



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 janvier 2009
N° CERTA-2009-ACT-003

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-03

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-2009-ACT-003>

Gestion du document

Référence	CERTA-2009-ACT-003
Titre	Bulletin d'actualité 2009-03
Date de la première version	16 janvier 2009
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-2009-ACT-003.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-2009-ACT-003/>

1 Une mauvaise gestion du DNS

1.0.1 Présentation

Cette semaine le CERTA a traité un incident lié à une entrée DNS obsolète. L'adresse IP du site Internet d'une administration française a changé sans que le responsable du service DNS ne prenne en compte cette modification. De ce fait, les requêtes à destination de ce site n'affichaient plus les pages demandées. Pire encore, l'adresse IP d'origine ayant été réattribuée le site Web a donné l'apparence de présenter un tout autre contenu provoquant un problème d'image pour cette administration.

Le CERTA recommande de contrôler régulièrement les enregistrements DNS afin de supprimer les entrées inutiles et appliquer les modifications. Les changements d'adressage doivent être planifiés et contrôlés avant de libérer les anciennes adresses.

1.1 Documentation

– Note d'information CERTA-2008-INF-002, « Sur le bon usage du DNS » :

<http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-002/>

- Note d'information CERTA-2007-INF-001, « Conseils pour la gestion des noms de domaine » : <http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/>

2 Le retour de la tempête

2.1 Contexte

Le CERTA a régulièrement alerté le public sur les dangers que représente la banalisation des cartes de vœux électroniques. L'actualité indique qu'un nouveau code malveillant se propage via une *e-card* malveillante.

2.2 Description

Ce code, nommé par certains *Waledac*, ressemble dans sa conception au désormais très célèbre *StormWorm*, apparu sur l'Internet au cours de l'année dernière. Sa méthode de propagation repose sur l'envoi d'une carte de vœux électronique rédigée en anglais et contenant un lien. Le lien redirige l'internaute naïf vers un site d'aspect anodin (cf. image ??) contenant deux codes malveillants:

- un javascript ;
- un code exécutable (*Waledac*) proposé au téléchargement dès lors que l'internaute clique sur la page.



FIG. 1: Capture d'écran de la carte de vœux électronique

Une fois un poste infecté, *Waledac* récupère par différents biais un maximum d'adresses méls en local, et renvoie la même *e-card* à tous ces contacts. En outre, le poste infecté fait alors partie d'un réseau de machines compromises (*botnet*) utilisables pour tous types d'actions (DDoS, téléchargement et installation d'exécutables, etc.).

2.3 Contre-mesures

Fort heureusement, même si le code en lui-même n'est pas facile à analyser, il n'en reste pas moins aisé de le détecter. En effet, le nom de l'exécutable des souches actuelles sont toutes formées sur le schéma suivant : [préfixe]card[suffixe].exe, sachant que [préfixe] et [suffixe] peuvent être vides.

De plus, une fois installé, le code ne cache pas son activité :

- le processus [préfixe]card[suffixe].exe est présent dans la liste des processus ;

- la clef de registre suivante est créée :

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\PromoReg

En revanche, partant du principe que, une fois installé, le code peut télécharger et installer d'autres programmes malveillants, la désinfection du poste passe par une réinstallation complète de celui-ci. Sachant que le meilleur moyen pour ne pas être infecté est de ne jamais cliquer sur une carte de vœux électronique, même venant d'expéditeurs connus, et plus particulièrement ne jamais cliquer sur une pièce jointe ou sur un lien contenu dans un courriel suspect.

3 Forme de *phishing* originale

Une forme originale de *filoutage* a fait l'objet de discussions sur plusieurs sites de l'Internet cette semaine. Cette technique ne repose plus sur le classique courriel invitant l'utilisateur à se connecter sur un site frauduleux imitant un site officiel mais se fait au cours de la navigation. En effet, il est possible pour une personne malintentionnée, via différentes méthodes (*JavaScript*, *xul*, ...), de déterminer quels sont les sites qu'un utilisateur est en train de visiter sur les différents onglets de son navigateur.

On peut alors imaginer que, si l'utilisateur est en train de consulter via l'un de ses onglets le site d'un établissement financier ou un site commercial, la personne malveillante veuille l'exploiter. Il est alors possible de faire apparaître une fenêtre, en *JavaScript* par exemple, imitant la charte graphique du site visé afin de forcer l'utilisateur à entrer de nouveau ses identifiants et mots de passe sous le prétexte d'une session expirée. Il est alors facile d'intercepter ces derniers, l'utilisateur pensant à une demande légitime du site sur lequel il était connecté.

