Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 décembre 2005
N° CERTA-2005-ACT-051

**Affaire suivie par :**
CERTA

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité n° 2005-51**

| | |
|---|---|
| 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-051` |

## Gestion du document

| | |
|---|---|
| Référence | CERTA-2005-ACT-051 |
| Titre | Bulletin d'actualité n° 2005-51 |
| Date de la première version | 23 décembre 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

### 1.1 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 15 et le 22 décembre 2005.

### 1.2 Incident traité

Le CERTA a traité un cas de compromission suite à l'exploitation d'un mot de passe trivial utilisé pour le compte de l'administrateur. L'auteur de l'intrusion a utilisé un outil qui teste automatiquement plus de 3000 mots de passe pour le compte `root`. Les attaques de ce type sont très fréquentes, et laissent des traces très visibles dans les journaux des serveurs SSH. La machine ainsi compromise a été utilisée pour conduire d'autres attaques du même type.

Nous constatons que des machines de test sont souvent déployées avec un serveur SSH et des mots de passe faibles pour le compte `root`. Même si les données contenues sur la machine ne sont pas sensibles, il est important de garder à l'esprit que les compromissions ont souvent pour but de prendre le contrôle de ressources informatiques et de les utiliser pour réaliser d'autres attaques.

## 2 Fichier `hosts` et mises à jour automatiques

Certains éditeurs ont choisi de privilégier les mises à jour automatiques de leurs applications. Si ce mécanisme est souvent considéré comme pratique par les utilisateurs et les administrateurs, il n'en pose pas moins quelques problèmes :

- l'installation des fichiers est souvent transparente et on ne sait pas toujours si la mise à jour s'est effectuée correctement ;
- la mise à jour automatique peut être facilement neutralisée par des codes malveillants.

De nombreux codes malveillants modifient le fichier `%windir%/system32/drivers/etc/hosts` qui agit comme un résolveur de noms sous Windows, afin de renvoyer un grand nombre de noms de machine vers l'adresse 127.0.0.1 (on voit souvent les sites de mises à jour de Windows et des principaux éditeurs d'antivirus ainsi neutralisés). Le fichier `hosts` ne contient par défaut (et hors commentaires) que la ligne :

```
127.0.0.1 localhost
```

## 3 Liens utiles

- Note d'information pour sur les systèmes obsolètes ;
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html
- Note d'information pour limiter l'impact du SPAM ;
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-004/index.html
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien)
  http://www.auscert.org.au/render.html?it=1935

## 4 Rappel des avis et mises à jour émis

Durant la période du 16 au 22 décembre 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-491 : Vulnérabilité de Trend Micro ServerProtect
- CERTA-2005-AVI-492 : Multiples vulnérabilités dans JRun de Macromedia
- CERTA-2005-AVI-493 : Multiples vulnérabilités dans ColdFusion de Macromedia
- CERTA-2005-AVI-494 : Vulnérabilité de Courier
- CERTA-2005-AVI-495 : Vulnérabilité de Sudo
- CERTA-2005-AVI-496 : Vulnérabilité de Xmail
- CERTA-2005-AVI-497 : Mise à jour des noyaux des distributions Linux
- CERTA-2005-AVI-498 : Vulnérabilité dans Cisco Clean Access
- CERTA-2005-AVI-499 : Vulnérabilité dans la bibliothèque libavcodec
- CERTA-2005-AVI-500 : Vulnérabilité dans VMware
- CERTA-2005-AVI-501 : Vulnérabilité dans McAfee Security Center
- CERTA-2005-AVI-502 : Vulnérabilité dans le client Progam Neighborhood de Citrix
- CERTA-2005-AVI-503 : Multiples vulnérabilités des systèmes AIX d'IBM
- CERTA-2005-AVI-504 : Vulnérabilité du paquetage ipsec-tools

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

- CERTA-2005-AVI-458-001 : Vulnérabilité de la solution IPsec Openswan
  (ajout des bulletins de sécurité Gentoo, Fedora Core 3 et 4, de la référence CVE, de la note de vulnérabilité US-CERT et correction du numéro de version des sources vulnérables)
- CERTA-2005-AVI-427-001 : Vulnérabilité de Apache 2.0
  (ajout des références aux bulletins de sécurité SUSE SUSE-SR:2005:028 et Mandriva MDKSA-2005:233)
- CERTA-2005-AVI-466-002 : Vulnérabilité de Netpbm
  (ajout de la référence au bulletin de sécurité RedHat RHSA-2005:843)
- CERTA-2005-AVI-467-002 : Vulnérabilité dans le navigateur Opéra
  (ajout des références aux bulletins de sécurité SUSE et Gentoo)

