'un ordinateur en fonction de la configuration du pare-feu :

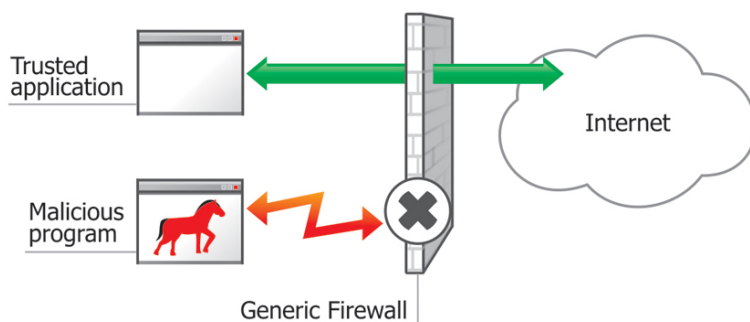
### 1. Sans pare-feu



L'accès au réseau et à Internet est autorisé sans aucune restriction. Les données légitimes (flèches vertes) et non autorisées (flèches rouges) peuvent accéder et quitter librement l'ordinateur. Les connexions (ports) de l'ordinateur sont exposées à n'importe quel type d'accès en entrée ou en sortie.

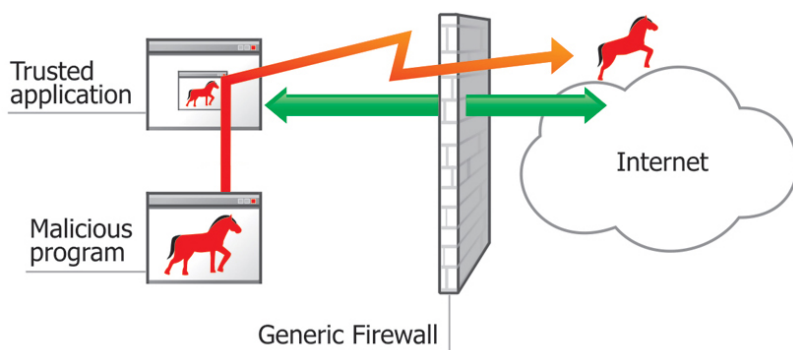
### 2. Windows XP ou autre pare-feu de base

a) Les programmes malveillants ne peuvent pas envoyer directement les données



Ce type de pare-feu effectue un filtrage basique du trafic vers l'extérieur. Par exemple, il détectera et empêchera les programmes malveillants – comme les chevaux de Troie – de transmettre à un pirate informatique des informations non autorisées. Il serait toutefois incapable de détecter ce même programme malveillant s'il s'infiltrait dans une application sécurisée et s'il envoyait des données à partir de l'ordinateur en utilisant les autorisations d'accès de cette dernière (voir plus bas).

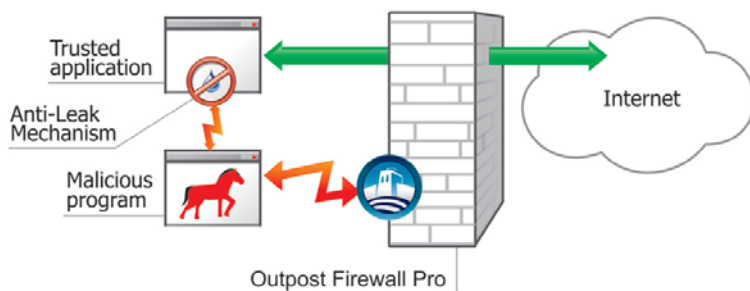
b) Un programme malveillant parvient à transmettre des données en détournant les autorisations d'une application sécurisée



Si le chemin direct est bloqué par le pare-feu, le programme malveillant essaiera ensuite de détourner une application sécurisée et d'utiliser ses autorisations pour sortir des données de la machine, en trompant le pare-feu.

Les pare-feu classiques sont incapables de détecter des communications suspectes entre des programmes, permettant ainsi aux programmes malveillants de se connecter au site pirate désigné, d'où la mise en danger des informations personnelles.

### 3. Outpost Firewall Pro



Les contrôles anti-fuite évolués de Outpost Firewall Pro ne se contentent pas de détecter et d'éviter que des applications malveillantes n'envoient des données directement à partir de la machine. Outpost Firewall Pro v4.0 surveille également l'activité entre les applications, assurant que les logiciels malveillants ne puissent pas utiliser les autorisations des applications pour transmettre des données à partir du PC.

L'association de ces deux fonctions offre une protection multi-niveau contre la fuite délictueuse des informations personnelles.

Vous trouverez un peu plus loin des informations sur les techniques utilisées par les pirates informatiques pour essayer de faire passer des données à travers les défenses externes des pare-feu, et sur la façon dont Outpost 4.0 protège les utilisateurs contre chacune d'entre elles, sans exception.

### Outils utilisés pour tester la vigilance du pare-feu

Comme indiqué précédemment, les pare-feu doivent être en mesure de surveiller l'activité vers l'extérieur des programmes. Même si un programme tente de se faire passer pour une autre application qui a été préconfigurée comme « approuvée » par le pare-feu, un pare-feu compétent doit pouvoir détecter ce détournement d'application et empêcher les données d'être transmises ainsi depuis le PC.

La communauté de sécurité des informations a développé des outils spéciaux pour tester la capacité des pare-feu à reconnaître l'interactivité des programmes non autorisés et empêcher les programmes malveillants de se connecter au réseau en utilisant l'ID d'un programme légitime. Baptisés « tests de fuite », ces outils logiciel simulent une tentative d'envoi de données depuis un PC par un logiciel malveillant,

de telle sorte que l'utilisateur voit la façon dont son pare-feu peut réagir face à une telle menace.

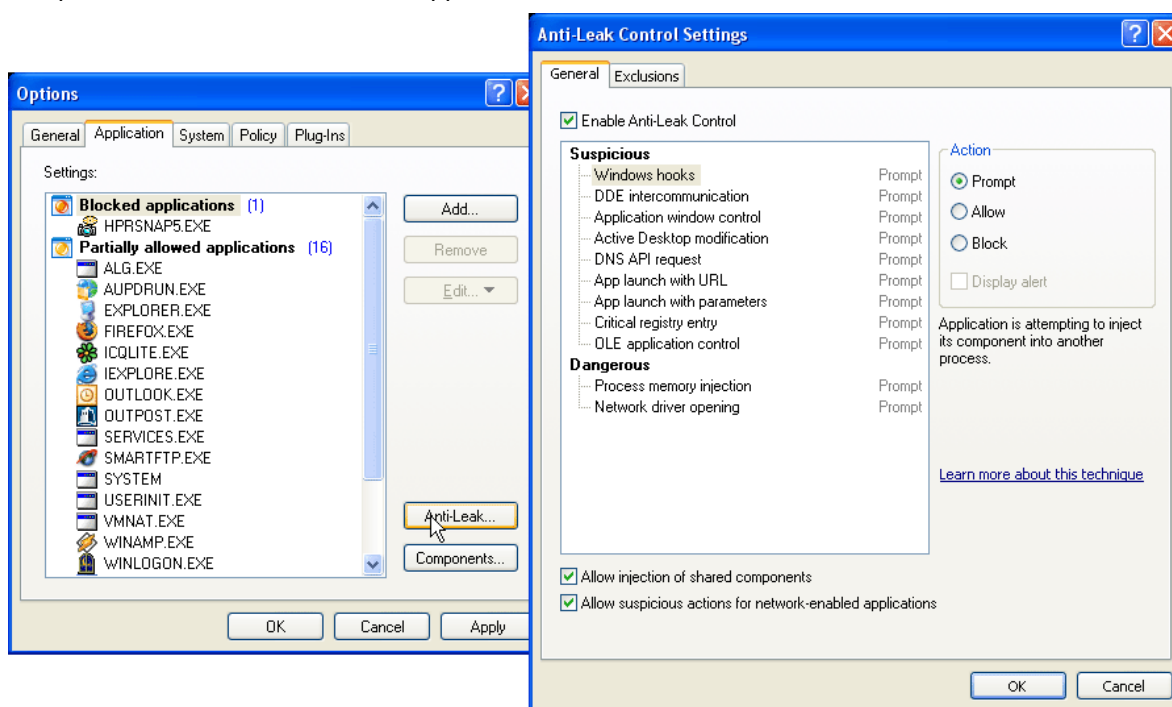
Les tests de fuite utilisent toute une variété de techniques et de mécanismes pour tester la capacité d'un pare-feu à empêcher les transmissions non autorisées de données vers l'extérieur. Il s'agit d'utilitaires légitimes qui envoient uniquement des informations permises par l'utilisateur aux emplacements tests isolés, et incapables d'endommager le système.

Certaines personnes affirment que les tests de fuite ne sont pas des situations réelles, et qu'ils ne représentent donc que des exemples de laboratoire. Mais comme les techniques qu'ils utilisent peuvent être et ont été utilisées par des programmes malveillants actuels, ils sont un précieux indicateur de la capacité réelle des pare-feu à faire face aux attaques.

