Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 juillet 2007
N° CERTA-2007-ACT-030

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-30

Gestion du document

Référence	CERTA-2007-ACT-030
Titre	Bulletin d'actualité 2007-30
Date de la première version	27 juillet 2007
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-2007-ACT-030.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-2007-ACT-030/

1 Le danger des barres d'outils additionnelles dans les navigateurs

De plus en plus de barres d'outils additionnelles sont proposées à l'utilisateur. Que ce soit dans un navigateur, dans un client de messagerie, ou plus directement pour le système d'exploitation, ces greffons sont censés faciliter la vie de l'utilisateur en offrant de nombreux services additionnels :

- accès plus rapide à un moteur de recherche ;
- accès plus rapide à un site commercial, la plupart du temps octroyant des remises ;
- recherche optimisée (dans les messages électroniques, sur le disque dur, . . .) ;
- . . .

Malheureusement, ces barres d'outils additionnelles présentent de gros risques pour le système d'information. En premier lieu, ces outils ne sont pas exempts de failles, et il n'est pas rare que celles-ci ne soient pas corrigées. Ainsi, un greffon de navigateur permettant d'accéder et de gérer plus facilement son compte sur un grand site de réseaux sociaux a été victime d'une faille cette semaine. Un simple script contenu dans une page web suffit à exploiter cette vulnérabilité, et à exécuter du code arbitraire à distance sur la machine victime.

Autre danger de ces greffons : l'atteinte à la confidentialité. En effet, le comportement sur le réseau de ces logiciels laisse parfois très perplexe, la plupart envoient des informations vers des serveurs non contrôlés. Le

contenu de ces informations dépend des greffons, certains étant plus « indélicats » que d'autres, en envoyant un grand nombre de données personnelles.

Les problématiques sont donc sensiblement les mêmes que celles inhérentes aux extensions (cf. CERTA-2007-ACT-014 et CERTA-2007-ACT-023), et pour certains greffons, proche des problématiques posées par les espiogiciels. Le CERTA recommande donc de ne pas installer cette sorte de greffons, étant donné le risque induit par celui-ci par rapport à la faible valeur ajoutée proposée.

L'administrateur doit rester vigilant quant à l'installation de telles barres sur les navigateurs des utilisateurs. Une manière pour visualiser certaines d'entre elles consiste à analyser les journaux du serveur relai Web (ou proxy). En effet, les barres ont une tendance à modifier le champ `User-Agent`, qui devrait être par défaut celui du navigateur. Toute chaîne de caractères suspecte sera donc un signe, soit d'une compromission, soit d'une installation sauvage. Cette méthode n'est bien sûre pas absolue, car ce champ peut être aisément modifié, mais c'est l'observation d'anomalies comme celles-ci dans les journaux que l'administrateur peut mettre en évidence certains problèmes sur les machines du réseau.

2 Vulnérabilité dans BIND

Cette semaine, le CERTA a publié un avis de sécurité (CERTA-2007-AVI-333) relatif à une vulnérabilité dans le serveur `DNS` (*Domain Name Server* `BIND`. Ce serveur est largement deployé et utilisé sur l'Internet pour effectuer la résolution de noms de machines et de domaines. Une vulnérabilité dans la version 9.x de `Bind` a été découverte et concerne une faiblesse dans la façon dont les identifiants de requêtes `DNS` ou « *Query IDs* » sont fixés. Il est en effet possible de prévoir, dans certains cas, l'identifiant qui sera utilisé dans la prochaine requête. En connaissant celui-ci, il est alors possible de forger de fausses réponses à destination d'un serveur voulant mettre à jour son cache. Un utilisateur malintentionné peut ainsi réaliser une attaque de type *DNS Cache Poisoning*. Si l'attaque est fructueuse, le serveur cible pourtant légitime repondra dès-lors de fausses informations à ces clients.

Cette vulnérabilité mise en conjonction avec une faille comme celle décrite dans CERTA-2007-ACT-022 et CERTA-2007-ALE-012 relative aux mises à jour non-maîtrisées des extensions du navigateur Firefox pourrait permettre de propager de façon discrète du code malveillant. Ainsi lors de la mise à jour d'une extension Firefox, le navigateur pourrait télécharger une fausse mise à jour à partir d'un domaine usurpé avec cette technique de *Cache Poisoning*.

Le CERTA recommande de mettre à jour, s'il est utilisé, le serveur DNS BIND interne et/ou externe dans les plus brefs délais.

