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 avril 2007
N° CERTA-2007-ACT-017

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-17

Gestion du document

Référence	CERTA-2007-ACT-017
Titre	Bulletin d'actualité 2007-17
Date de la première version	27 avril 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-017.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-017/

1 Les incidents traités cette semaine

1.1 Attaques sur *GuppY*

Le CERTA a traité cette semaine un cas de défigurations multiples sur un même serveur suite à l'exploitation d'une vulnérabilité de `GuppY` évoquée dans la référence CVE CVE-2007-0639.

Cette attaque permet d'exécuter du code arbitraire à distance. Dans ce cas précis, la vulnérabilité a été exploitée pour installer un `phpshell` (interpréteur de commandes écrit en `PHP`) sur le serveur. Ce `phpshell` a ensuite été utilisé pour réaliser de nombreuses actions malveillantes dont le vol du contenu d'une base de données, d'identifiants de connexion, ainsi que l'ajout de multiples pages de défiguration.

Les attaques sur `GuppY` par cette faille laissent des traces dans les journaux de type `access.log` de la forme suivante :

```
adresse_IP_attaquant - - [date] "POST /error.php?err=999 HTTP/1.0" 200
```

Un outil permettant l'exploitation de cette faille a été rendu public à la fin du mois de janvier 2007. Il est donc vivement recommandé de mettre `GuppY` à jour (version 4.5.18).

Documentation

Référence CVE CVE-2007-0639 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0639

1.2 Les noms de domaines, loués et non vendus

Un incident récent rappelle que l'enregistrement d'un nom de domaine auprès d'un bureau d'enregistrement n'est pas l'acquisition *ad vitam æternam* de ce nom, mais le droit d'utiliser ce nom pour une durée limitée. Ceci implique qu'un renouvellement de cette location du nom doit être entrepris. En l'absence de tacite reconduction dans le contrat initial et pour n'avoir pas surveillé l'échéance, un service a perdu le nom de domaine (en `.org`) de son site web. Le CERTA rappelle donc qu'il faut surveiller les données contenues dans les bases *whois*. En particulier :

- les coordonnées des responsables doivent être tenues à jour ;
- à l'approche de la date d'échéance, ces responsable doivent être alertés pour qu'ils entreprennent les démarche de prolongation de la détention du nom de domaine.

2 Vulnérabilité Quicktime

En début de semaine, il a été annoncé qu'une vulnérabilité non corrigée existait dans Safari, le navigateur de MacOS X. Or, celle-ci ne concernait pas directement le navigateur mais la mise en œuvre de l'application QuickTime par ce dernier. Plus précisément, c'est même le support de Java dans Quicktime qui est impacté. Ce qui était une vulnérabilité relative à un navigateur particulier sur un système d'exploitation donné est ainsi devenu une faille plus "générique" pouvant toucher d'autres systèmes d'exploitation comme Microsoft Windows disposant de l'application QuickTime et d'une machine virtuelle Java.

Le CERTA recommande donc de ne pas visualiser de video par l'intérmédiaire de Quicktime et d'utiliser un autre lecteur video dans l'attente d'un correctif.

3 Adobe Photoshop

Une vulnérabilité a été identifiée dans certaines versions de l'outil de manipulation de fichiers graphiques Adobe Photoshop, dont Creative Suite 2 et Creative Suite 3. Cette vulnérabilité concerne les fichiers aux formats `BMP`, `DIB` ou `RLE` (voire `PNG`), et provoquerait, à son exploitation, un débordement de tampon.

L'application, installée par défaut, n'ouvre pas les fichiers aux formats impliqués ; en d'autres termes, l'installation ne modifie pas l'association entre les extensions `.bmp`, `.dib`, `.rle` et `.png` et l'application qui doit les ouvrir par défaut. Ceci limite l'impact de cette vulnérabilité, mais des précautions doivent être prises, dans l'attente d'un correctif par l'éditeur :

- ne pas ouvrir des documents avec les extensions `.bmp`, `.dib` ou `.rle` avec Adobe Photoshop, ou vérifier que les fichiers proviennent d'une source de confiance ;
- suivre les publications du CERTA. Un avis sera publié quand un correctif officiel sera proposé par l'éditeur ;
- vérifier que Photoshop n'est pas le visualiseur par défaut de documents pour les extensions susmentionnées.

