

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-52

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2006-ACT-052>

Gestion du document

Référence	CERTA-2006-ACT-052
Titre	Bulletin d'actualité 2006-52
Date de la première version	29 décembre 2006
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-2006-ACT-052.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-2006-ACT-052/>

1 Activité en cours

1.1 Sites orphelins

Un incident traité par le CERTA a mis en lumière la cessation du suivi du site web d'un service quand le concepteur du site a quitté ce service. Faute de repreneur, la configuration n'a pas évolué en fonction des utilisations et de la menace. Un intrus a pu profiter du faible niveau de sécurité du site.

Le suivi d'un site web peut pâtir, non seulement d'un mouvement de personnel, mais aussi d'une réorganisation.

Recommandations

Le CERTA recommande :

- de maintenir la liste des responsables des sites, techniques (exploitation, administration, développement) et éditoriaux ;
- d'assurer la redondance des personnes et les relais ;
- de documenter et de maintenir les développements et les configurations ;
- de réviser périodiquement la configuration pour l'adapter aux utilisations et à la menace.

1.2 Défigurations

Le CERTA a traité cette semaine un cas de défiguration de site web suite à l'exploitation de droits permissifs sur la commande PUT. Les attaques de ce type ainsi que les moyens de se protéger ont été évoqués dans le bulletin d'actualité CERTA-2006-ACT-048. Ces attaques sont plus fréquentes qu'il n'y paraît puisque leurs auteurs ne modifient pas systématiquement la page d'accueil, mais se contentent parfois d'ajouter une page web (par exemple, ajout de la page `hacked.html` à la racine).

Il est conseillé de vérifier dans l'arborescence de vos sites web qu'aucun fichier n'a été ajouté et de lire régulièrement vos journaux de connexions.

1.3 Arnaques par courriel ou autre système de messagerie

Le CERTA constate de plus en plus d'arnaques à la fausse mise à jour. Concrètement, il s'agit d'envoyer à une victime un message en utilisant la messagerie électronique traditionnelle, les messageries instantanées ou des services comme `Windows Messenger Service`. Le contenu de ce message, souvent alarmiste, incite la victime à se rendre sur un site web pour y télécharger une mise à jour. Ces « mises à jour » sont généralement des codes malveillants et ne sont pas toujours en téléchargement libre. En effet, dans certains cas, il est nécessaire de remplir un formulaire d'achat et de communiquer les coordonnées bancaires. Des sommes d'argent sont ensuite débitées des cartes sans qu'aucun logiciel n'ait réellement été téléchargé.

Le CERTA recommande d'être particulièrement prudent avec ces messages. Les conseils donnés dans le bulletin d'actualité CERTA-2006-ACT-049 concernant les courriels sont valables également pour la messagerie instantanée et pour les fenêtres `pop up` de `Windows Messenger Service`. Votre responsable sécurité vous conseillera utilement.

Il est également recommandé de filtrer les ports 1026/udp et 1027/udp et de désactiver le service `Windows Messenger Service`, tel qu'indiqué dans l'article suivant de Microsoft (pour Windows XP) :

<http://www.microsoft.com/windowsxp/using/security/learnmore/stopspam.mspx>

2 Ver de décembre 2006 visant Symantec

2.1 Présentation des faits

Le CERTA a publié le 28 mai 2006 l'avis CERTA-2006-AVI-221, concernant une vulnérabilité des produits Symantec AntiVirus et Client Security. Il s'agit de la vulnérabilité SYM06-010 de référence CVE-2006-2630. Cette vulnérabilité, de type « débordement de pile » (ou `stack overflow`), est exploitable à distance, par le biais du port TCP 2967. En effet, les machines utilisant ces produits se mettent en écoute sur ce port, pour communiquer avec la console de gestion distante.

Pour rappel, les versions vulnérables sont :

- Symantec Client Security pour Windows, version 3.1 ;
- Symantec Client Security pour Windows, version 3.0 ;
- Symantec Antivirus Corporate Edition pour Windows, version 10.1 ;
- Symantec Antivirus Corporate Edition pour Windows, version 10.0.

Le CERTA a noté, depuis le 12 décembre 2006, une forte augmentation du trafic à destination de ce port TCP. Ceci est lié à la propagation virulente d'un ver.

2.2 Détails concernant le ver

Un ver, surnommé `Yellow Worm` (ou `W32.Sagevo` par Symantec) exploite actuellement la vulnérabilité des produits Symantec décrite dans le paragraphe précédent. Ces produits sont largement répandus, et les mises à jour n'ont pas été nécessairement appliquées sur toutes les machines depuis mai 2006.

