Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 décembre 2008
N° CERTA-2008-ACT-052

**Affaire suivie par :**
CERTA

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité 2008-52**



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2008-ACT-052 |
| Titre | Bulletin d'actualité 2008-52 |
| Date de la première version | 26 décembre 2008 |
| 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.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-052.pdf
Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-052/

## 1 Le dernier de l'année

Ce numéro 052 du bulletin d'actualité du CERTA est le dernier de l'année 2008. C'est pour nous l'occasion de vous souhaiter d'excellentes fêtes de fin d'année.

L'année 2008 aura été riche en événements dans notre domaine d'activité. Dans l'immédiat, soyez vigilants avec l'envoi des tradionnelles cartes de voeux électroniques ; elles peuvent être réellement moins sympathiques que leur aspect virtuel ne le laisserait penser !

Les bulletins d'actualité contribuent au retour d'expérience : n'hésitez pas à nous solliciter afin d'améliorer notre production toujours perfectible. Notre seul objectif est de vous aider au mieux dans votre prise de décision (par prévention ou par réaction) pour la sécurité de votre réseau.

Bonne cyberannée à tous !

## 2 Périphériques de saisie sans-fil

Le CERTA a été sollicité pour un incident de sécurité mettant potentiellement en cause l'existence d'un enregistreur de frappes clavier. En effet, à première vue, les frappes clavier réalisées sur l'un des postes du réseau se retrouvaient immédiatement affichées à l'écran d'un autre poste de ce même réseau.

Après investigation, il est apparu que les deux postes en question étaient équipés de clavier et souris sans-fil pour l'un et d'une souris sans-fil pour l'autre, et par conséquent, tout ce qui était saisi par le poste disposant du clavier sans-fil était également reçu par le poste équipé du récepteur pour la souris sans-fil.

Le CERTA recommande de conduire une analyse des risques liés à l'utilisation des équipements sans-fil en fonction des besoins opérationnels. En effet, le bénéfice apporté par l'usage d'équipements de ce type doit être supérieur aux risques qu'ils entraînent.

# 3 DNS Changer v. 2.0

## 3.1 Les faits

Une nouvelle mouture du code malveillant *DNS Changer* a récemment fait son apparition sur l'Internet. Cette nouvelle version se distingue de la précédente par son mode opératoire permettant la modification des paramètres *DNS*.

Pour rappel, la précédente version détaillée dans les bulletins d'actualité CERTA-2008-ACT-047 et CERTA-2008-ACT-049, tentait de modifier les configurations des boîtiers de connexion à l'Internet afin que ces derniers distribuent des paramètres de résolution de noms erronés. Ces paramètres, une fois enregistrés, permettaient de rediriger les flux *DNS* vers des serveurs malveillants.

Cette variante, reconnue par certains éditeurs d'anti-virus sous le nom *Trojan.Flush.M*, installe un pilote réseau *NDISProt.sys* ou *ndisprot.inf* autorisant ainsi la réception et l'émission de paquets Ethernet. Une fois compromise, la machine se transforme en serveur *DHCP* afin de propager des configurations *DNS* malveillantes et rediriger tous les ordinateurs du réseau en *DHCP* -sans avoir à y installer des logiciels malveillants- vers des serveurs de noms malintentionnés basés à l'étranger.

## 3.2 Les recommandations

Le CERTA réitère les mêmes conseils :

- surveiller le trafic *DNS* afin de s'assurer que celui-ci s'effectue vers des serveurs légitimes ;
- contrôler la configuration *DNS* des clients ;
- utiliser un compte aux droits limités afin de prévenir une tentative d'installation d'un nouveau pilote.

## 3.3 Documentation

- Bulletin d'actualité CERTA-2008-ACT-047 du 21 novembre 2008 :
  htpp://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-047.pdf
- Bulletin d'actualité CERTA-2008-ACT-049 du 05 décembre 2008 :
  htpp://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-049.pdf

# 4 Voyants lumineux et fausses interprétations

## 4.1 Le cas des claviers

L'activation des lumières d'un clavier est configurable, comme l'illustrent plusieurs liens cités dans la section Documentation de cet article. Les voyants sont utilisés par défaut pour afficher des modes bien connus : majuscules, verrou numérique et défilement. En réalité, l'affectation de l'affichage du voyant, qui dépend d'un état du clavier, est programmable.

