Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 janvier 2009
N° CERTA-2009-ACT-001

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-01

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-001`

Gestion du document

Référence	CERTA-2009-ACT-001
Titre	Bulletin d'actualité 2009-01
Date de la première version	02 janvier 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-001.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-001/

1 Incidents de la semaine

1.1 Un ancien traitement peu rigoureux

Cette semaine le CERTA a participé au traitement d'un incident relatif au dépôt d'un kit de filoutage (*phishing*) sur un site Internet. A la suite de l'information de la compromission, le responsable du site en question a pris contact avec son administrateur technique pour analyser le problème. Cette analyse a révélé que les troubles venaient d'une compromission antérieure qui n'avait pas fait l'objet d'un traitement rigoureux. En effet, seules les conséquences de la précédente compromission avaient été corrigées. Les attaquants n'ont donc eu aucune difficulté à revenir modifier ce site Web.

Lors d'une compromission, les conséquences et autres traces laissées par l'attaquant ne sont que la partie visible de l'iceberg. Avant de remettre un service en production, il est préférable de s'assurer que la vulnérabilité exploitée a été correctement corrigée. Le CERTA rappelle que suite à une compromission, d'autant plus quand la cause n'a pas été clairement identifiée, il est indispensable de réaliser un audit de sécurité. Il est par exemple parfaitement inefficace de changer les mots de passe si une porte dérobée est présente. Les bons réflexes, suite à un incident, sont détaillés dans la note d'information du CERTA CERTA-2002-INF-002.

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

1.2 Un hébergement tout en un

Les causes de la compromission d'un site Web peuvent être multiples :

– une vulnérabilité dans le code ou l'application utilisée ;
– une compromission d'un serveur ;
– une compromission des identifiants utilisés pour ce connecter au serveur ;
– ...

Le CERTA a reçu l'appel d'une victime suite à la compromission de son site Internet. Son hébergeur lui a suggéré de modifier son mot de passe de connexion, le site de la victime ne contenant qu'une page PHP ne faisant appel à aucune directive « sensible » de ce langage. Peu de temps après cette modification, son site a de nouveau été modifié à son insu. L'hébergeur a alors pris la décision de suspendre le compte de la victime le temps de trouver la cause de la compromission. Or, la suspension de compte chez cet hébergeur entraine l'arrêt de tous les services associés : Web, messagerie, DNS. La réaction de l'hébergeur peut se comprendre, mais la victime ne peut à présent plus recevoir de courrier électronique, ce qui pourrait mettre en péril l'existence de sa société.

Le CERTA rappelle que le choix d'une solution d'hébergement doit intégrer les possibilités de réaction face à l'incident : service d'analyse, passage en mode dégradé, ...

Documentation

– Note d'information sur les bonnes pratiques concernant l'hébergement mutualisé : http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/
– Note d'information sur les mots de passe : http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/

2 Les faiblesses dans MD5 exploitées

Le 30 décembre 2008, à Berlin, a eu lieu la vingt-cinquième conférence en sécurité informatique du CCC (*Choas Computing Congress*). Lors de cette conférence, une présentation a fait grand bruit. En effet, au cours de cette présentation, une équipe de chercheurs a annoncé avoir exploité les faiblesses de l'algorithme MD5 découvertes depuis 2004 afin de créer de faux certificats totalement valides et acceptés automatiquement par les navigateurs usuels.

2.1 Qu'est-ce que MD5 ?

L'algorithme MD5 (*Message Digest 5*) est une fonction mathématique dite fonction de hachage (*hash fonction*). À partir d'un bloc de données initial, cette fonction permet d'obtenir un nouveau bloc de données unique de 128 bits. Cette empreinte, ou *hash*, est censée respecter les propriétés suivantes :

– il est très difficile de retrouver le message initial à partir de la signature ;
– à partir d'un message donné, et de sa signature, il est très difficile d'engendrer un autre message qui donne la même signature ;
– il est très difficile de trouver deux messages aléatoires qui donnent la même signature (résistance aux collisions).

C'est cette résistance aux collisions qui a été mise à mal théoriquement en 2004 pour l'algorithme MD5. Depuis longtemps, MD5 est considéré comme non sûr et n'est pas recommandé par la DCSSI.

2.2 Utilisation de MD5 dans les certificats

Si l'on simplifie la vision des choses, un certificat est un fichier constitué d'ensembles de données, complétés de la signature de celles-ci qui permet de les certifier par une autorité de confiance. La signature des données d'un certificat est réalisée en appliquant une fonction de hachage au bloc de données que l'on veut signer, puis en chiffrant l'empreinte obtenue avec la clef privée de l'autorité de certification.

