Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 juin 2007
N° CERTA-2007-ACT-026

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-26

Gestion du document

Référence	CERTA-2007-ACT-026
Titre	Bulletin d'actualité 2007-26
Date de la première version	29 juin 2007
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-2007-ACT-026.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-2007-ACT-026/

1 Attaques contre *EVA-WEB*

Depuis le début de la semaine, de nombreuses attaques ciblant l'applicatif *EVA-WEB* ont eu lieu. Ces attaques exploitent une vulnérabilité de type `php include` rendue publique et corrigée en janvier 2007. Elles laissent des traces très significatives dans les journaux visibles en effectuant des recherches du type :

```
egrep '(aide|perso).http' access_log
```

Le CERTA recommande l'application du correctif de sécurité disponible à l'adresse suivante :
http://www.spip-edu.edres74.net/article.php3?id_article=210
Le CERTA invite également les administrateurs de sites utilisant *EVA-WEB* à rechercher dans leurs journaux d'éventuelles attaques à l'aide de la commande indiquée précédemment.

2 Sage comme une image ?

Une manière de cacher du code consiste à le dissimuler dans un fichier d'image dont la spécification du format est laxiste.

En effet, une propriété de certains formats de fichiers permet à des images GIF, JPG ou BMP par exemple d'être également des scripts PHP fonctionnels.

Cette propriété est par exemple représentée par les commentaires de texte insérés dans le fichier image, interprétables par PHP qui y retrouve les balises attendues.

Il peut s'agir d'une image GIF par exemple.

```
certa@labo:~$ file MonImage.gif
monImage.gif: GIF image data, version 89a, 50 x 80
```

Cette image pourra être visualisée par tout outil de dessin. Mais elle pourra également être interprétée directement dans un script PHP. Des preuves de faisabilité intégrant du code comme `phpinfo()` ou `alert(0);` ont été rapidement publiées. Par exemple, la page HTML suivante affichera une alerte :

```
certa@labo:~$ cat page.html
<_img src=MonImage.gif></_img>
<!-- affiche l'image dans le navigateur -->
<_script src=MonImage.gif></_script>
<!-- exécute l'alerte incluse dans le fichier -->
```

Les motivations qui peuvent pousser à utiliser de telles images peuvent être :

- certaines applications de téléchargement, notamment écrites en PHP, filtrent et vérifient uniquement le type MIME indiqué. Les images sont rarement refusées. Rien n'empêche, cependant, une personne malveillante de modifier l'en-tête de sa requête, et d'y insérer une image particulière en ajoutant le paramètre `Content-Type: image/gif`. Le type MIME n'est pas représentatif du contenu du fichier. C'est donc une façon incidieuse d'introduire un script.
- D'autres tests pour vérifier qu'il s'agit d'une image consistent à vérifier sa taille par la commande dédiée `getimagesize()` sous PHP. D'autres encore vérifient simplement l'extension. Dans tous les cas, ces politiques de filtrage ne sont clairement pas suffisantes pour éviter l'exécution de tels fichiers.
- les extensions de fichiers passées à l'interpréteur PHP dépendent souvent de la configuration du serveur Web. Or cette configuration est souvent méconnue des développeurs et mainteneurs de sites.

Une page insérée sur un site et contenant de telles images peut donc passer inaperçue. Un rapide survol du code source des pages par l'administrateur ne permettra pas de visualiser le code injecté.

Les sites hébergeant de telles images peuvent également servir de relais pour exécuter indirectement du code. Par exemple, si l'image `MonImage.gif` est placée sur SiteA :

- SiteA peut être un hébergeur d'images, ce service étant proposé sur plusieurs sites directement ;
- SiteA a une faille d'inclusion dans son code ayant permis l'insertion illégitime de l'image ;
- SiteA autorise le téléchargement de fichiers, ou des commandes de type `PUT`, ou `php_include()` ;

La personne malveillante peut inciter un utilisateur à cliquer sur le lien :

`http://SiteA.addresse/images/MonImage.gif?les_commandes_malveillantes`

Le code malveillant sera exécuté à partir du script hébergé par SiteA.

