Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 juin 2009
N° CERTA-2009-ACT-024

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-24

Gestion du document

Référence	CERTA-2009-ACT-024
Titre	Bulletin d'actualité 2009-24
Date de la première version	12 juin 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-024.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-024/

1 Incidents de la semaine

1.1 Traitement des dénis de service

Une remontée récente sur un déni de service auprès du CERTA a permis de constater l'état de détresse des techniciens chargés de gérer le problème. Le principe de ces attaques vise à rendre inaccessible un site ou un serveur, par exemple par saturation de requêtes, bien souvent dans le contexte d'un réseau de machines zombies.

Les contre-mesures sont quant à elles plutôt difficiles à mettre en place puisque la plupart de ces attaques reposent sur des services ou protocoles normaux sur l'Internet. Qui plus est, il est particulièrement difficile de distinguer les flux malfaisants des flux normaux licites. Seuls les fournisseurs d'accès peuvent généralement mettre en place un filtrage efficace. Cette opération est souvent contractuelle et nécessite une préparation.

Il est donc recommandé dans une telle situation :

– en tout premier lieu, de veiller au recueil et à la conservation de toutes les traces et indices liés à l'incident et susceptibles de servir devant la justice ultérieurement. Les journaux doivent naturellement être activés et protégés (réf. note CERTA-2000-INF-001) ;
– de procéder à une analyse des journaux afin de bien faire la différence entre un véritable déni de service et un dysfonctionnement du système l'amenant à s'auto saturer.

– Note d'information CERTA-2000-INF-001, « le déni de service distribué », 21 février 2000 :
http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-001/

1.2 Arnaque aux noms de domaine

Cette arnaque n'est pas nouvelle, des plaintes remontent au moins de mars 2009, mais elle touche des organismes français, administrations ou entreprises. Elle utilise des ressorts classiques.

1.2.1 Le scénario

Une société, par exemple ntwifinetworks.com à la date de rédaction de ce document, vous envoie un courriel *au ton inquiétant* et au sujet du style *"Domaine Dispute et Enregistrement"*. Elle vous indique qu'elle a reçu une demande d'enregistrement semblable à votre nom de domaine avec simplement un suffixe ou un domaine de premier niveau différent. Par exemple, le possesseur de certa.ssi.gouv.fr apprend la demande de prétendu demande d'enregistrements de certa.ssi.gouv.cn, certa.ssi.gouv.com.cn, certa.ssi.gouv.net.cn, certa.ssi.gouv.hk, certa.ssi.gouv.asia. Le courriel stipule que la réponse doit impérativement parvenir *rapidement*, dans les cinq jours, pour éviter des différends.

Le site de la société précédemment citée arbore les logos des organismes officiels et bien connus de l'Internet et des télécommunications, l'IANA, l'ICANN, l'ITU, l'AFNIC…

1.2.2 L'effet recherché

Le client effrayé sera incité à acheter les noms de domaine mentionnés voire d'autres, pour une centaine de dollars pièce. La menace de typosquattage peut être avancée par les vendeurs pour pousser à la consommation.

1.2.3 Les enseignements et les recommandations

Les ficelles utilisées sont traditionnelles : suggérer une menace et donner un sentiment d'urgence à la réponse qui doit être apportée.

Face aux messages présentant ces caractéristiques, il faut garder la tête froide et se renseigner sur l'émetteur. Ces caractéristiques (élément affectif, menace, urgence) se retrouvent dans les canulars avec, en plus l'incitation à propager largement. La vigilance doit se déclencher sur les mêmes critères.

L'organisme destinataire doit évaluer lui-même les risques liés à la présence de noms de domaine plus ou moins voisins. Ainsi le nom de domaine cert.xx existe pour de nombreux pays sans que cela induise une confusion dans les esprits.

1.3 Des données confidentielles retrouvées sur Internet

1.3.1 Présentation

Une recherche de fichiers au format `SQL` a permis de mettre en évidence la présence d'une sauvegarde de base de données, contenant des informations ministérielles non publiques, accessibles sur l'Internet. Après analyse, il s'est avéré que ces fichiers appartenaient à un développeur qui avait réalisé des sauvegardes d'un projet sur son espace personnel sans avoir conscience qu'elles étaient publiquement accessibles, ni qu'elles seraient indexées et donc très facilement trouvables.

Le CERTA recommande la plus grande prudence lors de la manipulation de données confidentielles. C'est une bonne pratique de faire régulièrement ce type de recherches sur ses données et sur ses sites, comme cela l'a été présenté lors du dernier bulletin d'actualité (CERTA-2009-ACT-023, « *Surveiller son site avec des moteurs de recherche* »).