– CERTA-2005-AVI-478-003 : Vulnérabilité dans Webmin/Usermin
(ajout de la référence au bulletin de sécurité SUSE)
– CERTA-2005-AVI-482-002 : Vulnérabilité de cURL/libcURL
(ajout des références aux bulletins de sécurité Gentoo GLSA 200512-09 et RedHat RHSA-2005:875)
– CERTA-2005-AVI-483-001 : Multiples vulnérabilités dans Xpdf et les bibliothèques dérivées
(ajout des références aux bulletins de sécurité Gentoo GLSA 200512-08, RedHat RHSA-2005:867, RedHat RHSA-2005:868 et RedHat RHSA-2005:878)
– CERTA-2005-AVI-486-002 : Vulnérabilité de Perl
(ajout des références aux bulletins de sécurité SUSE SUSE-SA:2005:071, RedHat RHSA-2005:880 et RedHat RHSA-2005:881)
– CERTA-2005-AVI-426-001 : Vulnérabilités de phpBB
(ajout du site de téléchargement de phpBB, de la référence au bulletin de sécurité Debian DSA-925 et des références CVE)
– CERTA-2005-AVI-458-002 : Vulnérabilité de la solution IPsec Openswan
(ajout du bulletin de sécurité SuSE)

# 5 Actions suggérées

## 5.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'inf ormation de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'orga nisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel règlementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

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. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

## 5.2 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.

## 5.3 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.

## 5.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiate. 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.

### 5.5 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.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le COSSI/CERTA peut vous aider dans ce travail d'analyse.

### 5.6 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 inexpliqués 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.

### 5.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, la DCSSI dispose d'un centre de formation :

http://www.formation.ssi.gouv.fr

## 6 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.

| Port | Protocole | Service | Porte dérobée | Référence possible CERTA |
|---|---|---|---|---|
| 21 | TCP | FTP | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 22 | TCP | SSH | – | http://www.certa.ssi.gouv.fr/site/CER |
| 23 | TCP | Telnet | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 25 | TCP | SMTP | – | http://www.certa.ssi.gouv.fr/site/CER |
| 42 | TCP | WINS | – | http://www.certa.ssi.gouv.fr/site/CER |
| 80 | TCP | HTTP | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 111 | TCP | Sunrpc-portmapper | – | http://www.certa.ssi.gouv.fr/site/CER |
| 119 | TCP | NNTP | – | http://www.certa.ssi.gouv.fr/site/CER |
| 135 | TCP | Microsoft RPC | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |

| | | | | |
|---|---|---|---|---|
| 137 | UDP | NetBios-ns | – | http://www.certa.ssi.gouv.fr/site/CER |
| 139 | TCP | NetBios-ssn et samba | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 143 | TCP | IMAP | – | http://www.certa.ssi.gouv.fr/site/CER |
| 389 | TCP | LDAP | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 443 | TCP | HTTPS | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 445 | TCP | Microsoft-smb | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 1023 | TCP | – | Serveur ftp de Sasser.E | – |
| 1080 | TCP | Wingate | MyDoom.F | – |
| 1433 | TCP | MS-SQL-Server | – | http://www.certa.ssi.gouv.fr/site/CER |
| 1434 | UDP | MS-SQL-Monitor | – | http://www.certa.ssi.gouv.fr/site/CER |
| 2100 | TCP | Oracle XDB FTP | – | http://www.certa.ssi.gouv.fr/site/CER |
| 2745 | TCP | – | Bagle | – |
| 3127 | TCP | – | MyDoom | – |
| 3128 | TCP | Squid | MyDoom | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 3306 | TCP | MySQL | – | – |
| 3389 | TCP | Microsoft RDP | – | http://www.certa.ssi.gouv.fr/site/CER |
| 4899 | TCP | Radmin | – | – |
| 5000 | TCP | Universal Plug and Play | Bobax, Kibuv | http://www.certa.ssi.gouv.fr/site/CER |
| 5554 | TCP | SGI ESP HTTP | Serveur ftp de Sasser | – |
| 6070 | TCP | BrightStor ARCserve/Enterprise Backup | – | http://www.certa.ssi.gouv.fr/site/CER |
| 6101 | TCP | Veritas Backup Exec | – | http://www.certa.ssi.gouv.fr/site/CER |
| 6112 | TCP | Dtspcd | – | http://www.certa.ssi.gouv.fr/site/CER |
| 6129 | TCP | Dameware Miniremote | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 8866 | TCP | – | Porte dérobée Bagle.B | – |
| 9898 | TCP | – | Porte dérobée Dabber | – |
| 10000 | TCP | Webmin, Veritas Backup Exec | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 10080 | TCP | Amanda | MyDoom | – |
| 11768 | TCP | – | Netdepix | – |
| 15118 | TCP | – | Netdepix | – |