Le ver se présente comme suit :

- il modifie un ensemble de fichiers sur le système infecté, notamment la bibliothèque `wuauclt.dll` ;
- il injecte du code via le processus `svchost.exe` ;
- il modifie les deux clés de registre suivantes :

```
HKLM\SYSTEM\CurrentControlSet\Services\wuauserv (attribut << Start >>)
HKLM\SYSTEM\CurrentControlSet\Services\wuauserv\Parameters (attribut << ServiceDll
```

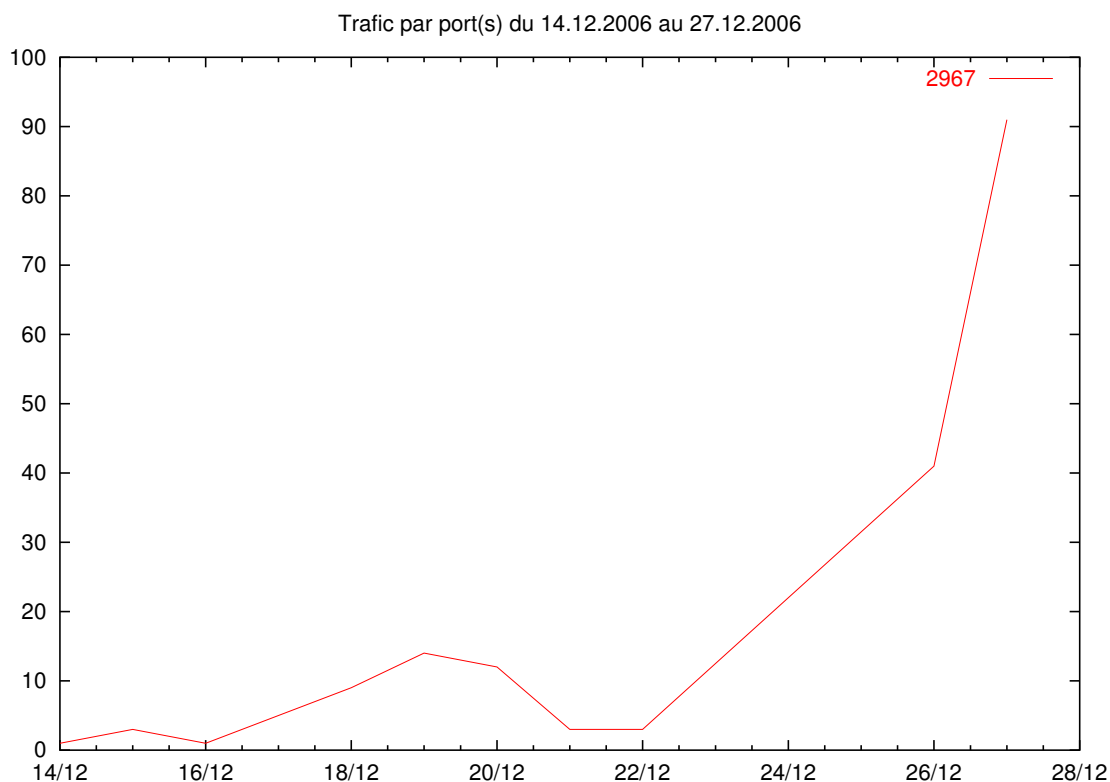


FIG. 1: Evolution du trafic observé à destination du port TCP 2967 du 12.12.2006 au 27.12.2006

- il fait participer la machine compromise à un réseau de machines zombies, ou *botnet* ;
- il installe différents programmes, dont un pour capturer les frappes au clavier (*keylogger*) ;
- il balaie la plage d'adresses locales de la machine infectée à la recherche de nouvelles victimes suivant l'algorithme suivant :
 - si l'adresse est de la forme 192.168.X.X, il balaie des adresses qui suivent 192.168.0.1 ;
 - si l'adresse est de la forme 10.X.X.X, il balaie des adresses qui suivent 10.0.0.1 ;
 - sinon, si l'adresse est de la forme A.B.C.D, il balaie des adresses qui suivent A.B.C'.0, avec $C' = C - 10$ ou 0 si $C - 10 < 0$.
- Dans tous les cas, la tentative de connexion se fait à destination du port TCP 2967.