Ainsi, dans le fichier de configuration du serveur graphique X.org, il est possible d'ajouter des options (`XkbOptions`).

```
Section "Input Device"
        Identifier "Generic Keyboard"
        ...
        Option "XkbOptions" "grp:alt_shift_toggle,grp_led:scroll"
        ...
```

Le voyant « Scroll Lock » indiquera alors un changement de groupe correspondant à l'appui sur les touches « alt+shift ». D'autres applications, comme *blinkd*[1], *ledcontrol*, *mailleds* ou *tleds* sous Linux se chargent d'assurer l'utilisation des voyants pour visualiser d'autres événements : réception d'un courrier électronique, balayage de ports, etc.

On retrouve ces mêmes facilités quel que soit le système d'exploitation utilisé.

L'objet de ce paragraphe n'est pas de lister toutes les possibilités offertes mais plus simplement de montrer la faisabilité et la relative facilité à manipuler les voyants du clavier.

Le lecteur peut se demander quel usage malveillant est bien applicable ici, hormis gêner l'utilisateur ou faire fuir de l'information sous forme de clignotements lumineux.

La question est alors : est-ce bien différent pour les autres voyants existants, et en particulier pour ceux associés aux interfaces sans-fil, Bluetooth ou Wi-Fi ?

## 4.2 Le cas des interfaces sans-fil

L'activation des lumières est une action indépendante de la connexion.

À valeur d'exemple, certains portables DELL sous Ubuntu 8.04 peuvent avoir une connexion Wi-Fi active mais pas de voyant lumineux si les modules complémentaires `linux-backports-modules-XXX` ne sont pas installés.

Il existe différentes façons d'intervenir pour modifier le comportement des voyants. Cela peut se faire directement via le BIOS, le système d'exploitation et les pilotes, les combinaisons de touches configurées, etc.

Les ordinateurs portables disposent parfois d'un interrupteur (radio *killswitch*), qu'il soit physique ou logique (registre mémoire). Le fait d'avoir une touche avec une icône Wi-Fi ou Bluetooth ne suffit pas pour affirmer que le Wi-Fi est géré de manière matérielle. Un ensemble d'astuces est maintenu, par exemple, selon le modèle de cartes sur le site du projet RFSwitch (cf. section Documentation).

En fonction des pilotes utilisés et des systèmes d'exploitation, les diodes ne clignotent pas toujours comme attendu. Plusieurs discussions sur les forums confirment ces comportements inattendus (exemple sous Ubuntu Gutsy avec les pilotes ipw3945 et iwlwifi pour certaines cartes Intel).

Le voyant peut ne pas fonctionner malgré des activités de l'interface. Cela peut être dû à un problème système ou à une compromission.

En résumé :

- l'interface peut être active et connectée malgré l'absence de voyant ;
- le voyant peut être allumé et l'interface non opérationnelle ;
- etc.

Il est donc très difficile, de manière générale, de garantir l'état de son interface sans-fil à l'instant *t*. Dans le monde filaire, débrancher le câble présente bien moins d'ambiguïté.

## 4.3 Que faut-il en retenir ?

Les voyants sont des indicateurs. Ils ne sont pas liés directement à l'état de la connexion. Ils sont souvent manipulables de manière logicielle. La confiance ne peut donc pas s'appuyer complètement sur eux.

En terme de connexion Wi-Fi, la seule garantie de ne pas établir à son insu de communications reste d'enlever physiquement la carte de son support.

## 4.4 Documentation


- Note d'information DELL concernant les LED WiFi sous Ubuntu 8.04, mai 2008 : http://linux.dell.com/wiki/index.php/Ubuntu_8.04/Issues/WiFi_LED_does_not_work
- Rapport de bogue Debian, "caps-lock led on thinkpad does not work anymore", septembre 2007 : http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=440743
- M. J-J Zölde-Fejer, "Changing X.org keyboard with a shortcut - independently of desktop environment", octobre 2008 : http://www.technographer.net/changing-xorg-keyboard-with-a-shortcut-independently-of-desktop-environment/
- Exemple de module Linux, "Flashing keyboard LEDs" : http://tldp.org/LDP/lkmpg/2.6/html/x1194.html


[1] Cette application ouvre un service accessible sur un port TCP donné à toute adresse IP par défaut. Attention à son usage donc.

