Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 mai 2007
N° CERTA-2007-ACT-019

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-19

Gestion du document

Référence	CERTA-2007-ACT-019
Titre	Bulletin d'actualité 2007-19
Date de la première version	11 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-019.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-019/

1 Les incidents traités cette semaine

1.1 La propagation de codes malveillants par support USB

Le CERTA a traité cette semaine la compromission d'une machine. Il apparaît que l'infection ait eu lieu suite à l'insertion d'une clé USB contenant un code malveillant. La clé contient un fichier particulier, nommé `autorun.inf`, qui exécute une application au moment de l'insertion. L'application installe un Cheval de Troie, et attend également que d'autres supports de données amovibles USB soient branchés pour y copier les mêmes fichiers dont le `autorun.inf`.

Le CERTA souhaite insister sur trois points particuliers :

1. tout support de données amovible peut servir pour la propagation *a priori*. Cela inclut les lecteurs multimedia, comme les `iPod`, les disques durs externes, les appareils de photo numériques, ou bien même les assistants digitaux personnels (`PDA`) branchés en USB ;
2. l'infection se fait automatiquement, à cause de la propriété `autorun` du système d'exploitation Windows. Des clés USB particulières `U3` utilisent la même approche. Il est donc important de désactiver par défaut cette fonctionnalité ;

3. il ne faut pas sous-estimer les risques d'infection par USB. Plusieurs codes malveillants ont récemment vus le jour et ont été signalés par des éditeurs d'antivirus.

Le CERTA rappelle à cette occasion que la note d'information CERTA-2006-INF-006 a été publiée à ce sujet. Elle évoque la problématique de ces supports, ainsi que quelques bonnes pratiques à appliquer.

2 Activités sur les ports TCP 3628 ou 5168

Le CERTA a publié cette semaine l'avis CERTA-2007-AVI-210 concernant le produit ServerProtect de *Trend Micro*. Parmi les vulnérabilités identifiées, certaines concernent les démons `SpntSvc.exe` et `EarthAgent.exe`, en écoute sur les ports TCP 5168 et 3628 respectivement par défaut.

Cet outil, par ailleurs, permet de centraliser l'administration de l'antivirus distribué sur les machines. Il doit donc être suffisamment sécurisé, à la hauteur de son rôle dans les tâches antivirales effectuées sur les systèmes du réseau.

Quelques personnes ont signalé sur des forums de sites Web un accroissement de l'activité sur les ports susmentionnés ces derniers jours. Ceux-ci ne sont pas communément sollicités dans le bruit de fond global de l'Internet. Cette augmentation a également été constatée par le CERTA, même si le nombre absolu de tentatives de balayage reste encore faible. Il y a donc une forte probabilité que de premières machines (zombies ?) cherchent à exploiter les récentes vulnérabilités.

Recommandations du CERTA

- il est conseillé aux utilisateurs de cette application de vérifier la politique de filtrage mise en place et la bonne application des mises à jour ;
- il est conseillé de filtrer, sauf exception, ces ports en connexions sortantes, afin d'éviter qu'une machine interne compromise génère un tel trafic. De manière générale, il est primordial d'avoir une politique de connexion sortante restrictive.
- il est conseillé de consulter les journaux de rejets des pare-feux, afin de vérifier que ces ports n'apparaissent pas. Toute activité anormale impliquant ces ports peut être signalée au CERTA.

3 Lancement de la plate-forme *Signal Spam*

Depuis jeudi 10 mai 2007, la plate-forme `Signal Spam` est ouverte au publique. Cette association à pour vocation de réduire le nombre de courriels indésirés (*spam*) qui circulent sur l'Internet. Après une inscription rapide sur le site, chaque internaute a la possibilité de déclarer un courrier non-sollicité simplement, par un formulaire sur le site Web ou en cliquant sur le bouton de l'extension (`plugin`) de son gestionnaire de courrier. Actuellement, les logiciels de messagerie pris en compte sont `Microsoft Outlook 2003` et `2007` et `Mozilla Thunderbird`.