3 Sur la cohabitation de deux navigateurs, la suite

3.1 Nouvelle vulnérabilité sur Firefox

L'article *Sur la cohabitation de deux navigateurs sur un poste de travail* dans le bulletin d'actualité CERTA-2007-ACT-028 du 13 juillet 2007 détaillait une vulnérabilité fonctionnant seulement si `Mozilla Firefox` et `Microsoft Internet Explorer` sont installés. En effet, l'URI `FirefoxURL` appelée dans le contexte d'une navigation sur `Internet Explorer` permet de passer des commandes malveillantes non contrôlées, notamment du Javascript, au navigateur `Firefox`.

Cette semaine une nouvelle vulnérabilité nécessitant également la présence de deux navigateurs a été publiée par un chercheur. Elle est de nouveau causée par un mauvais traitement de certaines URI.

La rencontre d'une URI connue par un navigateur se traduit normalement par le lancement de l'application associée dans la base de registre, avec comme argument le reste de l'URL. La faille ici consiste à notamment utiliser les caractères `%00` ce qui cause `Firefox` de ne pas lancer l'application associée, mais de traiter l'URI comme une de type `Filetype` (normalement inaccessible depuis l'extérieur). Il est ainsi possible de lancer des exécutables présents sur le poste d'une personne accédant à une URL de ce type, avec des arguments.

Cette vulnérabilité fonctionne au moins sur `Microsoft Windows XP SP2` avec `Firefox 2.0.0.5`, seulement si `Internet Explorer 7` est installé. A la date de rédaction de ce document, il n'est pas encore clair ce qu'est le rôle joué par `Internet Explorer` dans cette faille qui concerne au moins `Mozilla Firefox` et `Netscape Navigator`. Il semble que l'installation de `Internet Explorer 7` change la manière dont `Windows XP` traite les URI, toutefois `Internet Explorer 7` n'est pas directement touché par la faille. Il semble que les utilisateurs de `Windows Vista` ne sont pas touchés.

3.2 Contournement

La vulnérabilité sera corrigée dans la prochaine version de Firefox (2.0.0.6) mais aucune date de sortie n'a pour le moment été annoncée. Les autres navigateurs basés sur le moteur de rendu `Gecko` semblent également concernés. Le CERTA a donc émis l'alerte CERTA-2007-ALE-013 et recommande ainsi l'application d'un contournement provisoire, consistant à désactiver la mise en oeuvre de tout protocole par défaut et à ne réactiver que ceux nécessaires à une navigation classique (HTTP, HTTPS ou FTP éventuellement). Cette mesure doit s'adapter aux besoins.

Pour désactiver tous les *protocol handlers* :

- dans la barre d'adresse de `Firefox`, taper `about:config` ;
- dans le filtre, taper `protocol` pour obtenir la liste des options utiles ;
- mettre les valeurs *network.protocol-handler.external.news*, *network.protocol-handler.external.snews*, *network.protocol-handler.external.mailto*, *network.protocol-handler.external.nntp* et *network.protocol-handler.expose-all* à false en double-cliquant dessus ;

Pour activer les *protocol handlers* nécessaires à une navigation classique :

- dans la fenêtre `about:config`, faire un clic-droit, choisir l'option `Nouvelle` et `valeur booléenne` ;
- donner le nom *network.protocol-handler.expose.http* et lui donner la valeur `true` ;
- faire de même en donnant les noms *network.protocol-handler.expose.https* et *network.protocol-handler.expose.ftp*.

Ce contournement peut toutefois être trop contraignant et gêner la navigation. Un autre contournement consiste à forcer l'affichage d'avertissements (champs *network.protocol-handler.warn-external.X* à `true`).

Le CERTA rappelle également l'importance de vérifier les liens, de cliquer avec précautioin, ou de taper manuellement l'adresse. Il est aussi recommandé de lancer le navigateur avec un utilisateur disposant de privilèges limités.

3.3 Références

Alerte du CERTA CERTA-2007-ALE-013 du 27 juillet 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-013/index.html

4 Production de codes malveillants

Les techniques de détection de codes malveillants ne permettent de détecter que ce qui est connu (signatures, ou heuristiques, comportements, etc.).

Depuis de nombreuses années, il existe des outils automatisés de création de codes malveillants, qui savent produire des programmes inconnus et par conséquent indétectables pendant un certain temps.

