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 avril 2010
N° CERTA-2010-ACT-013

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-13

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-2010-ACT-013`

Gestion du document

Référence	CERTA-2010-ACT-013
Titre	Bulletin d'actualité 2010-13
Date de la première version	02 avril 2010
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-2010-ACT-013.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-2010-ACT-013/

1 Attaques contre SPIP

Après les services `FTP` et `SSH`, c'est au tour des `CMS` (*Content Management Software*) tels que *SPIP* de faire l'objet d'attaques par dictionnaire. Celles-ci se caractérisent par des rafales de requêtes `POST`.

Après avoir réussi à accéder frauduleusement au site, les attaquants ont déposé des pages à caractère publicitaire.

Les attaques qui nous ont été signalées remontent au début du mois de mars 2010.

Il est souhaitable que les administrateurs de site fonctionnant avec *SPIP* vérifient la présence ou non de traces de telles attaques. D'une manière générale, les webmestres doivent s'assurer que les mots de passe utilisés pour gérer leur site sont robustes. Il faut s'attendre à ce que dans un futur proche, tous les `CMS` fassent l'objet d'attaques par dictionnaire.

2 Durcissement de la configuration des systèmes Windows (6/8) : désactivation de l'autorun et de l'autoplay des lecteurs USB

Les fonctionnalités *autorun* et *autoplay* correspondent aux actions réalisées lors du montage d'un lecteur (fixe, amovible, CD-ROM, réseau ou autre), par l'explorateur de fichiers de Windows à travers la bibliothèque `shell32`.

La fonctionnalité *autorun* consiste à lire un fichier (`autorun.inf`) à la racine du lecteur nouvellement monté pour exécuter une action automatique, le plus souvent pour lancer un programme d'installation sur les CD-ROM. Les clés USB de type U3 émulent un CD-ROM et peuvent exécuter un code malveillant à l'insu de l'utilisateur lorsque celui-ci insère la clé dans son ordinateur.

La fonctionnalité *autoplay* est apparue avec Windows XP et consiste à parcourir le contenu du périphérique inséré pour proposer des actions qui dépendent des types de fichiers découverts (par exemple lire des fichiers son avec le lecteur par défaut, afficher des images, explorer le contenu, etc.). Depuis Windows XP, la fonctionnalité *autorun* n'est plus utilisée lors de l'insertion de périphériques de type amovible : seule la fonctionnalité *autoplay* est utilisée. Si un fichier `autorun.inf` est présent à la racine, les actions décrites dans ce fichier seront fusionnées avec les actions par défaut *autoplay*. Cette fonctionnalité a été pervertie par des virus en dupant l'utilisateur qui pouvait croire qu'il réalisait une action légitime d'affichage de contenu.

Les fonctionnalités *autorun* et *autoplay* peuvent être complètement désactivées pour tous les types de lecteurs en modifiant une valeur dénommée `NoDriveTypeAutoRun` de type `DWORD` pour que sa donnée vaille `0xFF` dans la clé :
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer`.

Ce paramètre peut également être positionné *via* les stratégies de groupe. Il se trouve dans la *Configuration ordinateur* (*Modèles d'administration*, *Système*), et est dénommé « *Désactiver le lecteur automatique* ». Il doit avoir la valeur « activé », en spécifiant « tous les lecteurs ».

Une fois ce paramètre activé, aucun programme n'est lancé automatiquement lors de l'insertion d'un CD-ROM et aucune fenêtre de choix d'action n'est affichée lors de l'insertion d'une clé USB, limitant le risque d'exécution involontaire de code malveillant placé au préalable sur ces supports.

Un bogue avait pour conséquence d'utiliser quand même la fonctionnalité *autorun* lorsque l'utilisateur double-cliquait sur l'icône du lecteur ou utilisait son menu contextuel, malgré le fait que cette fonctionnalité ait été désactivée. Ce bogue a été corrigé par la mise à jour Microsoft 967715[1] en 2009.

3 Journaux d'événements sur IPhone

L'importance et l'utilité des journaux d'événements n'est plus à démontrer dans le cadre de la résolution d'incidents, mais encore faut-il savoir les trouver.