4 Les événements sous Microsoft Vista

4.1 Numérotation des événements

La numérotation des événements (Event IDs) sous Windows Vista a changé par rapport aux précédentes versions, mais garde des correspondances. En effet, pour retrouver l'identifiant d'un événement sur une version précédente de Windows il faut soustraire 4096 au numéro de l'événement sur Vista. Toutefois certains événements ont été fusionnés et d'autres sont nouveaux donc cette correspondance ne fonctionne pas toujours.

Voici à valeur d'exemple quelques correspondances, et quelques nouveaux identifiants :

- l'EventID `4624` sous Vista correspond à l'EventID `528` sous XP ;
- l'EventID `4634` sous Vista correspond à l'EventID `538` sous XP ;
- l'EventID `4624` sous Vista correspond aussi à l'EventID `540` sous XP.

Quelques sites offrent en ligne des commentaires associés à chaque identifiant d'événements. Parmi ceux-ci :

http://www.eventid.net/ Ce site ne couvre cependant pas, à la date de rédaction de ce document, les identifiants sous Microsoft Vista.

4.2 Visualisation des événements

Les événements sur Windows Vista sont stockés sous un format binaire, mais leur visualisation peut se faire en XML. De nombreuses améliorations ont été ajoutées au visionneur d'événements, notamment en ce qui concerne leur filtrage et regroupement. De même, de nouvelles catégories ont été ajoutées, et de nombreuses applications sous Windows ont leur propre groupe d'événements prédéfini.

4.3 Sauvegarde des événements

Sur toutes les versions de Windows, les événements contiennent des éléments dynamiques. Par exemple, la description d'un utilisateur se fait avec son SID et non son nom. De cette manière, si un compte change de nom après la journalisation d'un événement, le nom du nouveau compte apparaîtra. Ceci peut poser problème lors de la sauvegarde ou exportation d'événements particuliers, puisque les éléments dynamiques ne sont alors plus disponibles. Par exemple, un message d'une application ne sera plus compréhensible si l'événement est visionné sur un autre ordinateur ou si l'application en question est désinstallée (car le fichier de messages de l'application en question n'est alors plus disponible).

La sauvegarde d'événements sur Windows Vista peut se faire en trois formats différents : XML, EVTX et texte. Les deux premiers ne contiennent pas les éléments dynamiques mais permettent d'avoir les éléments utilisés comme pointeurs (les SID, par exemple). Le format texte, quant à lui, contient la valeur de ces pointeurs à un instant donné (l'exportation). Il est recommandé d'utiliser ces deux types de formats si l'on souhaite enregistrer des événements.

5 Réservation de noms de domaine

Le CERTA appelle l'attention des ministères à propos de la réservation de noms de domaine ambigus auprès de l'AFNIC. Ces réservations nous semblent ambigus dans la mesure où elles ont été faites par des particuliers et font référence à des noms ou services officiels. On peut citer à titre d'exemples les cas suivants déposés par des particuliers:

- impotsgouvr.fr
- sncftgv.fr
- administration24h24hgouv.fr
- socialgouv.fr
- wwwcg72.fr
- wwwservice-public.fr
- ww-anpe.fr
- wwwwanpe.fr
- wwwassedic.fr
- apostefinnance.fr
- carburantgouvernement.fr

Sans préjuger des motivations des personnes qui ont réservé ces noms de domaines, ce type de réservations (*typosquatting*) pourrait servir par exemple à la mise en place de sites de filoutage (*phishing*) ou permettre de diffuser de fausses informations liées à un service de l'Etat. l'AFNIC propose sur son site des informations liées au contournement de sa charte :

- Lignes directrices de lutte contre les violations manifestes de la charte :
  http://www.afnic.fr/doc/ref/juridique/violation-charte

6 Détournement des requêtes *DNS*

Une société proposant des solutions de sécurité a récemment identifié un Cheval de Troie, dont la particularité consiste à modifier la configuration `DNS` de la machine infectée.