## Nouvelle fonctionnalité de protection des données dans Outpost Firewall Pro 4.0

Outpost 4.0 offre un certain nombre d'améliorations conçues pour enrayer définitivement le vol de données, comprenant un total de douze nouvelles fonctions anti-fuite.

Dans l'onglet Application de la fenêtre Options d'Outpost, une nouvelle option « Anti-fuite » a été ajoutée, grâce à laquelle vous pouvez régler le niveau de protection vers l'extérieur contre les comportements non autorisés des applications :



Vous verrez un peu plus tard la façon dont ces nouvelles fonctions travaillent dans le contexte de différents tests de fuite pour fournir à votre PC la protection multi-niveau indispensable d'Outpost.

## Présentation des tests de fuite

Pour obtenir des informations détaillées sur les tests de fuite, consultez [Firewall Leak Tester](#) et [PC Flank](#). Le nombre de tests de fuite augmente en permanence, ainsi que leur capacité et leur sophistication dans l'utilisation de nouvelles techniques de passage à travers le pare-feu. Les développeurs de logiciels pare-feu tels qu'Agnitum testent constamment leurs produits en s'appuyant sur des tests de fuite courants, un peu comme un nouveau modèle de voiture dont la maniabilité et la performance sont testées sur une piste de course avant de pouvoir être commercialisé.

Même s'il est en mesure de passer tous les tests de fuite courants, cela ne signifie pas que votre pare-feu

est sûr à 100 pour cent (aucune garantie n'est donnée au niveau de la sécurité), mais tout porte à croire qu'il sera capable de résister face aux tentatives déterminées de vols de données. Comme vous pouvez le constater sur les sites indiqués ci-dessus, aucun pare-feu n'a encore pu passer tous les tests de fuite existants – jusqu'à ce jour. Outpost Firewall Pro v4.0 passe chaque test sans aucune hésitation – une bonne indication sur sa capacité à mettre les pirates informatiques en échec.

Mais commençons par examiner les différentes méthodes utilisées par les pirates informatiques pour tenter de voler des informations sur votre PC.

## Méthodes de vol d'informations

Les tests de fuite étant basés sur différentes techniques (ou une combinaison de techniques) pour obtenir des informations à travers les défenses externes des pare-feu, cette partie présente une liste des techniques existantes et examine en détail tous les tests de fuite, notant à chaque fois la façon dont Outpost reconnaît et riposte face aux attaques simulées.

### Technique de fuite n°1 « Substitution de nom de fichier »

Cette approche représente l'un des types d'attaques les plus faciles à combattre. Elle utilise un programme qui se renomme afin de porter le même nom que celui d'un programme légitime de l'ordinateur, et qui accède à Internet en se faisant passer pour un bon programme.

### Technique de fuite n°2 « Application lancée par le biais d'une URL »

Les programmes utilisant cette technique démarrent un programme tiers ayant accès à Internet (généralement un navigateur web) avec l'URL du site auquel il doit se connecter. Le processus peut se dérouler dans une fenêtre masquée pour cacher l'activité à l'utilisateur.

### Technique de fuite n°3 « Manipulation avec des règles approuvées »

Une technique rarement utilisée mais efficace qui implique un programme exploitant la manière dont le pare-feu traite les règles d'autorisation d'accès dans le système. Pour ce faire, le test tente d'accéder à des ports approuvés à l'aide du pare-feu et transmet un trafic non autorisé par son intermédiaire.

### Technique de fuite n°4 « Requête DNS usurpée »

La conversion d'adresses DNS est utilisée pour diriger une application capable de se connecter à Internet vers une adresse IP numérique correspondante relative au serveur cible distant. Elle convertit une adresse de nom d'hôte fournie par l'utilisateur (par ex. [www.agnitum.fr](http://www.agnitum.fr)) en une adresse IP, de telle sorte que la machine peut comprendre la commande et accéder au site demandé (par ex. 67.15.103.130). La technique de la requête DNS usurpée signifie que des données sensibles sont communiquées à un serveur DNS détourné ou illégal sous les traits d'une requête DNS normale.

### Technique de fuite n°5 « Injection de composant »

Cette technique est utilisée lorsqu'un programme malveillant lance une autre application sur un ordinateur et injecte son composant interne ou un fichier .DLL dans le processus cible. Le composant injecté demande ensuite à l'application capturée d'accéder au réseau, essayant ainsi de tromper le pare-feu.

### Technique de fuite n°6 « Injection de processus »

Tout comme le processus d'injection d'un composant dans un programme approuvé, une application malveillante peut injecter son contenu complet dans le bloc mémoire d'une application approuvée, ouvrant une nouvelle branche du processus parent et accédant au réseau avec les accès d'autorisation du programme approuvé.

### Technique de fuite n°7 « Intercommunication DDE »

Cette technique est utilisée par un programme pour envoyer des commandes à un autre (généralement un navigateur) qui les exécutera. Grâce à l'appel de procédure DDE, les programmes peuvent gérer et partager des contenus les uns avec les autres. La technique DDE du contrôle d'application dans un test de fuite est utilisée pour vérifier si le pare-feu peut reconnaître un programme utilisant l'interaction DDE pour contrôler l'activité d'une application capable de se connecter à Internet.

### **Technique de fuite n°8 « Utilisation d'OLE pour contrôler des applications »**

Une approche relativement récente qui utilise le mécanisme de contrôle inter-programme OLE (abréviation de la commande « Object Linking and Embedding », liaison et incorporation d'objets) dans les tests de fuite. OLE est un mécanisme Windows qui permet à un programme de gérer le comportement d'un autre programme.

### **Technique de fuite n°9 « Contrôle de fenêtres d'application via des messages Windows »**

Une application peut contrôler le contenu et les commandes d'autres fenêtres par le biais de messages Windows. Certains tests de fuite utilisent cette technique pour contrôler l'activité d'applications capables de se connecter au Web et accéder ainsi au réseau par leur intermédiaire.

### **Technique de fuite n°10 « Accès direct à l'interface réseau »**

Si le principe de l'accès direct à l'interface réseau est utilisé, le test crée une couche réseau supplémentaire en injectant dans le système le pilote du périphérique correspondant ; il envoie/réceptionne le trafic par cette couche, en évitant les canaux de communication standard contrôlés par le pare-feu. Cette technique permet au test de fuite (ou n'importe quelle autre application) d'envoyer et de réceptionner des données, compliquant le processus de filtrage des données via le pare-feu. C'est un peu complexe dans l'environnement Windows XP, car le réglage de la configuration système nécessite une certaine dextérité au niveau du testeur, mais c'est un bon moyen de tester la robustesse d'un pare-feu.

### **Technique de fuite n°11 « Accès via la modification de Windows Active Desktop »**

Les tests de fuite peuvent créer une page HTML renvoyant vers un site Web particulier et le définir comme étant un Windows Active Desktop (AD). Si l'AD est activé, il est autorisé à se rendre à l'adresse du site Web contenue sur la page HTML, agissant au nom du système et évitant ainsi les détecteurs du pare-feu.

### **Technique de fuite n°12 « Modification de la base de registre système »**

La base de registre est un référentiel universel des paramètres du système et de la configuration des programmes. La modification de son contenu peut engendrer des erreurs dans les applications, voire une défaillance du système. Les tests de fuite utilisant cette technique apportent de petites modifications aux éléments de la base de registre, permettant à un processus non vérifié d'accéder au réseau sans aucune restriction, et ce malgré la présence d'un pare-feu, en ajoutant ses composants aux applications et en agissant en leur nom.

## **Considérons à présent les tests de fuite à proprement parler**

Nous allons maintenant observer attentivement l'un après l'autre les différents tests de fuite et examiner la façon dont réagit Outpost Firewall Pro 4.0. Les tests de fuite sont triés en fonction de la technique qu'ils utilisent, et un bref commentaire accompagne les résultats de chaque test.

Il existe actuellement dix-huit tests de fuite et nous avons testé Outpost avec chacun d'entre eux. C'est parti.

