SÉCURITÉ INFORMATIQUE

numéro 22 décembre 1998

SÉCURITÉ DES SYSTÈMES D'INFORMATION

La sécurité informatique en trois actes

L'Acte I de la sécurité informatique, c'est la prévention : désactiver de notre système informatique tout ce qui n'est pas utile et qui peut constituer une faiblesse de sécurité, mettre en place une démarche pour définir des règles et des procédures de sécurité et en contrôler l'application.

éditorial

L'Acte II, c'est la simulation : éprouver les systèmes pour identifier les vulnérabilités avant que des indélicats ne le fassent et n'en abusent. Des outils logiciels ont été développés pour éprouver la résistance de nos équipements et signaler les failles. Ils permettent d'identifier les composants qui peuvent constituer des faiblesses.

Enfin l'Acte III, c'est l'épreuve du feu : la détection des intrusions. Beaucoup d'intrusions passent inaperçues, particulièrement quand les pirates se servent de vos machines comme relais pour en attaquer d'autres. Des dispositifs logiciels opèrent comme des vigiles pour détecter les tentatives d'intrusions et vous en informer.

Ces outils sont-ils utilisables dans l'environnement de nos laboratoires de recherche ? Sont-ils efficaces ? Sont-ils compatibles avec les moyens courants dont nous disposons pour l'administration de nos systèmes ?

Ce sont à ces questions que le présent numéro s'efforce de répondre en privilégiant l'expérience d'administrateurs qui ont expérimenté ces outils sur leur parc informatique.

La scène va donc se passer dans un environnement classique de laboratoire.

Christian Michau
Directeur de l'Unité Réseaux CNRS (UREC)
Tél. : 01 44 27 42 60
Fax : 01 44 27 42 61

Simulation et détection

Un pas de plus dans la sécurité informatique

De plus en plus, nous sommes convaincus de la nécessité de mettre en place, au sein des laboratoires, une politique de sécurité informatique afin que la «Mémoire Électronique» de la Recherche ne soit pas systématiquement violée par des intrusions, toujours plus fréquentes, via le réseau.

Les systèmes ne sont pas fiables, et il existera toujours, pour certains, le besoin de trouver les failles et d'exploiter celles encore existantes, quel que soit le mode de *prévention* utilisé ; aussi, parallèlement aux techniques de prévention, tant au niveau matériel et logiciel (par des mises à jour régulières et des configurations correctes) qu'au niveau des accès à ceux-ci (au moyen de systèmes d'identification et d'authentification), il est nécessaire d'envisager la mise en œuvre de méthodologies basées sur la *simulation* d'intrusion et d'exploitation des failles ainsi que celles visant à faire de la *détection* d'intrusion.

C'est ainsi que dernièrement (les 14, 15 et 16 septembre) s'est tenue, à Louvain-La-Neuve (Belgique), la première conférence internationale RAID'98 (*Recent Advances in Intrusion Detection*) permettant de faire le point sur l'état de l'art dans le domaine des systèmes de détection d'intrusion. 130 personnes de 45 pays, représentant aussi bien le monde académique, industriel que gouvernemental, étaient présentes, dont 50% d'Européens et parmi eux 10 Français, pour suivre les trente exposés dont deux tables rondes.

Les premières recherches dans le domaine des IDS (*Intrusion Detection Systems*) ont commencé il y a environ dix ans ; quelques systèmes, aux fonctionnalités très spécifiques, sont déjà commercialisés, mais nombreuses sont les questions posées au sujet des IDS, car actuellement les systèmes développés ont plus une approche industrielle que scientifique, et ils comportent beaucoup d'insuffisances. Parmi ces questions, les plus fréquentes rencontrées sont :

1. Comment peut-on définir un IDS ?
2. Existe-t-il des standards et y a-t-il un intérêt à une standardisation des composants d'un IDS ?
3. Les IDS et la légalité : comment interpréter légalement et de façon crédible les résultats d'une détection d'intrusion ?
4. Existe-t-il des moyens pour mesurer les performances d'un IDS et comparer les différents systèmes et leurs méthodologies ?
5. Comment peuvent-ils s'intégrer aux autres systèmes de sécurité ?

IDS, principes, standards, législation, performances ?

