Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 mai 2009
N° CERTA-2009-ACT-018

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-18

Gestion du document

Référence	CERTA-2009-ACT-018
Titre	Bulletin d'actualité 2009-18
Date de la première version	04 mai 2009
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-2009-ACT-018.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-2009-ACT-018/

1 Un outil de développement mis en ligne

Cette semaine, le CERTA a participé au traitement d'un incident relatif à la compromission d'un serveur Web. La mise en évidence de la compromission a débuté par la découverte d'un kit de filoutage (ou *phishing*). La vulnérabilité exploitée était en fait assez simple : il n'y avait aucun mot de passe pour le compte d'administration de la base de données. Le responsable du serveur avait, en effet, installé une boite à outils pour le développement Web que l'on trouve sur l'Internet. Ce kit permet d'installer, en une fois, les services *Apache*, *MySQL*, *PHP* et *Perl*. Bien que ce kit semble régulièrement mis à jour, ses auteurs indiquent qu'il n'est pas destiné à la production et qu'il n'y a aucune sécurité par défaut :

- aucun mot de passe pour le compte d'administration de la base de données ;
- le serveur de base de données accessible depuis le réseau ;
- le logiciel *phpMyadmin* accessible depuis le réseau ;
- des identifiants par défaut de certaines applications connues.

Cet incident révèle plusieurs types de problèmes :

- la mise à disposition sur l'Internet d'un applicatif qui n'est pas destiné à la production ;
- l'utilisation d'une installation par défaut malgré les avertissements des auteurs de l'outils ;
- l'absence de sécurité de ce kit d'installation.

2 Actualités Microsoft

2.1 Office 2007 Service Pack 2

La semaine dernière, Microsoft a publié le service pack 2 pour sa suite bureautique Office 2007. Cette mise à jour comprend l'ensemble des correctifs publics publiés jusqu'en février 2009 et de nouveaux correctifs spécifiques au service pack. Ceci inclut, en plus des mises à jour de sécurité, des mises à jour de stabilité et de performance ainsi que quelques nouvelles fonctionnalités.

Pour plus d'informations, se référer à l'article KB953195 de la base de connaissances de Microsoft (cf. Documentation).

2.2 Autres nouveautés

Pour les abonnés *Technet* et *MSDN*, Microsoft a également publié les logiciels suivants :

– service pack 2 pour Windows Vista et Windows Server 2008 ;

– Windows 7 release candidate.

Pour rappel, le service pack 2 est en fait le premier service pack de Windows Server 2008 (ce dernier correspondant à Windows Vista service pack 1). Ces mises à jour seront disponibles pour le grand public très prochainement.

En ce qui concerne Windows 7, il s'agit encore d'une version de test et il n'est donc pas recommandé d'installer ce système sur une machine de production.

2.3 Documentation

– Description de Office 2007 Service Pack 2 :
http://support.microsoft.com/953195

– Description du service pack 2 pour Windows Vista et Windows Server 2008 :
http://technet.microsoft.com/en-us/library/dd335036.aspx

– Bloc-notes de P. Saulière, Microsoft France :
http://blogs.technet.com/pascals/archive/2009/05/04/windows-vista-sp2-et-windows-server-2008-sp2-sur-technet-et-msdn.aspx

3 Les antivirus et les fichiers d'archivage

3.1 Présentation

Les fichiers d'archivage (`.zip`, `.gz`, `.rar`, `.cab`, etc.) ont toujours constitué un problème pour les antivirus. En effet, un code malveillant peut être contenu dans l'archive ou dans un des fichiers qu'elle contient. Pour analyser les fichiers contenus dans une archive, il est nécessaire que l'antivirus décompresse celle-ci à l'aide de préprocesseurs spécifiques à chaque mode d'archivage.

Ces préprocesseurs de décompression font malheureusement l'objet de vulnérabilités. En particulier, un chercheur en sécurité informatique a trouvé des vulnérabilités dans quasiment toutes les passerelles d'antivirus permettant de contourner le mécanisme de vérification des archives. Concrètement, l'exploitation de la vulnérabilité permet à un code malveillant inclus dans une archive de traverser une passerelle d'antivirus. Les conséquences sont variables : si cette archive est ensuite manipulée par un utilisateur, il est possible qu'un antivirus sur le poste client réagisse lors de l'exécution du code malveillant. Par contre, si la protection antivirale ne repose que sur la passerelle, alors l'archive pourra être perçue comme sûre par les utilisateurs.

Les éditeurs d'antivirus réagissent différemment à ces problèmes : certains sortent un correctif ainsi qu'un avis de sécurité (voir par exemple avis CERTA-2009-AVI-033), d'autres font des corrections « silencieuses » (le moteur de l'antivirus est mis à jour automatiquement) ou encore choisissent de ne pas traiter cette vulnérabilité.

Le CERTA n'a pas connaissance de cas d'exploitation de ces vulnérabilités. Le chercheur ayant fait ces découvertes tient un bloc-notes (*blog*) dans lequel il cite les différents produits d'antivirus ainsi que les réactions des éditeurs. Il ne donne pas de détails quant aux vulnérabilités.