2.1 Recommandations du CERTA

Le CERTA recommande donc fortement aux administrateurs :

- de bien vérifier au cours d'un téléchargement la nature de l'image, en la renommant, ou mieux, en la convertissant par exemple ;
- d'avoir une politique de nommage cohérente des images ;
- de vérifier régulièrement l'intégrité des répertoires et des fichiers du site sur le serveur Web ;
- de regarder avec attention les journaux du serveur Web, afin de détecter toute requête anormale (`GET MonImage.gif?variable=`).

Le CERTA rappelle enfin aux utilisateurs de désactiver le JavaScript par défaut, et de ne l'utiliser que sur des sites de confiance, quand cela est nécessaire ;

3 De nouveaux formats pour les applications bureautiques

Le CERTA a publié dans son bulletin d'actualité CERTA-2007-ACT-024 une mise en garde contre les informations qui peuvent se dissimuler dans les documents bureautiques Office. Les données visibles par le biais de l'application ne sont pas nécessairement celles présentes dans le fichier. D'autres peuvent subsister.

Depuis 2006, de nouveaux formats, dits « ouverts » ont fait leur apparition. Parmi ceux-ci, deux se distinguent actuellement :

- `OpenDocument` : sa version 1 est actuellement proposée par les suites *Open Office* version 2, *Sun Star Office*, *Koffice*, *Neo Office* ou *Abiword*. Il est standardisé sous l'ISO/IEC 26300:2006 et les extensions des fichiers associées sont notamment `.odt`, `.ods`, `.odp`, `.odg` ;
- `Open XML` : ce standard ECMA-376 est utilisé essentiellement dans la suite *Microsoft Office 2007*. Les extensions associées les plus courantes sont `.docx`, `.xlsx`, `.pptx`, `.accdb`, ou alors `.docm`, `.xlsm` ou `.pptm` s'ils contiennent des macros ;

La compatibilité entre ces deux formats est plus ou moins assurée par des outils tiers ou offerts par les différentes applications, mais ils gardent chacun des caractéristiques propres. Hormis le fait qu'un document est en réalité un fichier compressé ZIP contenant différents fichiers XML, voici les structures classiques de chacun d'eux :

1° une fois décompressé, un fichier `Open XML` peut contenir :
   - `[Content_Types].xml` qui décrit les fichiers de l'archive ;
   - `word/styles.xml` qui contiennent les styles du document ;
   - `word/settings.xml` qui donnent certains paramètres pour le document ;
   - les fichiers `.rel` dans le répertoire `_rels` qui indiquent les relations entre les différents fichiers XML composant le document ;
   - un répertoire `embeddings` qui peut contenir les fichiers imbriqués dans le document ;
   - un répertoire `media` qui regroupent les différentes images, sons et autres fichiers annexes.

2° une fois décompressé, un fichier `OpenDocument` peut contenir :
   - `content.xml` qui est le corps du document ;
   - `styles.xml` qui donne la description du style du document ;
   - `meta.xml` qui produit les méta-données du document, comme le nom de l'auteur ou le titre ;
   - `settings.xml` qui fournit les paramètres globaux du document ;
   - `META-INF/manifest.xml` qui décrit les fichiers de l'archive ;
   - les images ou objets éventuels.

Malgré l'apparente clarté de ces deux formats, il y a quelques problématiques à prendre en compte avant de déployer et utiliser de tels formats :

- la gestion des « macros » n'est pas simple. Les deux formats prennent en compte différents langages comme `Basic`, `Javascript`, `Java` ou `Python`. Dans `OpenDocument`, leur exécution peut être liée à des événements, comme l'ouverture ou la fermeture du document, et elles ne sont pas signées avec le reste du document.
- les objets `OLE` lient très étroitement l'application de bureautique à la version du système d'exploitation Windows. Leur format propre n'est pas forcément « ouvert » (OLE2) ;
- les scripts ne sont pas directement interprétés, mais peuvent l'être suite à une conversion particulière ;
- les macros peuvent être ou non signalées, en fonction des documents imbriqués. De manière générale, les imbrications de documents peuvent toujours être trompeuses ;
- l'interprétation de ces documents repose sur le désarchivage, la décompression, et l'encodage. En d'autres termes, la fragilité des bibliothèques associées peut être également l'objet d'une exploitation par ces documents.

