Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 mars 2009
N° CERTA-2009-ACT-010

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-10

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-010`

Gestion du document

Référence	CERTA-2009-ACT-010
Titre	Bulletin d'actualité 2009-10
Date de la première version	06 mars 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-010.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-010/

1 Incidents traités cette semaine

1.1 Infections par un *bot*

Le CERTA a été informé de l'infection de nombreuses machines par un code malveillant qui se caractérise par les éléments suivants :

- connexion à un serveur `IRC` sur le port 6667/tcp ;
- sondages de nombreux réseaux sur le port 22/tcp (`SSH`).

Une telle activité n'est pas nouvelle, mais, jusqu'à présent, elle était plutôt associée à des machines fonctionnant sous une distribution *Linux* quelconque. Or il s'agit, pour les incidents de cette semaine, de machines infectées fonctionnant sous *Windows*. Pour un de ces incidents, le code malveillant a été retrouvé sous le nom :

```
C:\WINDOWS\security\lsass.exe
```

Une différence fondamentale entre les distributions *Windows* et *Linux* est qu'il n'y pas de client `SSH` installé par défaut dans le système d'exploitation de *Microsoft*. Par conséquent, les connexions sortantes en `SSH` émanant de tels postes peuvent être un révélateur de compromission pour l'administrateur du réseau. La mise en place de règles spécifiques de filtrage en sortie ainsi qu'une lecture régulière des journaux d'événements réseaux permettent de mettre facilement en évidence les incidents de ce type.

1.2 De l'importance des remontées d'information

Une personne travaillant dans une administration a été contactée par un utilisateur. Ce dernier lui a signalé qu'une page d'un site Web provoquait un erreur de son antivirus au cours de la navigation. Le site en question n'est pas directement géré par la personne (autre ville, autre service), mais elle a transféré cette donnée pour information au CERTA et à sa chaîne fonctionnelle SSI.

L'analyse du site par le CERTA montre que ce dernier est effectivement compromis. L'intégralité des pages a été modifiée par l'insertion d'une ligne discrète de type `iFrame`. La navigation sur ces pages force ainsi le navigateur à se connecter à l'insu de l'utilisateur à une série de sites conduisant *in fine* à des codes JavaScript exploitant des vulnérabilités `Flash` et `PDF` du navigateur.

Cet incident permet de rappeler l'importance des remontées d'incidents. Certains événements peuvent paraître anodins mais permettent de révéler un problème de sécurité important. Il ne faut donc pas s'appuyer sur un sentiment trop hâtif et il ne faut pas hésiter à transférer l'information. C'est là tout l'intérêt d'une chaîne fonctionnelle SSI où chacun est acteur de la sécurité de l'ensemble.

2 Retour sur la vulnérabilité PDF

Le 23 février 2009, le CERTA a émis une alerte concernant une vulnérabilité portant sur le format PDF et plus particulièrement Adobe Reader.

La vulnérabilité de type débordement de mémoire permet à un utilisateur malintentionné d'exécuter du code arbitraire à distance. Le savoir-faire est disponible sur l'Internet et des cas d'exploitation ont d'ores et déjà été signalés. Les codes d'exploitation peuvent avoir recours à du code JavaScript Adobe. Il est donc préférable de s'assurer que l'interprétation de JavaScript n'est pas activée par défaut dans la configuration Adobe.

Au delà de l'application Adobe Reader, de nombreux autres lecteurs alternatifs de fichiers au format PDF sont affectés au moins par un déni de service.

La surface d'attaque liée à cette vulnérabilité peut être étendue, en plus de l'ouverture de fichier avec l'application vulnérable, à l'explorateur de fichiers de Microsoft Windows. Cela est dû à l'installation d'une extension par Adobe Reader. Cette extension est appelée par l'explorateur de fichiers notamment pour l'affichage en mode miniature des icônes et lors de la sélection du fichier par l'utilisateur. D'autres scénarios peuvent être envisagés.

L'application faisant appel à cette extension, "Adobe PDF Shell Extension", devient alors vulnérable à un fichier PDF spécialement construit.

Un contournement provisoire pour les systèmes Windows a été proposé dans l'alerte CERTA-2009-ALE-001 afin de restreindre la surface d'attaque sur le système. Une clé de registre permet de désactiver l'utilisation de l'extension "Adobe PDF Shell Extension".

Comme tout contournement, il peut avoir des effets de bord non contrôlés et il convient de le tester au préalable.

Ce contournement n'empêche pas la compromission par ouverture d'un fichier malveillant.

Documentation

– Alerte CERTA-2009-ALE-001 :
http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-001/

3 Les metatag HTML

3.1 Le contexte

Les données *meta tag* du format *HTML* permettent de définir certaines propriétés d'une page *HTML*. Ainsi il est possible via les propriétés *meta content* de définir, par exemple, les droits d'accès et de référencement pour les robots des différents moteurs de recherche.

