Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 avril 2009
N° CERTA-2009-ACT-017

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-17

Gestion du document

Référence	CERTA-2009-ACT-017
Titre	Bulletin d'actualité 2009-17
Date de la première version	24 avril 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-017.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-017/

1 Incidents de la semaine

1.1 Chronologie d'une infection

Le CERTA a traité cette semaine le cas d'une machine infectée par un code malveillant appelé `Virut`. L'objectif de l'analyse de cet incident était de comprendre comment la machine, pourtant à jour de tous les correctifs, avait pu être infectée.

L'analyse montre que la machine est infectée par plusieurs codes malveillants, l'un d'entre eux correspondant à une page Web stockée dans l'historique d'`Internet Explorer`. Or le navigateur utilisé par défaut est `Mozilla Firefox`. Cette page Web ne contient qu'un `iframe`, vers un site de téléchargement de `Virut`. La page a été consultée sur un site connu de stockage de publicité. En particulier, cette page était régulièrement consultée du fait de la présence d'un `adware` (publiciel). L'installation de cet `adware` est lié à l'utilisation d'un jeu (de type puzzle) en version gratuite pour un mois, téléchargé sur l'Internet.

En s'appuyant sur les dates du système et des différents historiques, nous pouvons reconstruire la chronologie suivante :

– courant octobre 2008, une version d'évaluation d'un jeu de type puzzle est téléchargé légitimement à l'aide de `Mozilla Firefox`. L'installation de ce jeu provoque l'infection de la machine par un `adware` ;

– à partir de ce moment-là, la machine va régulièrement utiliser `Internet Explorer` pour télécharger des pages publicitaires ;
– le 31 décembre 2008, la page publicitaire téléchargée ne contient qu'un `iframe` qui pointe vers un code malveillant appelé `Virut`. L'histoire ne dit pas si cet `iframe` a été volontairement déposé par les webmestres du site de publicité, ou s'il s'agit d'une compromission ;
– `Virut` se propage à de très nombreux exécutables du système (plusieurs centaines d'occurrences sur la machine) entre fin décembre 2008 et avril 2009, date à laquelle il endommage un fichier au point de le rendre inutilisable. C'est ce qui va déclencher la détection de l'infection du système.

Un antivirus à jour aurait-il permis d'empêcher l'infection ? Rien n'est moins sûr, certains codes malveillants ayant comme fonctionnalité de neutraliser les antivirus. Le problème vient ici de la confiance en un fichier téléchargé. Ce n'est pas parce qu'il vient d'un site a priori sûr que le fichier ne contient pas de code malveillant.

1.2 Des en-têtes HTTP utiles surprenantes

Une administration ne parvenait pas à afficher la page Web d'un site. Il s'avère en réalité qu'il ne s'agit pas d'un problème de sécurité mais d'interprétation des réponses HTTP.

Voici un exemple d'échange en HTTP posant problème, vu par le navigateur client :

```
GET /HTTP/1.1
Host: www.Mon_Site_Interrogé.tld
User-Agent: xxxxxxxxxxxxx
Accept: text/html,application/xhtml+xml,...
Accept-Encoding: gzip, deflate
(...)
```

```
HTTP/1.x 200 OK
Date: Thu, 23 Apr 2009 15:21:31 GMT
P3P: CP="NON DSP COR CURa PSAa OUR STP NAV"
Etag: "xxxxxxxxxxxxxxxxxxxxxxxxxx"
Expires: Thu 23 Apr 2009 15:23:19 GMT
Last-Modified: Wed, 04 Dec 2013 21:43:02 GMT
Content-Type: text/html; charset=ISO-8859-1
Content-Language: fr
Content-Encoding: gzip
Age: 6
Vary: Accept-Encoding
Transfer-Encoding: chunked
X-Cache: MISS from Proxy_utilise
Proxy-Connection: close
Connection: close
```

