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 mai 2009
N° CERTA-2009-ACT-022

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-22

Conditions d'utilisation de ce document :	`http://www.certa.ssi.gouv.fr/certa/apropos.html`
Dernière version de ce document :	`http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-022`

Gestion du document

Référence	CERTA-2009-ACT-022
Titre	Bulletin d'actualité 2009-22
Date de la première version	29 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-022.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-022/

1 Les incidents de la semaine

1.1 Sécurité et contrat d'hébergement

Cette semaine, le CERTA est intervenu dans le traitement de plusieurs compromissions de sites Web. À de nombreuses reprises, la réponse de l'administrateur du site fut que son hébergeur lui avait conseillé d'effacer les fichiers frauduleux sans lui donner plus d'informations sur l'origine de la compromission. Cependant, la seule suppression de fichiers malveillants est inutile si l'origine de la compromission n'est pas comprise. Pire encore, supprimer un fichier sans avoir corrigé la faille de sécurité exploitée revient à avertir l'individu auteur de la compromission de la découverte de cette dernière. Il risque alors de revenir, de façon plus sournoise, en cachant mieux ses traces.

1.2 Quand le ménage laisse une porte ouverte

Lors du traitement d'une autre compromission d'un site Web, le CERTA a pris contact avec le responsable du site qui lui a alors indiqué que ce dernier avait fait l'objet d'une compromission il y a plusieurs semaines. Cet incident a été traité par le prestataire développant le site Web. Suite à la précédente intrusion, les corrections du

CMS utilisé ont été appliquées. Cependant, les individus, auteurs de la première compromission, avaient pris soin de laisser derrière eux des fichiers malveillants pouvant servir de portes dérobées (*backdoor*) afin de conserver le contrôle de serveur.

Le CERTA rappelle que, suite à une compromission, il convient de repartir sur des bases saines et ne pas se contenter de faire un ménage succinct du système de fichiers. Les bonnes pratiques pour réagir à la suite d'un incident sont décrites dans la note d'information CERTA-2002-INF-002.

1.3 Documentation

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

2 Vulnérabilité dans DirectShow

2.1 Présentation

Cette semaine, le CERTA a publié l'alerte CERTA-2009-ALE-009 portant sur une faille non corrigée dans Microsoft DirectShow. La vulnérabilité, présente dans la bibliothèque `quartz.dll` peut être exploitée au moyen d'un fichier vidéo spécialement conçu. La faille réside dans la manière dont DirectShow traite les fichiers au format QuickTime (au moyen du filtre *QuickTime Movie Parser*). L'installation de QuickTime n'est pas suffisante pour corriger la vulnérabilité car il est possible d'appeler directement le filtre de DirectShow vulnérable. La désactivation d'extensions habituellement utilisées par QuickTime n'est pas non plus suffisante.

La vulnérabilité est présente sur les systèmes suivants :

– Windows 2000 Service Pack 4 ;
– Windows XP Service Pack 2 et Service Pack 3 ;
– Windows Server 2003 Service Pack 2.

Les versions 7.0, 8.1, et 9.0x de DirectX sont concernées. Les systèmes Windows Vista et Windows Server 2008 ne sont pas impactés car le composant *QuickTime Movie Parser* a été retiré de DirectShow.

Plusieurs vecteurs d'attaque sont possibles pour compromettre un système vulnérable. Selon Microsoft, les attaques observées jusqu'à présent ont utilisé le contrôle ActiveX du lecteur Windows Media. De cette manière, la visite d'un site web spécialement conçu par une victime provoque l'exécution de code arbitraire sur la machine vulnérable. Toutefois, d'autres modules de navigateurs peuvent également être concernés et il ne suffit donc pas de désactiver ce contrôle ActiveX. L'ouverture d'un fichier spécialement conçu, envoyé en pièce jointe d'un courriel peut aussi compromettre une machine vulnérable. La pré-visualisation ou le passage de la souris sur un fichier malveillant peut également suffire à déclencher la faille.

