Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 mars 2009
N° CERTA-2009-ACT-011

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-11

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-011`

Gestion du document

Référence	CERTA-2009-ACT-011
Titre	Bulletin d'actualité 2009-11
Date de la première version	13 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-011.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-011/

1 Incidents traités cette semaine

1.1 Vulnérabilités PDF et exploitations

Le CERTA a traité cette semaine des incidents avec une méthode de compromission présentant plusieurs points communs :

- quelques utilisateurs ont été destinataires de courriels usurpant une adresse légitime ;
- les courriels contenaient plusieurs pièces jointes, la majorité au format PDF.

Les fichiers PDF analysés exploitent deux types de vulnérabilités :

- celles associées à la fonction Adobe JavaScript `Collab.CollectEmailInfo()` corrigée en 2008 et mentionnées dans le bulletin d'actualité CERTA-2008-ACT-020 ;
- la vulnérabilité récente touchant l'interprétation des flux encodés en JBIG2 dans un fichier PDF et faisant l'objet de l'alerte CERTA-2009-ALE-001.

Ces incidents sont assez représentatifs de la problématique de ces vulnérabilités : les antivirus ont beaucoup de difficultés à les détecter. Il est donc très important de prendre plusieurs mesures préventives dont :

- désactiver l'interprétation de JavaScript dans Adobe par défaut ;

– mettre à jour les applications dès que les correctifs sont disponibles ;
– être très circonspect lors de la réception soit d'un courriel provenant d'un expéditeur mal connu, soit d'un courriel inattendu d'un expéditeur connu. Dans ce dernier cas, l'analyse de l'en-tête peut s'avérer utile.

L'alerte CERTA-2009-ALE-001 mentionne plusieurs contournements provisoires ainsi que l'avancement des publications de correctifs par Adobe selon les versions des logiciels.

1.2 Un site à l'abandon

1.2.1 Présentation

Cette semaine le CERTA a informé le propriétaire d'un site Web de la compromission de ce dernier. En effet des attaquants avaient réussi à contourner les mesures de sécurité du site afin d'y déposer des fichiers malveillants. L'administrateur du serveur a informé le CERTA que ce site n'était plus utilisé depuis plusieurs mois et que suite à l'information du CERTA, le site serait totalement supprimé car inutile.

Les sites abandonnés comme celui-ci posent plusieurs problèmes :
– les correctifs de sécurité ne sont plus appliqués ;
– personne ne suit les journaux des connexions afin de découvrir une tentative d'attaque ou une attaque réussie ;
– les contacts mentionnés sur le site ne sont plus valides ;
– une attaque avérée ne sera pas détectée et traitée immédiatement.

Dans le cas d'un site ou de pages Web devenus inutiles, le CERTA recommande de supprimer toutes les applications et pages (exemple : CMS et autres composants) potentiellement vulnérables et de prévenir, éventuellement, les internautes de cette disparition au moyen d'un page statique.

1.2.2 Documentation

– Note d'information CERTA-2002-INF-002 sur les bons réflexes en cas d'intrusion sur un système d'information :
http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/

1.3 Comportements étranges...

Cette semaine, le CERTA a traité un incident concernant plusieurs compromissions dans une administration. Comme bien souvent, ces compromissions ont été facilitées par l'utilisation d'un logiciel non mis à jour.

Les postes étaient infectés par un enregistreur de frappes clavier (ou *keylogger*) qui envoyait ces informations sur un serveur distant. Le code malveillant a pu être repéré par l'impossibilité pour les utilisateurs d'effectuer certaines combinaisons de touches, notamment les accents circonflexes et les trémas. Cette propriété est assez courante pour un enregistreur de frappes.

S'il ne faut évidemment pas se reposer sur ce genre de symptôme pour détecter la présence de codes malveillants, le CERTA rappelle que tout comportement suspect d'une machine (problèmes de touches, messages d'erreur, utilisation anormale du CPU, etc.) doit être remonté à son administrateur réseau qui pourra alors investiguer le problème.

Ce sont souvent des comportements bizarres qui permettent de mettre en évidence un incident. Ils ne doivent pas être sous-estimés.

2 La mise à jour qui dérape

Cette semaine un éditeur d'antivirus a publié une mise à jour qui, suite à une erreur humaine, n'a pas été signée. Cette absence de signature a provoqué des alertes au sein même des logiciels de l'éditeur. Les utilisateurs ont observé des demandes d'autorisation d'accès à l'Internet d'un fichier exécutable. Ce fichier, légitime et appartenant aux applications de l'éditeur, a ainsi provoqué une certaine panique chez certains des utilisateurs mais aussi une euphorie chez certaines personnes malveillantes.

