Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 juin 2007
N° CERTA-2007-ACT-024

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-24

Gestion du document

Référence	CERTA-2007-ACT-024
Titre	Bulletin d'actualité 2007-24
Date de la première version	15 juin 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-024.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-024/

1 Les incidents traités cette semaine

1.1 Ajout d'*iframes*

Le CERTA a récemment traité deux cas particuliers de compromission de serveur Web. Contrairement à ce que nous pouvons constater habituellement, il n'y a pas eu de défiguration. L'intrus a profité de vulnérabilités sur le serveur pour ajouter des cadres (*iframes*) dans des pages Web. Le code est inséré dans chaque page du site Web (ou du serveur, selon les droits obtenus lors de la compromission) après la balise de fin `</html>`. Le principe de ces cadres est de rediriger les visiteurs vers un site tiers pratiquant le *pay-per-click* (paiement d'un affilié à chaque visite). Ces redirections permettent à l'intrus de s'enrichir.

Le ou les auteurs de ces intrusions semblent utiliser plusieurs vulnérabilités affectant divers composants optionnels du gestionnaire de contenus (CMS) *Joomla!*. Les attaques affectant ce logiciel sont si nombreuses qu'il est parfois difficile, lors d'une analyse, de faire le tri entre celles qui échouent et celles qui réussissent. Il est important de préciser que la conséquence de ces intrusions peut aussi être l'ajout de code malveillant sur chaque page afin d'exploiter une vulnérabilité du navigateur des visiteurs du site.

Ces intrusions sont assez difficiles à détecter visuellement. Dans les cas que nous avons traités, il était possible de mettre en évidence les pages « infectées » en effectuant la recherche suivante dans l'arborescence du site Web :

```
grep -R "aff=" *
```

Une meilleure façon consiste à mettre en œuvre un logiciel de contrôle d'intégrité qui surveille les modifications des fichiers.

1.2 Cas de filoutage

L'un des deux serveurs concerné par l'ajout d'*iframes* a également été utilisé pour héberger un faux site bancaire de filoutage (*phishing*). Les propriétaires de ce serveur ont, dans un premier temps, arrêté la machine, mais l'ont relancé peu de temps après en pensant avoir fait le nécessaire (notamment en supprimant le site de *phishing*). La conséquence a été l'installation d'un second site de *phishing* ciblant une autre banque.

Nous rappelons que l'installation d'un faux site bancaire est avant tout une conséquence visible d'une vulnérabilité présente sur le serveur. Le fait d'enlever le site de *phishing* ne supprime pas la vulnérabilité de la machine et il faut par conséquent s'attendre à ce que le problème revienne très rapidement. La lecture des journaux permet généralement de comprendre comment l'intrusion s'est déroulée et ainsi de corriger la faille exploitée, mais elle ne suffit pas non plus. Dans la plupart des cas, les intrus ajoutent des portes dérobées sur le serveur afin de pouvoir revenir à leur guise.

La meilleure méthode à employer consiste à procéder ou à faire procéder à une analyse d'incident basée sur une image physique du disque dur (afin de préserver les traces et indices) puis de réinstaller le serveur (de préférence après analyse de l'incident). Le CERTA reste à disposition de ses correspondants pour les assister dans ces démarches.

2 Vulnérabilités de Safari pour Windows

Depuis le 11 juin 2007, la version beta pour Windows du navigateur Safari 3 est disponible pour le grand public. Cette sortie a créé un engouement tel que plus d'un million de téléchargements ont d'ores-et-déjà été recensés pour ce produit, selon l'éditeur, à la date de rédaction de ce bulletin.

Cependant, seulement quelques heures après la mise à disposition du navigateur, plusieurs vulnérabilités ont été rapportées par des chercheurs connus, notamment ceux ayant participé au *Month of Browser Bugs* de juillet 2006. A ce jour, près d'une vingtaine de vulnérabilités ont été découvertes, principalement au moyen d'outils de tests aléatoires (*fuzzing*). Plusieurs permettent l'exécution de code arbitraire à distance et des dénis de service à distance. Plusieurs de ces vulnérabilités ont même été diffusées avec du code de faisabilité, rendant plus aisée l'exploitation de celles-ci.

