Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 octobre 2009
N° CERTA-2009-ACT-043

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-43

Gestion du document

Référence	CERTA-2009-ACT-043
Titre	Bulletin d'actualité 2009-43
Date de la première version	23 octobre 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-043.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-043/

1 MS08-067 : un an après

1.1 Rappel des faits

Une année s'est écoulée depuis la sortie hors cycle du correctif *MS08-067* de `Microsoft`. Pour rappel, ce correctif comble une vulnérabilité du service *Serveur* de `Microsoft Windows`. Cette faille exploitable via *RPC* promettait l'apparition rapide de vers afin de compromettre tous les machines vulnérables.

En effet, moins d'un mois après l'édition du correctif, de nouveaux codes malveillants dénommés, en autre, *Conficker* font leurs apparitions. *Conficker/Downadup/Kido* obtient un très fort écho médiatique.

1.2 Constat et recommandations

Malheureusement, aujourd'hui encore, le CERTA et ses homologues relèvent de nombreuses compromissions de machines au travers de cette vulnérabilité. Cette date anniversaire est donc une occasion de rappeler les bonnes pratiques à mettre en œuvre pour éviter une infection par le ver *Conficker* ou tout autre code malveillant utilisant les mêmes méthodes de propagation :

– appliquez le correctif de sécurité de `Microsoft` ;

– n'ouvrir les partages de fichiers et d'imprimantes que si nécessaire ;
– désactiver l'exécution automatique au branchement d'un support amovible (clé USB, CD-ROM, ...) ;
– ne jamais connecter un support amovible d'origine inconnue ou non vérifié ;
– vérifiez que les pare-feux n'autorisent pas de connexion entrante inutile, notamment sur le port 445 ;
– modifiez les mots de passe par défaut des boitiers d'accès à l'Internet (*box*).

Enfin, d'autres bonnes pratiques, comme utiliser des mots de passe fort ou consulter régulièrement les journaux d'événements des équipements comme le pare-feu ou le serveur *proxy* restent toujours applicables.

1.3 Documentation

– Bulletin de sécurité Microsoft MS08-067 du 23 octobre 2008 :
http://www.microsoft.com/france/technet/security/bulletin/MS08-067.mspx
http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx
– Référence CVE CVE-2008-4250 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
– Outil de suppression de logiciels malveillants Microsoft Windows :
http://support.microsoft.com/?kbid=890830
http://www.microsoft.com/france/securite/malwareremove/default.aspx
– Déploiement de l'outil de suppression de logiciels malveillants Microsoft Windows dans un environnement d'entreprise :
http://support.microsoft.com/kb/891716

2 Linux s'invite dans les téléviseurs

Après les équipements informatiques, les *smartphones* et autres assistants personnels, c'est au tour des téléviseurs d'avoir leur *firmware* basé sur le noyau Linux. Il est en effet possible aujourd'hui d'acheter ce type de téléviseur, et donc d'ajouter un nouvel équipement dans le système informatique domestique, sans forcément en être conscient.

Et il n'aura pas fallu longtemps avant de voir des méthodes de modification de ces *firmwares* apparaître. Ces derniers sont chiffrés à l'aide d'une méthode relativement simple (chiffrement *XOR* avec une clé évidente). Il est donc très facile de télécharger un exemplaire du *firmware* sur le site du constructeur, de le déchiffrer, d'y appliquer des modifications. Il suffit ensuite de chiffrer de nouveau en suivant la même méthode et en s'assurant que les mécanismes de contrôle (non sécurisés, par exemple `CRC-32`) soient validés.
Typiquement, la modification classique apportée au *firmware* est le démarrage automatique d'un démon permettant l'ouverture d'un *shell*.

On peut imaginer un très large éventail de modifications possibles du téléviseur lorsqu'un *shell* est à disposition : connexion au réseau *WiFi* domestique, lecture des partages *NFS* et *CIFS*, etc.

Du point de vue de la sécurité, l'ajout du téléviseur dans le parc informatique augmente la surface d'attaque. On peut prédire l'apparition prochaine de vulnérabilités sur ce type d'équipements, voire de codes malveillants d'autant plus qu'ils fonctionnent bien souvent avec des processeurs *ARM*. C'est-à-dire ceux que l'on retrouve dans plusieurs *smartphones* bien connus.
Il est donc important d'intégrer ce risque pour le système d'information lorsque ce type d'équipement se situe dans le système d'information, via un port réseau traditionnel. Ce type de téléviseur moderne intègre aussi maintenant des capacités de traitement de protocole multimédia comme *UPnP* ou *DLNA*. Il est, par exemple, facile de dissimuler à l'arrière de la télévision une clé USB *WiFi* et une clé de stockage afin de voler des informations accessibles par ce réseau sans fil.

3 De l'information utile ?

Un constat assez rapide de l'existant : les journaux applicatifs des serveurs de résolution de noms (*DNS*) sont rarement exploités, voire souvent ignorés. Pourtant, ces mêmes journaux fournissent nombre d'informations qui peuvent se révéler utiles pour réaliser de multiples tâches :
– la détection grossière de machines participant à des campagnes d'émission de pourriels ;

- la surveillance de fuites d'informations par les techniques de tunnels cachés par *DNS* ;
- la découverte de machines compromises cherchant à communiquer vers des domaines ou des noms de mauvaise réputation se retrouvant dans des listes noires fournies par différents éditeurs ou par des projets communautaires associés à la sécurité ou vers des pays avec lesquels l'organisme n'a aucune relation ;
- le contrôle et la surveillance des procédures de mise à jour : la plupart des applications et des systèmes d'exploitation cherchent à communiquer vers des serveurs identifiables ou vers « leur maison-mères ». Il est donc possible :
  - de s'assurer que, si une base de mise à jour est fournie en interne dans le réseau (serveur miroir ou de type WSUS), cette politique est bien appliquée par tous les systèmes d'information ;
  - d'identifier des applications ne respectant pas la politique de sécurité en vigueur ;
  - de détecter des tentatives de corruption de cache *DNS* associé aux processus de mises à jour.