Les premiers ont cherché sur l'Internet des solutions afin de déterminer l'origine et la dangerosité du fichier exécutable et les seconds ont tenté de conduire les premiers sur de fausses solutions antivirales ou sites malveillants en tout genre.

L'éditeur affirme que cette mise à jour n'est été diffusée que pendant un court délai et que peu de personnes ont été touchées. Cet incident permet néanmoins de tirer quelques enseignements :

– la capacité de réaction des attaquants est très grande dès qu'il s'agit de leurrer les utilisateurs. Ils ont réussi à monter en quelques heures des sites malveillants permettant, via une bonne indexation de certains moteurs

de recherche, de pousser des personnes à installer des logiciels à l'origine douteuse contenant des chevaux de Troie ;
– une mesure de sécurité qui n'est pas correctement respectée peut aboutir à une compromission. Les mises à jour doivent être récupérées sur les sites officiels avec toutes les garanties d'authentification et d'intégrité. En cas de doute ou d'anomalie détectée, il convient de s'informer directement auprès de l'éditeur.

3 Interfaces actives et réseaux ouverts

Devant le nombre croissant de supports publicitaires utilisant la technologie Bluetooth pour intéragir avec les utilisateurs, le CERTA tient à rappeler les risques inhérents à cette technologie.

La note d'information CERTA-2007-INF-003 recommande aux utilisateurs de désactiver leurs interfaces réseau Bluetooth lorsque celui-ci n'est pas indispensable. De plus, il est fortement recommandé de ne pas procéder à un jumelage d'appareils dans un environnement non sûr. Cette même note d'information recense également les risques spécifiques liés à l'utilisation de technologie, sans oublier les risques affectant plus généralement les réseaux sans-fil.

De manière générale, les supports publicitaires imposent une configuration très laxiste de l'équipement pour pouvoir communiquer les informations. La portée n'est pas un argument suffisant, comme il a été souligné dans l'article « Portée et Bluetooth » du bulletin d'actualité CERTA-2008-ACT-017. La portée ne dépend pas que de la puissance du signal d'émission. Des antennes externes branchées sur des cartes peuvent, par exemple, considérablement augmenter la qualité de réception.

– Note d'information CERTA-2007-INF-003 relative au Bluetooth :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-003/
– Bulletin d'actualité CERTA-2008-ACT-017, « Portée et Bluetooth » :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-017.pdf

4 Le système de fichiers ext4

4.1 Présentation

La nouvelle version du système de fichiers `Extended Filesystem 4` est désormais considérée comme stable et n'est plus estampillée expérimentale dans le noyau `Linux` depuis sa version 2.6.28.

Hormis des capacités revues à la hausse en terme de taille maximale de fichier ou de partitions, ce système de fichiers apporte son lot de nouveautés dont certaines peuvent présenter un intérêt non négligeable pour la sécurité :
– un mécanisme de récupération de fichiers (*undelete*) intégré. Ce mécanisme n'est pas mis en oeuvre pour le moment mais le format du système de fichier peut le supporter nativement ;
– des informations supplémentaires apparaissent dans le contenu des inœuds (*inodes*) comme la date de suppressions d'un fichier ou une granularité de temps descendue à la nanoseconde (milliseconde auparavant).

Ces deux fonctionnalités sont assez prometteuses surtout dans un contexte d'autopsie suite à un incident. Il existe, par ailleurs, une certaine compatibilité ascendante entre `ext4` et `ext3` et des outils standards de migration vers `ext4`. Cependant, certaines nouvelles fonctionnalités introduites dans le nouveau format ne permettent pas d'avoir le même niveau de compatibilité que l'on a entre `ext2` et ext3.

Par exemple, un des changements majeurs est le mécanisme d'allocation par `extents`[1] « casse » le mécanisme d'allocation traditionnelle s'appuyant par des blocs d'adresses indirectes ou doublement indirectes.

Ainsi lorsque l'on convertira un système de fichiers `ext3` en `ext4`, l'actuelle partie allouée du système restera de type `ext3` et les nouveaux fichiers créés le seront « à la mode » `ext4` par `extents`. Dans ce cas, on ne pourra plus monter le système `ext4` en `ext3` car le format `ext3` ignore totalement la logique d'`extents`. Ceci peut être crucial lors d'une récupération d'un système endommagé avec un outil ne supportant que l'`ext3` au maximum.

4.2 Recommandations

Bien que le système `ext4` semble très prometteur tant en terme de performances que de fonctionnalités offertes et dans la mesure où toutes les distributions `GNU/Linux` ne le proposent pas nativement, il reste préférable d'attendre un support et une intégration plus accrus dans les distributions avant d'envisager une migration de ses sytèmes de fichiers `ext3` vers ce nouveau format. Il n'en reste pas moins que certaines des fonctionnalités offertes seront assez appréciables dans un contexte de traitement d'incident.