Recommandations

Le CERTA recommande donc de surveiller et de filtrer correctement (entrée et sortie de réseau) les paquets à destination du port TCP 2967. Il est également vivement conseillé de vérifier que les produits Symantec utilisés sont à jour.

Liens utiles

- Avis du CERTA CERTA-2006-AVI-221 du 28 mai 2006 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-221/>
- Analyse du ver Yellow Worm par eEye :
<http://research.eeye.com/html/alerts/AL20061215.html>
- Vulnérabilité Symantec SYM06-010 du 25 mai 2006 :
<http://securityresponse.symantec.com/avcenter/security/Content/2006.05.25.html>

3 Nabaztag et autres objets autonomes communicants

La tentation est grande, après Noël, d'amener au bureau son Nabaztag, si celui-ci a été livré au pied du sapin. En effet, cet objet communicant, qui se présente sous la forme d'un lapin, est une machine autonome : elle se connecte sur divers sites, pour récupérer les courriels et les lire à haute voix au propriétaire, ou bien pour lire des flux de données RSS (journaux d'actualité, activités boursières, avis du CERTA, etc.). Les derniers modèles sont équipés de microphone, et les fonctionnalités sont multiples.

Cependant, cette machine, pour accéder à Internet, doit passer par une connexion Wi-Fi ouverte ou employant du WEP (ancienne version du Nabaztag) ou du WPA (pour la plus récente).

Il faut donc bien comprendre qu'il s'agit d'offrir un accès au réseau à une machine avec un système d'exploitation et des services. Les activités de cette machine ne sont pas maîtrisées : les mises à jour n'existent pas ou ne sont pas annoncées, et les échanges d'informations ne sont pas documentés. En d'autres termes, connecter un tel objet revient à autoriser une machine non contrôlée à communiquer avec le réseau externe et éventuellement interne, avec tous les risques que cela comporte.

Le Nabaztag n'est cependant pas le seul appareil offrant aux utilisateurs la possibilité de se connecter, de manière autonome, à l'Internet. Il faut donc, de manière générale :

- vérifier que la politique de sécurité concernant les accès sans-fil est respectée ;
- auditer son réseau, pour déterminer les connexions sans-fil existantes, légitimes ou pas ;
- sensibiliser les utilisateurs aux risques associés à l'utilisation de tels objets dans un réseau professionnel.

4 Cartes de vœux

Plusieurs sites signalent un envoi massif de courriels, ne contenant aucun contenu, et ayant pour objet "Happy new year!". Un fichier malveillant est joint au message : `postcard.exe`. Certains antivirus le détectent déjà, mais d'autres risquent d'apparaître.

L'envoi de carte postale électronique, et notamment de vœux, est un vecteur de propagation de virus, chevaux de Troie ou autres contenus malveillants. Il est donc nécessaire, à l'approche de la nouvelle année, de renforcer la vigilance et de sensibiliser les utilisateurs. La note CERTA-2000-REC-002 rappelle quelques précautions à prendre lors de la réception de tels messages.

5 Ports observés

Le tableau 3 et la figure 2 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 21 et le 28 décembre 2006.

6 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.fr/site/CERTA-2000-INF-006/>
- Note d'information du CERTA CERTA-2006-INF-008 sur les outils d'indexation et de recherche : <http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-008/>

7 Rappel des avis émis

Durant la période du 22 au 28 décembre 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-570 : Multiples vulnérabilités dans le JRE Java de Sun
- CERTA-2006-AVI-571 : Multiples vulnérabilités sous Novell NetMail

8 Actions suggérées

8.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel réglementaire, 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.

8.2 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.

8.3 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.

8.4 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.

8.5 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.

8.6 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 inexplicables 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.

8.7 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>

9 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.