– Code "keyboard_leds" pour MacOS X :
http://osxbook.com/book/bonus/chapter10/kbdleds/download/keyboard_leds.c
– Modifications logicielles des cartes réseau, projet RFSwitch :
http://rfswitch.sourceforge.net/

# 5 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 18 et le 25 décembre 2008.

# 6 Liens utiles

– Mémento sur les virus :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
– Note d'information du CERTA sur l'acquisition de correctifs :
http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/
– Note d'information du CERTA sur les systèmes obsolètes :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/
– Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/
– Note d'information du CERTA sur les mots de passe :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/
– Note d'information sur la terminologie d'usage au CERTA :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/
– Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/
– Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
http://www.auscert.org.au/render.html?it=1935
– Note d'information du CERTA sur les risques associés aux clés USB :
http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/
– Note d'information du CERTA sur les outils d'indexation et de recherche :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/
– Note d'information du CERTA sur la gestion des noms de domaine :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/
– Note d'information du CERTA sur le bon usage de PHP :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/

# 7 Rappel des avis émis

Dans la période du 19 au 26 décembre 2008, le CERTA a émis les avis suivants :

– CERTA-2008-AVI-609 : Vulnérabilité Sun Solaris
– CERTA-2008-AVI-610 : Multiples vulnérabilités dans Novell Identity Manager
– CERTA-2008-AVI-611 : Vulnérabilité dans des produits Sophos
– CERTA-2008-AVI-612 : Vulnérabilités dans SPIP

– CERTA-2008-AVI-366-002 : Multiples vulnérabilités dans la machine virtuelle Java de Sun
(ajout de nouvelles références Red Hat)
– CERTA-2008-AVI-578-001 : Vulnérabilités de la machine virtuelle Java
(ajout des références CVE associées)
– CERTA-2008-AVI-608-001 : Vulnérabilité dans Moodle
(ajout de la référence CVE et du bulletin de sécurité Debian)

# 8 Actions suggérées

## 8.1 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'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme 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.

## 8.2 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 oeuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

## 8.3 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.

## 8.4 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.

## 8.5 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 CERTA peut vous aider dans ce travail d'analyse.

## 8.6 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.

## 8.7 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.ssi.gouv.fr/fr/formation/

# 9 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.

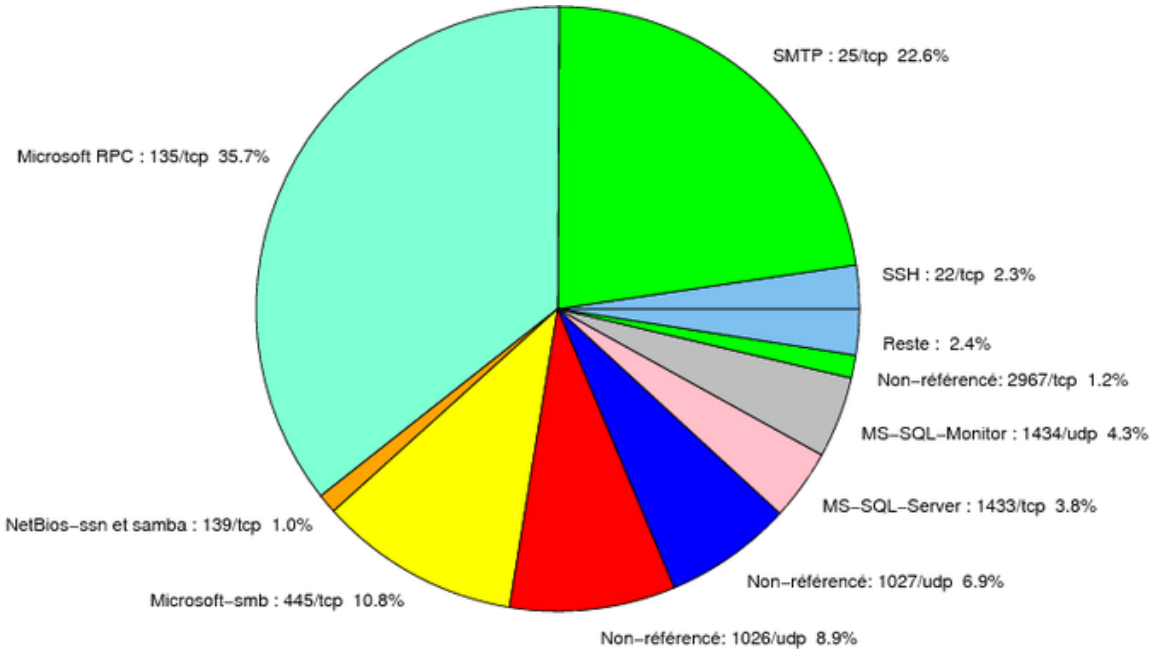


FIG. 1: Répartition relative des ports pour la semaine du 18.12.2008 au 25.12.2008