S'appuyant sur le contenu des fichiers traces des systèmes, sur les enregistrements fournis par des analyseurs (type *tcpdump*), sur la définition des profils des utilisateurs, sur leur comportement (heure de

suite page 3

CNRS CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Évaluation de trois logiciels de sécurisation d

«Security Scanner», «System Security Scanner», «RealSecure»

L'offre d'ISS s'articule autour des trois produits de base que sont «Internet Security Scanner», «System Security Scanner», et «RealSecure». Dans le cadre de l'UREC-CNRS, nous avons évalué ces produits sur le réseau LORIA. L'objectif était de vérifier leur capacité de détection des trous de sécurité sur les réseaux et éventuellement de détecter certaines anomalies. Nous n'avons pas cherché à prendre en compte l'ensemble des possibilités des logiciels, mais seulement à nous concentrer sur les critères importants définis par «la listes de contrôle» du CNRS, et à présenter un avis sur leurs facilités d'installation et d'utilisation.

Installation

Les produits d'ISS ont été mis en place au LORIA, sur des machines diverses: trois machines solaris, deux machines linux, deux machines Windows NT, deux machines SGI, une machine Digital Unix, un routeur Cisco.
L'objectif n'était pas de faire une plate-forme de test, dans le but de pousser ces logiciels à leurs limites, mais d'étudier leur installation et leur fonctionnement courant sur un réseau hétérogène, sur des serveurs et des stations utilisateurs, et d'en relever les éventuels problèmes.

Internet Scanner v5.1

«*Internet Security Scanner*» est un outil d'audit sécurité. Il est spécialisé dans la sécurité réseau. Cela signifie qu'il va tester la sécurité d'une machine distante, en essayant successivement toutes les vulnérabilités qu'il connaît, et présenter un rapport de ses découvertes. Il peut être utilisé «en interne», et scanner son propre réseau, mais aussi «de l'extérieur», pour valider l'installation d'un «pare-feu».

Fonctionnement

Après une installation facile, «*Internet Security Scanner*» est rapidement opérationnel. Il propose plusieurs niveaux de vérification, et il est possible de se faire facilement son propre fichier de test. La durée des «scans» varie fortement suivant les tests (plus de 7 minutes par machine pour le mode «*heavyscan*», le plus complet).

Notre avis

ISS semble avoir une batterie de trous de sécurité testés assez importante (en fait c'est un des plus complets sur le marché). Les licences sont un peu contraignantes, mais permettent tout de même deux choses :

- Empêcher quelqu'un de son réseau de s'en servir sur un autre réseau à des fins malveillantes.
- La licence ne se verrouille pas sur la machine source: il est donc possible de vérifier son réseau depuis différents endroits, ce qui permet de valider sa politique de sécurité (différents sous réseaux, interne/externe, etc.).

L'outil reste cependant assez basique. On peut le comparer tout à fait à «*SAINT*» (domaine public), la quantité de vulnérabilités testées en plus. Il se contente de fournir les trous de sécurité détectés, et s'arrête là. On aurait pu espérer un peu plus de «valeur ajoutée». En effet, il manque à notre goût :

- Un peu plus d'information «personnalisée» pour chaque trou de sécurité détecté. Une information par architecture (et non pas un petit texte de dix lignes systématique), avec par exemple un descriptif bref, et la possibilité d'un descriptif détaillé, les avis du CERT fournis (et non pas une simple URL sur le site principal), les commandes à faire dans un premier temps (prêtes à être copiées-collées), etc.
- Un système de mise à jour des versions qui permettrait d'être à jour plus rapidement (actuellement les 6 à 8 versions par an ne sont pas suffisantes).
- Des versions unifiées pour Windows et UNIX. Aujourd'hui, des versions distinctes (5.1 et 5.2) recherchent des vulnérabilités différentes. La version Windows NT trouve évidemment plus de bogues Windows que la version UNIX. Même si techniquement c'est compréhensible, ce n'est intellectuellement pas satisfaisant.

Il convient d'utiliser ISS en fonction de sa politique de sécurité. En effet, on peut par exemple exiger un «zéro défaut» depuis l'extérieur. Concernant l'interne, il est quasiment impossible d'obtenir ce «zéro défaut» si on utilise des services comme NIS ou NFS. On peut se limiter, dans ce cas, à certains niveaux de vulnérabilités (obtenir zéro vulnérabilité niveau «*High*» par exemple).

System Security Scanner v1.6

«*System Security Scanner*» est actuellement essentiellement tourné vers Unix (la version NT est toute récente). Nous ne l'avons donc testé que sur Unix. C'est un scanner orienté système. Son but est de tester les vulnérabilités sur une machine, permettant principalement à un compte local d'accéder aux privilèges de l'administrateur.