1.3.2 Documentation

Bulletin d'actualité du 05 juin 2009 :
http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-023.pdf

2 Bulletins Microsoft de Juin

Cette semaine, Microsoft a émis 10 bulletins de sécurité faisant état d'au moins 31 vulnérabilités et deux avis de sécurité. Selon les critères définis par l'éditeur, six bulletins sont critiques, trois importants et un modéré. Les produits suivants sont affectés :

- toutes les versions maintenues de Microsoft Windows ;
- toutes les versions maintenues d'Internet Explorer ;
- Microsoft Internet Information Services 5.0, 5.1, et 6.0 ;
- toutes les versions maintenues de Microsoft Office Excel ;
- Microsoft Works 8.5 et 9.0 ;
- toutes les versions maintenues de Microsoft Office Word.

L'une des mises à jour corrige l'alerte CERTA-2009-ALE-007 qui concernait le composant WebDav d'Internet Information Services. La vulnérabilité de Microsoft DirectShow, actuellement exploitée, n'est pas corrigée dans le lot de mises à jour. Il est urgent pour les personnes n'ayant pas appliqué les solutions de contournement proposées de le faire sans tarder.

Les deux avis de sécurité concernent d'une part, une mise à jour des « kill bits » ActiveX (désactivation des ActiveX vulnérables), et d'autre part une modification du comportement du DNS.

Dans le même temps, Microsoft a également émis les mises à jour manquantes du bulletin de sécurité MS09-017. Pour rappel, l'éditeur n'avait mis à disposition, au mois de mai, que les correctifs concernant PowerPoint sous Windows. Microsoft Office 2004 et 2008 pour Mac, ainsi que Microsoft Works 8.5 et 9.0 et le convertisseur de fichiers Open XML pour Mac, qui étaient également sujets à une ou plusieurs vulnérabilités, ont aujourd'hui des mises à jour disponibles. Il est très important d'effectuer les mises à jour pour ces produits. En effet, la vulnérabilité affectant Office 2004 pour Mac avait fait l'objet d'une alerte car des codes d'exploitation étaient apparus sur l'Internet pour la version PowerPoint de Windows (cf. alerte CERTA-2009-ALE-005 et bulletin CERTA-2009-ACT-020).

Comme à son habitude, Microsoft a également mis quelques informations intéressantes sur son bloc-notes « Security Research & Defense » pour certaines des vulnérabilités, notamment celles concernant Internet Explorer, Windows Search, les convertisseurs de Works et Windows RPC (cf. section documentation).

2.1 Documentation

- Bloc-notes « Security Research & Defense »
  http://blogs.technet.com/srd/
- « Mise à jour Microsoft du mois de mai » , bulletin d'actualité CERTA-2009-ACT-020 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-020.pdf
- Avis de sécurité KB971888, « Mise à jour pour la dévolution DNS », 09 juin 2009 :
  http://www.microsoft.com/france/technet/security/advisory/971888.mspx
- Avis de sécurité KB969898, « Ensemble de mises à jour pour les *kill bits* ActiveX », 09 juin 2009 :
  http://www.microsoft.com/france/technet/security/advisory/969898.mspx
- Bloc-notes de P. Saulière, « Bulletins de sécurité du 9 juiin » :
  http://blogs.technet.com/pascals/archive/2009/06/09/bulletins-de-s-curit-du-9-juin.aspx

3 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 04 et le 11 juin 2009.

4 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/

5 Rappel des avis émis

Dans la période du 05 au 12 juin 2009, le CERTA a émis les avis suivants :