Dans le cas de l'IPhone, `Apple` met à disposition l'application « Utilitaire de configuration IPhone » (*IPCU*) qui permet de configurer l'appareil (comme son nom l'indique) et de récupérer les journaux d'événements. À noter que l'appareil n'a pas besoin d'être synchronisé avec l'ordinateur utilisé, mais doit être déverrouillé par l'utilisateur.

En fonction de l'application, les données journalisées peuvent être plus ou moins verbeuses. Il est possible d'en modifier la granularité en obtenant un profil de configuration particulier auprès de `Apple`, dans le cadre d'un contrat de support. Parmi les informations intéressantes, on peut trouver les dates de déverrouillage de l'appareil, ce qui permet de savoir si quelqu'un y a accédé alors que celui-ci n'était pas en possession de l'utilisateur légitime.

Documentation

– « Apple - Support - iPhone - Enterprise » (téléchargement de l'utilitaire) :
http://www.apple.com/support/iphone/enterprise/

4 Mise à jour hors-cycle pour Internet Explorer

Microsoft a publié cette semaine le bulletin de sécurité MS10-018, qui correspond à une mise à jour hors-cycle pour Internet Explorer (avis CERTA-2010-AVI-146). Celle-ci corrige plusieurs vulnérabilités du navigateur

[1] `http://support.microsoft.com/kb/967715`

Web, dont une particulièrement critique qui avait été signalée par le CERTA le 10 mars 2010 dans son alerte : http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-004/index.html.

Cette alerte a donc été mise à jour cette semaine.

5 Fin du support de Firefox 3.0

Le CERTA a émis l'avis CERTA-2010-AVI-149 après la publication et la correction de dix vulnérabilités dans le navigateur Web Firefox. Les correctifs ont été publiés le 30 mars pour les branches 3.0, 3.5 et 3.6 du navigateur.

La fondation Mozilla, qui développe le logiciel Firefox, avait rappelé le 16 mars 2010 la fin du support de la branche 3.0 de Firefox. La version 3.0.19 est donc la dernière de cette branche.

Le premier avril, une vulnérabilité affectant la branche 3.6, démontrée lors de la conférence CanSecWest 2010, a été publiée et corrigée. Elle ne semble pas affecter la version 3.5.

La fondation Mozilla n'a pas étudié si la version 3.0 est vulnérable à cette attaque. Ceci illustre l'abandon du support de la branche 3.0 qui doit être implicitement considérée comme vulnérable.

Le CERTA invite fortement ses correspondants à migrer leur parc vers une branche maintenue (3.5 ou 3.6).

5.1 Documentation

- Wiki de la fondation Mozilla :
  https://wiki.mozilla.org/Platform/2010-03-16
- Bulletin de sécurité de la fondation Mozilla du 01 avril 2010 :
  http://www.mozilla.org/security/announce/2010/mfsa2010-25.html

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=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/

7 Rappel des avis émis

Dans la période du 26 mars au 01 avril 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-135 : Vulnérabilité dans spamass-milter
- CERTA-2010-AVI-136 : Multiples vulnérabilités dans Cisco IOS
- CERTA-2010-AVI-138 : Vulnérabilité dans cURL/LibCurl
- CERTA-2010-AVI-139 : Multiples vulnérabilités dans HP Project and Portfolio Center
- CERTA-2010-AVI-140 : Multiples vulnérabilités dans HP-UX
- CERTA-2010-AVI-141 : Multiples vulnérabilités dans les produits VMware
- CERTA-2010-AVI-142 : Vulnérabilités dans IBM WebSphere
- CERTA-2010-AVI-143 : Multiples vulnérabilités dans Apple MacOS X
- CERTA-2010-AVI-144 : Vulnérabilité dans phpCAS
- CERTA-2010-AVI-145 : Multiples vulnérabilités dans IBM Web Interface for Content Management
- CERTA-2010-AVI-146 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTA-2010-AVI-147 : Multiples vulnérabilités dans Apple iTunes
- CERTA-2010-AVI-148 : Multiples vulnérabilités dans HP SOA Registry Fondation
- CERTA-2010-AVI-149 : Multiples vulnérabilités dans Firefox
- CERTA-2010-AVI-150 : Multiples vulnérabilités dans Moodle
- CERTA-2010-AVI-151 : Vulnérabilités dans Apache ActiveMQ
- CERTA-2010-AVI-152 : Multiples vulnérabilités dans Oracle Java
- CERTA-2010-AVI-153 : Multiples vulnérabilités dans Apple QuickTime