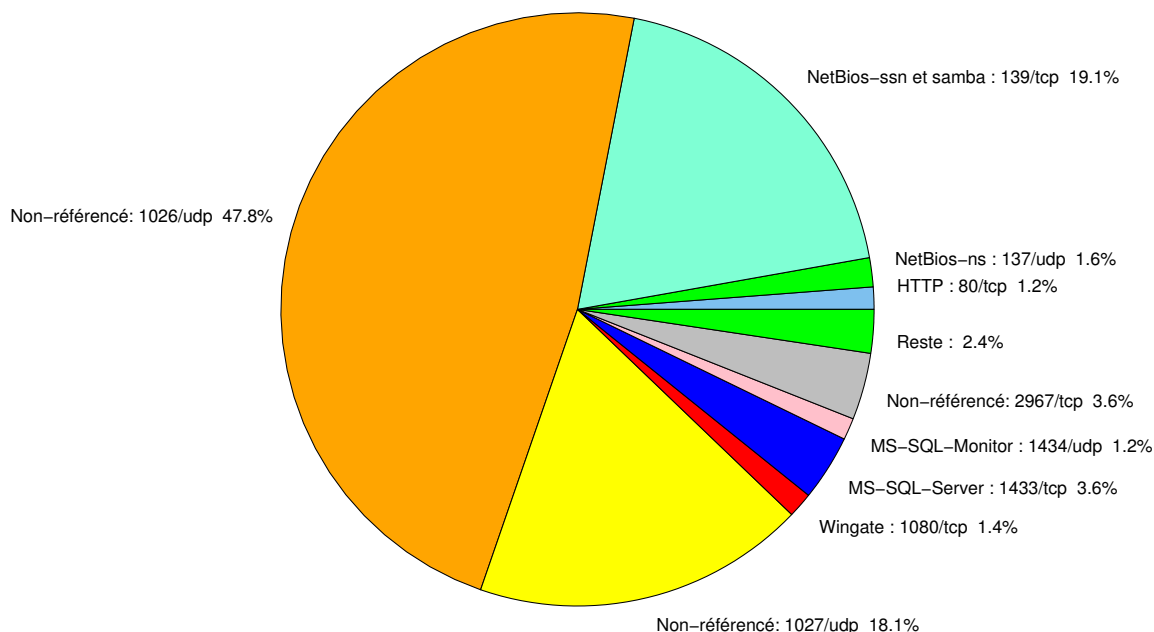


FIG. 2: Répartition relative des ports pour la semaine du 21.12.2006 au 28.12.2006

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	-	CERTA-2003-AVI-132 CERTA-2004-AVI-064 CERTA-2004-AVI-066 CERTA-2006-AVI-040
22	TCP	SSH	-	CERTA-2003-AVI-152 CERTA-2006-AVI-100
23	TCP	Telnet	-	CERTA-2003-AVI-209 CERTA-2003-AVI-131
25	TCP	SMTP	-	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	-	CERTA-2004-AVI-384
80	TCP	HTTP	-	CERTA-2004-AVI-195 CERTA-2004-AVI-239 CERTA-2006-AVI-055 CERTA-2006-AVI-069 CERTA-2006-AVI-156 CERTA-2006-AVI-315
106	TCP	MailSite Email Server	-	-
111	TCP	Sunrpc-portmapper	-	CERTA-2003-AVI-052
119	TCP	NNTP	-	CERTA-2004-AVI-340
135	TCP	Microsoft RPC	-	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	-	CERTA-2004-AVI-031
139	TCP	NetBios-ssn et samba	-	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-213 CERTA-2005-AVI-302 CERTA-2005-AVI-398 CERTA-2006-AVI-283 CERTA-2006-AVI-338
143	TCP	IMAP	-	CERTA-2005-AVI-185
389	TCP	LDAP	-	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126
443	TCP	HTTPS	-	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343
445	TCP	Microsoft-smb	-	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-302 CERTA-2006-AVI-283 CERTA-2006-AVI-338
1023	TCP	-	Serveur ftp de Sasser.E	-
1080	TCP	Wingate	MyDoom.F	CERTA-2006-AVI-232
1433	TCP	MS-SQL-Server	-	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	-	CERTA-2002-AVI-157
2100	TCP	Oracle XDB FTP	-	CERTA-2005-ALE-002

2381	TCP	–	HP System Management	CERTA-2006-AVI-248
2745	TCP	–	Bagle	–
2967	TCP	–	Symantec Antivirus	CERTA-2006-AVI-221
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	CERTA-2002-AVI-213
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6112	TCP	Dtspcd	–	CERTA-2002-ALE-001
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	CERTA-2005-AVI-229 CERTA-2005-AVI-313
10080	TCP	Amanda	MyDoom	–
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	–	CERTA-2005-AVI-310

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

port	pourcentage
1026/udp	47.77
139/tcp	19.14
1027/udp	18.13
2967/tcp	3.63
1433/tcp	3.58
137/udp	1.58
1080/tcp	1.37
80/tcp	1.21
1434/udp	1.18
4899/tcp	0.76
22/tcp	0.52
3128/tcp	0.36
25/tcp	0.15
15118/tcp	0.1
3127/tcp	0.07
143/tcp	0.05
11768/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	8
3	Paquets rejetés	9

Gestion détaillée du document

29 décembre 2006 version initiale.