Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 mai 2007
N° CERTA-2007-ACT-021

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-21

Gestion du document

Référence	CERTA-2007-ACT-021
Titre	Bulletin d'actualité 2007-21
Date de la première version	25 mai 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-021.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-021/

1 Les incidents traités cette semaine

1.1 Incidents liés à une récente vulnérabilité dans `Dokeos`

Les 23 et 24 mai 2007, des outils permettant d'exploiter une vulnérabilité non corrigée des versions 1.6.5 et 1.8.0 de `Dokeos` ont été publiés. Cette vulnérabilité est de type `SQL injection` et permet d'obtenir les droits de l'administrateur de la base de données. Un attaquant peut ainsi facilement modifier l'aspect de l'interface `Dokeos`, notamment en ajoutant des images et du texte. L'attaquant doit disposer d'un `SESSION_ID` pour réaliser son attaque. Ceci peut être facilement obtenu en créant un compte utilisateur.

Le CERTA recense déjà 3 attaques sur des sites `Dokeos` 1.6.5 survenues le 25 mai 2007. Les traces laissées dans les journaux sont assez caractéristiques :

```
access_log-20070525.gz:IP_attaquant - - [25/May/2007:00:31:24 +0200]
"GET /dokeos/claroline/tracking/courseLog.php?scormcontopen=-999)
%20UNION%20SELECT%20CONCAT[...]
HTTP/1.1" 200 3375 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)"
```

Ces attaques peuvent être facilement mises en évidence à l'aide de commandes telles que :

```
grep "=-999" access_log
```

Dans les cas traités par le CERTA, l'attaquant avait recherché, à l'aide du moteur `Google`, les sites utilisant `Dokeos` en version 1.6.5. Il est donc fortement conseillé aux administrateurs d'effectuer ce type de recherche (sur les versions 1.6.5 et 1.8.0) sur les réseaux qui sont sous leur responsabilité.

En l'absence de correctif pour cette vulnérabilité, le CERTA recommande de désactiver les pages `Dokeos`.

1.2 La navigation et la confiance

Cette semaine, le CERTA a traité un incident qui montre l'intérêt de suivre les indications relatées dans ses différentes publications. En effet, l'analyse d'une machine a permis de mettre en évidence son infection par un enregistreur de frappes clavier (*keylogger*, cf. CERTA-2006-INF-002).

Le propriétaire de la machine a enchainé plusieurs erreurs issues d'un manque de précaution. Tout d'abord, il est allé consulter un site n'offrant pas toutes les garanties de confiance, tout en ayant autorisé l'interprétation de javascript. Malheureusement, ce site contenant un script hostile qui, une fois exécuté, cherche et installe un logiciel malveillant contenant un cheval de troie et un enregistreur de frappes du clavier. Cet utilisateur ne disposant pas de logiciel antivirus, l'installation du code malveillant n'a pas rencontré de problème.

L'effet néfaste d'un tel logiciel est qu'il est spécialement et exclusivement conçu pour enregistrer tout ce qui se fait sur un ordinateur, et transmettre ces informations à une personne tiers qui en fera par la suite usage suivant leur nature :

- informations à caractère personnel (formulaires en ligne, ...);
- informations bancaires (code de carte bleue, RIB, mot de passe d'accès à une gestion de compte en ligne, ...) ;
- informations autres (messages électroniques, documents de travail, ...).

Un tel incident aurait pu être évité en respectant des règles simples de comportement vis-à-vis de l'outil informatique :

- éviter de naviguer sur des sites qui n'inspirent pas une totale confiance ;
- désactiver l'interprétation de contenu dynamique par défaut (javascript, java, ActiveX, etc.), et ne réactiver cette possibilité qu'en cas de nécessité et sur un site de confiance ;
- éviter de cliquer sur des contenus suspects (liens HTML dans une page web ou dans un courriel, pièces jointes, ...) ;
- en complément, installer un logiciel antivirus et le mettre régulièrement à jour.