Trois failles ont été corrigées avec la publication de la version 3.01 de Safari pour Windows, et sont détaillées dans l'avis CERTA-2007-AVI-265 :

- un débordement de mémoire (CVE-2007-3185) ;
- une injection indirecte de code ou *cross-site scripting* (CVE-2007-2391) ;
- une erreur dans la validation des URL (CVE-2007-3186).

L'arrivée d'un nouveau navigateur sur Microsoft Windows élargit l'alternative lorsque d'autres navigateurs présenteront des failles non corrigées. Toutefois, il convient de rappeler que la version Windows de Safari n'est pas encore finale, qu'elle est toujours vulnérable et que de nouvelles vulnérabilités seront probablement découvertes pour cette version beta. Ainsi, comme lors des sorties de Firefox 2 et Internet Explorer 7 en octobre 2006 (bulletin d'actualité CERTA-2006-ACT-043), il est recommandé d'attendre que Safari 3 soit plus stable pour l'utiliser.

Documentation

- Avis du CERTA CERTA-2007-AVI-265 du 15 juin 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-265/index.html
- Avis Apple APPLE-SA-2007-06-14 du 14 juin 2007 :
  http://lists.apple.com/archives/Security-announce/2007/Jun/msg00000.html

3 Les duperies financières

Parmi les nombreux courriers électroniques non sollicités qu'il est possible de recevoir, certains se présentent de la manière suivante :

- ils sont écrits en français ;
- ils semblent être envoyés par une personne résidant dans un autre pays ;

– ils proposent :
    1° des objets à vendre, aussi bien rares (peintures, animaux exotiques, statues, etc.) que courants (appareils électroménagers, ordinateurs ou téléphones portables, etc.) ;
    2° des « cadeaux », ou « dons », où le correspondant demande uniquement de régler les frais de transport.

Cette approche est différente de l'escroquerie appelée « escroquerie nigériane », qui se présente souvent sous la forme d'une lettre écrite par une personne prétendant avoir beaucoup d'argent, mais qui a besoin d'aide pour l'exporter vers la France. Ce service serait rémunéré.

Les conséquences pour la victime sont néanmoins assez similaires. Dans la majorité des cas :

1° les personnes intéressées doivent effectuer un paiement. Les garanties présentées ne sont pas particulièrement suspectes, les comptes indiqués pouvant être dans des banques connues ;

2° de nouveaux frais peuvent être exigés pour poursuivre la duperie : les frais de douane ou de transport par exemple ont été oubliés, et il faudrait refaire un nouveau virement. De faux documents et de faux acteurs peuvent intervenir pour consolider le scénario ;

3° de nouveaux montants peuvent être demandés comme moyen de chantage, sous peine de rendre public cette tentative de fraude ;

4° des techniques d'intimidation peuvent se produire, au cours par exemple de rencontres réelles avec des complices basés en France ;

5° etc.

La meilleure solution est d'éviter de tomber dans cet engrenage dès le début, en ne répondant pas à ce genre de courrier. Le CERTA recommande donc à ces correspondants de sensibiliser leurs utilisateurs à ce genre de fraude, et à filtrer ou marquer les courriers indésirables identifiés comme tels.

Une note d'information traite des différentes formes de canulars par courrier électronique qui posent des problèmes similaires :

http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-005

4 Les données de connexion

De nombreux utilisateurs se connectent à distance au réseau de travail, par le biais d'une liaison `VPN` (*Virtual Private Network*). Cette solution crée un réseau virtuel, isolé en principe du réseau physique sous-jacent. Cela permet de former un tunnel, entre la machine cliente de l'utilisateur et le serveur, qui peut être construit à partir d'une méthode d'authentification des interlocuteurs, et de chiffrement des données échangées.