Le serveur du site Web distant utilise une fonctionnalité nommée `P3P` qui permet au serveur Web de préciser à l'internaute sa politique de protection de données personnelles. `P3P` (pour *Platform for Privacy Preferences*) est un projet à l'initiative du consortium W3C. Lorsque ces informations sont vues par le navigateur, il peut prendre des décisions en fonction de sa propre configuration et de la politique proposée. Il s'agit d'un mécanisme de confiance, car rien n'oblige le site à respecter la politique affichée et rien n'oblige l'utilisateur a y croire. La politique déclarée par le site Web se trouve ainsi dans l'en-tête de réponse HTTP, avec une ligne de résumé appelée `Compact Policy`. Dans l'exemple ci-dessus, le site précise qu'il ne fournit aucun accès aux données identifiées (`NON`), qu'il met dans sa politique des éléments afin de régler les « disputes »/litiges (`DSP`), une politique de remédiation (`COR`) et de rétention (`STP`) et l'usage qui peut être fait des éléments (`NAV`). A la date de rédaction de cet article, encore peu de sites ont recours à cette technologie et peu de navigateurs l'interprètent utilement (exception faite de la gestion des *cookies* éventuellement).

On note également dans la réponse présentée ci-dessus l'utilisation d'une date pour le champ `Last-Modified` en 2013. Cette date n'indique en rien ce qu'elle devrait. Cette information erronée peut perturber les mises en cache éventuelles de proxy Web qui l'utilisent.

Enfin, on remarque que les données sont fournies au navigateur sous encodage de type "gzip". Ne connaissant pas la taille totale des données, le serveur les envoie en plusieurs blocs (*chunks*).

Le proxy utilisé a décidé de clore l'échange. Les trois détails précédents dans la réponse du serveur peuvent en être la cause.

En réalité, dans le cas présent, quelques tests ont montré que le problème provient uniquement de l'encodage gzip qui n'est pas autorisé par le proxy. Le navigateur de l'utilisateur précise qu'il supporte ce dernier et le serveur lui retourne donc les données en conséquence. Il s'agit de la configuration par défaut du navigateur Mozilla Firefox 3.0.X. Cela est visible via le menu `about:config` et la variable `network.http.accept-encoding`.

Il est important de vérifier que la politique appliquée au niveau des passerelles de filtrage correspond aux configurations mises en œuvre par ailleurs sur les postes clients. Ce qui pouvait être un incident de sécurité n'en était ici finalement pas un.

2 Un botnet de machines Mac OS X

2.1 Les faits

Récemment, de nombreux articles ont annoncé la découverte d'un réseau de machines zombies installées avec le système d'exploitation `Mac OS X`. La méthode d'infection est assez classique : des versions non officielles des logiciels *iWorks '09* et *Adobe Photoshop CS4* sont proposées en téléchargement sur des réseaux de partage en pair à pair. Ces versions ont été modifiées afin qu'un code malveillant soit installé en même temps que l'application désirée.

Le code malveillant en question est désigné par différents noms selon l'éditeur de la solution antivirale :

- OSX.Iservice pour Symantec ;
- OSX/iWorkServ pour F-Secure ;
- OSX/IWService pour McAfee ;
- OSX_KROWI pour Trend ;
- ...

Le cheval de Troie se présente sous la forme d'un *package* souvent dénommé *iWorkService.pkg*. Il permet à l'attaquant via une porte dérobée d'exécuter de nombreuses commandes sur la machine compromise. Le flux entre le canal de contrôle et la machine est de plus chiffré par l'algorithme *AES*.

2.2 Les recommandations

Le CERTA rapelle que les applications doivent être téléchargées sur le site officiel de l'éditeur et qu'il ne faut en aucun cas faire confiance à des applications récupérées sur des réseaux qui ne sont pas de confiance. Il est, de plus, conseillé de vérifier la signature de l'archive après téléchargement lorsque celle-ci est disponible. Le code malveillant tente de contacter des machines extérieures sur des ports hauts. Il est donc recommandé de surveiller tout trafic vers l'Internet et de vérifier qu'une politique de filtrage des flux sortants est bien rigoureusement appliquée.

3 Procédures d'authentification multiples

L'authentification est la procédure permettant de vérifier l'identité présentée par une entité. Plusieurs sites Web proposent de l'effectuer pour une identité donnée (l'identifiant) en renseignant un mot de passe. Seulement ce dernier peut être oublié ou perdu. De nombreux sites Web offrent donc la possibilité de prouver son identité en répondant à une série de questions comme :

- le nom de jeune fille de la mère ;
- le titre du film favori ;
- la date de naissance ;
- le titre de chanson préférée ;
- la réponse à une question préalablement définie.