2 Quelques remarques pour les technologies sans-fil

2.1 Les pilotes de cartes sans-fil

Le CERTA a publié cette semaine l'avis CERTA-2007-AVI-223, concernant plusieurs vulnérabilités des pilotes Linux MadWifi. Certaines de ces vulnérabilités sont assez triviales à exploiter, car elles se limitent à envoyer un simple paquet « *dans les airs* ». Lorsque la trame est reçue par l'interface vulnérable, le passage des données au niveau des pilotes compromet la machine, avec les droits du pilote, i.e. ceux du système. Dans un autre cas, l'exploitation de la vulnérabilité a pour conséquence de rendre indisponible la connexion sans-fil jusqu'au redémarrage du service, voire du système.

Le CERTA a mentionné dans quelques bulletins d'actualité fin 2006 d'autres vulnérabilités impliquant des pilotes différents. Dans tous les cas, les remarques suivantes restent valables :

- les attaques sont simples à mettre en œuvre, et se limitent souvent à lancer une unique commande. Les détails intrinsèques de la vulnérabilité n'ont pas besoin d'être assimilés pour la réussite de l'exploitation ;
- les trames malveillantes sont difficilement détectables ;
- les paquets émis peuvent l'être à une distance importante, et il est possible de « tricher » sur les puissances d'émission ;
- les solutions de sécurité les plus courantes (WPA, IPsec par exemple) ne protègent pas de cette classe d'attaque, qui a lieu à un niveau protocolaire plus bas ;
- les mises à jour de pilotes sont souvent complexes, lorsqu'elles sont disponibles. Plusieurs systèmes utilisent de telles technologies (assistants personnels, disques durs externes, supports multimédia, etc.), mais qu'en est-il exactement de leurs mises à jour ?

Les motivations peuvent également être très variées :

– augmenter ses privilèges jusqu'au droit d'administration de la machine ;
– se servir du système vulnérable comme porte d'entrée à un réseau ;
– accéder aux données ;
– rendre le système inaccessible.

Quand plusieurs solutions reposent sur une telle technologie, il est important qu'elles n'en oublient pas les caractéristiques et les limites. Le sans-fil offre un accès difficilement maîtrisable à des interfaces. Cette problématique reste valable pour d'autres technologies comme le Bluetooth.

2.2 Les chevaux de Troie sur appareil mobile

Un éditeur d'antivirus a publié un article portant sur un nouveau code malveillant destiné au système d'exploitation Symbian. Généralement, ce système d'exploitation est utilisé sur certains téléphones portables.

Les codes malveillants affectant ce système d'exploitation tentent en général de se propager depuis l'équipement mobile au moyen de ses interfaces de communication, notamment via Bluetooth, ce qui limite la propagation de ce type de code malveillant. Ce dernier code malveillant est rendu disponible sur l'Internet par ses créateurs afin d'augmenter sa propagation (« Cheval de Troie »).

Il existe deux manières principales d'analyser un équipement mobile :

– installer une solution antivirale destinée au système d'exploitation, en l'occurrence Symbian ;
– synchroniser son équipement mobile avec son ordinateur personnel qui devra disposer d'une solution antivirale permettant l'analyse de tels appareils.

Il faut cependant considérer que la propagation de tels codes est souvent limitée, et que plusieurs variantes peuvent être méconnues des solutions antivirales basées sur des signatures. Par ailleurs, nettoyer le système mobile après l'infection n'est pas une opération toujours aisée.

Ces solutions sont relativement inefficaces. Actuellement, les meilleures pratiques recommandent de stocker peu d'informations sensibles sur un téléphone portable.

3 Les outils de travail à distance

Plusieurs articles sont apparus ces dernières semaines, vantant les mérites de nouvelles solutions offertes pour travailler à distance. Celles-ci fonctionnent sur le principe du « partage de contenu sur l'Internet ». Elles se présentent par exemple sous la forme suivante :

chaque utilisateur d'un même groupe partage un espace sur un site Internet. Ce site héberge leur informations personnelles, et notamment le suivi des modifications de projets (semblables aux solutions `cvs` - *Concurrent Versions System*) , leurs messages électroniques, leurs emplois du temps, etc. L'espace offert peut être important (plus de 50GB), et une conservation des interventions de chaque participant est activée. Pour plaire au plus grand nombre, les utilisateurs sont également accueillis par une page pouvant intégrer les divers logos et signes distinctifs du groupe ou de la société qui décide de l'utiliser. Sur leurs postes clients, ils peuvent également installer un logiciel, qui les prévient régulièrement des mises à jour.