Fonctionnement

Il doit être installé sur la machine à tester. Puis, après avoir fait une image du système (fonctionnalité de *tripwire*), on peut lancer un scan. Celui-ci va travailler sur différentes actions :

- Comparaison des fichiers systèmes avec l'image, et alerte en cas de modifications.
- Étude des fichiers système (passwd, inetd. conf, rhosts, etc.).
- Étude des droits des fichiers (suids, mauvais droits, etc.).
- Étude des binaires vulnérables au «*buffer overflow*», etc.

Notre avis

«*System Security Scanner*» teste une grande quantité de vulnérabilités. C'est plutôt bien. Nous pensons qu'il est le plus complet dans ce cas. Cependant, il ne nous a pas entièrement satisfaits. Il présente diverses lacunes :

- Le temps d'un audit complet d'une machine par «*System Security Scanner*» peut être très long (plusieurs heures).
- Les rapports sont assez mauvais. Ils ne factorisent pas selon le même bogue plusieurs fois rencontré. Sur des gros serveurs, on peut rencontrer plus de 1 000 fois le même bogue (cas typique de mauvais droits sur une arborescence).
- La méthode de déploiement de «*System Security Scanner*» sur un réseau ne nous a pas convaincus. Il est basé sur des agents résidents (daemon), par lesquels passent les mises à jour de version et les déclenchements de scan. Maintenir ce système de fonctionnement sur un grand parc de machine est difficile.

Globalement, «*System Security Scanner*» reste un système très basique de détection de vulnérabilité. Il n'essaye pas de s'adapter aux configurations du site, et bien souvent y trouve des vulnérabilités qui n'existent pas. De plus, arriver au zéro défauts avec S3 est quasi impossible : il est nécessaire pour cela de modifier grandement le système. La version fournie par les constructeurs est loin de passer les tests de S3.

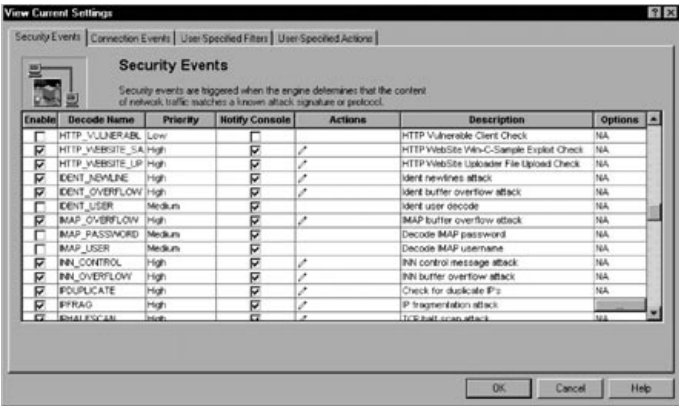
RealSecure v2.0

«*RealSecure*» n'est pas un scanner comme les deux précédents produits. C'est un produit de détection d'attaques en temps réel. Il se place sur une (ou plusieurs) machine sur l'entrée (ou les entrées) du réseau, et va écouter le trafic et l'analyser afin d'y trouver les traces de piratage. Un peu comme un antivirus a une base de signature des virus, «*RealSecure*» a une base de signature des attaques, et compare les paquets IP à cette base.

e systèmes

Fonctionnement

«*RealSecure*» se compose de moteurs et de consoles de management. Les moteurs sont à l'écoute du réseau, et y détectent les piratages, comme par exemple certains windows_OOB, IMAP_Overflow, etc. Il a une base de connaissance de signatures des attaques, et lorsqu'il relève un ou plusieurs paquets IP ayant ce motif, avertit d'une façon ou d'une autre l'administrateur. Voici un exemple de ce que «*RealSecure*» connaît et de la simplicité (clic clic) de configuration :



Nous avons installé et fait fonctionner avec diverses configurations «*RealSecure*» sur notre connexion Internet durant 2 mois. Il a découvert quelques attaques ou pré-attaques réelles, et aucun de nos quelques tests ne lui a échappé.

Notre avis

«*RealSecure*» est le meilleur outil d'ISS. Il fonctionne bien (nous n'avons pas eu de plantage violent, malgré NT). Les choses détectées semblent correspondre à des attaques ou pré-attaques réelles. Nous avons testé avec quelques outils de pirates (winnuke, saint, etc.). La base des attaques détectées est relativement complète, bien que certaines choses manquent (Socks, scan de ports évolués). Cette base de connaissance est actuellement incluse dans le logiciel, et il est nécessaire d'installer les nouvelles versions pour bénéficier des mises à jour de la base.