3.2 Les exemples

Grâce aux *meta tag*, il est possible de bloquer toute indexation par les robots, la recherche des liens dans les pages ou la mise en cache de site. L'exemple ci-dessous montre la portion de code à ajouter :

```
<META content=noindex,nofollow,noarchive name=robots>
```

A l'inverse, les *meta tag* permettent également d'autoriser une indexation de l'ensemble du site et des documents s'y trouvant. L'extrait *HTML* suivant illustre ces propriétés :

```
<META content=index,follow,all name=robots>
```

Des politiques de référencement sont utilisées par des sites malveillants afin de :

- rester discret et freiner les tentatives de découverte de réseau se cachant derrière un code malveillant ;
- faciliter l'indexation afin d'accroitre le nombre de visite sur le site et ainsi augmenter la rapidité de propagation d'un code malveillant.

3.3 Les recommandations

Que votre politique d'indexation soit l'une ou l'autre des solutions exposées ou une position intermédiaire, il est important de prêter attention à ces données qui ne sont pas visibles de l'extérieur. En effet, une modification de ces informations peut entraîner une rupture de la visibilité sur l'Internet ou provoquer une atteinte à la confidentialité de certaines données si elles sont indexées puis mises en cache alors qu'elles ne le devraient pas. Le CERTA recommande régulièrement de contrôler l'intégrité des pages d'un site web. Si cette solution n'est pas applicable, des contrôles plus ciblés sur ce type de données ou sur le fichier *.htaccess*, par exemple, peuvent être des indicateurs de compromission et peuvent éviter une fuite d'information involontaire.

4 Toujours plus d'idées pour le filoutage

4.1 Présentation générale

Un navigateur a plusieurs manières d'identifier le type de fichier que lui envoie un serveur. Il peut s'appuyer :

- sur l'extension du fichier ;
- sur le type MIME retourné par le serveur (`Content-Type`) dans l'en-tête HTTP ;
- sur la signature du fichier, et en particulier les premiers octets pouvant caractériser un en-tête de format connu.

La question est donc la suivante : comment réagit un navigateur quand ces informations sont incohérentes entre elles ? Prend-il l'initiative de choisir arbitrairement l'une d'elles comme fiable ?

4.2 Détails pour Internet Explorer

Les réponses varient selon les navigateurs. Un article récent rappelle le comportement d'Internet Explorer dans ce cas précis. Il adopte une méthode appelée *MIME sniffing* (ou plus précisément *FindMimeFromData*). Dans le cas d'une requête directe vers le fichier du serveur, il ne tient pas compte des informations précédentes mais s'appuie sur des tests effectués sur les 256 octets, au maximum, du fichier téléchargé.

Cette mesure a été initialement prise par méfiance des sites Web fournissant de fausses informations sur le type de contenu.

Ainsi, dans une réponse à une requête pour récupérer le fichier `certa.jpg`, le serveur peut répondre avec `Content-Type: image/jpeg` bien que le navigateur Internet Explorer interprétera finalement le contenu comme du HTML si le fichier s'avère ne pas être une image. D'autres navigateurs peuvent, eux, avoir des comportements différents et refuser d'interpréter une image inexistante.

Cette astuce peut être utilisée dans le cas de filoutage. L'utilisateur reçoit un courriel avec un lien pointant vers un fichier d'extension `.jpg`. Le serveur annonce également un type de contenu équivalent. En fonction du navigateur et de la configuration de celui-ci, une page de filoutage apparaîtra ou pas à l'écran.

Cette fonctionnalité peut être désactivée par clé de registre sous Windows XP SP2 par exemple.

Ce problème met plus largement en avant les disparités entre navigateurs. Celles-ci peuvent être exploitées par des personnes malveillantes pour adapter leurs actions en fonction des navigateurs.

4.3 Documentation

- Article Microsoft MSDN, « MIME Type Detection in Internet Explorer » :
  http://msdn.microsoft.com/en-us/library/ms775147.aspx
- Article Heise Security, « Risky sniffing - MIME sniffing in Internet Explorer enables cross-site scripting attacks » :
  http://www.h-online.com/security/Risky-MIME-sniffing-in-Internet-Explorer–/features/112589

5 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 26 février et le 05 mars 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 27 février au 06 mars 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-055-001 : Vulnérabilités dans Wireshark
- CERTA-2009-AVI-076-001 : Vulnérabilités d'Adobe Flash Player
- CERTA-2009-AVI-080 : Vulnérabilité dans Drupal
- CERTA-2009-AVI-081 : Vulnérabilité dans VMware ESX Server
- CERTA-2009-AVI-082 : Vulnérabilité dans Apache Tomcat
- CERTA-2009-AVI-083 : Vulnérabilités dans PHP
- CERTA-2009-AVI-084 : Vulnérabilités dans Cisco Unified MeetingPlace Web Conferencing
- CERTA-2009-AVI-085 : Multiples vulnérabilités dans Opera
- CERTA-2009-AVI-086 : Vulnérabilités de Firefox