Deux contournements protégeant totalement les systèmes existent. Le premier est préférable et consiste à désactiver le composant *QuickTime Movie Parsing* de `quartz.dll` en supprimant la clé de registre suivante :

```
HKCR\CLSID\{D51BD5A0-7548-11CF-A520-0080C77EF58A}
```

Le deuxième contournement peut avoir des effets de bord non négligeables. Il consiste à désinscrire la bibliothèque `quartz.dll` en changeant les ACL (*Access Control List*. Ceci a pour impact, par exemple, l'impossibilité de lire des fichiers vidéo avec Windows Media Player (dans une configuration par défaut). Ce contournement est décrit en détail dans le bulletin de Microsoft.

2.2 Documentation

– Alerte CERTA-2009-ALE-009 du 29 mai 2009 :
http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-009/index.html
– Bulletin de sécurité Microsoft KB971778 du 28 mai 2009 :
http://www.microsoft.com/france/technet/security/advisory/971778.mspx
http://www.microsoft.com/technet/security/advisory/971778.mspx
http://support.microsoft.com/kb/971778/fr/
– Bloc-Notes Microsoft SRD, "New vulnerability in quartz.dll Quicktime parsing", 28 mai 2009 :
http://blogs.technet.com/srd/archive/2009/05/28/new-vulnerability-in-quicktime-parsing.aspx

– Bloc-notes Microsoft MSRC, "Microsoft Security Advisory 971778 Vulnerability in Microsoft DirectShow Released", 28 mai 2009 :
http://blogs.technet.com/msrc/archive/2009/05/28/microsoft-security-advisory-971778-vulnerability-in-microsoft-directshow-released.aspx

3 Les points d'accès sans fil en libre accès

3.1 Présentation

Plusieurs fournisseurs d'accès offrent maintenant à leurs clients la possibilité de se connecter à un « réseau national Wi-Fi » dont les points d'accès sont dans les boitiers de connexion, ou « box ». Le principe est le suivant : chaque boitier se voit offrir, via une mise à jour, la possibilité de se transformer en point d'accès à l'Internet en libre service pour les clients de cet opérateur. Cette option peut être activée par défaut.

L'objet de cet article n'est pas de remettre en cause ces services, ni de citer toutes les problématiques associées aux technologies sans fil, mais de rappeler certains risques inhérents aux points d'accès dit « ouverts » :

– la bonne connexion à un point d'accès fourni par l'opérateur ne peut être garantie ;
– il est difficile de maîtriser toutes les données qui peuvent « fuir » naturellement d'une machine (mises à jour, requêtes en diffusion, etc.) ;
– il n'est pas suffisant de se connecter en HTTPS sur certains sites pour ne pas avoir ses communications interceptées. En fonction de la configuration du serveur interrogé, les fichiers de session (*cookies*) peuvent apparaître en clair et ainsi offrir un accès illégitime à une personne malveillante.

Malgré l'aspect pratique de ces points d'accès accessibles un peu partout en France, il faut être sensibilisé aux problèmes de sécurité existants et prendre la décision de s'y connecter en tout état de cause.

Chacun des dangers est rapidement détaillé ci-dessous.

3.2 Faux points d'accès

Un point d'accès est un système informatique qui, dans la majorité des cas, répond à certaines requêtes générales ("y-a-t-il un point d'accès ?") ou plus directes ("y-a-t-il le point d'accès `MAISON` présent à portée ?") ou qui annonce lui-même sa présence ("je suis le point d'accès `MAISON`"). Cela se fait par l'émission et la réception de trames de type "*Probe*" (sondage) ou "`Beacon`" (balise). L'ordinateur ou le téléphone mobile ne fait confiance qu'à la seule information de ces trames pour décider de s'associer. Il est tout à fait envisageable et réalisable avec les outils actuellement disponibles sur l'Internet de prétendre être un point d'accès de la même manière et ainsi tromper les équipements cherchant à se connecter.

Pour ces raisons, il n'est pas si simple d'être sûr de communiquer directement avec le point d'accès légitime mis à disposition par l'opérateur.

Une personne malveillante peut chercher à monter de tels faux points d'accès pour dérober les paramètres de connexion (identifiant/mot de passe), servir de point de passage obligé pour collecter les informations en transit (*man-in-the-middle*) ou agresser directement le système, une fois la communication au niveau réseau établie entre les deux équipements.