Conclusion générale

Nos tests des produits d'ISS ne sont pas passés complètement inaperçus, mais n'ont pas engendré de dysfonctionnement sur le réseau LORIA.

Les listes de contrôles ne sont pas remplaçables par l'un ou l'autre de ses produits. Ceux-ci permettent de valider la mise en place de celle-ci. Ces outils vont plus loin que les recommandations du CNRS UREC et leurs installations sont faciles. Mais ils ne renforcent pas la sécurité d'un site, ils mettent juste en lumière les problèmes à résoudre. Les versions testées des produits d'ISS sont déjà remplacées par des versions plus récentes. Il y a entre 6 et 8 versions par an. ISS a promis la mise en ligne des bases des signatures d'attaque, ainsi que des méthodes de «*push*» pour les mises à jour de celles-ci.
Les produits d'ISS sont à la base des outils de sécurité permettant de déceler des vulnérabilités ou des attaques aussi bien simples que très pointues. Leur faiblesse commune est le rapport brut, qu'ils produisent sans analyse. ISS a enfin annoncé «*Safesuite Decision*», un outil de corrélation des logs générés par leurs logiciels de sécurité. Nous n'avons pas évalué ce produit.
Les documents complets de nos tests sont accessibles sur :
http://www.loria.fr/moyens-infos/securite
Site d'ISS : http://www.iss.net

Bertrand Wallrich
Responsable de la sécurité au LORIA
Bertrand.Wallrich@loria.fr

suite de la page 1

connexion, déconnexion, environnements), sur des statistiques d'utilisation des applications, sur les avis des CERTs..., il est possible de construire des bases de données statiques (voire dynamiques, si on utilise les systèmes experts et l'Intelligence Artificielle) utilisables pour créer des scénarios d'attaques possibles (usage suspect ou anormal du système informatique). On parlera de «signature» d'une attaque lorsque plusieurs événements non usuels sont réunis et peuvent donc correspondre à une menace. Ces signatures permettent de créer des librairies.
Les IDS ne s'appuient actuellement sur aucun standard. On trouve cependant une volonté d'en définir, et il y a nécessité, surtout en ce qui concerne les fichiers d'enregistrement des événements (*logs*). Au sein de l'ISO (*International Organization for Standardization*), des groupes comme le TC68/SC2 (*Strategy, Security and General Opération*) définissent la norme ISO 13491 *Security Audit Checklist* mettant en évidence que les IDS sont des outils de sécurité ; d'autres, comme le SC27 (*Security Techniques*), préparent un projet NP15947 sur le *Intrusion Detection Framework*, et le groupe de travail IDS de l'IETF (*Internet Engineering Task Force*) s'intéresse en priorité à la définition de protocoles de communication des événements, à la sémantique associée aux événements, à la définition de formats standards d'enregistrement d'événement et à une standardisation des rapports d'incidents.
Il n'est pas facile de vérifier qu'une intrusion est effective, mais surtout il est difficile de déterminer si celle-ci correspond à une curiosité inoffensive ou à une volonté réelle de nuire. D'autre part, il est essentiel de considérer que les *logs* peuvent être utilisées par l'appareil judiciaire : elles doivent donc être fiables (synchronisation), inaltérables et illisibles (par les utilisateurs) ; certains IDS offrent des systèmes de clés et des canaux cryptés pour réaliser les enregistrements.
Il n'est pas aisé de mesurer les performances des IDS : l'analyse de trafic et l'enregistrement de traces engendrent des volumes importants de données, difficilement

Quelques IDS

- AAFID : architecture distribuée et agents capables de réaliser des actions indépendantes
  http://www.cs.purdue.edu/coast/projects/autonomous-agents.html
- ASAX : scénarios d'attaques, normalisation des enregistrements d'audit, système expert http://www.info.fundp.ac.be/~cri/DOCS/asax.html
- BRO : filtrage de trafic réseau, scripts d'interprétation et analyse spécifique pour des applications telles que finger, ftp, portmap et telnet
  http://www.usenix.org/publications/library/proceedings/sec98/paxson.html
  http://www-nrg.ee.lbl.gov/bro-info.html
- IDLE : sur le principe de librairies standardisées utilisant XML
- GASSATA : outil d'analyse de traces utilisant un algorithme génétique
  http://www.supelec-rennes.fr/rennes/ren/rd/ssi/Bienvenue.html
- MIDAS : s'appuie sur une méthode statistique
- NADIR : analyse de l'activité des utilisateurs et détection des anomalies en utilisant un système expert
  http://nadir.lanl.gov/overviewShortDescription.html
  http://www.c3.lanl.gov/~gslentz/nadirTemplate.shtml
- NIDAR : analyse de trafic, et communication avec une librairie de signatures d'attaques par canal de communication authentifié
- NIDES : basé sur des statistiques d'utilisation et un système expert
  http://www.geek-girl.com/ids/0049.html
- Sentinel : prototype s'appuyant sur le Réseau de neurones
- Real Secure : filtrage de trafic réseau et utilisation de signatures d'attaques http://www.iss.net/ ■