De petits scripts « maison » et des commandes standards (grep, cut, sed, perl, etc.) permettent bien souvent de mettre en place plusieurs vérifications et d'assurer assez simplement les tâches précédentes.

Il ne s'agit ici que d'illustrations de l'exploitation possible, à des fins de sécurité dans son réseau, des journaux des serveurs de résolution de noms. À cette fin, on notera l'importance que la politique de filtrage garantisse que tous les flux *DNS* transitent bien nécessairement par les serveurs dont les journaux sont analysés.

Il convient cependant de garder à l'esprit qu'il existe des contraintes juridiques fortes notamment en matière de surveillance du trafic réseau. Le CERTA recommande donc de respecter ces dernières et de se rapprocher d'un service juridique avant de mettre en place de telles mesures.

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=1937
- 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 16 au 22 octobre 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-446 : Vulnérabilités dans Symantec SecurityExpressions
- CERTA-2009-AVI-447 : Vulnérabilités dans phpMyAdmin
- CERTA-2009-AVI-448 : Vulnérabilités dans Xpdf et dérivés

– CERTA-2009-AVI-449 : Multiples vulnérabilités dans Cisco Unified Presence
– CERTA-2009-AVI-450 : Vulnérabilité dans ZFS pour Sun Solaris et Sun OpenSolaris
– CERTA-2009-AVI-451 : Multiples vulnérabiltés dans les produits VMware
– CERTA-2009-AVI-452 : Multiples vulnérabilités des produits Oracle
– CERTA-2009-AVI-453 : Multiples vulnérabilités dans WordPress

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

– CERTA-2009-AVI-323-001 : Vulnérabilités dans Apache APR-Utility (ajout de la référence au bulletin de sécurité IBM PK93225)
– CERTA-2009-AVI-391-001 : Multiples vulnérabilités dans Bugzilla (ajout de la référence au bulletin de sécurité Debian)

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, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique63.html

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.

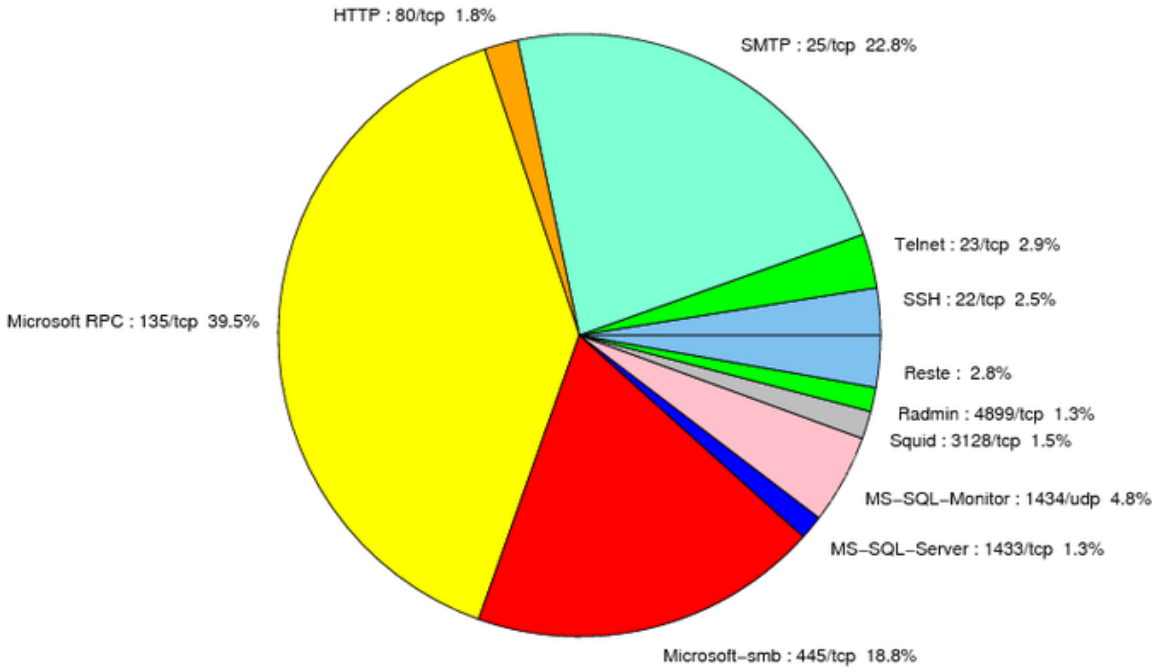

FIG. 1: Répartition relative des ports pour la semaine du 16 au 22 octobre 2009

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	39.48
25/tcp	22.84
445/tcp	18.77
1434/udp	4.78
23/tcp	2.97
22/tcp	2.52
80/tcp	1.94
3128/tcp	1.48
4899/tcp	1.29
21/tcp	0.77
2967/tcp	0.64
3389/tcp	0.58
1080/tcp	0.51
143/tcp	0.19
2100/tcp	0.06

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

23 octobre 2009 version initiale.