Sur la machine de l'utilisateur, cette solution se matérialise par l'installation et le lancement d'un « client VPN ». Dans plusieurs cas, ce client enregistre ou offre la possibilité d'enregistrer l'identifiant et le mot de passe de la connexion, pour faciliter les futures tentatives d'accès. Ces derniers peuvent être stockés dans les fichiers de profil de l'utilisateur, ou sous forme de clé de registre. Certains clients proposent d'obfusquer ou de chiffrer la clé, mais cela n'est pas systématique, et les techniques utilisées peuvent présenter des faiblesses. Certains clients utilisent également une interface réseau virtuelle, leur permettant d'utiliser une adresse `MAC` spécifique. Cependant une telle adresse peut aussi être usurpée.

Ce compte (identifiant et mot de passe) offre donc un point d'accès au réseau, et celui-ci n'est souvent pas considéré comme tel, ou à la même mesure que d'autres. En effet, la vente ou la perte du portable peut impliquer la récupération de ses données. la personne malveillante dispose alors de tous les détails permettant un accès (nom et adresse du serveur, identifiant, mot de passe). Elle peut en profiter pour utiliser les services proposés (navigation ou messagerie) ou chercher à continuer son intrusion dans le réseau.

Il faut donc que les différents acteurs considèrent ce risque, et prennent quelques mesures.

– L'administrateur devrait :
    – sensibiliser les utilisateurs à ce risque ;
    – avoir une politique de gestion de comptes stricte et renouveler régulièrement les mots de passe ou utiliser une technologie à base de mots de passe non rejouables ;
    – vérifier parmi les échecs de connexion si d'anciens identifiants et mots de passe n'ont pas été réutilisés.
– l'utilisateur devrait :
    – installer les clients `VPN` sur des machines de confiance uniquement ;
    – signaler la perte ou la vente de son portable ;
    – ne pas vendre le disque dur associé mais le restituer au service administratif pour un nettoyage efficace ;

– éviter d'utiliser les stockages de mots de passe, et opter pour frapper ces derniers à chaque nouvelle connexion.

5 Le mélange de fonctionnalités

Certains vendeurs de matériels réseau, tel *Cisco*, proposent dans certains de ses équipements comme les routeurs des fonctionnalités de mise en cache des requêtes de résolution de nom `DNS` : un routeur, en examinant les paquets contenant les requêtes `DNS` provenant d'autres machines du réseau interne, répondra à la requête en lieu et place du vrai serveur `DNS`. Cette fonctionnalité permet d'économiser de la bande passante à l'image d'un mandataire (*proxy*) `HTTP`.

Cependant, cela pose des problèmes de sécurité. En effet, compte tenu du type de matériel, le cache `DNS` sera généralement de petite taille, il serait donc possible à un attaquant soit de saturer ce cache soit de le poluer avec de fausses entrées afin de réaliser des attaques de type « homme du milieu » (*Man in the Middle*). Une attaque ciblée s'en trouve d'ailleurs facilitée puisque l'attaquant peut cibler le routeur de la victime directement plutôt que le `DNS` de son hébergeur ou de son FAI, ce qui est souvent plus délicat. Enfin, on peut s'intéroger sur la pertinence de rajouter des fonctionnalités de niveau élevé, couteuse en ressources, comme la gestion `DNS` dans des équipements conçu nativement pour faire du routage.

Un serveur `DNS` a une fonction propre, et il est donc assez facile d'adapter une politique de sécurité claire à son sujet, que ce soit les règles de filtrage des flux, ou des listes de contrôle d'accès par exemple. Un équipement qui combine plusieurs fonctions dispose rarement d'autant d'attention, alors que, paradoxalement, sa compromission peut affecter plusieurs services (le routage, la résolution de noms, etc.).

Le CERTA recommande donc d'éviter l'usage de boîtes multi-fonctions, dans la mesure du possible. Le gain initial espéré peut dissimuler des problèmes de sécurité plus coûteux.

