Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 août 2009
N° CERTA-2009-ACT-032

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-32

Gestion du document

Référence	CERTA-2009-ACT-032
Titre	Bulletin d'actualité 2009-32
Date de la première version	07 août 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-032.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-032/

1 Incidents de la semaine

1.1 Un déni de service révélateur

Cette semaine le CERTA a reçu une demande d'assistance pour faire face à une attaque en déni de service. Le serveur Web visé ne contenait qu'une page de taille réduite et la bande passante qui lui était allouée était donc limitée. La semaine dernière, le nombre de connexions entrantes a soudainement augmenté, provoquant un engorgement de la connexion. Les adresses à l'origine des requêtes étant réparties dans le monde, cela menait tout d'abord à penser à une attaque en déni de service par un *botnet*. La lecture des journaux a montré immédiatement que les requêtes `GET` entrantes concernaient des pages extérieures et obtenaient le code retour 200 (`OK`). L'analyse fût simple, le serveur présentait un défaut de configuration, il était utilisé en tant que serveur mandataire depuis l'extérieur. La solution a consisté à modifier la configuration. Le serveur perdant son intérêt, les requêtes se sont arrêtées d'elles-mêmes.

Le CERTA recommande la lecture régulière des journaux. Si le débit n'était pas venu à manquer, le défaut de configuration n'aurait pas été détecté et la machine aurait pu être utilisée pour mener des attaques vers d'autres cibles.

1.2 La porte d'entrée n'est pas toujours celle attendue

Le CERTA a traité cette semaine la compromission d'un serveur Web. Des pages malveillantes ont été insérées et des pages légitimes modifiées. L'hébergeur a fourni au responsable du site un extrait des journaux applicatifs correspondant à la date supposée de l'incident.

L'analyse effectuée par le CERTA n'a mis en évidence aucune trace particulière permettant d'expliquer le problème. Des journaux complémentaires ont été demandés, dont ceux du système d'exploitation du serveur. Il est clairement apparu dans le journal `auth.log` que des accès frauduleux à un compte FTP donné ont été menés depuis différentes adresses IP dans le monde. Les traces obtenues ont montré que ces accès remontaient à une semaine au moins.

Cet incident permet de rappeler qu'il est important de ne pas présumer des méthodes de compromission avant d'avoir obtenu quelques données tangibles. En particulier, il ne faut pas restreindre son analyse aux quelques heures ou jours précédents la découverte de l'incident.

Dans le cas présent, des bonnes pratiques auraient permis d'éviter que le problème se produise :

- restreindre l'accès au service FTP ;
- renforcer la politique de mots de passe de chaque utilisateur FTP ;
- sensibiliser les utilisateurs FTP à ne pas se connecter depuis une machine qui n'est pas de confiance ou au travers d'un réseau Wi-Fi public.

Par ailleurs, la consultation régulière des journaux permet d'identifier des signes éventuels de compromission. Attendre un dysfonctionnement ou une marque manifeste de défiguration ne peut être suffisant et satisfaisant.

2 Retour sur l'alerte CERTA-2009-ALE-014

Aujourd'hui même le CERTA publie une alerte concernant le logiciel de messagerie `Thunderbird` : `CERTA-2009-ALE-014`. En effet, même si la fondation `Mozilla` a publié des correctifs de sécurité pour son navigateur Internet `Firefox`, `Thunderbird` reste, pour sa part, dans le numéro de version 2.0.0.22. En y regardant de plus près, il apparaît d'ailleurs que cette version ne met pas en œuvre la totalité des correctifs publiés depuis le début de l'année.

Voici les vulnérabilités non encore corrigées dans la version actuelle de `Mozilla Thunderbird` :

MFSA2009-18 : cette vulnérabilité n'a pas été corrigée dans `Thunderbird` car celle-ci nécessite l'activation de l'interprétation du *JavaScript*, option désactivée par défaut

MFSA2009-19 : cette vulnérabilité n'a pas été corrigée dans `Thunderbird` car celle-ci nécessite l'activation de l'interprétation du *JavaScript*, option désactivée par défaut.

MFSA2009-31 : cette vulnérabilité est présente au niveau de la vérification des scripts *XUL*. Cette vulnérabilité n'est pas corrigée dans `Thunderbird 2.0.0.22`.

MFSA2009-34 : ce bulletin de sécurité traite de plusieurs défaillances des produits Mozilla provoquant une corruption mémoire pouvant être exploitée dans certains cas. Cette vulnérabilité n'est pas corrigée dans `Thunderbird 2.0.0.22`.

MFSA2009-42 et MFSA2009-43 : ces deux bulletins de sécurité traitent de différentes vulnérabilité dans l'interprétation des certificats SSL. Ces vulnérabilités ne sont pas corrigées dans `Thunderbird 2.0.0.22`.

Cette latence dans la mise à jour de `Thunderbird` est relativement régulière. Même si les vulnérabilités décrites touchent le navigateur de manière plus importante, le client de messagerie reste un vecteur d'attaque assez sensible et il convient de bien mesurer le risque de telles failles.