Cependant, les articles oublient souvent de mentionner quelques problèmes de sécurité, qu'il est important de prendre en compte :

– l'ensemble des données, mais aussi des actions, du groupe de travail se trouvent hébergées chez une machine tiers, et éventuellement à l'étranger. Celle-ci n'apporte aucune garantie sur les moyens mis en œuvre pour protéger la confidentialité et l'intégrité des données.
– il peut se produire un déséquilibre, entre l'effort mis d'une part pour sécuriser le réseau administré, et la volonté explicite d'autre part d'exporter un maximum d'informations et de données par le biais de ce logiciel. Connaître les emplois du temps, les relations entre personnes, leurs contributions aux différents projets sont autant d'informations qui peuvent ensuite être exploitées à des fins malveillantes (courriers ciblés de *phishing*, tentatives d'ingénierie sociale, etc.) ;
– le logiciel implique (c'est aussi son argument de vente) une connexion permanente entre les machines de l'utilisateur et le site de partage. Ce dernier doit donc être en mesure de contacter les machines clientes quand une intervention du groupe est faite. Comment cela est-il géré au niveau des pare-feux locaux ? Très souvent, de tels logiciels ajoutent des exceptions, ouvrant un accès supplémentaire à la machine de l'utilisateur. L'authentification est-elle robuste ?

L'objectif n'est pas ici de dénigrer de telles solutions, mais d'insister sur le fait que des problèmes de sécurité peuvent apparaître avec leurs utilisations. L'utilisateur doit donc rester vigilant, malgré les éloges publiées dans certains magazines. Le CERTA recommande également aux administrateurs de sensibiliser les utilisateurs à ces problématiques et vérifier régulièrement dans leurs journaux que des connexions depuis leur réseau vers de tels sites de partage de travail n'apparaissent pas.

4 Publications de Microsoft : *MOICE*

Microsoft a publié cette semaine deux mises à jour qui sont de simples corrections de bogues et non des correctifs de sécurité.

La première concerne une correction dans le système d'analyse des mises à jour déjà présente sur le système qui pouvait dans certaines conditions cesser de répondre. La seconde concerne l'installation d'un outil permettant de convertir des documents Microsoft Office 2007 avec la suite Office 2003 de façon sécurisée. Ainsi, selon Microsoft, ce système nommé `MOICE` (Microsoft Office Isolated Conversion Environment) permet d'effectuer la conversion dans un contexte limité réduisant ainsi les possibilités qu'un éventuel document construit d'une façon particulière exécute du code arbitraire.

5 Rappels sur la vulnérabilité *ANI*

La vulnérabilité `ANI`, qui a fait l'objet de l'alerte CERTA-2007-ALE-008, est corrigée depuis le 03 avril 2007. Pour rappel, elle permet l'exécution de code arbitraire à distance au moyen d'un fichier de données animées spécialement construit. Ceci ne nécessite aucune interaction de la part de l'utilisateur car les navigateurs interprètent directement ces types de fichiers.

Du code d'exploitation circule massivement sur l'Internet, profitant de la vulnérabilité pour installer des chevaux de Troie (par exemple sous la forme de *keyloggers*). Même si le correctif est disponible, il faut savoir que tout nouvel ordinateur, notamment sous Windows Vista, est vulnérable lors de son premier démarrage. Il est également vulnérable aux autres failles dernièrement corrigées par Microsoft et donc publiques. Ceci est d'autant vrai que les antivirus pouvant être inclus avec la solution commerciale ne sont également pas à jour avant la première connexion.

Il faut donc faire très attention à effectuer les mises à jour du système d'exploitation dès la première utilisation de l'ordinateur et sa connexion à l'Internet. Parmi les actions dangereuses, il y a :

- la navigation vers des sites Web autres que celui de Microsoft Update ;
- le branchement de supports multimédia (clés USB, disques durs externes, lecteurs de musique, etc.) ;
- l'installation de logiciels annexe comme ceux de messagerie instantanée ;
- l'utilisation d'un client de messagerie pour recevoir et lire le courrier.