3.2 Documentation

– Article sur le *blog* de Thierry Zoller :
http://blog.zoller.lu/2009/04/case-for-av-bypassesevasions.html

4 Les procédures de mises à jour de Mozilla Firefox

4.1 Introduction

Le CERTA recommande régulièrement de maîtriser les connexions sortantes de son réseau, et en particulier les procédures de mises à jour. Celles-ci sont indispensables mais doivent être faites avec précaution. Il faut donc au minimum :

- s'assurer de bien communiquer avec le ou les sites de mises à jour légitimes ;
- pouvoir vérifier l'intégrité des données récupérées ;
- contrôler les informations échangées avec les sites distants pour éviter des fuites d'information ;
- avoir la possibilité d'effectuer les mises à jour hors connexion ;
- pouvoir éventuellement garantir la discrétion des mises à jour (ne pas annoncer à tous les applications et les versions utilisées, etc.).

Qu'en est-il par exemple des procédures de mises à jour pour le navigateur Mozilla Firefox ?

4.2 Concernant le navigateur Mozilla Firefox

Le navigateur Mozilla Firefox est relativement déployé. Or il semble que la procédure de mise à jour de ce dernier n'est pas vraiment maîtrisée par les utilisateurs. L'objet de cette section est donc de reprendre les points essentiels de mises à jour.

La procédure de mise à jour automatique sous Mozilla Firefox se fait en plusieurs étapes distinctes :

1° le navigateur vérifie régulièrement sur les serveurs de Mozilla si des mises à jour sont disponibles. Cette vérification a lieu à chaque démarrage du navigateur ainsi qu'à certains intervalles de temps précisés dans la configuration (`about:config`) par la variable `app.update.interval`. Il s'agit en secondes de la durée avant un nouveau test. La valeur par défaut est fixée à 86400, soit 1 jour. Cette valeur est prise en compte si la variable `app.update.enabled` est à *true*.

2° le navigateur émet à chaque vérification une requête en HTTPS (GET) précisée dans la variable `app.update.url`. Elle est généralement de la forme :

```
https://aus2.mozilla.org/update/3/Firefox/3.0.9/2009XXXXXX/...fr/.../default/defau
```

La version indiquée dans l'adresse réticulaire (3.0.9) est la dernière version installée sur la machine. L'adresse précise aussi le type de plate-forme et la langue installée. Cette vérification a pour objectif de récupérer un fichier nommé `update.xml`. Il se présente sous la forme suivante :

```
Si aucune mise à jour n'est annoncée :

<updates></updates>

Si une mise à jour est disponible :


<updates>
<update type="minor" version="3.0.10" extensionVersion="3.0.10"
    buildID="200904XXXX"
    detailsURL="http://www.mozilla.com/fr/firefox/3.0.10/releasenotes/">

<patch type="complete"
    URL="http://download.mozilla.org/?product=firefox-3.0.10-complete&os=xx&lang=f
    hashFunction="SHA1" hashValue="xxxxxxxxxxxxxxxxxx" sizeValue="xxx">

<patch type="partial"
    URL="http://download.mozilla.org/?product=firefox-3.0.10-partial&os=xx&lang=fr
    hashFunction="SHA1" hashValue="xxxxxxxxxxxxxxxxxx" sizeValue="xxx">
</updates>
```

Le lecteur voit donc ici que le fichier indique ensuite deux possibilités de téléchargement (partiel ou complet) vers un nouveau site. La communication se fait ici en clair. Une mise à jour partielle applique un patch de différence binaire tandis qu'une complète procède aux remplacements de tous les fichiers impliqués dans la mise à jour.

3° le téléchargement aux adresses indiquées ci-dessus d'un fichier au format `.MAR` (pour *Mozilla ARchive*). Son intégrité est vérifiée par le navigateur en comparant l'empreinte annoncée dans le fichier `update.xml` avec celle obtenue après calcul sur le fichier reçu. Le fichier est une archive contenant les fichiers de mise à jour ainsi qu'un index. Cet index précise simplement les endroits (offsets) où aller chercher les fichiers insérés dans le `.MAR`, ainsi que leurs noms et les droits associés.

4.3 Mises à jour hors connexion

Le lecteur aura compris à la lecture du précédent paragraphe qu'il est donc bien possible de faire une mise à jour hors connexion des navigateurs Mozilla Firefox. Deux méthodes sont possibles :

- créer un serveur avec un fichier `update.xml` adéquat vers lequel les navigateurs vont chercher les mises à jour à installer. Il faut donc également changer l'adresse de la variable `app.update.url` dans la configuration des navigateurs. Une documentation existe à l'adresse suivante (néanmoins le lien n'est pas fonctionnel à la date de rédaction de cet article) :
  http://developer.mozilla.org/en/docs/Setting_up_an_update_server
- copier localement les fichiers de mises à jour .MAR dans des répertoires dédiés sur les machines et lancer l'applicatif fourni avec Firefox pour forcer les mises à jour. Le résultat de la mise à jour est consultable dans le fichier `update.status`. L'ensemble de la manipulation est documenté à l'adresse :
  https://wiki.mozilla.org/Software_Update:Manually_Installing_a_MAR_file

4.4 Références

- Documentation Mozilla concernant les procédures de mises à jour Firefox :
  https://wiki.mozilla.org/Software_Update
- Code source de la bibliothèque *libmar* :
  https://bugzilla.mozilla.org/show_bug.cgi?id=296303
- Description de la variable `App.update.interval` sur MozillaZine :
  http://kb.mozillazine.org/App.update.interval

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 23 et le 30 avril 2009.

