

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-06

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-006>

Gestion du document

Référence	CERTA-2009-ACT-006
Titre	Bulletin d'actualité 2009-06
Date de la première version	06 février 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-006.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-006/>

1 Un enregistreur de frappes plutôt collaboratif

Cette semaine le CERTA a traité un incident relatif à la compromission d'un site Internet. La nature de la compromission semblait suggérer que le serveur hébergeait des codes malveillants. L'analyse du CERTA indique que l'origine de la compromission est le vol d'un identifiant de connexion FTP. Ce vol semble provenir d'une machine d'un administrateur compromise par un enregistreur de frappes clavier. Les attaquants ont ensuite, à plusieurs reprises, déposés et modifiés des fichiers sur le serveur. En effet, le vol d'identifiant semble remonté à plusieurs mois. Ces fichiers contenaient une section de code JavaScript obscurcie, redirigeant l'internaute vers un site malveillant. L'analyse de la compromission indique également que le mot de passe volé n'a jamais été changé par l'administrateur.

Le CERTA rappelle aux administrateurs de sites Web qu'il est indispensable de contrôler régulièrement l'intégrité du serveur et des données présentes. En cas de doute sur la compromission d'une machine par un enregistreur de frappes clavier, il est fortement conseillé de modifier les mots de passes utilisés sur cette machine et de contrôler la sécurité des serveurs accédés. Le CERTA rappelle également qu'il est préférable de désactiver par défaut la prise en charge du JavaScript par le navigateur.

1.1 Documentation

- Note d’information du CERTA sur les bons réflexes en cas d’intrusion sur un système d’information :
<http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/>
- Note du CERTA sur les mots de passe :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/>

2 Compromission du serveur www.phpbb.com

2.1 Exploitation des vulnérabilités

Le 31 janvier 2009, un internaute a décrit sur son bloc-notes la manière dont il s’est introduit dans le serveur du projet `phpbb` et y a capturé beaucoup d’informations sensibles.

En résumé, le site du projet `phpbb` utilise l’outil `phplist` pour gérer ses lettres d’information par courriel. Cet outil souffre d’une vulnérabilité permettant la lecture non autorisée de fichiers et l’inclusion de fichiers locaux. Le code d’exploitation de la vulnérabilité a été publiée sur Internet le 14 janvier 2009. Le correctif n’a été publié par le projet `phplist` que le 29 janvier.

L’agresseur indique avoir commencé l’attaque le jour de la publication du code d’exploitation. L’exploitation de la vulnérabilité lui a permis de lire et de récupérer le fichier des comptes `/etc/passwd`, puis la configuration du serveur HTTP et enfin les fichiers journaux du serveur web `phpbb.com`.

La possibilité, pour un utilisateur des forums, d’ajouter une image (avatar) a permis à l’agresseur de charger des scripts malveillants. La vulnérabilité en permettait l’exécution. Cette nouvelle étape, plus la mémorisation dans des fichiers non chiffrés des identifiants et mots de passe d’administration, ont donné l’accès à la base de données des utilisateurs. L’agresseur indique avoir trouvé ainsi 400 000 adresses de courriels et autant de mots de passe stockés sous forme de condensés. Le condensé de certains mots de passe était produit par un algorithme faible (MD5 et absence de diversifiant (*salt*)). L’agresseur dit avoir ainsi retrouvé près de 29 000 mots de passe.

2.2 Recommandations

Pour les utilisateurs des forums sur `phpbb.com`, surtout si leur compte n’a pas été utilisé depuis longtemps :

- changer le mot de passe sur les forums de `phpbb.com` dès réouverture de ce site ;
- changer les mots de passe de tous les autres comptes en ligne, surtout s’ils correspondent au même identifiant ;
- prévoir de fermer la boîte aux lettres électronique dont l’adresse était dans le compte des forums sur `phpbb.com`.

Pour les gestionnaires de sites web :

- restreindre au possible l’accès à la configuration, aux journaux, aux fichiers et bases de données des comptes, etc. ;
- durcir la configuration PHP (voir documentation) ;
- protéger les mots de passe par des méthodes robustes ;
- suivre les évolutions de sécurité des logiciels utilisés et mettre à jour en conséquence ;
- suivre l’actualité des attaques contre les logiciels utilisés et prendre des mesures préventives en attendant la publication des correctifs ;
- surveiller régulièrement les journaux de connexions et d’erreurs pour détecter des attaques ou des tentatives.

