



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

**S . G . D . S . N**  
Agence nationale de la sécurité  
des systèmes d'information  
CERTA

Paris, le 11 mars 2005  
N° CERTA-2005-ACT-010

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité N°2005-10**

---

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>  
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2005-ACT-010>

---

### Gestion du document

Référence	CERTA-2005-ACT-010
Titre	Bulletin d'actualité N°2005-10
Date de la première version	11 mars 2005
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Activité en cours

Le tableau 3 montre les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 24 et le 03 mars 2005. Deux cas de défiguration de site web ont été traités par le CERTA. Pour l'un des deux cas, il s'agit de l'exploitation d'une faille de AWStats (voir avis CERTA-2005-AVI-035).

## 2 Les « rootkits »

Aujourd'hui, le grand public est familier avec les notions de virus, de vers (« worms » et « phpworms » comme évoqués dans le précédent bulletin d'actualité), de chevaux de Troie (« trojan »), de logiciels espion (« spyware ») et autres dénominations pour des codes malveillants (« malware »).

Ces dernières semaines, nous assistons à une recrudescence des références à la notion de « rootkit ».

Pourtant, les rootkits font partie du paysage de la sécurité informatique et des actes de pirate depuis de nombreuses années déjà.

Le CERTA tient à apporter un certain nombre d'explications et de précisions en faisant appel à son expertise et son expérience dans le domaine.

Le terme rootkit est en fait un terme générique qui fait référence aux mécanismes et techniques utilisés afin de permettre de dissimuler une activité illicite dans un système d'information.

Lorsque l'on parle de rootkit, on fait généralement référence à la période consécutive au piratage d'un système (piratage pouvant avoir eu lieu par l'exploitation d'une faille).

Il pourra s'agir d'un ou plusieurs programmes, accompagnés de fichiers de configuration (afin de personnaliser le rootkit selon le but recherché).

Un rootkit peut être sous forme binaire (déjà compilé pour une plate-forme) ou sous forme d'une archive, contenant tous les fichiers à compiler, à personnaliser et à installer sur la machine cible.

L'objectif recherché par un rootkit est de maintenir une présence illicite dans un système d'information, le plus longtemps possible, sans attirer l'attention par un comportement anormal du système d'information.

Il existe différentes techniques de camouflage utilisées par les rootkits :

- modification des binaires permettant de tracer l'activité d'une machine (par exemple sous UNIX `ls`, `ps`, `netstat`, ...). Cette technique est facilement détectable si l'on vérifie l'intégrité des binaires (comparaison par exemple de la signature MD5 du fichier avec une base de signatures) ;
- modification des bibliothèques utilisées par les binaires. Cette technique ressemble à la modification des binaires, à l'exception que ces derniers conserveront leur intégrité ;
- détournement des appels système. Cette technique est la plus élaborée, et la plus furtive, mais peut rendre le système instable.

Par ailleurs, l'installation d'un rootkit peut inclure des programmes d'attaque ou d'extraction d'informations sensibles (mots de passe de la machine, renifleur réseau etc), ou encore de modification du comportement de la journalisation.

Il existe des rootkits pour tous les systèmes d'exploitation.

De nombreux rootkits sont disponibles sur l'Internet, à la fois pour Windows, GNU/Linux, la famille des BSD (FreeBSD, OpenBSD et NetBSD), Solaris, MacOS X ...

Potentiellement tous les systèmes d'exploitation sont concernés par les rootkits.

Plusieurs classifications des rootkits sont possibles. On reprendra celle publiée par Bryce Cogswell et Mark Russinovich sur la page Internet de `RootkitRevealer` de sysinternals (<http://www.sysinternals.com>).

Une première classification possible concerne la persistance du rootkit au redémarrage de la machine. On classe donc les rootkits en rootkits persistants et rootkits basés en mémoire (sous entendu, ne survit pas à un redémarrage de la machine).

Une seconde classification, complémentaire de la première, concerne le mode d'exécution du rootkit : rootkit en mode utilisateur ou rootkit en mode noyau.

Parmi les rootkits les plus connus on pourra mentionner `AFX`, `Vanquish`, `HackerDefender` et `FU` pour la plate-forme Windows. Des virus récents tels `maslan` ou `Myfip.H` intègrent des techniques inspirées des rootkits.

Pour les plates-formes UNIX, les rootkits les plus courants sont `toRn`, `SuckIT`, `Adore`, `Knark` ...

Des outils de détection de rootkits existent depuis longtemps en utilisant des stratégies souvent différentes afin de maximiser les chances de détection.

Parmi les outils de détection de rootkits pour les plates-formes UNIX, on pourra mentionner `chkrootkit` et `Rootkit Hunter`.

