Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 septembre 2008
N° CERTA-2008-ACT-036

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-36

Gestion du document

Référence	CERTA-2008-ACT-036
Titre	Bulletin d'actualité 2008-36
Date de la première version	05 septembre 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-036.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-036/

1 Incidents traités cette semaine

1.1 Une idée reçue sur le filoutage et les liaisons sécurisées

Comme chaque semaine, et comme tout le monde, le CERTA reçoit des courriels frauduleux l'invitant à fournir ses informations personnelles et confidentielles en cliquant sur un lien qui est en fait un site de filoutage. Le pourriel dont parle cet article contenait un lien vers une page frauduleuse déposée sur un site légitime compromis. Ce qui fait l'originalité de l'adresse de la page de filoutage c'est que le site compromis utilisait la version chiffrée du protocole http : *https*. Donc la page de filoutage bénéficiait également du protocole chiffré. Or il n'est pas rare de lire des affirmations telle que : «*Un moyen sûr de savoir si l'on se trouve sur un site de confiance est la présence de https dans l'adresse et d'un cadenas dans la fenêtre de son navigateur*».

Ce pourriel est le contre-exemple typique de cette affirmation inexacte. La présence du cadenas indique uniquement que le navigateur affiche un page utilisant un certificat. Pour s'assurer de l'authenticité de ce dernier, il convient de consulter les informations du certificat en cliquant sur l'icône du cadenas de son navigateur. Le CERTA rappelle également qu'il ne faut en aucun cas suivre les liens présents dans les courriers électroniques.

1.2 Un hébergeur « recycle » un serveur compromis

Cette semaine, le CERTA a traité un incident relatif à la compromission d'un serveur dédié chez un hébergeur. À l'origine, la victime de cet incident a commandé un serveur dédié et pré-installé par son hébergeur. Ce dernier a donc fourni un serveur installé sous *Windows* comme demandé. La victime, confiante, n'a pas prêté attention à d'anciens profils désactivés mais toujours présents sur le serveur. Quelques mois plus tard une compromission est survenue. Lors de son analyse, le CERTA a mis en évidence que le serveur avait été compromis plusieurs mois avant sa livraison et que, loin d'avoir réinstallé correctement le serveur avant de le livrer, l'hébergeur n'a même pas pris le soin de nettoyer le serveur des différents codes malveillants toujours présents.

Le CERTA rappelle qu'en cas de compromission, il convient de suivre des règles élémentaires de sécurité décrites dans la note d'information concernant les bons réflexes en cas d'intrusion dans un système d'information, notamment de réinstaller complètement à partir de souches saines.

1.2.1 Documentation

- Note du CERTA sur les bons réflexes en cas d'intrusion sur un système d'information :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/

2 Cartes mère avec système d'exploitation embarqué

Depuis quelques temps, certaines cartes mère embarquent un système d'exploitation minimal. C'est le cas notamment des cartes de marque *Asus* et de leur environnement *Splashtop* (appelé également *Express Gate*). Le système d'exploitation, un mini-linux, est fourni avec quelques outils :

- le navigateur *Firefox* ;
- l'outil de messagerie instantanée *pidgin* ;
- le logiciel *Skype* ;
- un mécanisme permettant de réaliser des copies de disque dur appelé *Drive Xpert* ;
- un visualiseur de photos.

Il est assez difficile de connaître les versions des logiciels utilisés, car *Asus* utilise son propre système de numérotation.

Ce système d'exploitation présente deux avantages :

- le premier, assez évident, est que ce système peut être utilisé pour réaliser des recherches sur l'Internet en cas de problème matériel/logiciel ;
- le second, beaucoup plus discutable, est que l'on pourrait naviguer de façon « sécurisée ». L'argument avancé est qu'il n'y a pas d'écriture sur le disque. En fait, cela dépend du port SATA sur lequel le disque dur est connecté. En effet, si le disque dur est connecté à l'un des deux ports SATA accessibles depuis *Drive Xpert*, alors des écritures devraient être possibles. Les logiciels installés n'étant pas forcément à jour, de nombreux problèmes de sécurité subsistent.