A titre d'illustration récente, certaines sources sur l'Internet ont publié des articles portant sur des applications permettant de créer simplement des codes malveillants (codes d'exploitation, chevaux de Troie, etc.) via une interface graphique. Le code malveillant est donc créée par des manipulations conviviales de tout utilisateur sachant cliquer, et sans compétence technique particulière.

Par exemple, certaines interfaces laissent le choix à l'utilisateur de la méthode de communication (tunnels de communication, les mots de passe pour déchiffrer les données échangées, ainsi que la technique d'obfuscation du code). Elles demandent également à l'utilisateur ce qu'il souhaite faire sur la machine infectée : modifier des données, dérober des informations, installer un outil de capture de frappes clavier, etc. L'utilisateur n'est pas obligé de connaître toutes les subtilités des choix offerts. Quelques clics lui permettent ainsi de créer un exécutable adapté.

De plus, cette même personne peut alors user d'ingénierie sociale destiné à améliorer la propagation de son code malveillant dans un environnement ciblé. D'ailleurs, il n'est pas exclu que ce type d'application soit également un code malveillant de type cheval de Troie.

L'élément qui a été souligné dans ces publications est que des personnes sont prêtes à acheter de telles applications. Pour se prémunir contre des codes malveillants, comme le CERTA le rappelle régulièrement, il n'est pas possible de s'appuyer uniquement sur des outils, et la méfiance et un comportement sage des utilisateurs restent souvent la meilleure parade.

5 Les courriers indésirables et les fichiers Excel

Après les courriers indésirables détournant la technologie des images (captcha) pour duper les filtres, les différents contenus publicitaires logés dans des documents au format PDF et donc la plupart du temps considérés à tort comme légitimes, le temps est venu pour les e-pollueurs de remplir les boîtes de tableaux Excel contenant les informations à propager. L'utilisation de ce format a une double utilité. En effet il s'agit ici d'un cas de tentative d'attaque en Pump-and-Dump consistant à essayé de manipuler artificiellement le cours d'actions boursières en propageant des informations contrefaites, et d'en profiter pour spéculer à moindre risque. Ces informations étant d'ordre financières, quoi de plus légitime qu'un tableau de chiffres et des graphiques pour donner de la crédibilité à la fausse fuite montée de toutes pièces. L'autre intérêt vient du format propre à ce type de document qui permet de fractionner les données et les textes parmi des spécifications de colonnes propres au format, et ainsi les rendre indétectables par les filtres.

Pour lutter contre ce nouveau type de pourriels les recommandations décrites dans la note d'information CERTA-2005-INF-004 restent valables. Les moyens mis en œuvre pour tromper les outils de sécurité sont toujours innovants, mais le principe reste identique, et la vigilance de l'utilisateur est la première protection. En cas de doute, il ne faut pas hésiter à poser la question à son responsable informatique RSSI, ou au CERTA.

6 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 19 et le 26 juillet 2007.

7 Liens utiles

- Mémento sur les virus :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
- Note d'information sur l'acquisition de correctifs :
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/index.html
- Note d'information sur les systèmes obsolètes :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html
- Note d'information sur les bonnes pratiques concernant l'hébergement mutualisé :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/index.html
- Note d'information sur les mots de passe :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html
- Note d'information sur la terminologie d'usage au CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/index.html
- Note d'information sur les enjeux de sécurité liés à une migration vers IPv6 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/index.html
- 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 CERTA-2006-INF-006, Risques associés aux clés USB :
  http://www.certa.ssi.gouv.f r/site/CERTA-2000-INF-006/
- Note d'information du CERTA CERTA-2006-INF-009 sur les outils d'indexation et de recherche :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/
- Note d'information du CERTA CERTA-2007-INF-001 sur la gestion des noms de domaine :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/
- Note d'information 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 20 au 26 juillet 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-324 : Multiples vulnérabilités du navigateur Opera

– CERTA-2007-AVI-325 : Multiples vulnérabilités dans Citrix Access Gateway
– CERTA-2007-AVI-326 : Vulnérabilité d'IBM WebSphere
– CERTA-2007-AVI-327 : Vulnérabilité dans BIND
– CERTA-2007-AVI-328 : Vulnérabilité dans Kerio MailServer
– CERTA-2007-AVI-329 : Vulnérabilités dans plusieurs produits Computer Associates
– CERTA-2007-AVI-330 : Multiples vulnérabilités dans HP Oracle for OpenView
– CERTA-2007-AVI-331 : Vulnérabilité dans CA Message Queuing
– CERTA-2007-AVI-332 : Vulnérabilité dans Sun Java System Application Server
– CERTA-2007-AVI-333 : Vulnérabilité dans SUN Solaris Low Bandwidth proxy
– CERTA-2007-AVI-334 : Vulnérabilité dans des produits Cisco