DNS est un système qui permet de faire l'association entre un nom d'une machine et son adresse IP. Ainsi, quand un utilisateur tape dans son navigateur une adresse réticulaire (ou URL), une requête DNS est transmise à un serveur, qui indique à la machine de l'utilisateur l'adresse IP où se trouve le site demandé.

Dans le cas du code malveillant précédemment cité, la requête DNS du poste de l'utilisateur s'adresse à un serveur malveillant, qui peut rediriger l'utilisateur vers un autre site que celui demandé ; par exemple, un site de filoutage (*phishing*), un site publicitaire, ou un site contenant des pages malveillantes.

De manière plus incidieuse, le mauvais serveur DNS peut ne diriger l'utilisateur que ponctuellement, afin de ne pas éveiller les soupçons.

Recommandations du CERTA

Il existe plusieurs actions possibles pour détecter ce genre d'activité :

- vérifier régulièrement le ou les serveurs dans sa configuration réseau. Ils doivent correspondre à ceux légitimes fournis par le FAI ou l'administrateur. Sous Microsoft Windows, cela se fait de la manière suivante :
  - se rendre dans Démarrer -> Paramètres -> Connexions réseau
  - choisir une connexion, et cliquer avec le bouton droit sur Propriétés
  - sélectionner "Protocole Internet (TCP/IP)"
  - vérifier dans le cas où les serveurs ne sont pas imposés automatiquement (option DHCP), que les adresses renseignées sont correctes
- analyser si possible le trafic réseau pour détecter toute anomalie des échanges DNS. De simples observations des échanges entre adresses IP sources et destinations, associées aux ports 53 (TCP ou UDP) peuvent suffire dans le cas présent ;
- vérifier que la politique de filtrage prend en compte les flux DNS de manière stricte vers et depuis les serveurs DNS légitimes ;
- être vigilant et signaler tout comportement suspect à son responsable informatique ou son RSSI, quand le navigateur ne dirige pas vers la page demandée, ou affiche régulièrement des pages « *bizarres* ».

7 Dernières nouvelles concernant la vulnérabilité Windows DNS / RPC

Le CERTA a publié le 16 avril 2007 l'alerte CERTA-2007-ALE-010 concernant une vulnérabilité de Microsoft DNS Server. Cette dernière est actuellement exploitée par des codes malveillants.

Microsoft a annoncé par le biais de son bloc-notes (blog) que cette vulnérabilité, correspondant à leur avis de sécurité 935964, devrait être corrigée dans leur cycle mensuel de bulletins pour le mois de mai 2007.

http://blogs.technet.com/msrc/archive/2007/04/27/friday-update-on-microsoft-security-advisory-935964.aspx

8 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 avril 2007.

9 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

10 Rappel des avis émis

Durant la période du 20 au 27 avril 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-185 : Multiples vulnérabilités dans Apple MacOS X
- CERTA-2007-AVI-186 : Vulnérabilités dans des produits Check Point ZoneAlarm
- CERTA-2007-AVI-187 : Vulnérabilité de PostgreSQL
- CERTA-2007-AVI-188 : Vulnérabilités dans BrightStor ARCserve Backup Media Server
- CERTA-2007-AVI-189 : Vulnérabilité dans Courier-IMAP
- CERTA-2007-AVI-190 : Vulnérabilité du Netflow Collection Engine de Cisco
- CERTA-2007-AVI-191 : Vulnérabilité CISCO
- CERTA-2007-AVI-192 : Vulnérabilité dans Computer Associates CleverPath Portal
- CERTA-2007-AVI-193 : Vulnérabilité dans HP StorageWorks

Pendant la même période, l'avis suivant a été mis à jour :

- CERTA-2007-AVI-177-001 : Multiples vulnérabilités dans XOrg et XFree86
  (ajout de la référence Sun.)