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 07 et le 14 juin 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

Durant la période du 08 au 14 juin 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-256 : Multiples vulnérabilités dans le noyau Linux
- CERTA-2007-AVI-257 : Vulnérabilité dans Cisco Trust Agent
- CERTA-2007-AVI-258 : Vulnérabilité dans l'API Win32
- CERTA-2007-AVI-259 : Vulnérabilité de Outlook Express et Mail
- CERTA-2007-AVI-260 : Vulnérabilité dans Microsoft Visio
- CERTA-2007-AVI-261 : Vulnérabilité dans Microsoft Schannel
- CERTA-2007-AVI-262 : Vulnérabilité dans Windows Vista
- CERTA-2007-AVI-263 : Multiples vulnérabilités dans Internet Explorer

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

- CERTA-2007-AVI-082-001 : Vulnérabilités de Microsoft concernant un objet OLE associé à un fichier RTF (mise à jour du bulletin de sécurité Microsoft MS07-012 du 12 juin 2007)
- CERTA-2007-AVI-165-001 : Vulnérabilités dans Microsoft Content Management Server (CMS) (mise à jour du bulletin MS07-018 le 12 juin 2007 par l'éditeur)

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.

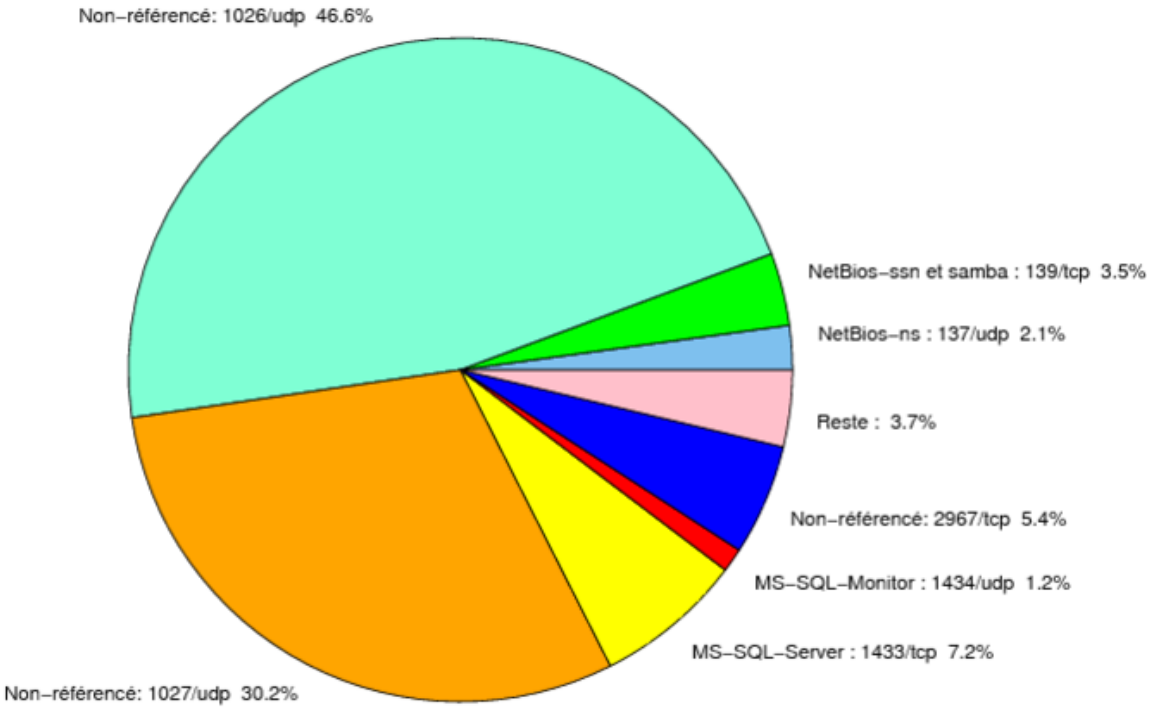

FIG. 1: Répartition relative des ports pour la semaine du 07.06.2007 au 14.06.2007

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	46.62
1027/udp	30.15
1433/tcp	7.23
2967/tcp	5.4
139/tcp	3.54
137/udp	2.14
1434/udp	1.16
4899/tcp	0.73
1080/tcp	0.43
25/tcp	0.36
3306/tcp	0.3
21/tcp	0.27
80/tcp	0.26
3128/tcp	0.2
15118/tcp	0.12
443/tcp	0.11
9898/tcp	0.04
143/tcp	0.02
5554/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

15 juin 2007 version initiale.