Malgré la faiblesse avérée de MD5, beaucoup de certificats utilisent malheureusement encore cet algorithme dans leur processus de signature. D'après les auteurs de l'article présenté au 25C3, sur 30000 certificats collectés, 9000 utiliseraient MD5 comme algorithme de hachage.

2.3 Impact de l'attaque

Grâce à leur attaque, les auteurs sont capable de créer un faux certificat signé indirectement par une autorité de certification valide et reconnue par tous les navigateurs.

Il est donc possible entre autres :

- de faire croire qu'une autorité de certification reconnue a délivré un certificat à un site malveillant ;
- d'agir en coupure d'une connexion à un site de confiance en imitant son certificat (attaque de type *man in the middle*).

2.4 Comment se prémunir de ces impacts ?

Lors de la création d'un certificat, il convient de choisir un algorithme réputé comme fiable. Par exemple, il est recommandé, dans le référentiel général de sécurité (RGS), d'utiliser l'algorithme SHA-256.

Si l'on se place du côté de l'utilisateur, il convient de vérifier les certificats proposés par le site Internet au cours d'une transaction particulièrement sensible (transfert d'argent, connexion par identifiants, données personnelles, etc.).

Si le certificat annoncé utilise l'algorithme MD5, l'utilisateur pourrait être en présence d'un certificat faible ou faux.

Documentation

- Référentiel Technique Cryptographique de la DCSSI :
  http://www.ssi.gouv.fr/fr/RGS/RGS_Mecanismes_cryptographiques_v1_11.pdf

3 Les cadeaux de Noël sur le réseau

Cette période de l'année qui suit Noël est souvent propice à l'apparition de gadgets sur le réseau. Ce fut déjà le cas il y a quelques années avec le célèbre *Nabaztag*.

Ce phénomène pose néanmoins un problème de sécurité. En effet, ces dispositifs sont des systèmes informatiques et devraient donc respecter la politique de sécurité du système d'information (PSSI). Leurs utilisateurs ne sont généralement pas conscients qu'il s'agit de véritables systèmes d'information et qu'ils comportent les mêmes risques qu'un ordinateur ou qu'une clé USB.

Pour prendre un exemple récent, la société *Samsung* a récemment indiqué que des CD d'installation du logiciel *Frame Manager* fourni avec des cadres photos étaient infectés par un code malveillant. La connexion de ce matériel à un ordinateur est donc susceptible d'infecter cette machine, puis le réseau local.

Un incident similaire avait affecté les cadres photos *Insignia* du producteur *Best Buy*. Les incidents de ce type sont amenés à se répéter.

Il est donc important, avant de connecter un tel dispositif (matériel et logiciel) sur le réseau, de s'assurer que celui-ci :

- respecte la politique de sécurité ;
- n'est pas déjà infecté par un code malveillant.

Une sensibilisation des utilisateurs est également nécessaire, surtout en cette période où de nombreux cadeaux de Noël (potentiellement infectés) sont remis en vente sur des sites spécialisés.

Documentation

- Annonce de Samsung concernant les cadres photos :
  http://www.samsung.com/fr/pdf/InformationConsommateurCadresPhotosSamsung.pdf
- Article du SANS du 07 janvier 2008 :
  http://isc.sans.org/diary.html?storyid=3817

4 Téléphones portables

Une conférence récente a permis de rappeler à certains utilisateurs de téléphones portables que ces derniers restent des systèmes d'information comme des ordinateurs avec des vulnérabilités potentielles.

Plus précisément, des chercheurs ont montré qu'il était possible de perturber la réception totale des messages de type SMS ou MMS de certains téléphones mobiles Nokia.

L'attaque en elle-même n'est pas excessivement complexe car elle consiste à envoyer des messages spécifiquement construits à la cible. Ces derniers sont mal interprétés par l'équipement et perturbent le fonctionnement du service de réception.

Le dysfonctionnement n'est pas toujours visible.

Cet événement permet de rappeler que les téléphones sont des appareils communiquants dont les fonctionnalités sont quasi aussi riches que celles des ordinateurs actuels. Les moyens de protection ne sont cependant pas encore très évidents et, compte-tenu de l'hétérogénéité du parc, dépendent très souvent de la version précise du modèle utilisé.

Le CERTA recommande donc la plus grande vigilance quant à leur utilisation et rappelle de ne pas mélanger les usages privés et professionnels. La politique de sécurité doit prendre en compte leur usage. Leur niveau de sécurité est-il suffisant pour manipuler des données professionnelles ? Peuvent-ils être branchés sur tout équipement du réseau ? etc.