Le CERTA recommande, en conclusion, de bien préparer la transition vers ces nouveaux formats. L'administrateur doit adapter ses règles de filtrage aux vicissitudes de ces derniers, et ne pas considérer, trop simplement, que l'« ouverture » de ses nouveaux formats soit nécessairement un signe de confiance. L'ouverture de ces formats ne signifie pas non plus que tout le contenu soit lisible et compréhensible. Des fichiers au format propriétaire peuvent très bien se dissimuler dans l'archive.

4 Rappel sur les mots de passe

Dans le bulletin d'actualité CERTA-2007-ACT-027 de la semaine dernière était publié un article sur les mots de passe. Celui-ci détaillait les principaux risques liés à ceux-ci :

- les mots de passe faibles, dérivés du nom de compte, de mots du dictionnaire, de dates, de noms propres, etc. ;
- les mots de passe mal protégés : stockés dans un fichier accessible par tous ;
- les mots de passe qui transitent en clair : utilisés par des applications non sécurisées comme Telnet et FTP, par exemple.

Le CERTA rappelle l'importance de ces trois points, et dans ce contexte avertit également du risque de l'utilisation d'outils en ligne en rapport avec des mots de passe ou clés de chiffrement.

Pour illustration, des outils de calcul en ligne de clés PSK WPA existent sur l'Internet, obtenus à partir de la *passphrase* et du *SSID* que l'on doit fournir. Certains fonctionnent uniquement en local avec du code Javascript, mais d'autres envoient les informations au serveur. Ces informations envoyées peuvent évidemment être utilisées à mauvais escient, soit directement contre le réseau de la machine client ou simplement pour renforcer des dictionnaires. Si les créateurs de l'outil peuvent être de bonne foi (le service a été proposé cette semaine dans le cadre d'un projet de bonne réputation), ces informations peuvent cependant être envoyées en clair, ou récupérées à cause d'un *keylogger* (enregistreur de frappes clavier) même si le code fonctionne uniquement en local sur le navigateur.

Il ne faut pas sous-estimer ce qu'il est possible de faire en JavaScript, et croire que son exécution sur le poste client implique que les données manipulées resteront sur le poste client uniquement.

Le CERTA recommande ainsi que l'utilisation de telles applications se fasse sur des postes isolés de l'Internet.

4.1 Documentation

Note d'information CERTA-2005-INF-001 « Les mots de passe »
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/

5 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 21 et le 28 juin 2007.

6 Liens utiles

- Mémento sur les virus :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
- Note d'information sur l'acquisition de correctifs :
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/index.html
- Note d'information sur les systèmes obsolètes :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html
- Note d'information sur les bonnes pratiques concernant l'hébergement mutualisé :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/index.html
- Note d'information sur les mots de passe :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html
- Note d'information sur la terminologie d'usage au CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/index.html
- Note d'information sur les enjeux de sécurité liés à une migration vers IPv6 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-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
- Note d'information du CERTA CERTA-2006-INF-006, Risques associés aux clés USB :
  http://www.certa.ssi.gouv.f r/site/CERTA-2000-INF-006/
- Note d'information du CERTA CERTA-2006-INF-009 sur les outils d'indexation et de recherche :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/

– Note d'information du CERTA CERTA-2007-INF-001 sur la gestion des noms de domaine :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/
– Note d'information sur le bon usage de PHP :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002

7 Rappel des avis émis

Durant la période du 22 au 28 juin 2007, le CERTA a émis les avis suivants :

– CERTA-2007-AVI-276 : Vulnérabilité de produit McAfee
– CERTA-2007-AVI-277 : Plusieurs vulnérabilités dans Apple MacOS X
– CERTA-2007-AVI-278 : Vulnérabilités dans Wireshark
– CERTA-2007-AVI-279 : Vulnérabilités dans Trend Micro OfficeScan
– CERTA-2007-AVI-280 : Vulnérabilité d'IBM Websphere
– CERTA-2007-AVI-281 : Vulnérabilité dans Wordpress
– CERTA-2007-AVI-282 : Vulnérabilités dans des produits Check Point
– CERTA-2007-AVI-283 : Vulnérabilité de produits Symantec
– CERTA-2007-AVI-284 : Vulnérabilités dans MIT Kerberos 5

Pendant la même période, les avis suivants ont été mis à jour :

– CERTA-2007-AVI-264-001 : Vulnérabilité dans OpenOffice
(ajout de la référence à StarOffice)
– CERTA-2007-AVI-275-001 : Multiples vulnérabilités dans Ingres
(ajout des produits affectés intégrant une version vulnérable d'Ingres, ajout des références CVE et d'un bulletin de sécurité Computer Associates)

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'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.