suite page 4

suite de la page 3

exploitables puisqu'il n'existe pas de standards ni de base de référence. Les IDS ne pourront s'intégrer dans les réseaux «hauts débits» que si l'on est capable d'intercepter les paquets aussi vite qu'ils arrivent (débit et quantité du trafic/performance de l'outil IDS), sinon se pose le problème de la cohérence des informations enregistrées; des solutions *hardward* seront indispensables. Il faut également résoudre les problèmes liés à la disponibilité rapide des signatures d'attaques, à la nécessité de profils utilisateurs standards (classifier les utilisateurs). L'utilisation des techniques d'*Information Retrieval* (employées dans les moteurs de recherche), basées sur l'indexation, semble offrir une complémentarité dans la recherche de scénarios d'attaques.

Peut-on les utiliser ?

Parmi tous ces produits, beaucoup sont encore au stade de prototype, et il faudra faire encore beaucoup de développements pour qu'ils jouent pleinement leur rôle de *détecteur d'intrusion*. Mais bien qu'ils ne correspondent pas à des standards et qu'ils ne puissent prétendre faire partie de l'appareil judiciaire, ils représentent toutefois un appui précieux dans l'administration des systèmes et des réseaux en aidant à réagir rapidement aux intrusions (par exemple, utilisation en entrée de site de *Real Secure*). Ils sont compatibles et complémentaires aux outils de simulation d'intrusion, tels que «Saint» (logiciel libre, http://wwdsilx.wwdsi.com/saint/), «Ballista» (utilisable sous *solaris*, http://www.idg.net/new-docids/ballista/), «ISS» (*Internet Scanner System* http://www.iss.net/), qui permettent de déceler les vulnérabilités; mais, dans tous les cas, ils doivent être utilisés avec précaution: pour la détection, ils peuvent s'apparenter à des techniques d'espionnage; pour la simulation, leur utilisation doit être faite après informations auprès des sites testés. L'article en page centrale rapporte les tests d'évaluation faits par le LORIA, sur ISS et Real Secure.

Nicole Dausque
CNRS/UREC
Nicole.Dausque@urec.cnrs.fr

Encore des inondations

De nombreux incidents, ayant pour origine des «inondations de courriers» («spam» en hexagon) nous sont signalés. Voici quelques sites où vous pourrez trouver des informations sur cette technique d'agression et surtout, comment se protéger et comment réagir :

1) Sur Jussieu www.ccr.jussieu.fr, le Kit Jussieu anti-spam :
http://www.ccr.jussieu.fr/anti-spam/rejet/index.html
le même Kit sur la fac de Versailles :
http://www.prism.uvsq.fr/~pda/kit-jussieu/anti-spam/
http://www.prism.uvsq.fr/~pda/kit-jussieu/support/

2) Un article sur le CRU (comité Reseaux des Universités) :
http://www.cru.fr/securite/Deontologie/spam.html

3) Quelques «foires aux questions» (FAQ) en anglais:
http://digital.net/~gandalf/spamfaq.html
http://www.cybernothing.org/faqs/net-abuse-faq.html
http://www.tezcat.com/~haz1/netabuse/netabuse.html

Surveillez vos arrières

Un groupe de pirates créé en 1984 et nommé «Cult of the Dead Cow» vient de mettre en circulation un «produit» qui s'annonce ravageur. Ils l'ont appelé «Back Orifice» (en abrégé «BO»). C'est une application client/serveur qui permet au logiciel client de surveiller, d'administrer, et d'effectuer à distance n'importe quelle action (réseau, multimédia, redémarrage, fichiers, …) sur la machine exécutant le serveur. Bref, cela signifie qu'il suffit que BO soit installé (d'une manière ou d'une autre…) sur votre machine pour que n'importe quel pirate puisse faire n'importe quoi chez vous. Pour la version 4.00.1 (celle qui en circulation actuellement), les systèmes vulnérables sont Windows 95/98. Il faut savoir que Back Orifice a été téléchargé, depuis le site Internet qui le distribue, 35 000 fois dans les 4 premières heures et 100 000 fois après 21 jours ! Il est évident que certains veulent nuire…