Le CERTA profite de l'exposé de ce scénario malveillant afin de rappeler quelques règles :

- n'activer l'exécution de code dynamique (*Flash*, *JavaScript*, ...) que sur les sites de confiance ;
- toujours se déconnecter proprement des sites nécessitant une authentification ;
- limiter sa navigation à un seul site lorsque celui est sensible (banques, commerces en ligne, extranet, ...) afin d'éviter des fuites d'information ;
- naviguer sur l'Internet avec un compte utilisateur aux droits limités ;
- toujours appliquer les correctifs sur l'ensemble des applicatifs (système d'exploitation, navigateur, logiciels, ...).

4 Systèmes embarqués et politique de mots de passe

4.1 Présentation

Plusieurs constructeurs proposent des équipements multimédia ou de stockage disposant de fonctionnalités avancées comme de la connectivité réseau filaire ou pas. On peut par ce biais accéder directement au contenu stocké dans l'équipement via différents protocoles : FTP, SMB, NFS, etc. Ces solutions peuvent être intéressantes car elles permettent de mutualiser un espace de stockage sur lequel on pourra réaliser des opérations de sauvegarde ou de duplication des données s'y trouvant. Ils peuvent aussi constituer une zone d'échange pratique à utiliser.

En fonction de la nature des données stockées et de sa position dans le SI, le contrôle d'accès à ce type de ressources devra être irréprochable. Or les différentes solutions rencontrées n'offrent pas toutes les mêmes niveaux de sécurité. Ainsi on pourra trouver, dans le pire des cas, des équipements proposant tous ces services activés avec un accès anonyme en lecture/écriture.

D'autres présenteront également l'intégralité de leurs services par défaut protégés par un mot de passe faible car disponible dans la documentation ou issu d'une dérivation d'un paramètre de l'équipement comme son adresse MAC. Dans ce dernier cas, on pourrait penser qu'utiliser l'adresse physique du périphérique réseau est une bonne idée mais il faut garder à l'esprit que les trois premiers blocs de l'adresse MAC varient seulement en fonction du constructeur. Ainsi dans l'adresse : 00:DE:AD:00:BE:EF, la partie 00:DE:AD représente le constructeur. La partie pseudo-aléatoire ne dépend plus que des trois blocs suivants (00:BE:EF dans l'exemple). Si l'attaquant a connaissance de la marque de l'équipement, il devient alors plus facile pour lui de trouver le mot de passe.

4.2 Recommandations

Concernant ces équipements, il faudra s'attacher entre autres, aux points suivants :

- s'assurer que l'on peut mettre à jour le système embarqué, et si oui, appliquer les mises à jour ;
- configurer l'équipement avec des mots de passe robustes chaque fois que cela est possible car certains ne permettent pas de changer le mot de passe ;

- désactiver les services non-utilisés et en préférer un seul ;
- définir une politique d'accès précise à l'équipement.

5 Ports observés

Le tableau 3 et la figure 2 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 08 et le 15 janvier 2009.

6 Liens utiles

- Mémento sur les virus :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/>
- Note d'information du CERTA sur l'acquisition de correctifs :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/>
- Note d'information du CERTA sur les systèmes obsolètes :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/>
- Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/>
- Note d'information du CERTA sur les mots de passe :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/>
- Note d'information sur la terminologie d'usage au CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/>
- Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/>
- 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 sur les risques associés aux clés USB :
<http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/>
- Note d'information du CERTA sur les outils d'indexation et de recherche :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/>
- Note d'information du CERTA sur la gestion des noms de domaine :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/>
- Note d'information du CERTA sur le bon usage de PHP :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/>

7 Rappel des avis émis

Dans la période du 09 au 16 janvier 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-010 : Vulnérabilité dans Asterisk
- CERTA-2009-AVI-011 : Multiples vulnérabilités dans les produits BlackBerry
- CERTA-2009-AVI-012 : Plusieurs vulnérabilités de SMB dans Windows
- CERTA-2009-AVI-013 : Vulnérabilités des produits Oracle
- CERTA-2009-AVI-014 : Multiples vulnérabilités dans IBM DB2
- CERTA-2009-AVI-015 : Vulnérabilité dans Avira Antivir
- CERTA-2009-AVI-017 : Vulnérabilités dans Cisco IOS
- CERTA-2009-AVI-018 : Vulnérabilité dans les produits Cisco ONS

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 oeuvre (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 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.ssi.gouv.fr/fr/formation/>

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.