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 œuvre (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 COSSI/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.

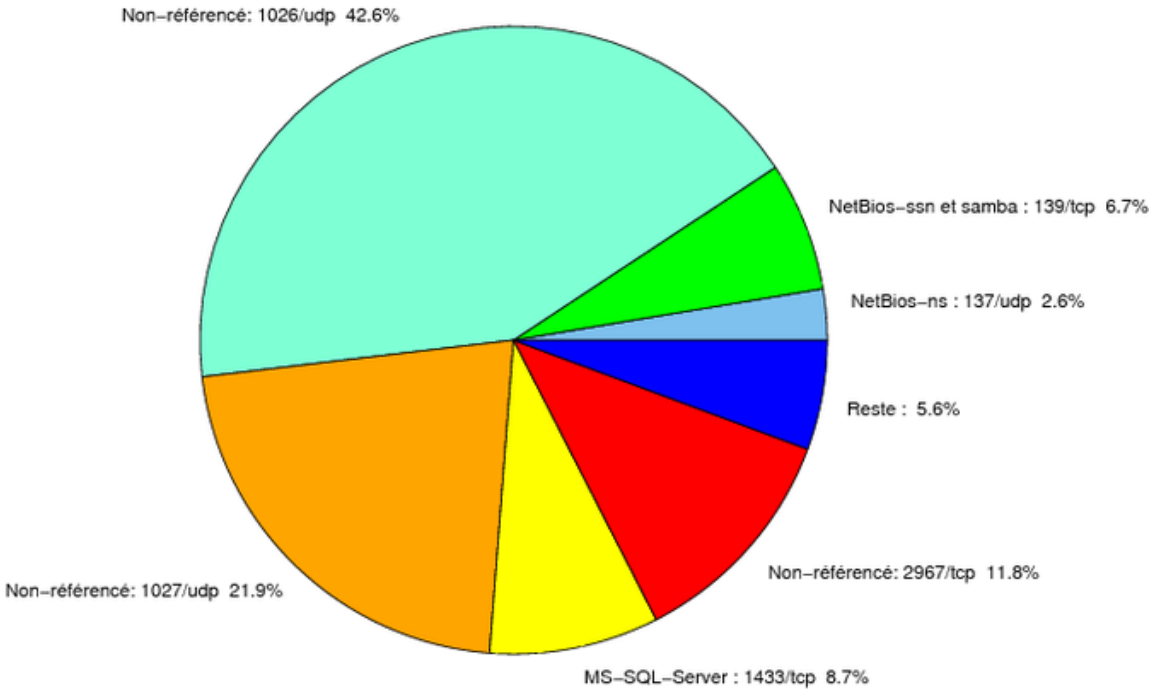

FIG. 1: Répartition relative des ports pour la semaine du 22.06.2007 au 28.06.2007

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CE
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
106	TCP	MailSite Email Server	–	–
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CE
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CE
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CE
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE

				http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CE
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CE
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CE
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CE
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CE
2381	TCP	–	HP System Management	http://www.certa.ssi.gouv.fr/site/CE
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CE
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CE
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CE
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CE
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
10080	TCP	Amanda	MyDoom	–
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CE
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CE

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

port	pourcentage
1026/udp	42.59
1027/udp	21.91
2967/tcp	11.83
1433/tcp	8.73
139/tcp	6.65
137/udp	2.62
4899/tcp	0.98
1080/tcp	0.91
1434/udp	0.75
21/tcp	0.36
3128/tcp	0.32
25/tcp	0.29
80/tcp	0.2
15118/tcp	0.18
3306/tcp	0.16
3127/tcp	0.09
443/tcp	0.05
9898/tcp	0.04
143/tcp	0.02
111/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

29 juin 2007 version initiale.