Récemment, le site de Sysinternals (<http://www.sysinternals.com>), réputé pour ses outils gratuits dans le monde de la sécurité informatique, a mis à disposition un outil pour plate-forme Microsoft Windows dénommé `RootkitRevealer`.

F-Secure a annoncé à la conférence CEBIT, qui se tient actuellement à Hanovre en Allemagne du 10 au 16 mars 2005, une fonctionnalité pour Microsoft Windows dénommée `F-Secure Blacklight`, permettant a priori de détecter et d'éliminer un certain nombre de rootkits.

D'autre part, Microsoft va prochainement mettre à disposition un outil de détection des rootkits appelé `Strider GhostBuster Rootkit Detection`.

Toutefois, il faut se montrer prudent avec ces produits. D'une part, ils peuvent modifier le système de fichiers, et rendre toute analyse a posteriori plus délicate. D'autre part, les rootkits peuvent intégrer des systèmes de protection contre ces outils pour les rendre inefficaces.

### 3 Rappel des avis et des mises à jour émis

Durant la période du 28 février au 04 mars 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-087 : Multiples Vulnérabilités dans Cyrus IMAP
- CERTA-2005-AVI-088 : Vulnérabilité de KCMS sous Solaris
- CERTA-2005-AVI-089 : Vulnérabilité dans les produits Trend Micro
- CERTA-2005-AVI-090 : Vulnérabilités du système Cisco ACNS

- CERTA-2005-AVI-091 : Vulnérabilité dans ftpd sous HP-UX
- CERTA-2005-AVI-092 : Vulnérabilité dans IBM Hardware Management Console
- CERTA-2005-AVI-093 : Vulnérabilités dans cURL/libcURL
- CERTA-2005-AVI-094 : Vulnérabilité de STSF Font Server Daemon
- CERTA-2005-AVI-095 : Multiples vulnérabilités dans Mozilla
- CERTA-2005-AVI-096 : Vulnérabilités dans phpBB
- CERTA-2005-AVI-097 : Vulnérabilité dans UW-imapd
- CERTA-2005-AVI-098 : Vulnérabilité de kppp
- CERTA-2005-AVI-099 : Vulnérabilités dans RealOne Player
- CERTA-2005-AVI-100 : Multiples vulnérabilités dans le logiciel de license de Computer Associates

Pendant cette même période, les mises à jour suivantes ont été publiées :

- CERTA-2005-AVI-049-007 : Vulnérabilité de PostgreSQL  
(ajout des références aux mises à jour de sécurité Fedora pour PostgreSQL)
- CERTA-2005-AVI-084-003 : Vulnérabilité dans Squid  
(ajout des références aux mises à jour de sécurité Fedora)
- CERTA-2004-AVI-244-007 : Vulnérabilité de PHP  
(ajout de la référence au bulletin de sécurité NetBSD)
- CERTA-2005-AVI-006-004 : Vulnérabilité de KDE  
(ajout de la référence au bulletin de sécurité NetBSD)
- CERTA-2005-AVI-038-005 : Multiples vulnérabilités dans SquirrelMail  
(ajout de la référence au bulletin de sécurité NetBSD)
- CERTA-2005-AVI-041-002 : Vulnérabilité de mailman  
(ajout de la référence au bulletin de sécurité NetBSD)
- CERTA-2005-AVI-068-003 : Vulnérabilité dans vim  
(ajout de la référence au bulletin de sécurité NetBSD)
- CERTA-2005-AVI-072-003 : Vulnérabilité du module Apache mod\_python  
(ajout de la référence au bulletin de sécurité NetBSD)
- CERTA-2005-AVI-073-002 : Vulnérabilité de ht://Dig  
(ajout de la référence au bulletin de sécurité NetBSD)
- CERTA-2005-AVI-082-002 : Vulnérabilité de gFTP  
(ajout de la référence aux mises à jour de sécurité NetBSD)
- CERTA-2005-AVI-084-004 : Vulnérabilité dans Squid  
(ajout de la référence au bulletin de sécurité NetBSD)
- CERTA-2005-AVI-085-001 : Vulnérabilité de unace  
(ajout de la référence au bulletin de sécurité Gentoo)
- CERTA-2005-AVI-085-002 : Vulnérabilité de unace  
(ajout de la référence au bulletin de sécurité NetBSD)
- CERTA-2005-AVI-097-001 : Vulnérabilité dans UW-imapd  
(ajout de la référence au bulletin de sécurité NetBSD)
- CERTA-2005-AVI-084-005 : Vulnérabilité dans Squid  
(ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2005-AVI-099-001 : Vulnérabilités dans RealOne Player  
(ajout références aux bulletins de sécurité RedHat RHSA-2005:265 et RHSA-2005:271)

## 4 Actions suggérées

### 4.1 Respecter la politique de sécurité

Quoique puisse suggérer ce document, la politique de sécurité en vigueur dans votre service doit primer.