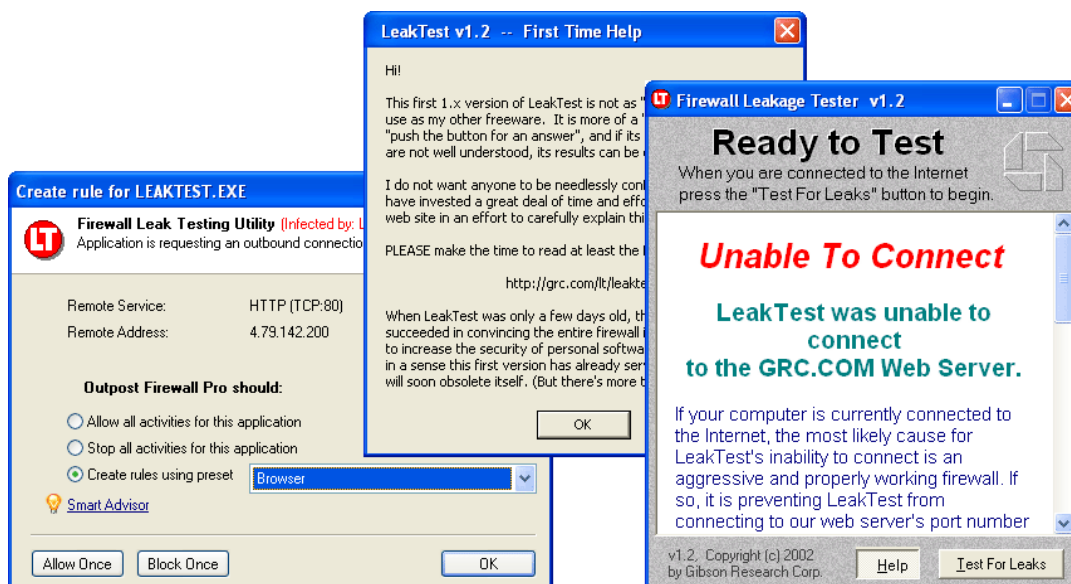
## Test de fuite n°1 « Firewall Leakage Tester »

| Nom/liens de téléchargement direct                      | Technique de détournement utilisée | Infos sur les tests de fuite/page d'accueil  | Fonction Outpost utilisée            |
|---|------------------------------------|--|--------------------------------------|
| <a href="#">Firewall Leakage Tester (test de fuite)</a> | Substitution de nom de fichier     |  LeakTest.exe<br>Firewall Leak Testing Utility<br>Gibson Research Corp. | Vérification de l'empreinte digitale |

C'est un test de fuite facile à passer qui utilise la technique de **substitution de nom de fichier** pour tester le pare-feu.

Le test tente de se renommer comme étant l'un des programmes autorisés d'un ordinateur (Internet Explorer par ex.) et utilise ce nom pour établir une connexion vers l'extérieur avec un serveur distant. Ce test met en échec les pare-feu se basant uniquement sur le nom de fichier pour identifier une application et ne procédant pas à une évaluation plus minutieuse (par ex. une vérification des empreintes digitales). Certains pare-feu échouent à ce test, bien qu'il soit assez facile.

La réaction de Outpost :





Outpost fait correspondre le nom d'un programme avec son identificateur unique ou ses empreintes digitales. SHA256 est utilisé pour identifier les applications par le biais de pré-règlages actualisés, et l'identification MD5 est effectuée pour identifier les applications dans les ensembles de règles de programmes actifs, bloquant la connexion du programme déguisé.

Pour l'utilisateur, cela signifie que toute application malveillante ou indésirable qui sollicite un accès vers l'extérieur en essayant d'incarner une application légitime sera détectée par Outpost, et l'utilisateur sera invité à autoriser ou refuser la connexion.

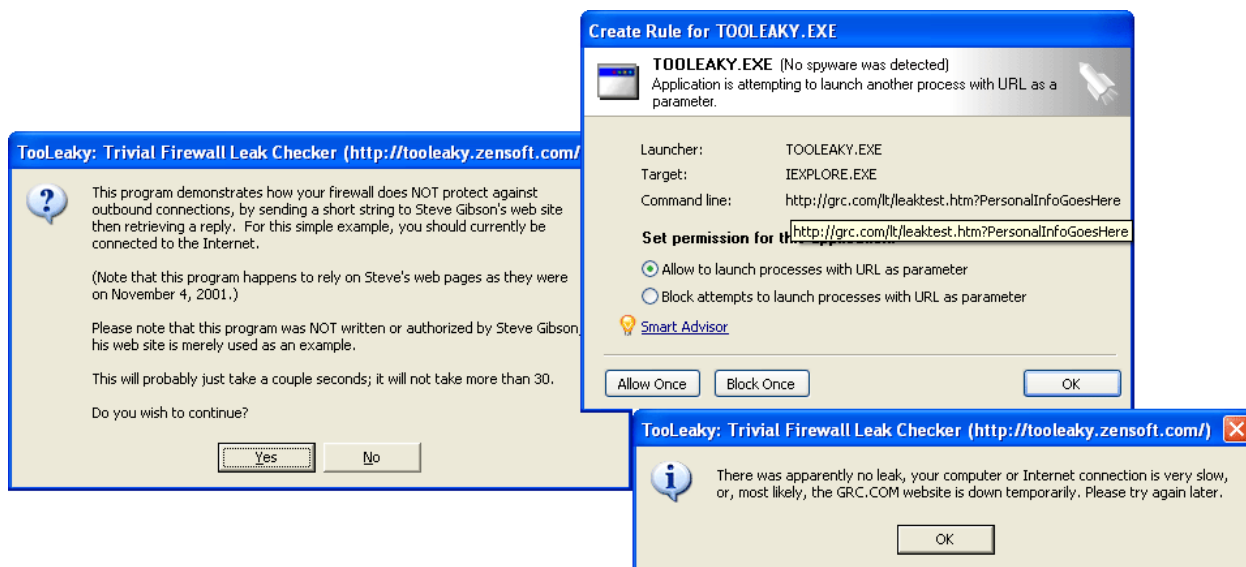


## Test de fuite n°2 « TooLeaky »

| Nom/liens de téléchargement direct | Technique de détournement utilisée                 | Infos sur les tests de fuite/page d'accueil  | Fonction Outpost utilisée  |
|------------------------------------|--|--|--|
| <a href="#">TooLeaky</a>           | Lancement d'une application par le biais d'une URL |  tooleaky.exe | « Lancement appl avec URL »<br> |

Ce test de fuite est une version légèrement plus évoluée du test précédent : il lance le navigateur Web par défaut avec une adresse Web préconfigurée dans une fenêtre masquée, dans le but de faire croire au pare-feu qu'une action légitime est en cours. Les pare-feu qui, par défaut, font confiance à une application sans chercher à savoir qui l'a réellement lancée au départ et quels sont les paramètres de connexion supplémentaires fournis échouent à ce test.

La réaction de Outpost :



The image displays three overlapping windows from the Outpost Firewall Pro interface:



- Top Window:** "Create Rule for TOOLEAKY.EXE". It shows a rule for "TOOLEAKY.EXE" with the target "IEXPLORE.EXE" and a command line containing a URL. The "Set permission for this rule" section has "Allow to launch processes with URL as parameter" selected.
- Middle Window:** "TooLeaky: Trivial Firewall Leak Checker (http://tooleaky.zensoft.com/)". It contains explanatory text and a "Do you wish to continue?" prompt with "Yes" and "No" buttons.
- Bottom Window:** A message box stating: "There was apparently no leak, your computer or Internet connection is very slow, or, most likely, the GRC.COM website is down temporarily. Please try again later." with an "OK" button.

Le contrôle anti-fuite « Lancement appl avec URL » d'Outpost détecte les applications qui tentent de démarrer un programme avec une URL cible et invite ensuite l'utilisateur à autoriser ou non cette activité pour un programme particulier.

Pour l'utilisateur, cela signifie qu'Outpost surveille chaque programme démarré sur un ordinateur et contrôle les autorisations de démarrage des programmes ayant accès à Internet, peu importe que la requête du programme soit légitime ou non.

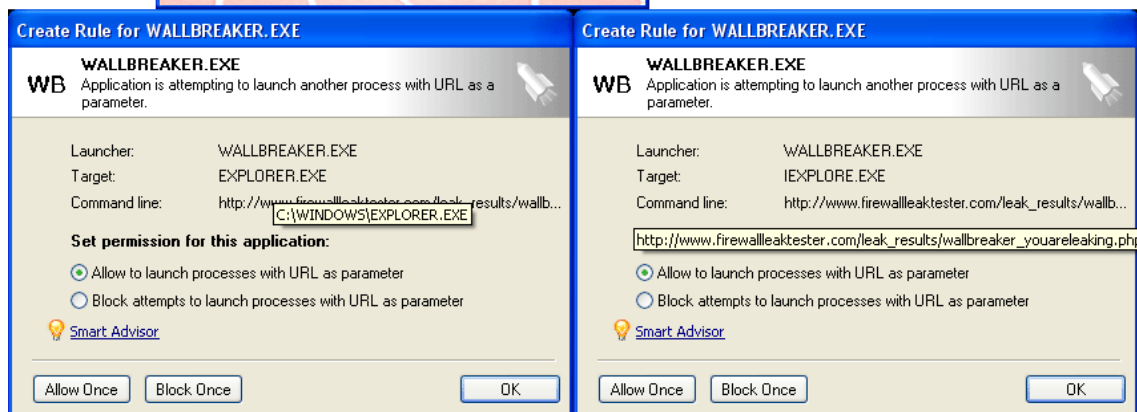
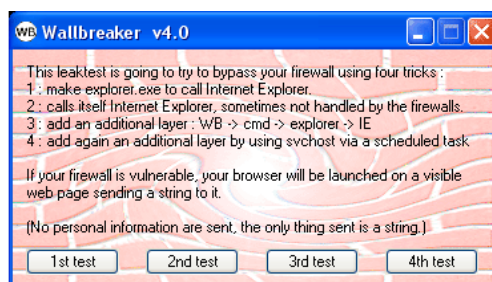
**PASSÉ**

### Test de fuite n°3 « WallBreaker »

| Nom/liens de téléchargement direct | Technique de détournement utilisée                 | Infos sur les tests de fuite/page d'accueil   | Fonction Outpost utilisée  |
|------------------------------------|--|---|--|
| <a href="#">WallBreaker</a>        | Lancement d'une application par le biais d'une URL |  WallBreaker.exe | « Lancement appl avec URL »<br> |

WallBreaker comprend plusieurs tests faisant appel à une variété de techniques pour tester l'efficacité de la défense externe du pare-feu. Il tente de dissimuler la séquence de lancement d'un programme et de masquer l'identité de l'application à l'origine dans une chaîne d'événements de lancement de programmes. L'objectif consiste à embrouiller suffisamment le pare-feu avec des commandes d'appel de programme superposées, de manière à ce que le pare-feu perde la trace de celui qui a effectivement lancé le programme approuvé. Il lance également un programme approuvé par l'intermédiaire d'une commande prédéfinie dans sa barre d'adresse, dans une fenêtre masquée.