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

– CERTA-2007-AVI-327-001 : Vulnérabilité dans BIND
(ajout des références aux bulletins de sécurité Debian)

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'inf ormation de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'orga nisme 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 œuvre (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 COSSI/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.formation.ssi.gouv.fr

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.

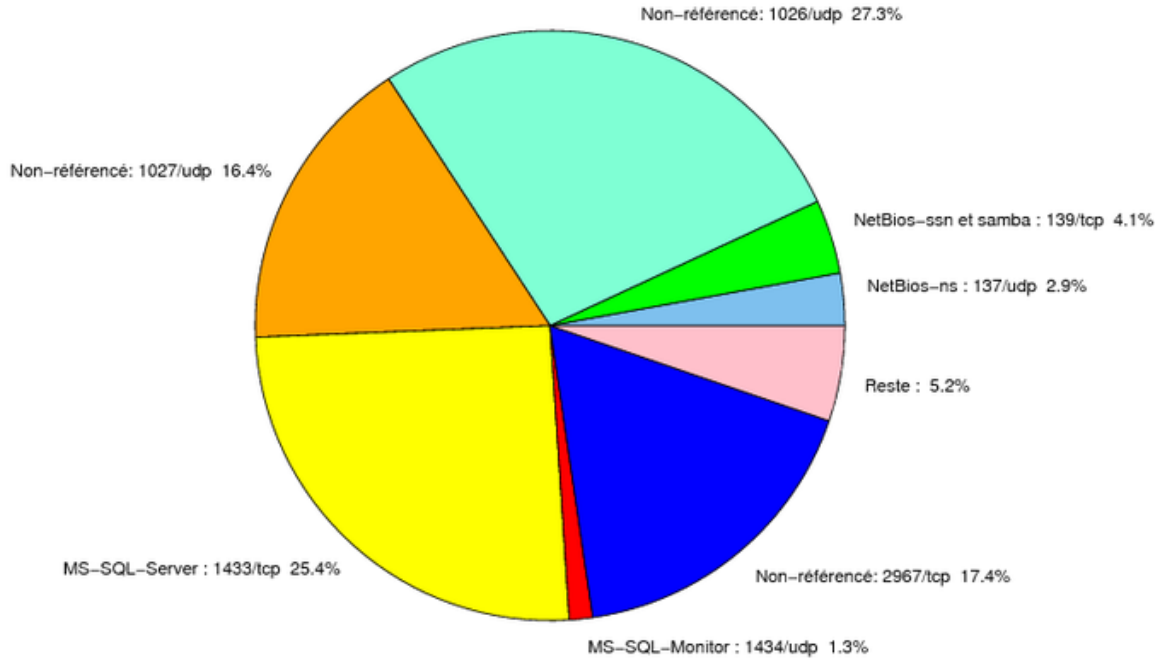

FIG. 1: Répartition relative des ports pour la semaine du 19.07.2007 au 26.07.2007

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CE
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
106	TCP	MailSite Email Server	–	–
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CE
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CE
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CE
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE

				http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CE
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CE
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CE
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CE
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CE
2381	TCP	–	HP System Management	http://www.certa.ssi.gouv.fr/site/CE
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CE
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CE
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CE
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CE
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
10080	TCP	Amanda	MyDoom	–
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CE
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CE

TAB. 2: Correctifs correspondant aux ports destination des paquets rejetés

port	pourcentage
1026/udp	27.31
1433/tcp	25.41
2967/tcp	17.44
1027/udp	16.39
139/tcp	4.05
137/udp	2.86
1434/udp	1.27
22/tcp	0.94
1080/tcp	0.86
4899/tcp	0.83
3128/tcp	0.64
15118/tcp	0.28
3306/tcp	0.25
25/tcp	0.23
443/tcp	0.17
3389/tcp	0.15
80/tcp	0.14
11768/tcp	0.12
143/tcp	0.06
3127/tcp	0.04

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

27 juillet 2007 version initiale.