Dans la majorité des cas, il s'agit de réponses personnelles. Mais le sont-elles réellement ?

La presse s'est faite l'écho récemment de comptes de célébrités ainsi compromis car des utilisateurs sont parvenus, une fois sur l'interface d'authentification, à renseigner leurs informations « personnelles ».

En réalité, ces informations étaient assez facilement prédictibles.

De manière générale pour ces systèmes, l'utilisateur doit bien garder à l'esprit que les réponses à ces questions doivent être suffisamment robustes. Elles sont utilisées dans une procédure d'authentification. Un pré-requis nécessaire est d'avoir une bonne connaissance des informations « personnelles » déjà mises en ligne par un moyen ou un autre dont :

- les profils des réseaux sociaux ;
- les participations à des listes de diffusion ou des groupes de travail ;
- des questionnaires d'enquête ou de satisfaction ;
- etc.

Il faut aussi que ces informations soient différentes (questions et réponses) pour chaque site, de la même manière qu'un mot de passe.

Si l'utilisateur estime que cette phase d'authentification n'est pas fiable ou pratique, il peut également choisir de renseigner une question et une réponse aléatoire (frappes clavier à l'aveugle) si cette procédure n'est pas directement désactivable.

4 Microsoft Office 2007 et les informations confidentielles

Dans le dernière version de la suite bureautique de Microsoft, une fonctionnalité a été ajoutée : le *Document Inspector*. Elle permet de vérifier la présence de données invisibles telles que des annotations, des informations personnelles ou du texte caché. Si cette fonctionnalité est offerte aux utilisateurs, un article du bloc-notes en ligne du MSDN explique comment utiliser l'*Open XML SDK* pour automatiser cette vérification. Cela peut être utile, entre autres, aux administrateurs de serveurs qui voudraient vérifier que des informations confidentielles ne se retrouvent pas disponibles publiquement par erreur.

Le CERTA recommande de manière générale la plus grande prudence lors de la publication en ligne de documents pouvant contenir des informations sensibles et de maîtriser au mieux les formats utilisés. Ces derniers sont souvent bien plus complexes que l'on peut penser.

- Article traitant du format Microsoft Word 2007 :
  http://blogs.msdn.com/brian_jones/archive/2009/02/06/removing-comments-from-a-wordprocessing-document-programmatically.aspx
- Article traitant du format Microsoft Excel et PowerPoint 2007 :
  http://blogs.msdn.com/brian_jones/archive/2009/02/06/removing-comments-from-excel-and-powerpoint-files.aspx

5 Nouvelle version de Ubuntu

La nouvelle version de la distribution `GNU/Linux` : `Ubuntu` est sortie cette semaine. La version 7.10 devient donc obsolète et ne fera plus l'objet de mises à jour. Par ailleurs, une des nouveautés présente dans cette version nommée *« Jaunty Jackalope »* est la présence de l'application `Eucalytus` qui permet selon ses développeurs de créer et déployer ses propres applications de *Cloud Computing*. Cette fonctionnalité n'est pour le moment proposée qu'en test mais il conviendra de rester circonspect en la matière. Pour le reste, il faudra s'attarder sur la configuration par défaut des applications installées ainsi que sur les services lancés par défaut même si les services réseau en écoute sont très restreints par défaut ; ce qui est une bonne chose. La configuration du pare-feu pourra être une bonne piste d'amélioration du niveau de sécurité après l'installation.

6 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 16 et le 23 avril 2009.