La réaction de Outpost :



Outpost Firewall Pro détecte facilement toutes les tentatives des tests de WallBreaker pour tromper le pare-feu, protégeant ainsi efficacement l'ordinateur contre ces types de lancement.

**PASSÉ**

## Test de fuite n°4 « Ghost »

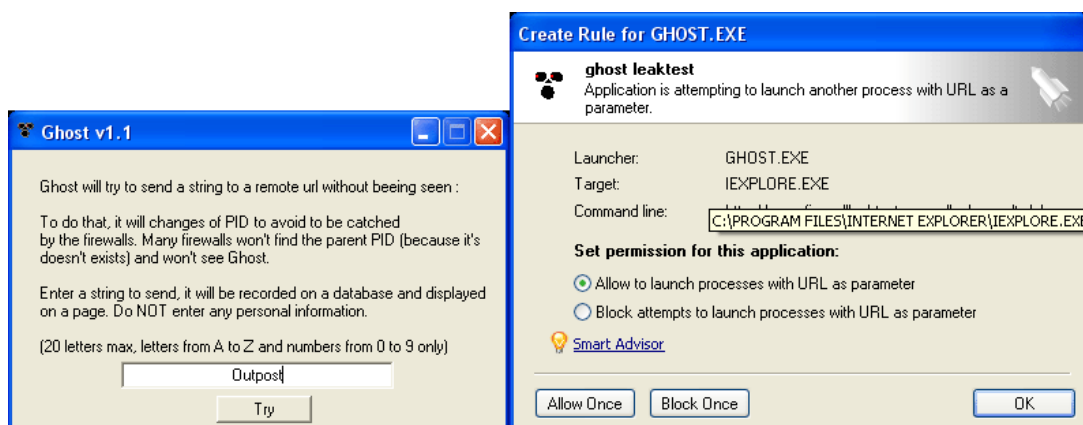
| Nom/liens de téléchargement direct | Technique de détournement utilisée                 | Infos sur les tests de fuite/page d'accueil  | Fonction Outpost utilisée  |
|------------------------------------|--|--|--|
| <a href="#">Ghost</a>              | Lancement d'une application par le biais d'une URL |  Ghost.exe<br>ghost leaktest<br>gkweb | « Lancement appl avec URL »<br> |

Le test de fuite « Ghost » utilise les techniques du lanceur en association avec l'adresse URL et la manipulation du PID (Process Identifier, identificateur du processus).

Le PID est un identificateur unique assigné à chaque processus ou programme démarré sur un ordinateur basé Windows. Il est utilisé par le système pour reconnaître les tâches actives en cours.

Le test de fuite « Ghost » change continuellement son PID en s'ouvrant et se fermant rapidement plusieurs fois de suite. L'objectif consiste à noyer le pare-feu sous différents numéros PID pour une même application, avec pour but d'empêcher le pare-feu d'être en mesure de reconnaître le processus d'origine.

La réaction de Outpost :



Pour l'utilisateur, cela signifie que Outpost peut détecter une application qui tente de désorienter le pare-feu en changeant son numéro PID. Outpost demandera simplement à l'utilisateur s'il autorise une application changeant constamment son identité à accéder à Internet, soit directement, soit via un programme tiers capable de se connecter à Internet.

**PASSÉ**

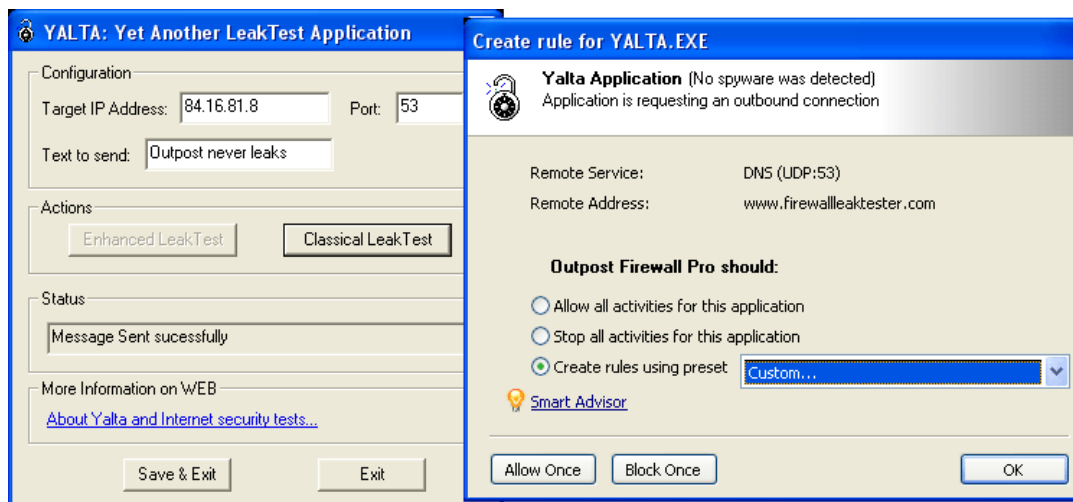
## Test de fuite n°5 « YALTA »

| Nom/liens de téléchargement direct                        | Technique de détournement utilisée      | Infos sur les tests de fuite/page d'accueil   | Fonction Outpost utilisée               |
|---|---|---|---|
| <a href="#">YALTA</a> (Yet Another Leak Test Application) | Manipulation avec des règles approuvées |  Yalta.exe<br>Yalta Application<br>Soft4Ever | Règles globales & accès par application |

Yalta est un test très puissant – il vérifie si le pare-feu est capable de détecter une activité de connexion d'apparence légitime initiée par un programme non autorisé. Pour ce faire, il essaie de transmettre des données en utilisant un protocole d'accès UDP classique via un port 21 (généralement utilisé pour le trafic FTP), afin de faire croire au pare-feu que les données sont transmises en toute légitimité. Il existe également un test évolué (non disponible sur les systèmes Windows XP) qui crée un nouveau pilote réseau et tente de transmettre des données par son intermédiaire, évitant la pile TCP/IP standard contrôlée par un pare-feu.

Les pare-feu qui n'identifient pas l'initiateur d'une connexion autorisée et qui vérifient uniquement si l'activité du programme est conforme à un modèle général de comportement acceptable échouent à ce test.



La réaction de Outpost :



Les captures d'écran ci-dessus indiquent que Outpost vérifie les autorisations d'une application avant de lui permettre d'effectuer une action généralement autorisée, et avertit l'utilisateur lorsqu'un comportement suspect est détecté.

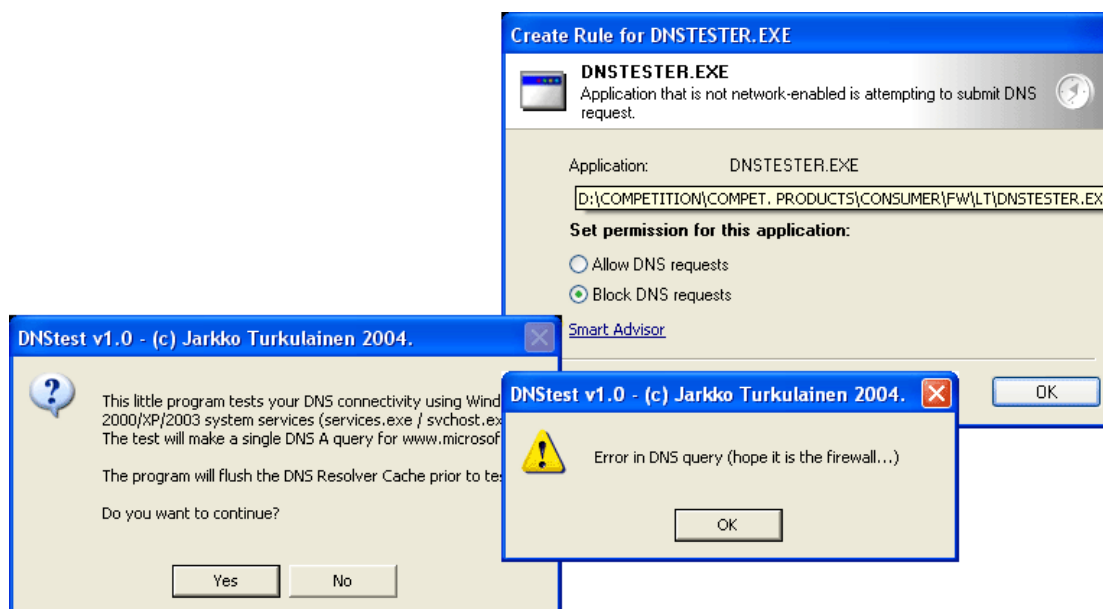
PASSÉ

## Test de fuite n°6 « DNSTester »

| Nom/liens de téléchargement direct | Technique de détournement utilisée | Infos sur les tests de fuite/page d'accueil   | Fonction Outpost utilisée  |
|------------------------------------|------------------------------------|---|--|
| <a href="#">DNSTester</a>          | Requête DNS usurpée                |  dnstester.exe | « Requête API DNS »<br> |