5.0.1 Liens utiles

- Alerte CERTA-2007-ALE-008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-008/CERTA-2007-ALE-008.html -
- Avis CERTA-2007-AVI-156 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-156/CERTA-2007-AVI-156.html

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 17 et le 24 mai 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 18 au 24 mai 2007, le CERTA a émis les avis suivants :

– CERTA-2007-AVI-221 : Vulnérabilité dans Norton Personal Firewall 2004
– CERTA-2007-AVI-222 : Vulnérabilités dans MySQL
– CERTA-2007-AVI-223 : Vulnérabilités dans les pilotes sans-fil MadWifi
– CERTA-2007-AVI-224 : Multiples vulnérabilités dans des produits Cisco
– CERTA-2007-AVI-225 : Vulnérabilité dans Vim
– CERTA-2007-AVI-226 : Vulnérabilité dans FreeType
– CERTA-2007-AVI-227 : Vulnérabilité dans Opera

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.

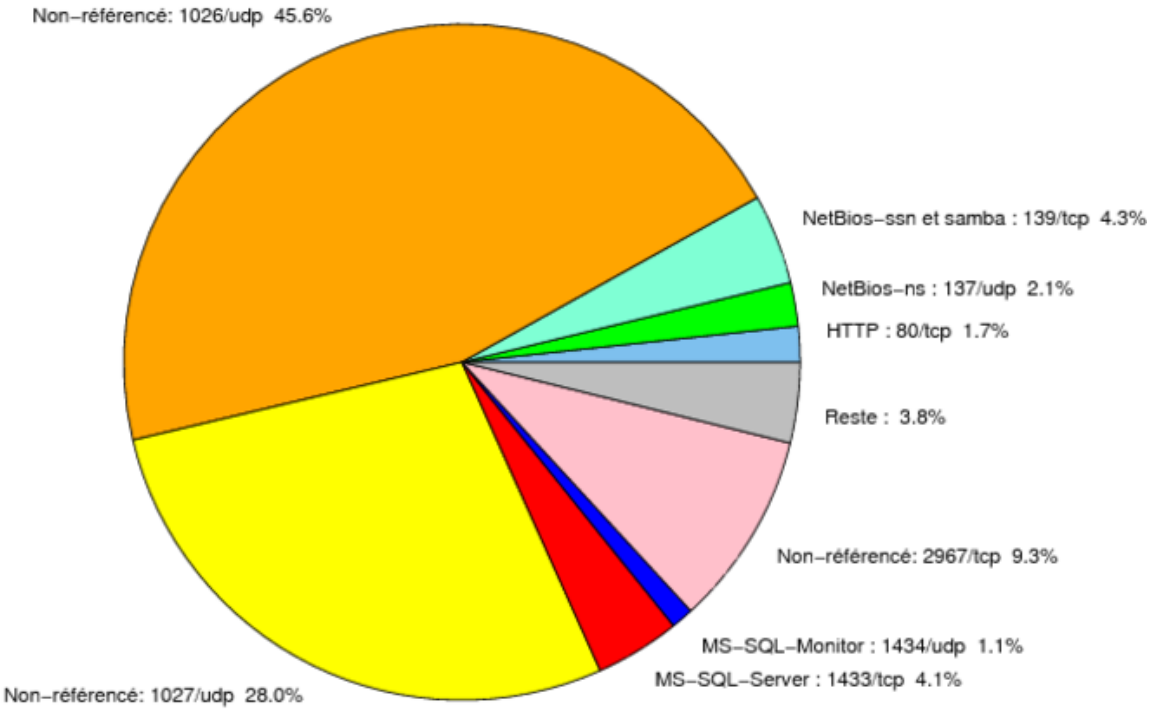

FIG. 1: Répartition relative des ports pour la semaine du 17.05.2007 au 24.05.2007

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	45.61
1027/udp	28
2967/tcp	9.31
139/tcp	4.3
1433/tcp	4.05
137/udp	2.08
80/tcp	1.7
1434/udp	1.07
22/tcp	0.7
4899/tcp	0.69
1080/tcp	0.48
3306/tcp	0.44
3128/tcp	0.4
23/tcp	0.25
25/tcp	0.21
15118/tcp	0.2
443/tcp	0.08
42/tcp	0.07
3127/tcp	0.06
3389/tcp	0.05
9898/tcp	0.04
5554/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

25 mai 2007 version initiale.