7 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/

8 Rappel des avis émis

Dans la période du 17 au 24 avril 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-148 : Vulnérabilité dans phpMyAdmin
- CERTA-2009-AVI-149 : Vulnérabilité dans mod_perl pour Apache
- CERTA-2009-AVI-150 : Vulnérabilité dans IBM AIX
- CERTA-2009-AVI-151 : Multiples vulnérabilités dans IBM BladeCenter Advanced Management Module
- CERTA-2009-AVI-152 : Vulnérabilité dans Apache Tomcat mod_jk
- CERTA-2009-AVI-153 : Vulnérabilité du noyau Linux
- CERTA-2009-AVI-154 : Multiples vulnérabilités des produits Oracle
- CERTA-2009-AVI-155 : Multiples vulnérabilités du gestionnaire de périphériques udev
- CERTA-2009-AVI-156 : Multiples vulnérabilités dans cups
- CERTA-2009-AVI-157 : Multiples vulnérabilités dans Mozilla Firefox
- CERTA-2009-AVI-158 : Vulnérabilité dans Dokeos
- CERTA-2009-AVI-159 : Vulnérabilité dans Plone
- CERTA-2009-AVI-160 : Vulnérabilité dans Citrix Presentation Server

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

- CERTA-2009-AVI-094-002 :
  (ajout des références aux bulletins Red Hat et Xpdf)
- CERTA-2009-AVI-133-001 : Vulnérabilités dans Kerberos
  (ajout des bulletins Novell)

9 Actions suggérées

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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.

9.6 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.

9.7 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/

10 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.

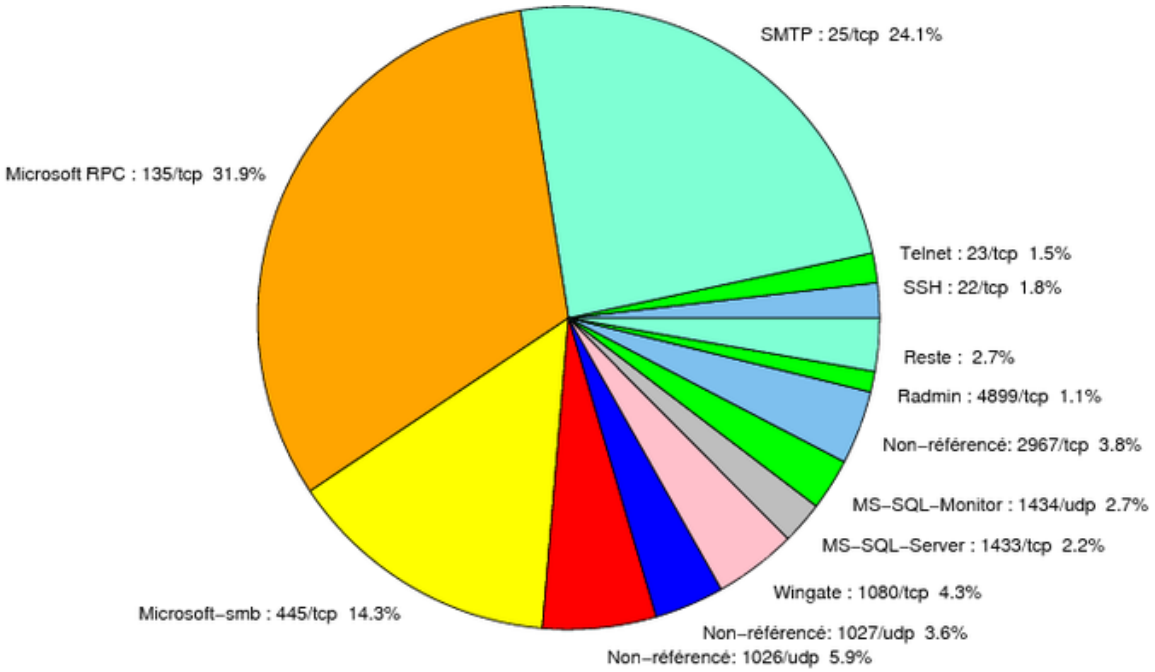

FIG. 1: Répartition relative des ports pour la semaine du 16 au 23 avril 2009

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	31.9
25/tcp	24.12
445/tcp	14.27
1026/udp	5.89
1080/tcp	4.28
2967/tcp	3.82
1027/udp	3.61
1434/udp	2.68
1433/tcp	2.21
22/tcp	1.8
23/tcp	1.54
4899/tcp	1.07
80/tcp	1
6112/tcp	0.67
21/tcp	0.53
3128/tcp	0.4
139/tcp	0.33
3389/tcp	0.26
3306/tcp	0.13

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

24 avril 2009 version initiale.