Dans l'attente des correctifs, le CERTA encourage les utilisateurs à se tourner vers un client de messagerie alternatif et mis à jour.

Documentation

- Alerte CERTA-2009-ALE-014 du 07 août 2009 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-014/

3 Claviers Apple de dernière génération

La société `Apple` livre depuis quelque temps avec ses ordinateurs de bureau (`iMac` ou `Mac Pro`) des claviers munis de microgiciels (*Firmware*) enrichissant les fonctionnalités de ces derniers. Ces *firmwares* sont présents dans les claviers filaires ou sans-fil.

Or, des chercheurs ont démontré récemment lors d'une conférence de sécurité qu'il était possible de reprogrammer ce microgiciel à des fins malveillantes.

Ainsi, ils ont présenté une attaque consistant en l'implémentation dans le clavier, et en plus du logiciel d'origine, d'un programme capable d'injecter des frappes clavier supplémentaires à l'insu de l'utilisateur. De ce fait, il leur a été possible également, sous certaines conditions, d'envoyer l'intégralité des frappes clavier vers une machine distante, et ce, de façon totalement invisible pour l'utilisateur.

Le fait d'inclure dans un périphérique de saisie une « intelligence » particulière de type microgiciel peut avoir des conséquences sur la sécurité si un attaquant réussi à modifier ce dernier. Ceci n'est pas forcement une chose triviale à réaliser compte tenu, par exemple, du peu de ressources disponibles dans un tel périphérique. Il n'en reste pas moins que ces manipulations peuvent être très efficaces pour qui voudrait collecter des informations à l'insu de sa victime.

Recommandations :

Les microgiciels des claviers `Apple` font l'objet de mises à jour ponctuelles par le constructeur, il conviendra donc de bien surveiller qu'il existe, par exemple, une correspondance entre le bulletin de sécurité du constructeur et l'application de la mise à jour par le système. Par ailleurs, afin de limiter les risques, il est recommandé de n'utiliser ce clavier qu'avec la machine avec lequel il a été livré.

4 De l'usage des réseaux sociaux

Les réseaux sociaux répondent à des phénomènes de mode. Chaque année, un nouveau service apparaît et enregistre toujours plus de visites et d'utilisateurs.

Les individus se connectent ainsi et enregistrent leurs données personnelles afin de bénéficier du service. Ce dernier, comme tout service à succès, est relativement pratique afin de motiver les utilisateurs à adhérer.

C'est alors un phénomène à levier : l'utilisateur invite ses contacts à le rejoindre et adhérer au service. C'est lui qui fait la promotion de ce service, aidé autant que possible par des coups publicitaires à grande échelle.

Les sociétés gérant ces réseaux sociaux sont bien souvent des entreprises aux salariés nombreux et aux capitaux importants. Il vient naturellement la question : comment se rémunèrent-ils ?

La réponse est relativement simple : par les profils enregistrés. Selon les services, cette opération peut varier légèrement mais il s'agit souvent de :

- fournir de la publicité ciblée en fonction des profils ;
- vendre des informations.

Plus un utilisateur présente d'informations dans son profil, plus la société y trouve son compte.

Cette économie se fait à la discrétion de l'utilisateur qui n'en a, souvent, pas pleinement conscience. Disséminer ces données personnelles sur plusieurs réseaux sociaux ne consiste pas seulement à profiter d'un service séduisant (« gazouiller », retrouver des amis d'enfance, entretenir un réseau de collègues, etc.) mais également à faire profiter à plusieurs sociétés, souvent méconnues, de toutes ces données.

L'utilisateur doit se poser la question dans ce sens : un inconnu l'aborde dans la rue et lui pose toutes les questions concernant ses données personnelles :

- bonjour, quelle est votre date de naissance ?
- et vous êtes né dans quelle ville ?
- vous travaillez dans quelle société ? À quel poste ? Et votre salaire moyen est ?
- pour vos passe-temps, vous allez régulièrement au cinéma ? Vos films favoris sont ?
- vous avez une photo de vos amis sur vous ? Je peux la voir ?
- ...

Les utilisateurs qui multiplient les réseaux sociaux arrivent ainsi à fournir à des inconnus beaucoup plus d'informations sur leur vie privée, leurs envies et leurs motivations que quiconque dans leur entourage proche ne connaît. Certaines rubriques apparaissent également dans les questions « secrètes » utilisées par d'autres sites afin de récupérer un mot de passe oublié. Un profil trop bien rempli peut ainsi diminuer la sécurité d'autres comptes.

Il faut également garder à l'esprit que les deux seules premières informations suffisent très généralement à retrouver le nom de l'individu, comme des études récentes américaines l'ont montré.

Il ne s'agit évidemment pas ici de disserter sur l'usage des réseaux sociaux. Mais, compte-tenu de l'utilisation accrue de ces derniers et du phénomène de masse qui l'entoure, le CERTA invite ses correspondants à sensibiliser leurs utilisateurs sur les différents problèmes que ces usages suscitent.