11 Actions suggérées

11.1 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.

11.2 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.

11.3 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.

11.4 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.

11.5 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.

11.6 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.

11.7 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

12 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.

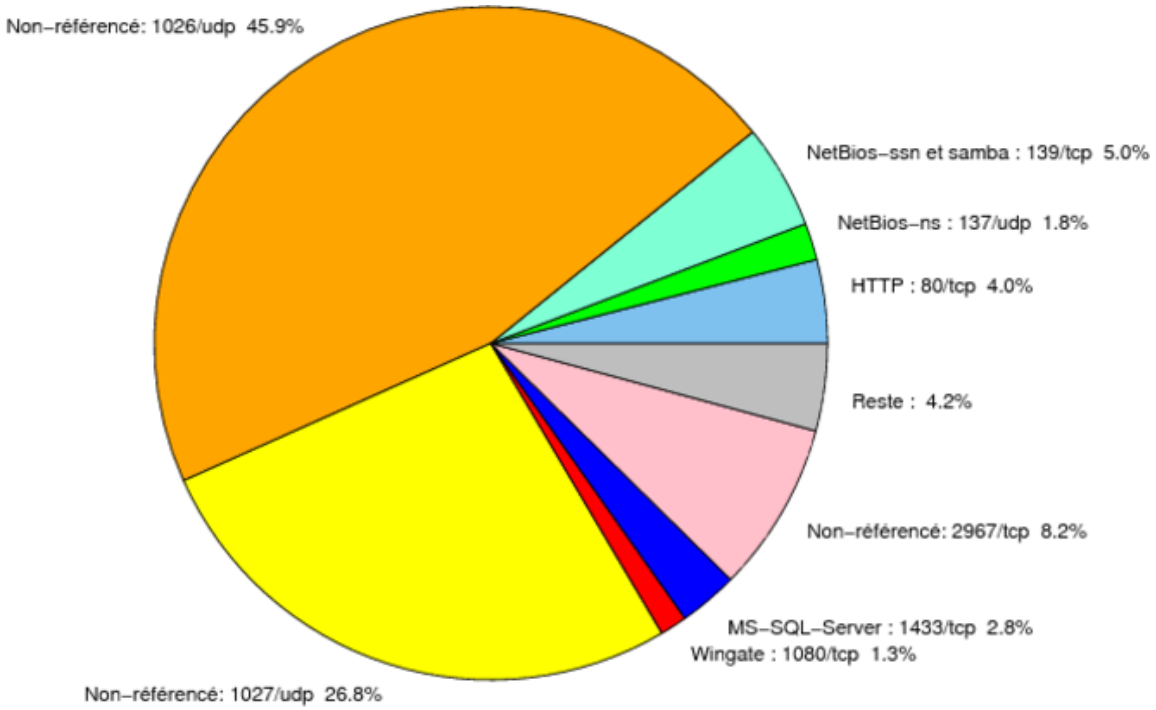

FIG. 1: Répartition relative des ports pour la semaine du 19.04.2007 au 26.04.2007

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	45.87
1027/udp	26.79
2967/tcp	8.18
139/tcp	5.02
80/tcp	4
1433/tcp	2.83
137/udp	1.77
1080/tcp	1.3
1434/udp	0.91
4899/tcp	0.86
22/tcp	0.53
3128/tcp	0.42
23/tcp	0.34
25/tcp	0.32
443/tcp	0.24
21/tcp	0.15
2100/tcp	0.08
143/tcp	0.07
3389/tcp	0.04
5554/tcp	0.03
9898/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

27 avril 2007 version initiale.