– CERTA-2009-AVI-210 : Vulnérabilité dans Kerberos sous Sun Solaris
– CERTA-2009-AVI-211 : Multiples vulnérabilités de Apache Tomcat
– CERTA-2009-AVI-212 : Multiples vulnérabilités dans IBM WebSphere Application Server
– CERTA-2009-AVI-213 : Vulnérabilité dans Microsoft Active Directory
– CERTA-2009-AVI-214 : Multiples vulnérabilités dans Microsoft Internet Explorer
– CERTA-2009-AVI-215 : Vulnérabilités dans Internet Information Services (IIS)
– CERTA-2009-AVI-216 : Vulnérabilités dans Microsoft Office Excel
– CERTA-2009-AVI-217 : Vulnérabilités dans le gestionnaire de files d'impression de Microsoft Windows
– CERTA-2009-AVI-218 : Vulnérabilité dans Microsoft Windows Search
– CERTA-2009-AVI-219 : Vulnérabilité dans Microsoft Works
– CERTA-2009-AVI-220 : Vulnérabilités dans le noyau Windows
– CERTA-2009-AVI-221 : Vulnérabilité de Windows RPC
– CERTA-2009-AVI-222 : Vulnérabilité de Microsoft Office
– CERTA-2009-AVI-223 : Multiples vulnérabilités dans Apple Safari
– CERTA-2009-AVI-224 : Multiples vulnérabilités dans Adobe Reader et Acrobat
– CERTA-2009-AVI-225 : Vulnérabilité de la bibliothèque libpng
– CERTA-2009-AVI-226 : Vulnérabilité dans SonicWALL SSL-VPN
– CERTA-2009-AVI-227 : Vulnérabilité dans le webmail de Kerio MailServer
– CERTA-2009-AVI-228 : Vulnérabilité dans HP OpenView Network Node Manager
– CERTA-2009-AVI-229 : Vulnérabilités dans FreeBSD
– CERTA-2009-AVI-230 : Vulnérabilité dans Sun Solaris

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

– CERTA-2009-AVI-195-001 : Vulnérabilités dans ntpd
(ajout du bulletin de sécurité FreeBSD)
– CERTA-2009-AVI-209-001 : Multiples vulnérabilités dans Joomla!
(ajout des bulletins 20090601 et 20090602)

6 Actions suggérées

6.1 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.

6.2 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.

6.3 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.

6.4 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.

6.5 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.

6.6 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.

6.7 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/

7 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.

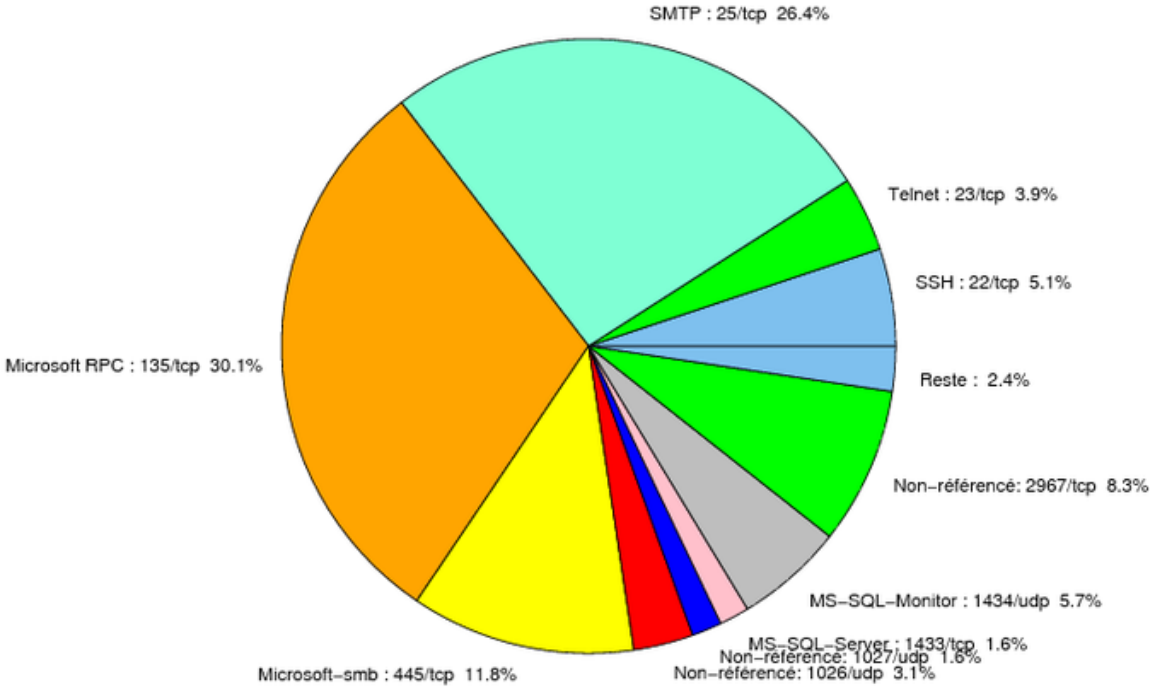

FIG. 1: Répartition relative des ports pour la semaine du 04 au 11 juin 2009

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
80/tcp	85.82
135/tcp	30.11
25/tcp	26.37
445/tcp	11.81
2967/tcp	8.46
1434/udp	5.7
22/tcp	5.31
23/tcp	3.93
1026/udp	3.14
1433/tcp	1.57
139/tcp	0.78
4899/tcp	0.39
3389/tcp	0.19

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

12 juin 2009 version initiale.