3.3 Fuite naturelle d'informations

Ces réseaux sans fil à grande échelle fonctionnent bien souvent sans chiffrement particulier des communications.

Or une machine est par défaut relativement bavarde. Plusieurs applications peuvent chercher à se mettre automatiquement à jour (système d'exploitation, antivirus, navigateur, lecteur PDF, etc.). Elles peuvent également chercher à communiquer avec des systèmes connus (messagerie instantanée, partage de fichiers, imprimantes réseau, etc.). Ce sont autant d'informations sur la machine, l'utilisateur et son usage qui transitent dans les airs, en clair, et sont ainsi récupérables par des personnes malveillantes.

L'utilisation de ces informations par ces derniers permet d'affiner la phase d'attaque, de mieux tromper l'utilisateur et de le rediriger vers d'autres codes malveillants.

3.4 Le HTTPS ne fait pas tout

Ce point avait été détaillé dans un précédent bulletin d'actualité CERTA-2008-ACT-033 (section 3, « Contournement HTTPS »).

http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-033.pdf

3.5 Quelques recommandations

Il n'est pas toujours simple de trouver des boitiers ou « box » sans interface sans fil. Si ce service n'est pas souhaité, il faut s'assurer que les interfaces sans fil du boitier sont bien désactivées. Cette manipulation reste souvent logicielle, offerte par l'opérateur via une interface. En cas de doute, il est possible, sans toucher à l'équipement, de le mettre dans un coffre métallique qui servira alors de cage de Faraday.

Les équipements peuvent s'apparier automatiquement, sans autorisation préalable de l'utilisateur. Les interfaces sans fil doivent donc être désactivées par défaut, la meilleure solution étant de disposer d'une interface sans fil physiquement amovible. Il est enfin important de sensibiliser son entourage aux risques encourus afin de prendre la meilleure décision.

4 XSS utilisant la visualisation des PDF

4.1 Présentation

Une injection de code indirecte, ou XSS (*Cross Site Scritping*), consiste à exécuter du code dans le navigateur d'un internaute, et cela dans le contexte d'un site tiers. Il est possible de modifier le contenu du site visé ou d'utiliser une fonctionnalité proposée par le site, classiquement le moteur de recherche, pour injecter le code dans un lien proposé à la victime.

Une méthode utilise la fonctionnalité offerte par de nombreux sites qui permet de visualiser un document au format PDF, sans avoir à le télécharger. Par exemple, certains *webmails* permettent de visualiser directement un fichier PDF joint à un message. Pour cela, le document est interprété au niveau du serveur et est servi dans un format lisible par les navigateurs, sans module additionnel. Le problème vient du résultat de l'interprétation du fichier. En effet, si du code malveillant se trouve dans le document et qu'il n'est pas correctement « nettoyé » avant d'être présenté à l'internaute, le code s'exécutera dans le contexte du site. Dans le cas de la pièce jointe, du code pourrait alors s'exécuter dans le contexte du *webmail*, pour lequel les scripts sont souvent autorisés afin d'être utilisés de façon optimale.

Le CERTA recommande la plus grande prudence lors de l'interprétation des documents au niveau du serveur afin d'éviter une compromission locale (Ex: CERTA-2009-AVI-201).

Le CERTA recommande de bloquer par défaut l'interprétation des scripts et de ne pas autoriser l'ouverture arbitraire de documents via le navigateur.

4.2 Documentation

– Exemple de vulnérabilité permettant l'exécution de code sur un serveur, lors de l'interprétation d'un fichier au format PDF :
http://www.certa.ssi.gouv.fr/CERTA-2009-AVI-201/

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 21 et le 28 mai 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 22 au 29 mai 2009, le CERTA a émis les avis suivants :

– CERTA-2009-AVI-196 : Vulnérabilités dans Sun Solaris
– CERTA-2009-AVI-197 : Vulnérabilité du serveur TFTP des équipements Cisco
– CERTA-2009-AVI-198 : Vulnérabilité dans Wireshark
– CERTA-2009-AVI-199 : Vulnérabilité dans DokuWiki
– CERTA-2009-AVI-200 : Multiples vulnérabilités de Novell GroupWise
– CERTA-2009-AVI-201 : Vulnérabilités dans les produits BlackBerry
– CERTA-2009-AVI-202 : Vulnérabilité dans Sun Java System Portal Server
– CERTA-2009-AVI-203 : Vulnérabilités de libsndfile
– CERTA-2009-AVI-204 : Vulnérabilité dans Citrix Password Manager

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.