DNSTester utilise des requêtes DNS récursives pour tenter d'envoyer des données en toute discrétion à travers le pare-feu. En usurpant ainsi une requête DNS, DNSTester imite l'approche utilisée par des programmes malveillants pour extraire des données sensibles à partir d'un système, par le biais de requêtes illégitimes vers le service client DNS (svchost.exe). Le rôle du service client DNS consiste à retrouver les adresses DNS résolues par le serveur DNS, de telle sorte que les applications peuvent retrouver rapidement sur Internet les hôtes distants adéquats.



La réaction de Outpost :



Outpost vérifie les autorisations dont dispose l'application pour accéder au service client DNS, et invite l'utilisateur à prendre une décision si une requête non conforme est détectée, protégeant ainsi les utilisateurs contre l'exploitation du service DNS.

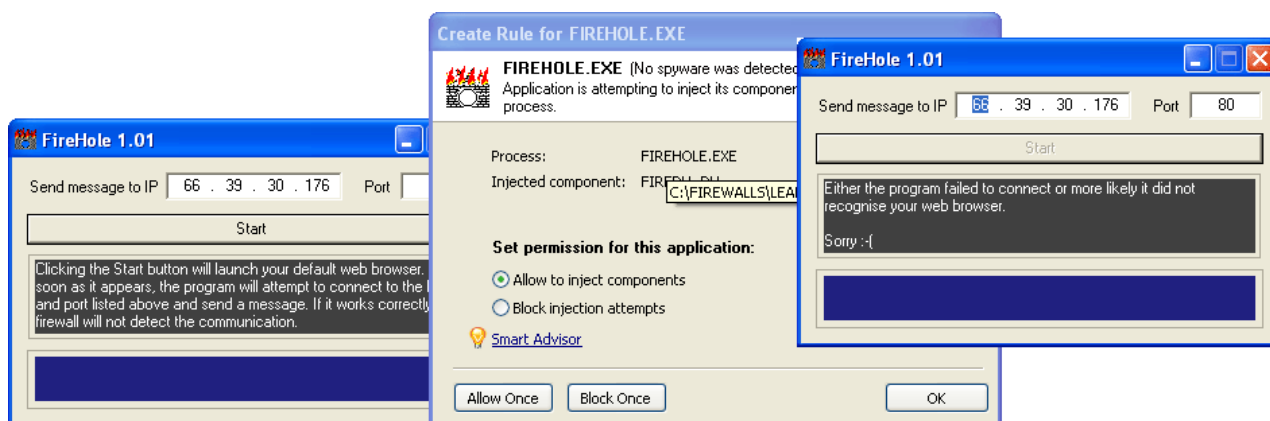
**PASSÉ**

### Test de fuite n°7 « FireHole »

| Nom/liens de téléchargement direct | Technique de détournement utilisée | Infos sur les tests de fuite/page d'accueil  | Fonction Outpost utilisée  |
|------------------------------------|------------------------------------|--|--|
| <a href="#">FireHole</a>           | Injection de composant             |  firehole.exe | « Raccordements Windows »<br> |

Ce test de fuite lance le navigateur Web par défaut et injecte un petit fichier – un fichier exécutable portant une extension DLL (connu en tant que « composant » dans l'application principale) – dans le navigateur, qui ordonne ensuite à ce dernier de se connecter à un serveur distant malveillant. Cette technique est appelée « injection de composant » et n'est pas détectée par les pare-feu qui ne contrôlent pas les modules internes d'une application et les connexions qu'ils établissent.



La réaction de Outpost :



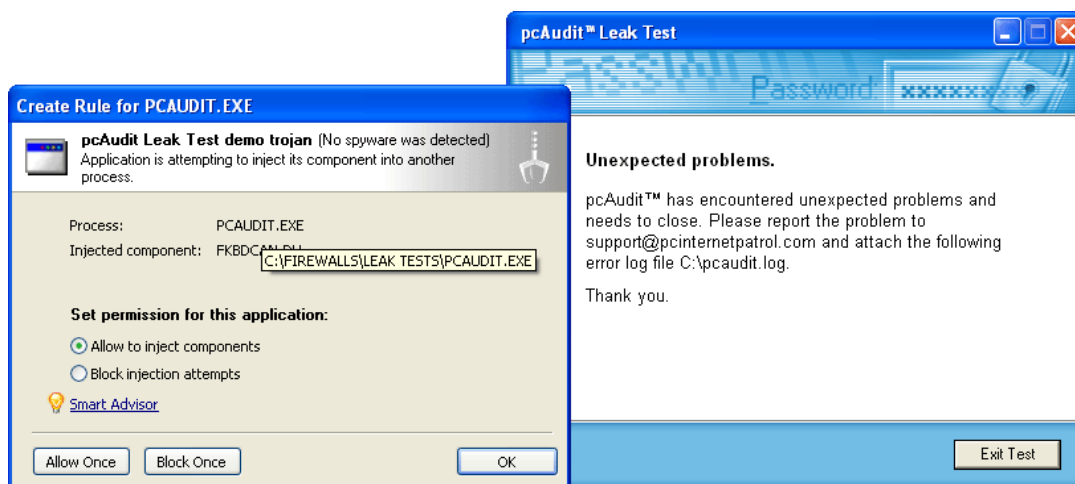
Si Outpost découvre une application tentant d'injecter un bout de code dans un autre processus et d'accéder au réseau par son intermédiaire, l'utilisateur en est averti et décide ensuite d'autoriser ou non le processus.

**PASSÉ**

## Test de fuite n°8 « pcAudit »

| Nom/liens de téléchargement direct | Technique de détournement utilisée | Infos sur les tests de fuite/page d'accueil  | Fonction Outpost utilisée  |
|------------------------------------|------------------------------------|--|--|
| <a href="#">pcAudit</a>            | Injection de composant             |  <p>pcaudit.exe<br/>pcAudit Leak Test demo trojan<br/>Internet Security Alliance, LLC</p> | « Raccordements Windows »<br> |



Le test de fuite pcAudit utilise le même principe que le programme FireHole de la page précédente – en injectant un composant dans l'espace mémoire d'un programme approuvé. Si le test aboutit à un résultat négatif (échec), pcAudit affiche une page de résultats très instructive et facile à comprendre : le bureau de l'utilisateur est affiché accompagné des dernières lignes de texte saisies ainsi que de données clé relatives à l'ordinateur hôte. Si Outpost est actif, la réponse est encore plus simple :



Cela signifie que Outpost est parvenu à empêcher le test de fuite d'envoyer des données à partir de l'ordinateur de l'utilisateur.

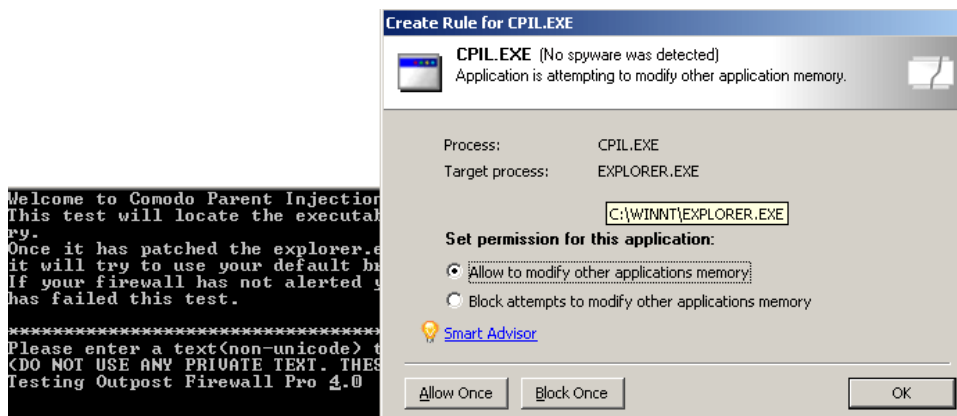
**PASSÉ**

### Test de fuite n°9 « Comodo Parent Injection Leak Test »

| Nom/liens de téléchargement direct                       | Technique de détournement utilisée | Infos sur les tests de fuite/page d'accueil  | Fonction Outpost utilisée   |
|--|------------------------------------|--|---|
| <a href="#">Comodo Parent Injection Leak Test (CPIL)</a> | Injection de processus             |  cpil.exe | « Injection dans la mémoire d'un processus »<br> |

Le test de fuite Comodo est un nouveau programme qui utilise la technique d'injection de composant dans l'Explorateur de Windows (explore.exe) pour accéder au réseau au nom de l'Explorateur. Le test fonctionne uniquement sous Windows 2000 et n'est pas compatible avec Windows XP SP2.