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

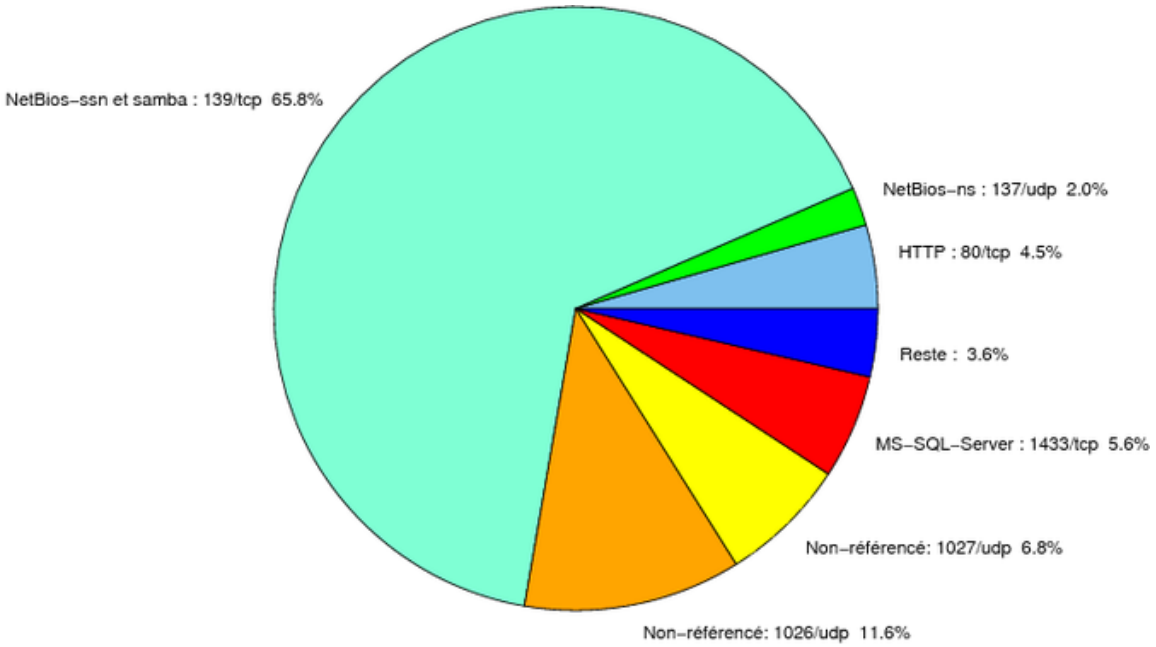


FIG. 1: Répartition relative des ports pour la semaine du 15.12.2005 au 22.12.2005

# Liste des tableaux



# Gestion détaillée du document

**23 décembre 2005** version initiale.

| port | pourcentage |
|---|---|
| 139/tcp | 65,76 |
| 1026/udp | 11,63 |
| 1027/udp | 6,84 |
| 1433/tcp | 5,59 |
| 80/tcp | 4,46 |
| 137/udp | 2,04 |
| 1434/udp | 0,81 |
| 4899/tcp | 0,79 |
| 1080/tcp | 0,54 |
| 42/tcp | 0,22 |
| 15118/tcp | 0,2 |
| 22/tcp | 0,16 |
| 3306/tcp | 0,14 |
| 6129/tcp | 0,13 |
| 10000/tcp | 0,09 |
| 5554/tcp | 0,07 |
| 9898/tcp | 0,06 |
| 2100/tcp | 0,05 |
| 5000/tcp | 0,04 |
| 1023/tcp | 0,03 |
| 6101/tcp | 0,02 |
| 6112/tcp | 0,01 |

TAB. 3: Paquets rejetés