L'utilisation d'*Express Gate* peut éventuellement constituer un contournement de la politique de sécurité, notamment du fait des logiciels qui y sont contenus. Il est cependant possible, via le BIOS, de désactiver *Express Gate* puis de protéger l'accès au BIOS par un mot de passe.

2.1 Documentation

- Article d'Asus concernant Splashtop :
  http://usa.asus.com/news_show.aspx?id=8750

3 Nouveau navigateur : Google Chrome

3.1 Présentation générale

Google a mis à disposition du public, cette semaine, une première version de test (bêta) de son navigateur pour les systèmes Windows XP et Vista. Ce dernier, nommé `Google Chrome` est la version estampillée « Google » du projet libre `Chromium`.

Le nouveau navigateur propose plusieurs fonctionnalités intéressantes :

- l'utilisateur accède à une configuration et une interface simplifiées ;

– il y a un processus pour chaque manipulation d'onglets et celui-ci dispose de droits très réduits ;
– la barre de navigation sert également d'accès au moteur de recherche. Elle est appelée « omnibox » (que l'on peut traduire par « boîte à tout faire ») ;
– une navigation plus discrète laissant moins de traces sur le poste de l'utilisateur et accessible via la combinaison de touches clavier `Ctrl - Shift - n` ;
– il existe un accès à certaines adresses particulières, comme `about:`, `about:cache`, `about:crash`, `about:dns`, `about:histograms`, `about:memory`, `about:network` ou `about:plugins` ;
– les informations de l'utilisateur sont stockées sous forme de fichier SQLite (format 3) ;
– etc.

L'objectif de cet article n'est pas d'établir une comparaison entre différents navigateurs. Au contraire, une certaine diversité dans le choix des applications est une bonne chose. Il tient cependant à rappeler certaines défiances à avoir vis-à-vis des versions de test encore instables et n'ayant pas fait l'objet de contrôles complets.

3.2 Problématique des versions de test

3.2.1 Des remarques et des vulnérabilités

La presse a rappelé cette semaine qu'une version de test pouvait souffrir de défauts et de vulnérabilités. Dans la version disponible du navigateur, on remarque par exemple que :

– l'interprétation de certaines adresses réticulaires ne s'effectue pas correctement, provoquant l'arrêt complet du navigateur ;
– la version actuelle de Google Chrome n'utilise pas la dernière version du moteur WebKit. Or le moteur intégré actuellement souffre de quelques vulnérabilités qui ont déjà été rencontrées avec des navigateurs comme Safari ou Epiphany ;
– le choix des moteurs de recherche « par défaut » est limité à ceux fournis dans la version de base ;
– l'utilisation de l'option avancée « Activer la protection contre le phishing et les logiciels malveillants » induit des écritures et des téléchargements de listes sur le disque (fichiers pouvant dépasser les 50Mo) ;
– l'`omnibox` ne permet pas de manière simple de déterminer si les données entrées sont directement utilisées comme adresse de site sur lequel on souhaite naviguer ou si elles sont envoyées à un autre service pour retourner une recherche ou des suggestions. Par défaut, il est préférable de désactiver l'option « Afficher des suggestions pour les requêtes et les URL entrées dans la barre d'adresse » ;
– la gestion des fichiers de session Google (*cookies*) se complique davantage avec l'utilisation de nouveaux fichiers pour la mise à jour du navigateur (cf. article « Contournement HTTPS publié dans CERTA-2008-ACT-033) ;
– etc.

Une simplification de l'interface d'accès et de la configuration du navigateur se fait au détriment d'un réglage de configuration et de sécurité plus fin.