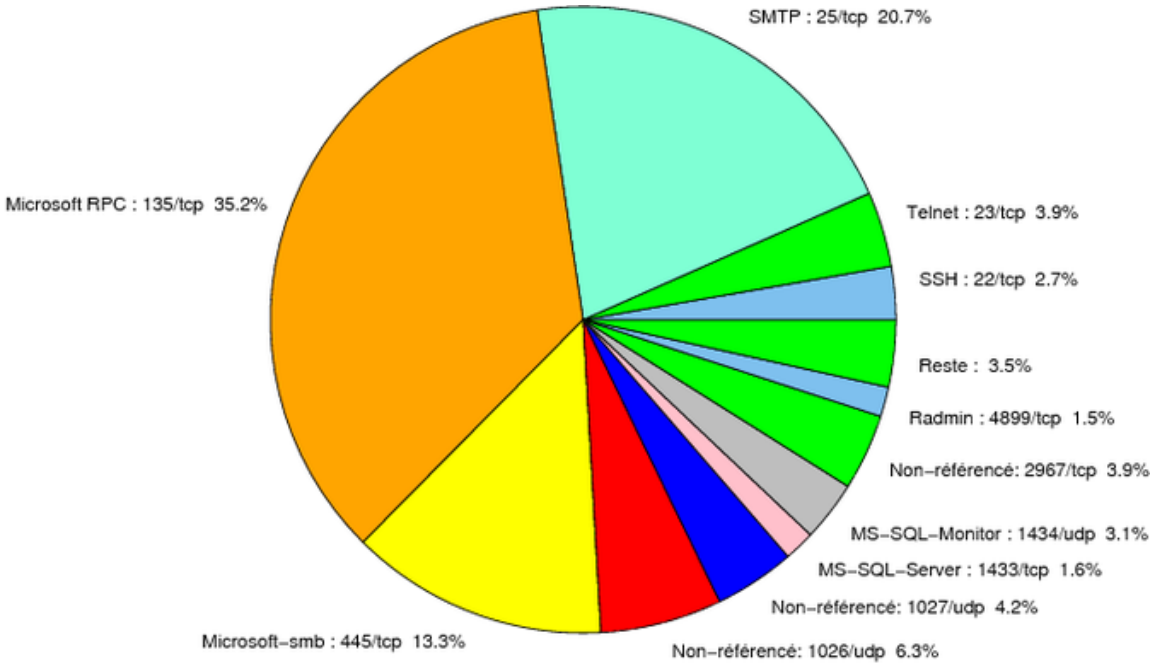

FIG. 1: Répartition relative des ports pour la semaine du 21 au 28 mai 2009

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/CERT
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERT
6106	TCP	Symantec Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERT
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
6502	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CERT
6503	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CERT
6504	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CERT
8080	TCP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CERT
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CERT
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/CERT
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CERT
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CERT
54345	TCP	HP Mercury	–	http://www.certa.ssi.gouv.fr/site/CERT
65535	UDP	LANDesk Management Suite	–	http://www.certa.ssi.gouv.fr/site/CERT

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

port	pourcentage
135/tcp	35.22
25/tcp	20.72
445/tcp	13.33
1026/udp	6.28
1027/udp	4.17
2967/tcp	3.93
23/tcp	3.88
1434/udp	3.11
22/tcp	2.73
1433/tcp	1.58
4899/tcp	1.53
80/tcp	1.19
21/tcp	0.71
3389/tcp	0.43
5554/tcp	0.38
3128/tcp	0.33
3306/tcp	0.23
143/tcp	0.09
3127/tcp	0.04

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

29 mai 2009 version initiale.