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 24 avril au 01 mai 2009, le CERTA a émis l'alerte et les avis suivants :

- CERTA-2009-ALE-006 : Multiples vulnérabilités dans Adobe Reader et Adobe Acrobat
- CERTA-2009-AVI-161 : Vulnérabilités dans Symantec Brightmail Gateway
- CERTA-2009-AVI-162 : Vulnérabilité dans Google Chrome
- CERTA-2009-AVI-163 : Multiples vulnérabilités dans HP StorageWorks
- CERTA-2009-AVI-164 : Vulnérabilités dans apt
- CERTA-2009-AVI-165 : Vulnérabilité dans FreeBSD
- CERTA-2009-AVI-166 : Vulnérabilité dans Mozilla Firefox
- CERTA-2009-AVI-167 : Vulnérabilités dans des produits Symantec
- CERTA-2009-AVI-168 : Multiples vulnérabilités dans des produits Symantec
- CERTA-2009-AVI-169 : Vulnérabilité dans Citrix Web Interface
- CERTA-2009-AVI-170 : Vulnérabilité dans HP-UX

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.

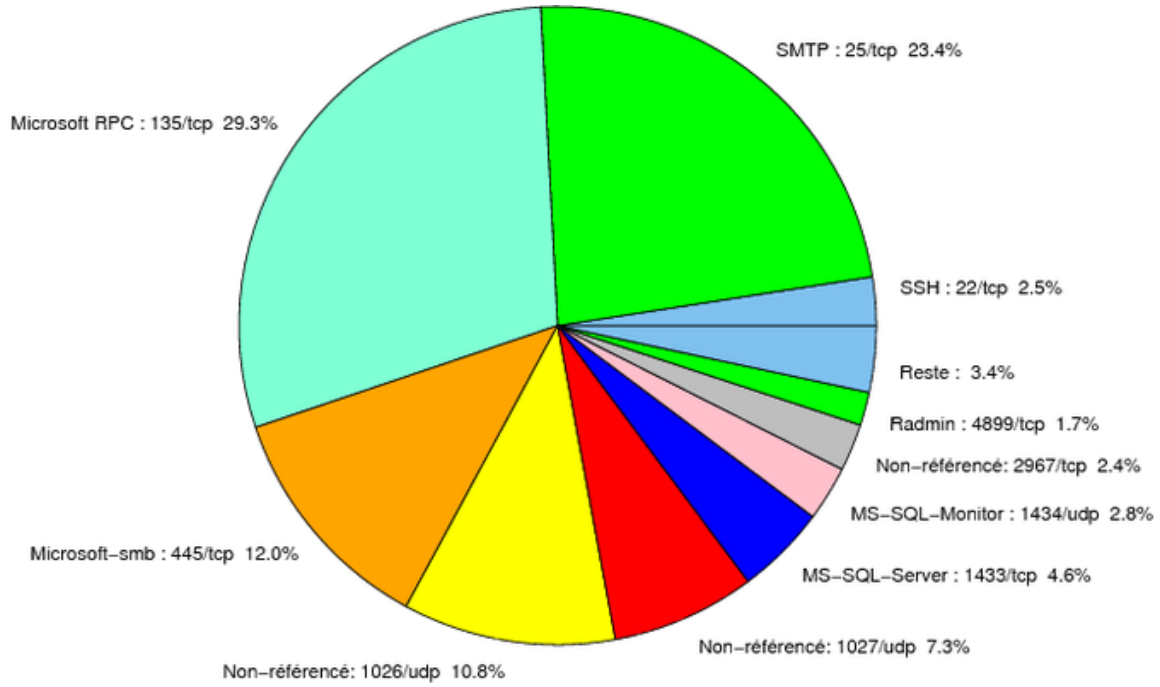

FIG. 1: Répartition relative des ports pour la semaine du 23 au 30 avril 2009

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	29.32
25/tcp	23.38
445/tcp	11.95
1026/udp	10.78
1027/udp	7.29
1433/tcp	4.58
1434/udp	2.77
22/tcp	2.45
2967/tcp	2.39
4899/tcp	1.67
80/tcp	1.09
23/tcp	0.77
3128/tcp	0.38
3389/tcp	0.19
3306/tcp	0.12
1080/tcp	0.06

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

04 mai 2009 version initiale.