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

- CERTA-2009-AVI-292-001 : Vulnérabilités dans HP-UX (ajout de la référence au bulletin de sécurité HP #01961959)
- CERTA-2009-AVI-482-007 : Vulnérabilité du protocole SSL/TLS (ajout des bulletins de sécurité Apple, Bluecoat, Cisco, Debian, Fedora, Gentoo, openBSD, ProFTPd, RedHat et Suse)
- CERTA-2010-AVI-002-001 : Vulnérabilité dans NTPD (ajout de la référence au bulletin de sécurité HP)
- CERTA-2010-AVI-112-001 : Multiples vulnérabilités du serveur HTTP Apache (ajout des références aux bulletins de sécurité RedHat et Ubuntu)
- CERTA-2010-AVI-137 : Vulnérabilités dans les imprimantes laser Lexmark (liens enrichis de &locale=EN&userlocale=EN_US (appel COTIC))

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

http://www.ssi.gouv.fr/site_rubrique67.html

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.

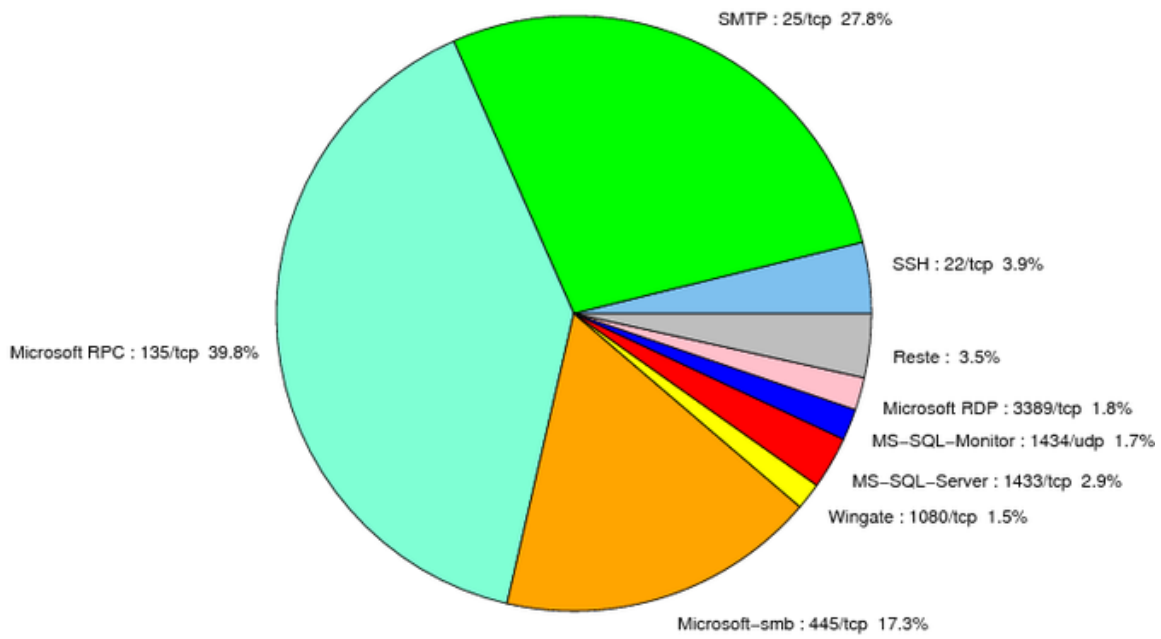

FIG. 1: Répartition relative des ports pour la semaine du 26 mars au 01 avril 2010

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	39.78
25/tcp	27.75
445/tcp	17.34
22/tcp	3.85
1433/tcp	2.85
3389/tcp	1.77
1434/udp	1.69
1080/tcp	1.46
2967/tcp	0.92
23/tcp	0.69
4899/tcp	0.61
3128/tcp	0.3
3306/tcp	0.23
21/tcp	0.15

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

02 avril 2010 version initiale.