Cette extension est disponible par téléchargement après inscription sur le site. Une version `Webmail` de cette extension est envisagée.

Références

- site officiel du projet `Signal Spam` :
  http://www.signal-spam.fr
- note d'information du CERTA sur la limitation de l'impact du SPAM :
  http://www.certa.ssi.gouv.fr/CERTA-2005-INF-004

4 Vol de comptes de jeu en ligne

Depuis la fin des années 90, les jeux en ligne ne cessent de se développer. Certains d'entre eux sont regroupés dans une catégorie appelée *MMOG* (*Massively Multiplayer Online Game*). Il est généralement nécessaire de disposer d'un compte pour pouvoir jouer à un *MMOG*, et de payer un abonnement. Le paiement de cet abonnement se fait typiquement par carte bancaire, ce qui implique de transmettre des coordonnées bancaires. Les coordonnées personnelles telles que le nom, le prénom, la date de naissance, l'adresse et le numéro de téléphone sont parfois demandées.

Les données personnelles et bancaires ainsi transmises sont souvent conservées en ligne par l'éditeur du jeu. Ainsi, en cas de réabonnement, l'utilisateur n'a pas à ressaisir toutes ces informations. La saisie et la modification de ces informations se fait généralement par l'interface de gestion du compte (éventuellement, il peut s'agir d'un site web). L'éditeur prétend que son site est sûr en s'appuyant sur l'utilisation du protocole `https` et d'un mot de passe pour garantir la confidentialité des données pendant le transport entre le navigateur et le site du jeu. En d'autres termes, la confidentialité des données personnelles et bancaires reposent sur les seuls identifiants et mots de passe utilisés pour accéder au jeu en ligne.

Comme bien souvent dans les transactions en ligne, le point le plus fragile est le poste de l'internaute qui utilise ce jeu. Prendre le contrôle d'un poste d'un joueur qui se connecte à un tel site permet d'avoir accès avec les droits du joueur à ses coordonnées bancaires et personnelles.

Ainsi, un ou plusieurs codes malveillants exploitent actuellement la vulnérabilité des ordinateurs des joueurs du jeu en ligne très populaire *World of Warcraft* afin de capturer les données bancaires accessibles sur le compte du joueur sur le jeu en ligne.

Le CERTA attire l'attention sur le point faible de tout service en ligne : l'ordinateur de l'utilisateur. Afin de limiter les risques lors de la consommation en ligne, il est important de limiter l'exposition de ses données personnelles : par exemple en utilisant des pseudonymes quand c'est possible ou en payant à la livraison, dans une boutique ou en ligne mais avec des cartes prépayées.

5 Mises à jour et fins de support

Le CERTA a mis à jour aujourd'hui sa note d'information concernant les logiciels obsolètes : CERTA-2005-INF-003. Dans ce rafraîchissement, on notera en particulier :

- la fin du support de Windows 2003 RTM (Service Pack 0) ;
- la sortie de la version 4.0 (Etch) de Debian ;
- la sortie de la version 4.1 de OpenBSD.

Le CERTA réinvite à cette occasion ses correspondants à lui fournir des listes des logiciels utilisés, afin d'affiner sa veille technologique.

6 Particularités du Cheval de Troie *Trojan.Kardphisher*

Récemment, un nouveau cheval de Troie, nommé par certains éditeurs d'antivirus `Trojan.Kardphisher`, a été découvert. Celui-ci n'utilise aucune nouveauté particulière mais son fonctionnement est intéressant.

Après installation et redémarrage du système d'exploitation, le cheval de Troie présente une fausse fenêtre d'activation Windows très ressemblante à celle de Microsoft sur Windows XP. Il est expliqué que la clé du produit a été utilisée plusieurs fois et qu'il est donc nécessaire, pour vérification, que l'utilisateur entre ses informations bancaires (numéro, code PIN, date d'expiration...). Il est spécifié, pour rassurer la victime, que son compte ne sera pas débité. L'utilisateur ne peut pas interagir avec Windows tant que la fenêtre est ouverte.