5 Note d'information

Cette semaine le CERTA a publié une note d'information CERTA-2008-INF-005 relative à la gestion des journaux d'événements. Ce document a pour but d'aider à la mise en œuvre d'une politique complète de journalisation. Il y est précisé :

- les préalables à la mise en place d'une infrastructure complète de gestions de journaux ;
- les bonnes pratiques en matière d'architecture de centralisation ;
- la nature des éléments à journaliser ;
- un certain nombre de conseils lors de l'exploitation des journaux pouvant aider dans la détection d'incidents de sécurité.

Documentation

- Note d'information CERTA-2008-INF-005 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-005/

6 Vulnérabilités dans SPIP

De très nombreux sites Internet sont construits avec un logiciel dénommé SPIP. Un correctif très important vient d'être diffusé afin de corriger plusieurs failles, décrites dans l'avis CERTA-2008-AVI-612, qui affectent ce gestionnaire de contenu. L'une de ces vulnérabilités permet d'exécuter du code à distance. Afin d'éviter de multiples défigurations de sites Internet via cette faille facilement exploitable, il est recommandé de faire appliquer le correctif.

7 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 25 décembre 2008 et le 01 janvier 2009.

8 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/

9 Rappel des avis émis

Dans la période du 26 décembre 2008 au 02 janvier 2009, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-612 : Vulnérabilités dans SPIP
- CERTA-2008-AVI-613 : Vulnérabilité de phpPgAdmin
- CERTA-2008-AVI-614 : Vulnérabilité du noyau FreeBSD

10 Actions suggérées

10.1 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.

10.2 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.

10.3 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.

10.4 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.

10.5 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.

10.6 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.

10.7 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/

11 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.

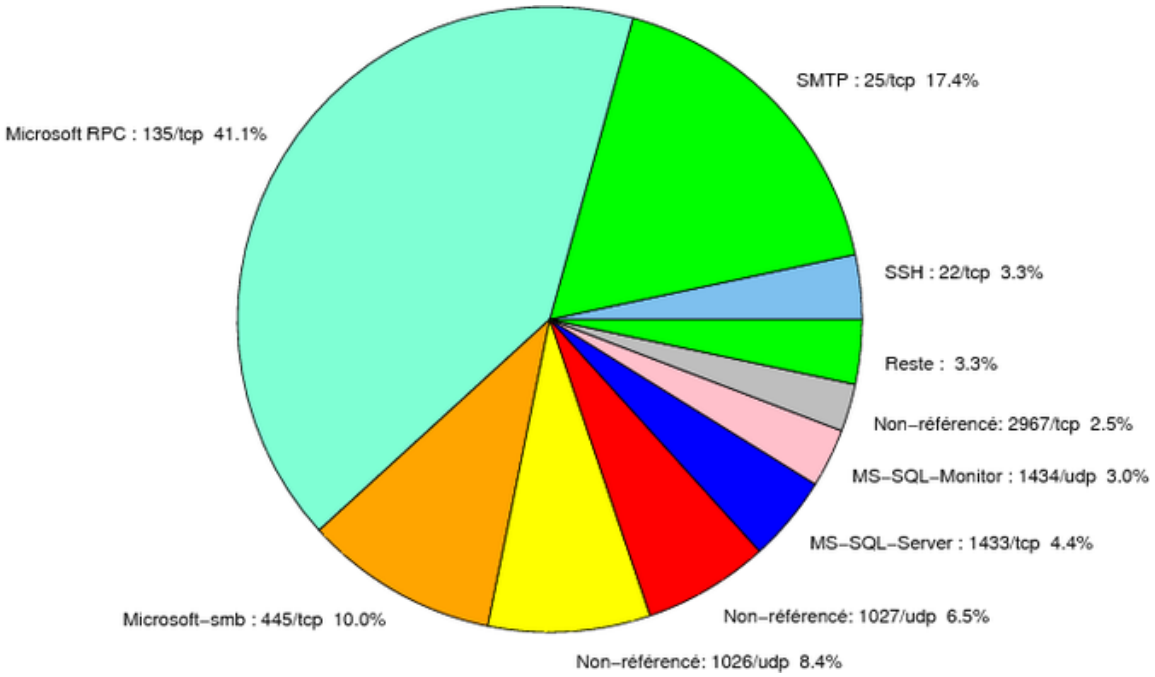

FIG. 1: Répartition relative des ports pour la semaine du 25.12.2008 au 01.01.2009

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	41.07
25/tcp	17.37
445/tcp	10.03
1026/udp	8.39
1027/udp	6.51
1433/tcp	4.44
22/tcp	3.33
1434/udp	3.04
2967/tcp	2.46
139/tcp	0.62
21/tcp	0.57
23/tcp	0.48
4899/tcp	0.43
80/tcp	0.28
3128/tcp	0.14
1080/tcp	0.09
3389/tcp	0.04

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

02 janvier 2009 version initiale.