La réaction de Outpost :



Les utilisateurs d'Outpost sous Windows 2000 sont ainsi assurés que Outpost passe sans le moindre problème le test de fuite Comodo Parent Injection.

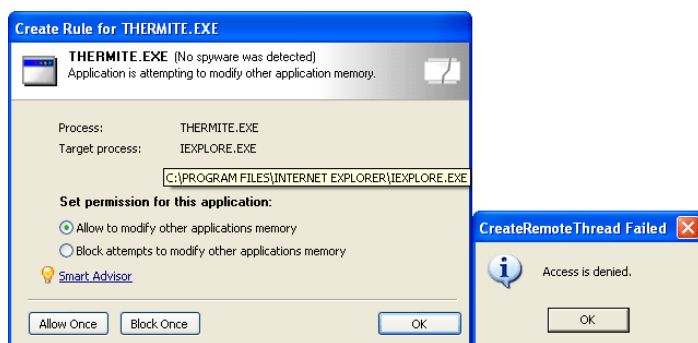
**PASSÉ**

### Test de fuite n°10 « Thermite »

| Nom/liens de téléchargement direct | Technique de détournement utilisée | Infos sur les tests de fuite/page d'accueil  | Fonction Outpost utilisée   |
|------------------------------------|------------------------------------|--|---|
| <a href="#">Thermite</a>           | Injection de processus             |  thermite.exe | « Injection dans la mémoire d'un processus »<br> |

Le test de fuite Thermite utilise une technique pirate sophistiquée pour essayer de contourner la protection du pare-feu. Il injecte tout son code directement dans la mémoire d'un autre processus, créant une nouvelle branche du processus parent et utilisant ce processus pour transmettre des données à travers le pare-feu. Le pare-feu est supposé ne pas remarquer qu'un programme autorisé a été détourné par du code malveillant.



La réaction de Outpost :



La technique employée par Outpost pour surveiller l'interaction des programmes sur un ordinateur lui permet de détecter si un programme tente de prendre le contrôle d'un autre programme et d'accéder au réseau en utilisant ses autorisations. Dans ce cas de figure, l'utilisateur est invité à autoriser ou non l'action.

**PASSÉ**

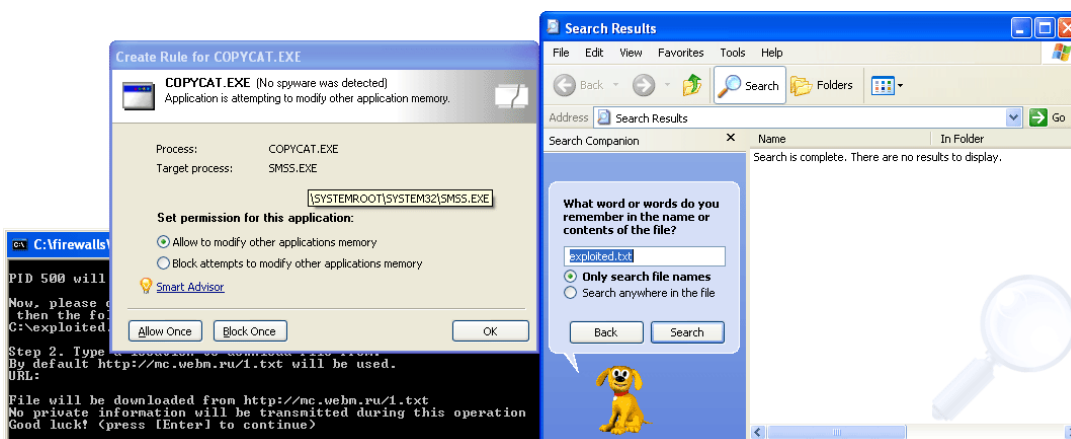
## Test de fuite n°11 « Copycat »

| Nom/liens de téléchargement direct | Technique de détournement utilisée | Infos sur les tests de fuite/page d'accueil   | Fonction Outpost utilisée   |
|------------------------------------|------------------------------------|---|---|
| <a href="#">Copycat</a>            | Injection de processus             |  copycat.exe | « Injection dans la mémoire d'un processus »<br> |

Le test de fuite Copycat est basé sur le même principe que le test de fuite Thermite – injection directe de code étranger dans la mémoire résidente d'un processus non autorisé. Ce test diffère en ce qu'il ne crée pas une nouvelle branche du processus parent, mais opère directement en utilisant le nom du processus détourné.

Si ce test réussit, votre pare-feu est vulnérable aux attaques par injection de processus.



La réaction de Outpost :



Outpost empêche Copycat de s'implanter dans le bloc mémoire d'un programme Windows interne, illustrant sa capacité à surveiller l'interaction des programmes et des processus locaux sur le système de l'utilisateur.

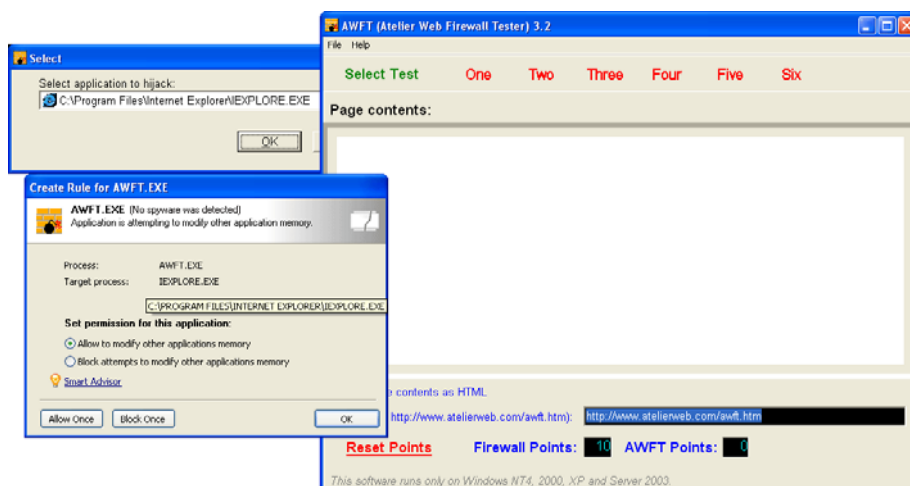
**PASSÉ**

### Test de fuite n°12 « Atelier Web Firewall Tester »

| Nom/liens de téléchargement direct                 | Technique de détournement utilisée | Infos sur les tests de fuite/page d'accueil  | Fonction Outpost utilisée   |
|--|------------------------------------|--|---|
| <a href="#">Atelier Web Firewall Tester (AWFT)</a> | Injection de processus             |  awft.exe | « Injection dans la mémoire d'un processus »<br> |

Le test AWFT comprend une suite de six tests regroupés en un programme. C'est un test très complexe qui combine plusieurs techniques conçues pour mettre les pare-feu en échec : injection de processus directement dans la mémoire d'un processus sécurisé, lancement du navigateur par défaut et modification de son bloc mémoire, création d'une branche supplémentaire dans l'espace mémoire d'un processus approuvé, et d'autres techniques.


La réaction de Outpost :



Le score maximum – indiquant le meilleur pare-feu – est de dix. C'est le résultat de Outpost Firewall Pro 4.0, ce qui signifie qu'il fournit une protection maximale contre les fuites d'informations.

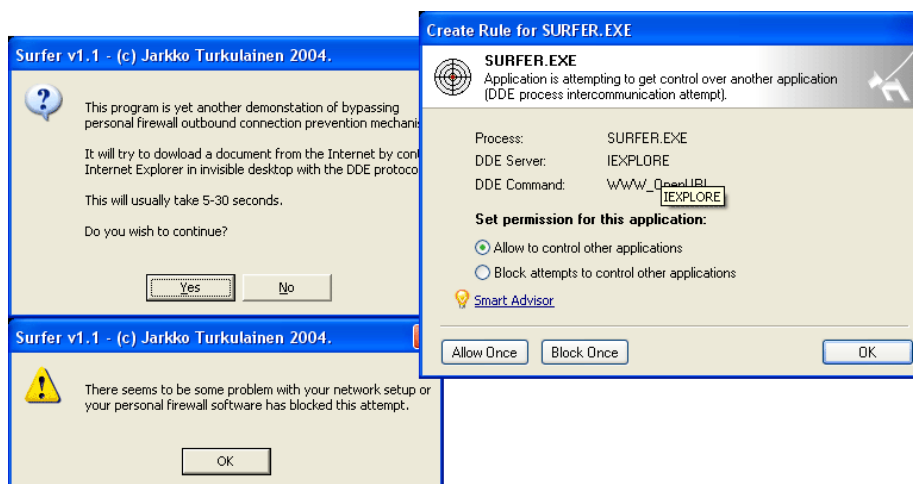


### Test de fuite n°13 « Surfer »

| Nom/lien de téléchargement direct | Technique de détournement utilisée | Infos sur les tests de fuite/page d'accueil  | Fonction Outpost utilisée   |
|-----------------------------------|------------------------------------|--|---|
| <a href="#">Surfer</a>            | Intercommunication DDE             |  surfer.exe | « Intercommunication DDE »<br> |

L'objectif du test Surfer consiste à éviter un pare-feu en utilisant la technique du contrôle DDE (Direct Data Exchange, échange direct de données) pour contrôler les actions d'une application approuvée. Le test lance le navigateur Web par défaut avec un paramètre URL via l'interface DDE.