Si l'utilisateur refuse d'entrer ses informations l'ordinateur s'éteint. En revanche, s'il accepte de les fournir il peut continuer à travailler sur Windows. Les informations entrées sont envoyées à l'attaquant.

Pour le moment, les systèmes d'exploitation Microsoft Windows 95, 98, NT, 2000, XP et Server 2003 sont concernés. Il est cependant possible que certaines variantes affectent Windows Vista.

Des instructions de suppression de ce code malveillant se trouvent sur le site suivant :
http://www.symantec.com/security_response/writeup.jsp?docid=2007-042705-0108-99

7 Courriers liés à Internet Explorer 7.0 Bêta

Une nouvelle campagne de courriels non sollicités contenant des liens vers un code malveillant prend de l'ampleur. Ces messages ont pour expéditeur `admin@microsoft.com` et pour sujet : `Internet Explorer 7.0 Beta`. Le code malveillant serait hébergé sur de nombreux sites.

Le texte contient une URL de la forme `http://XXXXX/update.exe`. Le fichier exécutable est bien évidemment un code malveillant, qui cherche ensuite à se connecter vers un serveur distant. L'originalité de ce courriel est qu'il a réussi à contourner plusieurs filtres antispam mis en œuvre. La raison est la suivante : le corps du texte est inséré dans des balises HTML `<style></style>`. Le contenu de ses balises ne sera pas

affiché par la majorité des clients de messagerie. Ce texte est visible en affichant le code source du courriel. Il est de la forme :

```
From :
X-Account-Key :
(...)
Subject : Internet Explorer 7.0 Beta
From : admin@microsoft.com
Importance : High
Content-Type : text/html
Date : ...

<_style>
        texte - liste de mots sans réelle importance
</_style>
<_a target="_blank" href="http://XXXXXX/update.exe" ><img src="http://YYY/ie.jpg">
<_style>
        texte - liste de mots sans réelle importance
</_style>
```

Le CERTA rappelle à cette occasion que le courrier électronique n'est pas, à la date de rédaction de ce document, le moyen de communication normal de Microsoft pour effectuer des mises à jour.

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 03 et le 10 mai 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 04 au 10 mai 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-200 : Vulnérabilités dans Mambo
- CERTA-2007-AVI-201 : Multiples vulnérabilités dans PHP
- CERTA-2007-AVI-202 : Vulnérabilités dans Novell SecureLogin
- CERTA-2007-AVI-203 : Plusieurs vulnérabilités dans Microsoft Excel
- CERTA-2007-AVI-204 : Plusieurs vulnérabilités dans Microsoft Word
- CERTA-2007-AVI-205 : Vulnérabilité dans Microsoft Office
- CERTA-2007-AVI-206 : Multiples vulnérabilités dans Microsoft Exchange
- CERTA-2007-AVI-207 : Multiples vulnérabilités d'Internet Explorer
- CERTA-2007-AVI-208 : Vulnérabilité dans CAPICOM
- CERTA-2007-AVI-209 : Vulnérabilité de l'interface Microsoft DNS RPC
- CERTA-2007-AVI-210 : Vulnérabilités dans Trend Micro ServerProtect
- CERTA-2007-AVI-211 : Vulnérabilité dans HP Tru64
- CERTA-2007-AVI-212 : Vulnérabilité de plusieurs produits de sécurité
- CERTA-2007-AVI-213 : Vulnérabilités dans SquirrelMail
- CERTA-2007-AVI-214 : Multiples vulnérabilités dans Novell NetMail
- CERTA-2007-AVI-215 : Vulnérabilité de Websphere
- CERTA-2007-AVI-216 : Vulnérabilité dans les produits Cisco