| 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<br>http://www.certa.ssi.gouv.fr/site/CER |
| 22 | TCP | SSH | – | http://www.certa.ssi.gouv.fr/site/CER<br>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<br>CERTA-2007-ALE-005-001 |
| 25 | TCP | SMTP | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 42 | TCP | WINS | – | http://www.certa.ssi.gouv.fr/site/CER |
| 69 | UDP | IBM Tivoli Provisioning Manager | – | 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<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 |
| 106 | TCP | MailSite Email Server | – | –<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<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<br>http://www.certa.ssi.gouv.fr/site/CER |
| 427 | TCP | Novell Client | – | 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<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<br>http://www.certa.ssi.gouv.fr/site/CER |

| | | | | |
|---|---|---|---|---|
| | | | | 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 | UDP | Microsoft-smb | – | http://www.certa.ssi.gouv.fr/site/CER |
| 1023 | TCP | – | Serveur ftp de Sasser.E | – |
| 1080 | TCP | Wingate | MyDoom.F | http://www.certa.ssi.gouv.fr/site/CER |
| 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 |
| 2381 | TCP | HP System Management | – | http://www.certa.ssi.gouv.fr/site/CER |
| 2512 | TCP | Citrix MetaFrame | – | http://www.certa.ssi.gouv.fr/site/CER |
| 2513 | TCP | Citrix MetaFrame | – | http://www.certa.ssi.gouv.fr/site/CER |
| 2745 | TCP | – | Bagle | – |
| 2967 | TCP | Symantec Antivirus | Yellow Worm | http://www.certa.ssi.gouv.fr/site/CER |
| 3104 | TCP | CA Message Queuing | – | http://www.certa.ssi.gouv.fr/site/CER |
| 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 |
| 3268 | TCP | Microsoft Active Directory | – | http://www.certa.ssi.gouv.fr/site/CER |
| 3306 | TCP | MySQL | – | – |
| 4899 | TCP | Radmin | – | – |
| 5000 | TCP | Universal Plug and Play | Bobax, Kibuv | 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 |
| 5151 | UDP | IPSwitch WS_TP | – | http://www.certa.ssi.gouv.fr/site/CER |
| 5151 | TCP | ESRI ArcSDE | – | http://www.certa.ssi.gouv.fr/site/CER |
| 5554 | TCP | SGI ESP HTTP | Serveur ftp de Sasser | – |
| 5900 | TCP | VNC | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 6014 | TCP | IBM Tivoli Monitoring | – | http://www.certa.ssi.gouv.fr/site/CER |
| 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 |
| 6106 | TCP | Symantec Backup Exec | – | 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 |
| 6502 | TCP | CA BrightStor ARCserve Backup | – | http://www.certa.ssi.gouv.fr/site/CER |
| 6503 | TCP | CA BrightStor ARCserve Backup | – | http://www.certa.ssi.gouv.fr/site/CER |
| 6504 | TCP | CA BrightStor ARCserve Backup | – | http://www.certa.ssi.gouv.fr/site/CER |
| 8080 | TCP | IBM Tivoli Provisioning Manager | – | 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 | – |
| 10110 | TCP | IBM Tivoli Monitoring | – | http://www.certa.ssi.gouv.fr/site/CER |
| 10916 | TCP | Ingres | – | CERTA-2007-AVI-275-001 |
| 10925 | TCP | Ingres | – | CERTA-2007-AVI-275-001 |
| 12168 | TCP | CA eTrust antivirus | – | http://www.certa.ssi.gouv.fr/site/CER |
| 13701 | TCP | Veritas NetBackup | – | http://www.certa.ssi.gouv.fr/site/CER |
| 18264 | TCP | CheckPoint interface | – | http://www.certa.ssi.gouv.fr/site/CER |
| 54345 | TCP | HP Mercury | – | http://www.certa.ssi.gouv.fr/site/CER |
| 65535 | UDP | LANDesk Management Suite | – | http://www.certa.ssi.gouv.fr/site/CER |

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

| port | pourcentage |
|---|---|
| 135/tcp | 35.7 |
| 25/tcp | 22.59 |
| 445/tcp | 10.77 |
| 1026/udp | 8.87 |
| 1027/udp | 6.85 |
| 1434/udp | 4.34 |
| 1433/tcp | 3.85 |
| 22/tcp | 2.32 |
| 2967/tcp | 1.22 |
| 139/tcp | 1.1 |
| 137/udp | 0.55 |
| 23/tcp | 0.48 |
| 80/tcp | 0.42 |
| 4899/tcp | 0.3 |
| 21/tcp | 0.24 |
| 3389/tcp | 0.18 |
| 3306/tcp | 0.12 |
| 3128/tcp | 0.06 |

TAB. 3: Paquets rejetés

# Liste des tableaux



# Gestion détaillée du document

**26 décembre 2008** version initiale.