Cette section précise néanmoins quelques mesures générales de nature à vous prémunir contre les agressions décrites dans ce document.

## 4.2 Concevoir une architecture robuste

A la lumière des enseignements tirés de ce qui a été présenté dans les bulletins d'actualité, il convient de vérifier que les applications mises en œuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

## 4.3 Appliquer les correctifs de sécurité

Le tableau 2 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

## 4.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiat. Un pare-feu correctement configuré peut retenir certaines attaques informatiques le temps d'appliquer les correctifs. Cependant un pare-feu peut donner une illusion de protection. Cette protection est brisée par la moindre introduction d'un ordinateur nomade dans la partie protégée. On remarque qu'il y a de nombreux paquets rejetés à destination de ports légitimement utilisés par des applications de prise de main à distance. La téléadministration correspond à une demande qui grandit avec la taille du parc à gérer. Les paquets rejetés montrent le risque associé à ce type d'application. Ce risque peut être amoindri par l'usage correct d'un pare-feu.

## 4.5 Analyser le réseau

De nombreux paquets rejetés étudiés correspondent aux ports ouverts par divers virus/vers/chevaux de Troie. Si votre politique de sécurité autorise le balayage des ports ouverts sur les postes de travail ou les serveurs, il peut s'avérer utile de le faire régulièrement afin de découvrir les machines potentiellement contaminées avant qu'un intrus ne le fasse à votre place.

## 4.6 Réagir aux incidents de sécurité

Organisez-vous pour réagir aux incidents de sécurité, en particulier, pour assurer une certaine continuité dans les équipes d'administration et de sécurité.

Le CERTA a pour mission de vous aider à répondre aux incidents de sécurité informatique.

Ne traitez pas les dysfonctionnements des machines à la légère. Dans certains incidents dans lesquels le CERTA intervient, les administrateurs des machines font spontanément part de petits dysfonctionnements inexplicables et d'apparence anodine qui s'avèrent, au cours de l'analyse, être liés à un incident majeur de sécurité. N'hésitez pas à prendre contact avec le CERTA si vous constatez de l'activité sur les ports décrits ci-dessus.

## 5 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

## Liste des tableaux

1	Gestion du document . . . . .	1
2	Correctifs correspondant aux ports destination des paquets rejetés . . . . .	5
3	Paquets rejetés . . . . .	6

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	CERTA-2004-AVI-066 CERTA-2004-AVI-064 CERTA-2003-AVI-132
22	TCP	SSH	–	CERTA-2003-AVI-152
23	TCP	Telnet	–	CERTA-2003-AVI-209 CERTA-2003-AVI-131
42	TCP	WINS	–	CERTA-2004-AVI-384
80	TCP	HTTP	–	CERTA-2004-AVI-195 CERTA-2004-AVI-239
111	TCP	Sunrpc-portmapper	–	CERTA-2003-AVI-052
119	TCP	NNTP	–	CERTA-2004-AVI-340
135	TCP	Microsoft RPC	–	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	–	CERTA-2004-AVI-031
139	TCP	NetBios-ssn et samba	–	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051
389	TCP	LDAP	–	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	–	CERTA-2002-AVI-157
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	CERTA-2002-AVI-213
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6112	TCP	Dtspcd	–	CERTA-2002-ALE-001
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214
8866	TCP	–	Porte dérobée Bagle.B	CERTA-2004-COM-001
9898	TCP	–	Porte dérobée Dabber	–
10080	TCP	Amanda	MyDoom	–
11768	TCP	–	Netdepix	–
15118	TCP	–	Netdepix	–

TAB. 2 – Correctifs correspondant aux ports destination des paquets rejetés

<b>port</b>	<b>pourcentage</b>
445/tcp	83,66
139/tcp	5,96
137/udp	2,77
4899/tcp	1,53
1433/tcp	1,22
1026/udp	0,87
15118/tcp	0,84
6129/tcp	0,57
1027/udp	0,53
80/tcp	0,45
5554/tcp	0,31
1434/udp	0,20
2745/tcp	0,17
1080/tcp	0,12
23/tcp	0,11
9898/tcp	0,10
22/tcp	0,10
42/tcp	0,08
6101/tcp	0,08
1023/tcp	0,07
3306/tcp	0,06
11768/tcp	0,06
3127/tcp	0,05
3128/tcp	0,03
21/tcp	0,02
5000/tcp	0,02
443/tcp	0,01
10080/tcp	0,01

TAB. 3 – *Paquets rejetés*

# **Gestion détaillée du document**

**11 mars 2005** version initiale.