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

- CERTA-2007-ALE-006-001 : Vulnérabilité dans le logiciel Microsoft Word
  (ajout des références aux bulletins de sécurité MS07-024 et CERTA-2007-AVI-204)
- CERTA-2007-ALE-010-002 : Vulnérabilité de Microsoft DNS Server
  (ajout des références aux bulletins MS07-029 et CERTA-2007-AVI-209)
- CERTA-2007-AVI-129-001 : Vulnérabilité dans CUPS
  (ajout des références Gentoo, Mandriva, Redhat et Suse)
- CERTA-2007-AVI-138-001 : Vulnérabilité dans file (ajout des références Debian, Mandriva, SuSE, Gentoo, Avaya, Redhat, Ubuntu)
- CERTA-2007-AVI-177-001 : Multiples vulnérabilités dans XOrg et XFree86
  (ajout des références OpenBSD, SuSE, et Gentoo)

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.

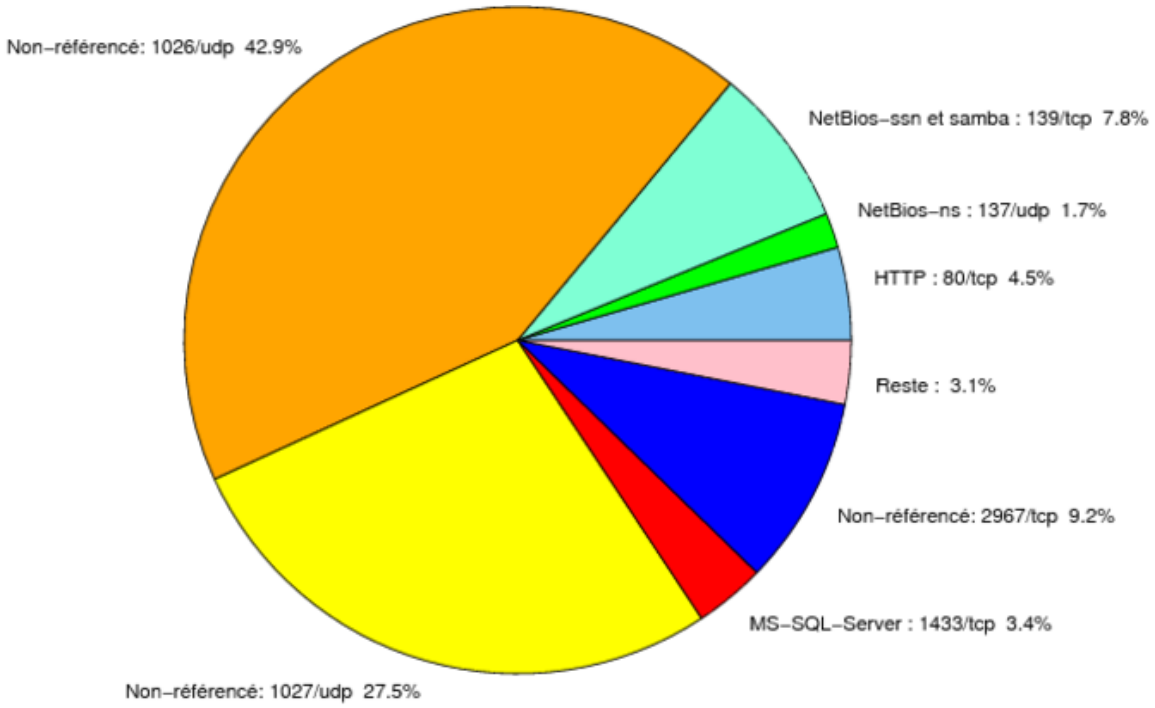

FIG. 1: Répartition relative des ports pour la semaine du 03.04.2007 au 10.05.2007

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	42.86
1027/udp	27.45
2967/tcp	9.17
139/tcp	7.79
80/tcp	4.49
1433/tcp	3.42
137/udp	1.69
1434/udp	0.71
4899/tcp	0.5
22/tcp	0.43
1080/tcp	0.28
25/tcp	0.27
21/tcp	0.19
3128/tcp	0.18
443/tcp	0.14
3306/tcp	0.09
15118/tcp	0.07
2100/tcp	0.05
143/tcp	0.03
111/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

11 mai 2007 version initiale.