3.2.2 Recommandations

Comme le CERTA l'a déjà préconisé à l'apparition des versions de tests de Firefox 3 et d'IE8, il est préférable de ne pas déployer actuellement une application dans une version qui n'est pas stable. Il faut également sensibiliser les utilisateurs afin qu'ils ne prennent pas l'initiative de l'installer sur leur poste, l'installation ne nécessitant pas de droits particuliers.

Il est possible de vérifier l'usage de ce navigateur en regardant les journaux de connexions d'une passerelle de navigation. Google Chrome n'a pas de valeur `user-agent` propre. Celui actuellement présenté par le navigateur est très semblable à celui de Safari, de la forme :

```
Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US) AppleWebKit/XX
                          (KHTML, like Gecko) Chrome/XX Safari/XX
```

où "XX" peut prendre différentes valeurs.

Sous Safari, la chaîne de caractères « `Chrome` » est normalement remplacée par « `Version` ».

Il ne faut enfin pas sous-estimer les risques de divulgations d'informations, comme cela a été évoqué dans la note CERTA-2006-INF-009.

Il peut être préférable, pour s'affranchir de certaines contraintes d'utilisation, d'utiliser directement le projet Chromium sous licence BSD. Celui-ci a aussi les derniers correctifs.

3.3 Documentation associée

- Site officiel du navigateur Google Chrome :
  http://www.google.com/chrome
- Site du projet Chromium :
  http://code.google.com/chromium
- Modifications apportées au développement du projet Chromium :
  http://codereview.chromium.org/
- Conditions d'utilisation EULA du navigateur Chrome :
  http://www.google.com/chrome/eula.html
- Discussions concernant les conditions d'usage et des changements effectués :
  http://tapthehive.s483.sureserver.com/chrome.html
- Note d'information du CERTA CERTA-2006-INF-009, « Outils d'indexation et de recherche » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/

4 Mise à jour semi-automatique de Firefox en version 3

Les utilisateurs de Firefox 2 vont se voir proposer, comme mise à jour de leur navigateur, la version 3, alors que jusque là les 2 « branches » évoluaient parallèlement. La version 2.0.0.X est maintenue jusqu'à mi-décembre 2008 et reste disponible au téléchargement (c.f. la section Documentation). Les modules additionnels ne fonctionnant pas tous avec la nouvelle version du navigateur, il peut être tentant de conserver l'ancienne. Cependant, la version 3 est disponible depuis plusieurs mois et il vaut mieux se poser la question du niveau de maintenance des modules concernés et, dans la mesure du possible, les abandonner, quitte à les réinstaller le jour où ils seront à nouveau compatibles. De manière générale, l'usage de ces modules est à éviter : ils sont dans la majorité des cas développés par des personnes tierces, ils ne sont pas audités et ils ne sont pas toujours convenablement maintenus.

4.1 Documentation

- Annonce de la mise à jour :
  http://developper.mozilla.org/devnews/index.php/2008/08/25/firefox-2-about-to-get-a-major-update/
- Présentation de fonctionnalités de protection de Firefox 3 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-028
- Téléchargement de Firefox 2 :
  http://www.mozilla.com/en-US/firefox/all-older.html

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 28 août et le 04 septembre 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 28 au 05 août 2008, le CERTA a émis les avis suivants :

– CERTA-2008-AVI-432 : Vulnérabilités dans Red Hat Directory Server
– CERTA-2008-AVI-433 : Vulnérabilité dans libxml2
– CERTA-2008-AVI-434 : Vulnérabilité de HP Enterprise Discovery
– CERTA-2008-AVI-435 : Vulnérabilités de AWStats Totals
– CERTA-2008-AVI-436 : Vulnérabilité dans IBM WebSphere
– CERTA-2008-AVI-437 : Vulnérabilité dans ClamAV
– CERTA-2008-AVI-438 : Vulnérabilité dans IBM AIX
– CERTA-2008-AVI-439 : Vulnérabilité du noyau de FreeBSD pour plateforme amd64
– CERTA-2008-AVI-440 : Multiples vulnérabilités dans VLC
– CERTA-2008-AVI-441 : Multiples vulnérabilités des équipements Cisco ASA et PIX
– CERTA-2008-AVI-442 : Multiples vulnérabilités dans Novell eDirectory
– CERTA-2008-AVI-443 : Vulnérabilité dans OpenOfficeorg
– CERTA-2008-AVI-444 : Multiples vulnérabilités dans Wireshark