La réaction de Outpost :



Étant donné qu'Outpost contrôle les commandes reçues par une application par le biais de l'interface DDE, il peut protéger le système de l'utilisateur en déterminant si l'activité est légitime.

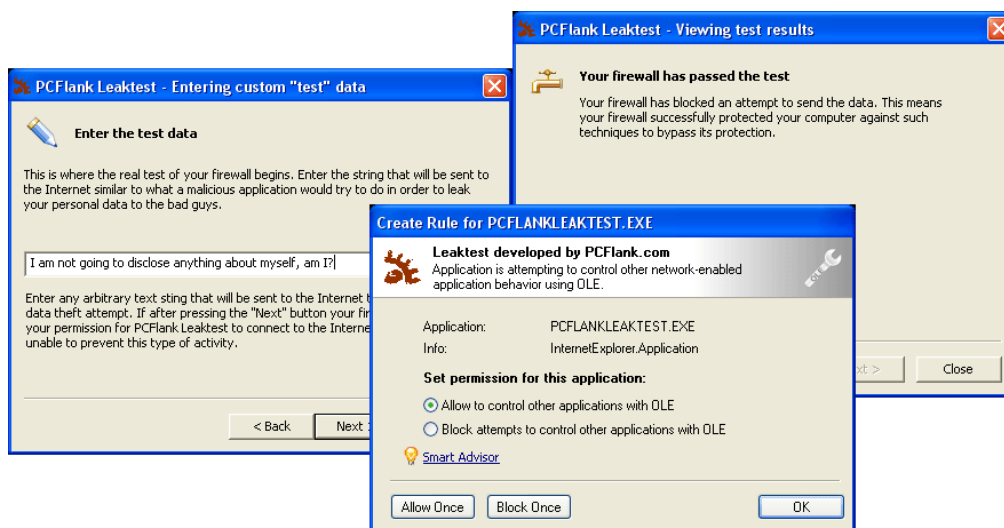
**PASSÉ**

## Test de fuite n°14 « Test de fuite PCFlank »

| Nom/liens de téléchargement direct    | Technique de détournement utilisée              | Infos sur les tests de fuite/page d'accueil   | Fonction Outpost utilisée   |
|---------------------------------------|---|---|---|
| <a href="#">Test de fuite PCFlank</a> | Contrôle d'application via l'automatisation OLE |  PCFlankLeaktest.exe<br>Leaktest developed by PCFlank<br>PCFlank.com | « Contrôle d'application OLE »<br> |

Le test de fuite PCFlank utilise l'intercommunication OLE (Object Linking and Embedding, liaison et incorporation d'objets) pour échanger des données et des commandes entre les applications. Le test utilise le modèle OLE pour manipuler l'activité d'Internet Explorer et envoyer les données spécifiées à l'emplacement test de l'auteur.





La réaction de Outpost :



Outpost peut détecter les communications OLE et inviter l'utilisateur à autoriser ou non l'application (dans ce cas le test de fuite PCFlank) à contrôler l'activité des autres applications. La réponse « non » bloque la transmission et protège les données de l'utilisateur.

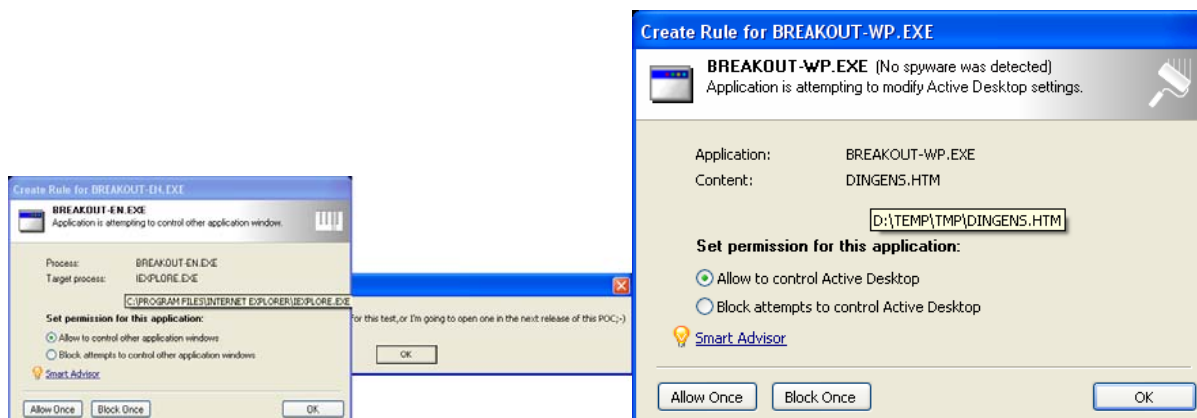
**PASSÉ**

### Test de fuite n°15 « Breakout »

| Nom/liens de téléchargement direct | Technique de détournement utilisée | Infos sur les tests de fuite/page d'accueil   | Fonction Outpost utilisée   |
|------------------------------------|------------------------------------|---|---|
| <a href="#">Breakout</a>           | Messages Windows                   |  breakout-en.exe | « Contrôle de la fenêtre d'une application »<br> |
| <a href="#">Breakout</a>           | Modification de Active Desktop     |  breakout-wp.exe |    |

Le test Breakout lance Internet Explorer en arrière-plan et tente de contrôler son comportement en utilisant la communication inter-processus « SendMessage API » qui permet à un programme de contrôler l'activité d'un autre programme dans un mode masqué. La même technique est utilisée pour le test afin que Windows Active Desktop affiche une page HTML créée localement et la définisse comme papier peint du Bureau. Les pare-feu ne contrôlant pas la manière dont les applications connectées à Internet interprètent les commandes d'autres programmes sous Windows échouent à ce test.



La réaction de Outpost :



Outpost avertit l'utilisateur dès qu'il détecte une tentative d'utilisation de fenêtres masquées.

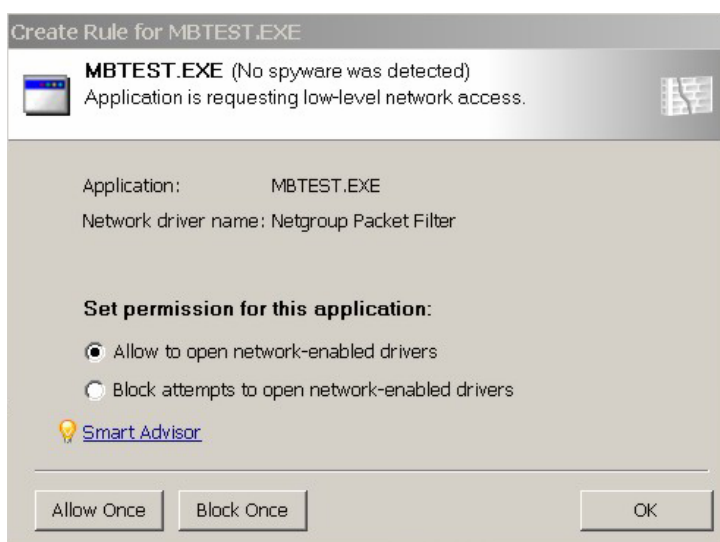
PASSÉ

### Test de fuite n°16 « MBtest »

| Nom/liens de téléchargement direct | Technique de détournement utilisée | Infos sur les tests de fuite/page d'accueil  | Fonction Outpost utilisée   |
|------------------------------------|------------------------------------|--|---|
| <a href="#">MBtest</a>             | Accès direct à l'interface réseau  |  mbtest.exe | « Ouverture d'un pilote réseau »<br> |

Le test de fuite MBtest crée un flux de paquets erratiques et les envoie vers l'adaptateur réseau, en contournant la pile TCP/IP standard surveillée par le pare-feu, avec pour objectif d'éviter les techniques de prévention des fuites.



La réaction de Outpost :



Outpost Firewall détecte une application tentant d'envoyer des données directement à un adaptateur réseau, et avertit l'utilisateur.