5 Fin de la branche 2.0.x de WordPress

L'équipe de développement de *WordPress* avait prévu de maintenir la branche 2.0.x de leur produit jusqu'en 2010. Cette fin de vie a finalement été anticipée au 30 juillet 2009, notamment parce que la prise en compte des modifications de sécurité pour ces versions aurait représenté une charge de travail trop importante, avec de sérieux risques d'instabilité.

Les administrateurs de site fonctionnant avec *WordPress* 2.0.x sont donc fortement incités à migrer vers des versions plus récentes.

Documentation

– Annonce de la fin de développement de la branche 2.0.x de WordPress :
http://wordpress.org/development/2009/07/the-wordpress-2-0-x-legacy-branch-is-deprecated/

6 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 01 et le 06 août 2009.

7 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/

8 Rappel des avis émis

Dans la période du 01 au 06 août 2009, le CERTA a émis les avis suivants :

– CERTA-2009-AVI-305 : Vulnérabilité Shockwave Flash pour les produits Adobe
– CERTA-2009-AVI-306 : Vulnérabilités dans Firefox
– CERTA-2009-AVI-307 : Vulnérabilité de l'OS iPhone d'Apple
– CERTA-2009-AVI-308 : Multiples vulnérabilités des cartes mère Intel

– CERTA-2009-AVI-309 : Multiples vulnérabilités du système d'exploitation Apple MacOS X
– CERTA-2009-AVI-310 : Vulnérabilité dans SPIP
– CERTA-2009-AVI-311 : Vulnérabilité dans Sun VirtualBox
– CERTA-2009-AVI-312 : Multiples vulnérabilités dans Sun Java JDK/JRE
– CERTA-2009-AVI-313 : Vulnérabilité de la plateforme Java sous Windows

9 Actions suggérées

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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.

9.6 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.

9.7 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/

10 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.

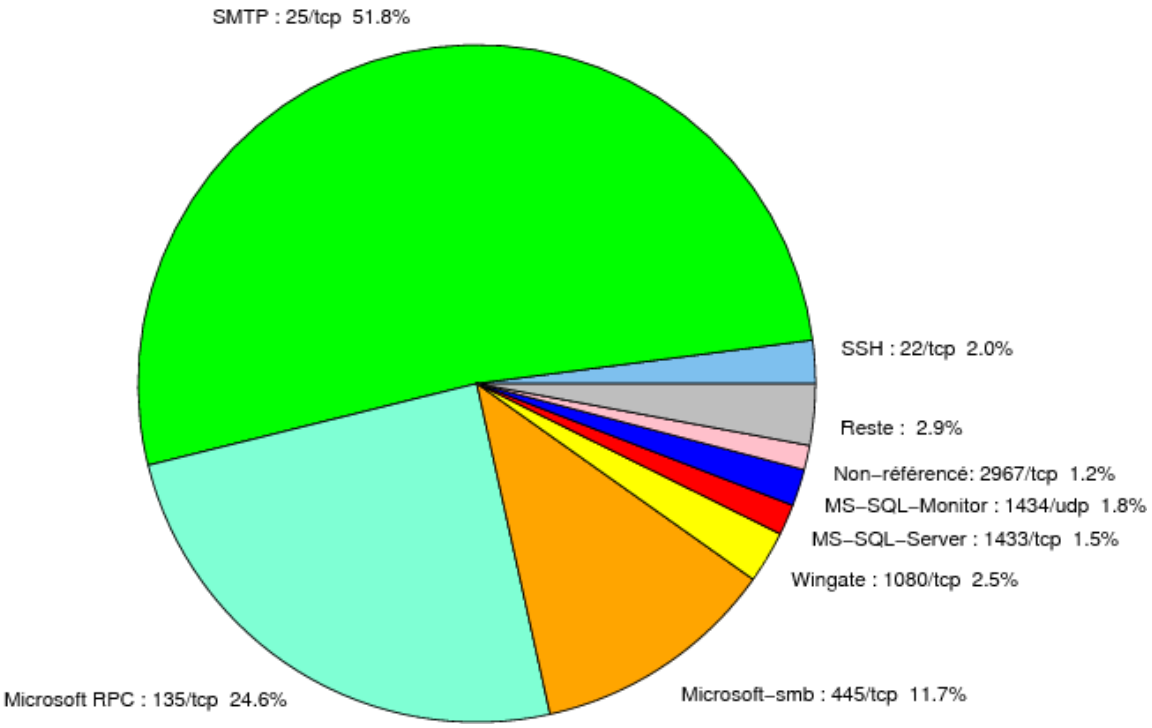

FIG. 1: Répartition relative des ports pour la semaine du 01 au 06 août 2009

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
25/tcp	51.83
135/tcp	24.59
445/tcp	11.71
1080/tcp	2.48
22/tcp	2.04
1434/udp	1.75
1433/tcp	1.46
2967/tcp	1.17
3128/tcp	0.87
80/tcp	0.73
3306/tcp	0.58
21/tcp	0.29
4899/tcp	0.14

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

07 août 2009 version initiale.