Durant la même période, les avis suivants ont été mis à jour :

- CERTA-2008-AVI-556-001 : Vulnérabilité dans GnuTLS
  (ajout des références aux bulletins de sécurité Gentoo, Debian, Red Hat, SuSE et Ubuntu)
- CERTA-2009-AVI-047-001 : Vulnérabilité dans Squid
  (ajout de la référence CVE et des bulletins de sécurité Debian, SuSE et Ubuntu)

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 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.

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 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.

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.

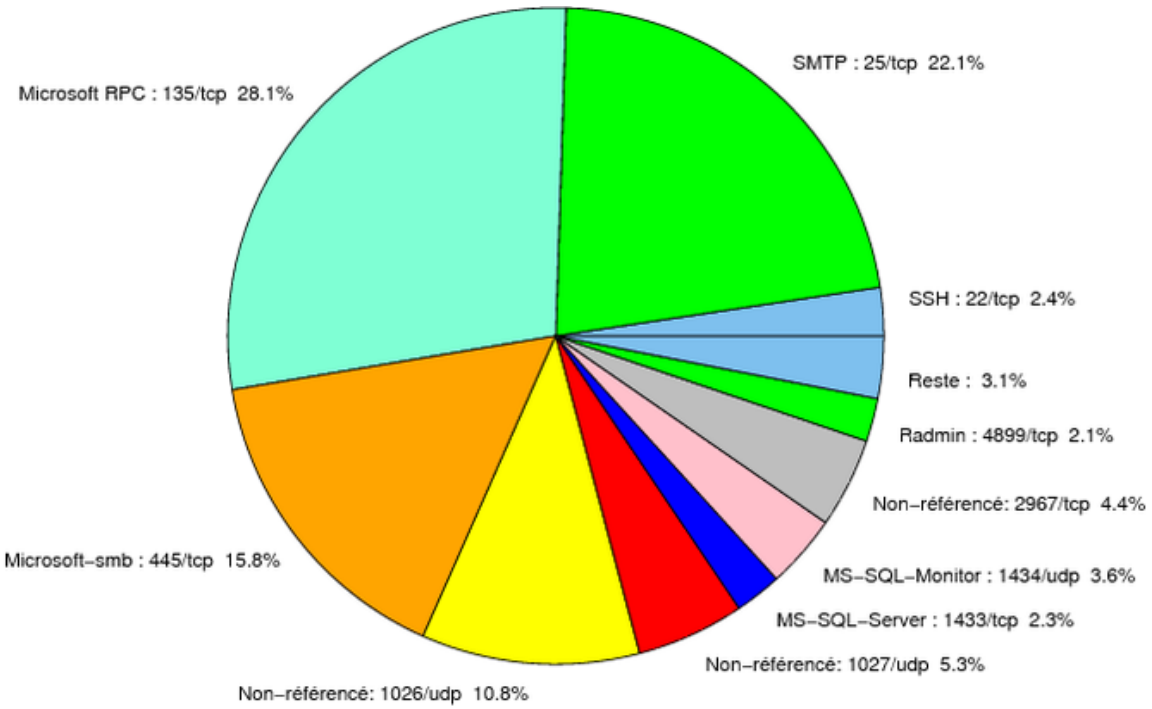

FIG. 1: Répartition relative des ports pour la semaine du 26.02.2009 au 05 mars 2009

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER CERTA-2007-ALE-005-001
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CER
69	UDP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
106	TCP	MailSite Email Server	–	– http://www.certa.ssi.gouv.fr/site/CER
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CER
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CER
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CER
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CER
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CER
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER

				http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CER
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CER
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CER
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CER
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CER
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6106	TCP	Symantec Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6502	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6503	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6504	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
8080	TCP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	http://www.certa.ssi.gouv.fr/site/CER
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CER
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CER
54345	TCP	HP Mercury	–	http://www.certa.ssi.gouv.fr/site/CER
65535	UDP	LANDesk Management Suite	–	http://www.certa.ssi.gouv.fr/site/CER

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

port	pourcentage
135/tcp	28.12
25/tcp	22.12
445/tcp	15.75
1026/udp	10.75
1027/udp	5.31
2967/tcp	4.43
1434/udp	3.62
22/tcp	2.37
1433/tcp	2.31
4899/tcp	2.12
137/udp	0.68
80/tcp	0.62
139/tcp	0.5
23/tcp	0.43
3306/tcp	0.25
3128/tcp	0.18
1080/tcp	0.12
3389/tcp	0.06

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

06 mars 2009 version initiale.