BO n'est pas un virus, mais un «cheval de Troie» (il ne se duplique pas automatiquement comme le font les virus). La méthode la plus commune pour être touché est l'installation d'un logiciel «piégé» récupéré sur des sites Internet douteux. Exemple de scénario d'installation :
Un serveur FTP, HTTP, Notes, met à la disposition de tout le monde un utilitaire de conversion de fichier (Word, PDF, …), nommé (par exemple) «wordconf.exe». En réalité, cet exécutable n'est autre que «BOSERVE.EXE» renommé. Une fois ce fichier téléchargé, il est vu comme un exécutable tout à fait inoffensif par n'importe quel antivirus. En effet, il ne possède aucune signature de réplication, et son exécution n'altère aucun secteur disque vital tel que le MBR (Master Boot Record, qui contient la table de partitions) ou un secteur de démarrage. Son exécution, qui est totalement silencieuse, ne va générer aucun message. L'utilisateur n'y prêtera pas une attention particulière (dans le cas d'un filtre de conversion, il n'y a rien de «visible» qui doive se produire).

Lors de sa première exécution, BOSERVE.EXE va procéder aux deux opérations suivantes :

1. Auto-renommage de «BOSERVE.EXE» en « .EXE» (blanc point EXE). Le nom du fichier se réduit à un espace, suivi de l'extension habituelle «exe» des exécutables ! Cela lui permet de passer presque inaperçu de l'utilisateur. En effet, une commande DOS telle que «dir *.exe» va afficher le nom court de ce fichier, qui est alors «exe~1» (sans extension).
2. Modification de la clef suivante de la base de registres: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices. La valeur par défaut de cette clef, vide en temps normal, se voit affecter la chaîne «.exe». Celle-ci contient la liste de toutes les applications lancées au démarrage de Windows, avant même l'ouverture d'une session utilisateur. Or l'éditeur de stratégies système «PolEdit» (fourni avec Windows) ne trouve aucune trace de BO (rubrique «Registre/Ordinateur local/Système/Programmes à exécuter/Exécuter services» qui sert à afficher et/ou éditer la liste des services). Cette anomalie s'explique simplement par le fait que BO, renommé en « .exe», est un service sans nom puisqu'inscrit dans la valeur par défaut de la clef de la BDR. Seul un examen approfondi de la BDR à l'aide de regedit peut repérer BO (et à la condition de connaître son nouveau nom « .exe»).

Moralité :
faites très attention aux logiciels que vous téléchargez.
Pour enlever BO de sa machine, il suffit de :
- supprimer le fichier « .exe» (situé dans le répertoire \windows\systeme) ;
- supprimer la chaîne « .exe» de la valeur par défaut de la clef HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
- redémarrer la machine.

Il est diffusé sur Internet depuis le 1er septembre 1998 un logiciel gratuit nommé «Back OriFix», (v1.01) émanant de l'entreprise canadienne «GroupAxion» dont le but est de supprimer BO. Il se présente sous la forme d'un fichier compressé de 1,5 Mo, alors que l'exécutable lui-même n'occupe que 96 Ko. La différence est due à l'utilisation d'une librairie Visual Basic très volumineuse (msvbvm50.dll). Back Orifix effectue une recherche complète de BO, affiche le fichier le concernant puis le supprime. En revanche, il ne restaure pas la Base de registres, ce qui est un oubli important.

Il est disponible à l'adresse suivante :
http://www.groupaxion.com/BOrifix/telechargement.html

SÉCURITÉ INFORMATIQUE
numéro 22 décembre 1998
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 5 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :
ROBERT LONGEON
Centre national de la recherche scientifique
Service du Fonctionnaire de Défense
c/o IDRIS - BP 167. 91403 Orsay Cedex
Tél. 01 69 35 84 87
Courriel : robert.longeon@cnrs-dir.fr
http://www.cnrs.fr/Infosecu

ISSN 1257-8819
Commission paritaire n° 3105 ADEP

Conseil et coordination : CNRS - MIST - Jacqueline Leclère • Conception et réalisation : La Souris 01 45 21 09 61