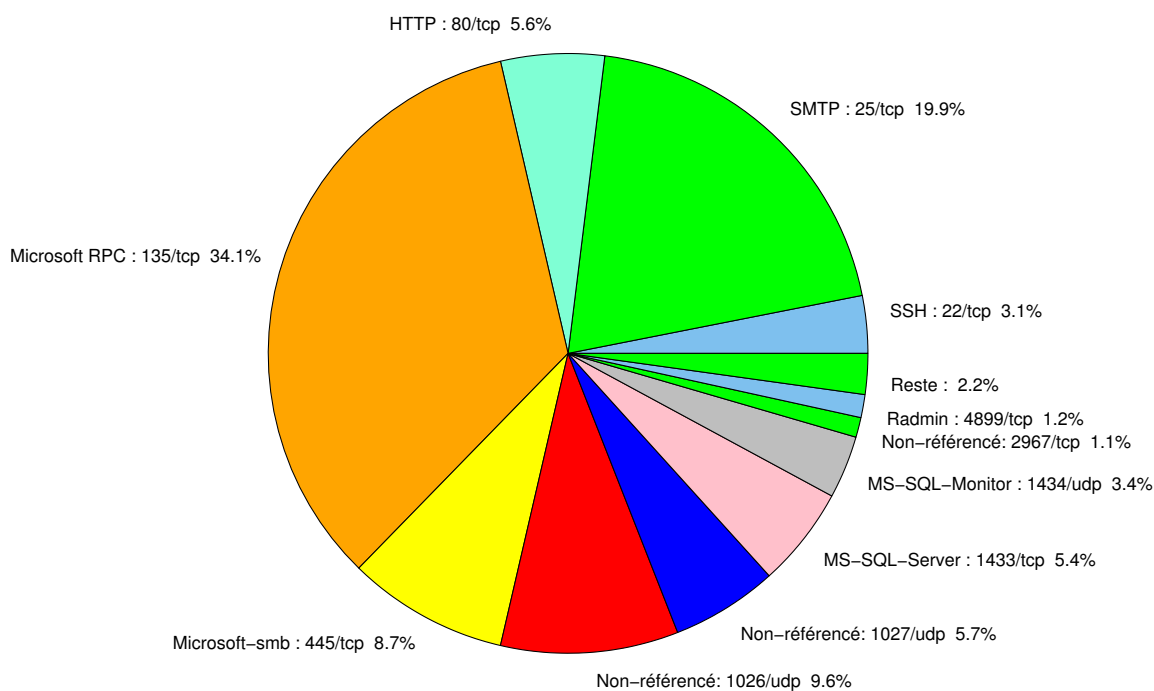


FIG. 2: Répartition relative des ports pour la semaine du 08.01.2009 au 15.01.2009

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 CERTA-2007-ALE-005-001
25	TCP	SMTP	–	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	–	CERTA-2004-AVI-384
69	UDP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-320
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	–	– CERTA-2007-AVI-008
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 CERTA-2007-AVI-321
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 CERTA-2007-AVI-294
427	TCP	Novell Client	–	CERTA-2006-AVI-538
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343 CERTA-2007-AVI-153
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 CERTA-2007-AVI-321 CERTA-2007-ALE-010
445	UDP	Microsoft-smb	–	CERTA-2007-ALE-010
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
2512	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2513	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	CERTA-2006-AVI-221
3104	TCP	CA Message Queuing	–	CERTA-2007-AVI-331
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3268	TCP	Microsoft Active Directory	–	CERTA-2007-AVI-294
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5151	UDP	IPSwitch WS_TP	–	CERTA-2007-AVI-312
5151	TCP	ESRI ArcSDE	–	CERTA-2007-AVI-367
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6014	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6106	TCP	Symantec Backup Exec	–	CERTA-2007-AVI-303
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
6502	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6503	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6504	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
8080	TCP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-153
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	–
10110	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	CERTA-2007-AVI-217
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	–	CERTA-2005-AVI-310
54345	TCP	HP Mercury	–	CERTA-2007-AVI-075
65535	UDP	LANDesk Management Suite	–	CERTA-2007-AVI-176

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

port	pourcentage
135/tcp	34.08
25/tcp	19.94
1026/udp	9.57
445/tcp	8.67
80/tcp	6.14
1027/udp	5.74
1433/tcp	5.4
1434/udp	3.38
22/tcp	3.09
4899/tcp	1.23
2967/tcp	1.07
139/tcp	0.56
23/tcp	0.33
137/udp	0.28
3306/tcp	0.22
143/tcp	0.05

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

15 janvier 2009 version initiale.