[1] un `extent` est un ensemble de blocs contigus sur un disque dur adressé uniquement par un seul inoeud

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 05 et le 12 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 06 au 13 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-087 : Vulnérabilité dans les routeurs Cisco 7600 Series
- CERTA-2009-AVI-088 : Vulnérabilité dans IBM Websphere Application Server
- CERTA-2009-AVI-089 : Multiples vulnérabilités dans IBM DB2
- CERTA-2009-AVI-090 : Vulnérabilités dans Foxit Reader
- CERTA-2009-AVI-091 : Vulnérabilités dans le noyau Microsoft Windows
- CERTA-2009-AVI-092 : Vulnérabilité dans le composant d'authentification Secure Channel de Microsoft Windows
- CERTA-2009-AVI-093 : Vulnérabilités dans les serveurs Windows DNS et WINS
- CERTA-2009-AVI-094 : Vulnérabilité dans l'interprétation JBIG2 des produits Adobe

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)
- CERTA-2009-AVI-073-001 : Vulnérabilité dans libpng
  (ajout des références aux bulletins de sécurité Gentoo, Red Hat et SuSE)

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.

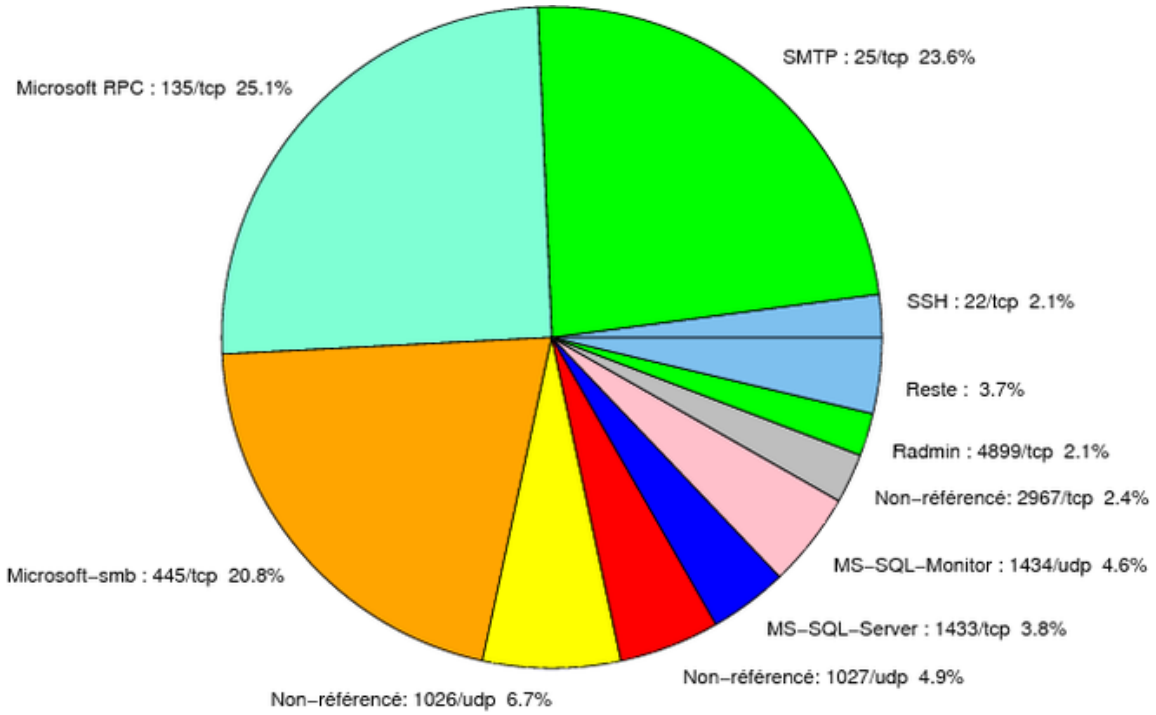

FIG. 1: Répartition relative des ports pour la semaine du 05 au 12 mars 2009

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	25.13
25/tcp	23.58
445/tcp	20.82
1026/udp	6.73
1027/udp	4.91
1434/udp	4.64
1433/tcp	3.84
2967/tcp	2.42
4899/tcp	2.15
22/tcp	2.08
80/tcp	0.8
137/udp	0.67
23/tcp	0.47
3389/tcp	0.26
143/tcp	0.13

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

13 mars 2009 version initiale.