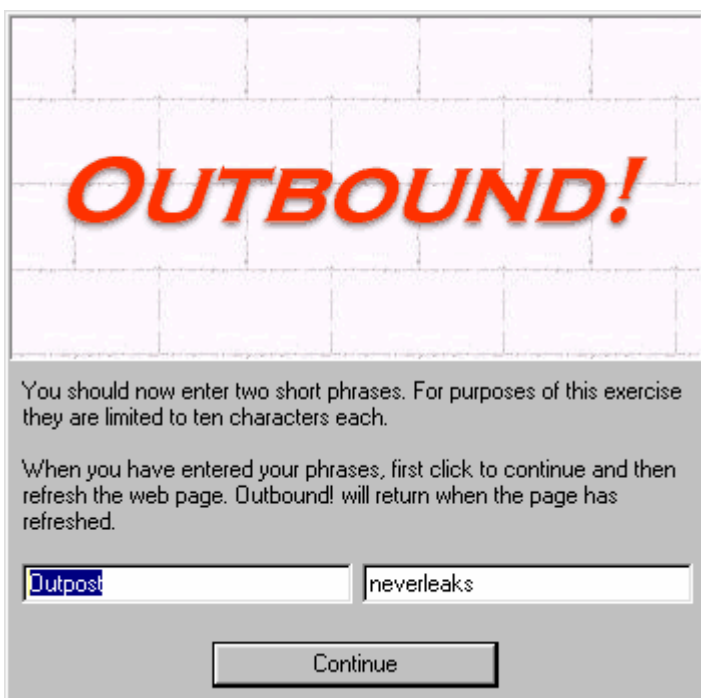
**PASSÉ**

### Test de fuite n°17 « OutBound »

| Nom/liens de téléchargement direct | Technique de détournement utilisée | Infos sur les tests de fuite/page d'accueil   | Fonction Outpost utilisée   |
|------------------------------------|------------------------------------|---|---|
| <a href="#">OutBound</a>           | Accès direct à l'interface réseau  | <br>outbound.exe | « Ouverture d'un pilote réseau »<br> |

OutBound est un test de fuite plus ancien dont le fonctionnement nécessite Windows 98 ainsi que l'installation de plusieurs pilotes de périphériques plus anciens. Outpost supportant encore des systèmes d'exploitation plus anciens tels que Windows 98 (contrairement à Microsoft), il était cependant important pour nous de passer ce test.

Tout comme le précédent test utilisant la même technique, OutBound tente d'envoyer des informations en ouvrant le pilote réseau et en envoyant des données à travers ce canal. Il apparaît toutefois dans nos essais que ce test de fuite ne fonctionne plus correctement ; le code test ne s'exécutait pas correctement et les informations n'étaient jamais transmises. Nous pensons qu'Outpost était à l'origine de ce problème d'exécution, bien que nous ne puissions pas le prouver.



**OUTBOUND!**

You should now enter two short phrases. For purposes of this exercise they are limited to ten characters each.

When you have entered your phrases, first click to continue and then refresh the web page. Outbound! will return when the page has refreshed.

**PASSÉ**

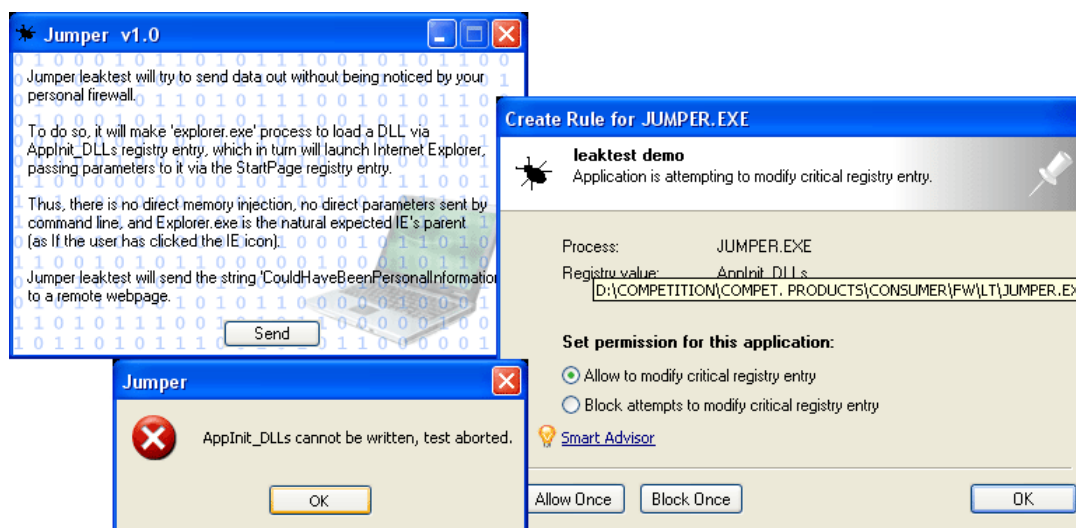
## Test de fuite n°18 « Jumper »

| Nom/liens de téléchargement direct | Technique de détournement utilisée          | Infos sur les tests de fuite/page d'accueil  | Fonction Outpost utilisée   |
|------------------------------------|---|--|---|
| <a href="#">Jumper</a>             | Modification de la base de registre système |  jumper.exe<br>leaktest demo<br><a href="http://www.firewallleaktester..">http://www.firewallleaktester..</a> | « Entrées sensibles de la base de registre »<br> |

Le test Jumper utilise les techniques du lanceur et de la modification de la base de registre pour outrepasser les détecteurs du pare-feu.

En falsifiant la base de registre, le test trompe Windows en chargeant la DLL du Jumper au prochain démarrage de l'Explorateur de Windows. La DLL malveillante modifie ensuite l'entrée de la base de registre correspondant à la page de démarrage du navigateur, de manière à pouvoir transférer les données sensibles contenues dans une adresse URL la prochaine fois qu'il sera démarré.

La réaction de Outpost :



Outpost surveillant les zones système sensibles de l'ordinateur, le blocage des écritures non autorisées dans la base de registre assure qu'aucune modification malveillante ne peut être effectuée.

**PASSÉ**

## Quelques mots d'Agnitum

Alexey Belkin, architecte logiciel en chef chez Agnitum, partage son point de vue concernant l'ajout de composants anti-fuite dans Outpost.

« Il a toujours fallu faire des concessions entre la sécurité et la convivialité. Prenons l'exemple d'un verrou de porte classique. Certaines personnes se contenteront d'un verrou ordinaire installé par une société, tandis que d'autres se sentiront davantage en sécurité avec un système de verrouillage plus sophistiqué nécessitant plusieurs clés. La dernière approche nécessite plus de temps, mais votre maison s'en trouvera plus sécurisée.

« La même approche peut être appliquée aux pare-feu – certains fournissent une protection basique contre les menaces simples, mais en même temps sont simples d'utilisation; tandis que d'autres sont plus puissants mais peuvent être longs et difficiles à configurer correctement.

« Nous avons conçu Outpost afin qu'il assure la protection des utilisateurs le plus efficacement possible contre un large éventail d'attaques malveillantes et d'intrusions pirates. Même si Outpost posera davantage de questions qu'un pare-feu basique pendant la période d'utilisation initiale, il fournit – comme vous pouvez le constater à partir du résultat de ces tests – la meilleure protection de sa catégorie contre toutes les méthodes de fuite d'informations connues. La nécessité de fournir une protection sûre est à nos yeux plus importante que l'agacement mineur suscité par quelques messages supplémentaires au cours des premiers jours d'utilisation. Nous prenons la protection des données très au sérieux, et nous pensons que vous devriez en faire de même.

« Nous avons fourni aux utilisateurs un moyen de réduire le nombre de questions posées par le pare-feu. Nous avons créé dans la section « anti-fuite » du logiciel un onglet Exclusions qui peut être utilisé pour régler le niveau de protection anti-fuite pour chaque application capable de se connecter à Internet de l'ordinateur de l'utilisateur. »

## Conclusion

Comme le montre cette analyse, Outpost Firewall Pro 4.0 passe tous les tests de fuite actuellement disponibles, prouvant de manière irréfutable que le logiciel propose le niveau de protection le plus élevé.

En résumé :

- les tests de fuite sont un moyen indépendant et sûr permettant d'évaluer la qualité de protection vers l'extérieur d'un pare-feu pour les accès spécifiques aux programmes.
- Il existe actuellement dix-huit tests de fuite connus, basés sur plus d'une douzaine de techniques d'interactivité des programmes.
- Outpost Firewall Pro 4.0 passe tous les tests de fuite actuels, fournissant une bonne protection contre les logiciels malveillants cherchant à établir des connexions non autorisées et divulguer des informations confidentielles.

En outre, des filtres puissants empêchent les informations protégées de quitter l'ordinateur, décourageant les attaques pirates les plus agressives.

La nouvelle version de Outpost Firewall Pro protégera les connexions Internet et réseau de l'utilisateur, quelle que soit l'évolution des logiciels malveillants.

## Contacts

Agnitum Ltd.  
Bolshoy Sampsonievskiy 60, Liter "A"  
St.Petersburg, Russie, 194044

Tél. : +7-(812)-3365246  
Télécopie : +7-(812)-3365244  
Email : [pr@agnitum.com](mailto:pr@agnitum.com), [www.agnitum.com](http://www.agnitum.com)