Pendant la même période, l'avis suivant a été mis à jour :

– CERTA-2008-AVI-428-001 : Vulnérabilités dans des mises à jour d'OpenSSH sous Red Hat
(ajout du CVE spécifique pour l'incident)

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.formation.ssi.gouv.fr

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.

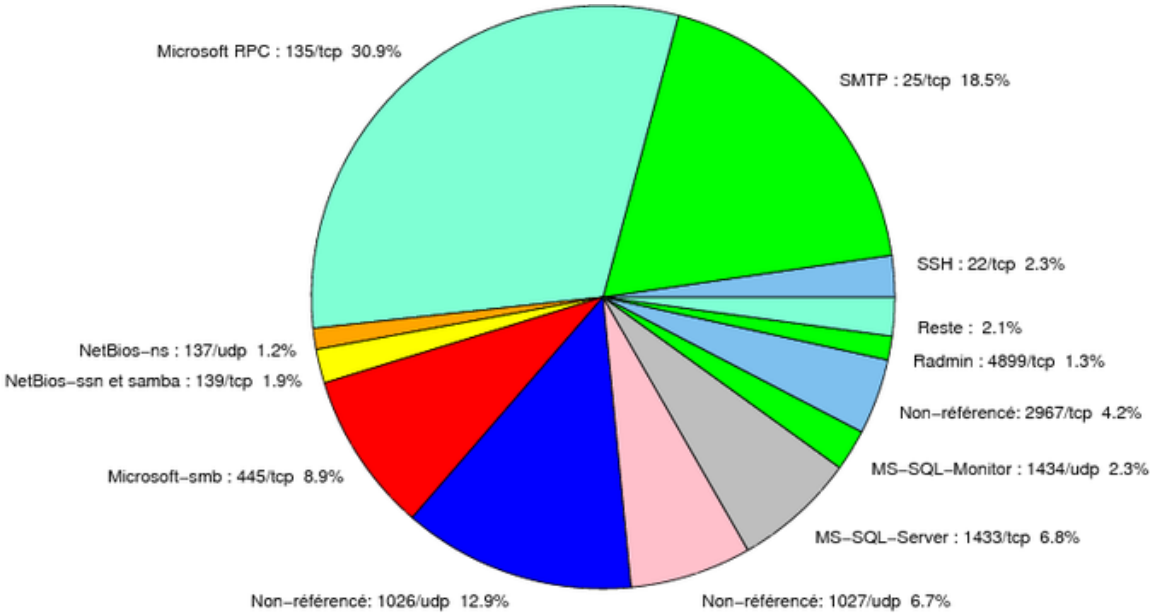

FIG. 1: Répartition relative des ports pour la semaine du 28.08.2008 au 04.09.2008

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER CERTA-2007-ALE-005-001
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CER 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 http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
106	TCP	MailSite Email Server	–	– 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 http://www.certa.ssi.gouv.fr/site/CER 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 http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER 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 http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER 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 http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER

				http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER 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 http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER 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 http://www.certa.ssi.gouv.fr/site/CER 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 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 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 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	30.88
25/tcp	18.53
1026/udp	12.88
80/tcp	12.65
445/tcp	8.96
1433/tcp	6.77
1027/udp	6.74
2967/tcp	4.18
1434/udp	2.29
3128/tcp	1.99
139/tcp	1.88
4899/tcp	1.31
137/udp	1.16
23/tcp	0.75
21/tcp	0.6
3306/tcp	0.11
143/tcp	0.07
1080/tcp	0.03

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

05 septembre 2008 version initiale.