2.3 Documentation

- Bulletin de sécurité du projet `phplist` du 20 janvier 2009 :
<http://www.phplist.com/?lid=274>
- Communiqué du projet `phpbb` du 02 février 2009 :
<http://area51.phpbb.com/phpbb/viewtopic.php?f=3&t=29973>
- Note d’information du CERTA *Du bon usage de PHP* du 20 mars 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/>

3 Nettoyage trop rapide de traces

Le CERTA a émis la note d'information CERTA-2002-INF-002 relative aux bons réflexes en cas d'intrusion sur un système d'information. Il y est indiqué notamment qu'il faut :

- déconnecter la machine du réseau ;
- prévenir le responsable sécurité et le CERT compétent ;
- faire une copie de disque afin de rechercher les traces et indices.

Il est particulièrement important de suivre ce mode opératoire : en effet, qu'il vous soit possible ou pas d'analyser les traces et indices importe assez peu d'une certaine façon, bien que ce soit le meilleur moyen d'en tirer une expérience en matière de sécurité. Si une machine du réseau a été compromise, rappelez-vous qu'elle a également pu servir à compromettre d'autres machines en dehors de votre réseau et que les victimes à suivre sont susceptibles de déposer plainte à leur tour.

L'enquête de police remontera nécessairement au matériel à l'origine de l'attaque (rebonds) et il est alors possible que vous soyez auditionné. Dans ce cadre-là, et si vous avez effacé les traces sur votre machine, vous risquez d'être poursuivi au titre de l'article 434-4 du Code Pénal qui punit du trois ans d'emprisonnement et 45 000 euros d'amende le fait de modifier l'état des lieux d'un crime ou d'un délit soit par altération, falsification ou effacement des traces ou indices soit par apport, déplacement ou suppression d'objets quelconques, mais aussi de détruire, soustraire, receler ou altérer un document public ou privé ou un objet de nature à faciliter la découverte d'un crime ou d'un délit, la recherche des preuves ou la condamnation des coupables.

Lorsque les faits prévus au présent article ont été commis par une personne qui, par ses fonctions est appelée à concourir à la manifestation de la vérité, la peine est portée à cinq ans d'emprisonnement et à 75 000 euros d'amende.

4 Faux codec et vrai code malveillant

Il arrive parfois qu'à l'occasion d'une visite d'un site Internet au contenu multimédia, il soit demandé à l'utilisateur l'installation d'un module complémentaire ou d'un codec afin de pouvoir lire une vidéo. Ce codec, lecteur de vidéo ou module complémentaire pour le navigateur peut se révéler être, dans les faits, un code malveillant permettant diverses actions malintentionnées (vol de données, prise de contrôle à distance, ...).

Il s'agit en fait d'un Cheval de Troie : c'est l'utilisateur qui provoque l'exécution de codes malveillants sur son système en croyant installer un codec.

Le CERTA profite de cette technique connue d'ingénierie sociale pour rappeler certaines précautions à mettre en oeuvre afin de limiter les risques d'une compromission lors de la navigation sur l'Internet :

- naviguer avec un compte utilisateur aux droits limités ;
- désactiver l'exécution de code dynamique (*Flash, JavaScript, ...*) sur des sites qui ne sont pas de confiance ;
- lorsque l'installation d'une application, d'un module ou codec supplémentaire est nécessaire, il est important de les télécharger sur le site de l'éditeur officiel et de contrôler la signature avant installation si celle-ci existe ;
- maintenir à jour le système d'exploitation, le navigateur et les modules ou extensions installés afin d'éviter toute installation silencieuse d'un code malveillant via l'exploitation d'une vulnérabilité.

5 La redirection d'URLs, une fonctionnalité risquée

Un article du bulletin d'actualité d'octobre 2008 (*CERTA-2008-ACT-042*) traite du problème de redirection d'un point de vue utilisateur. Abordons maintenant l'autre côté du problème. Tous les développeurs et webmasters, ou presque, sont sensibilisés à la sécurité de leurs sites et appliquent les recommandations en vigueur pour éviter de voir leurs URLs associées à des activités malveillantes. Malheureusement, cela ne suffit parfois pas. En effet, il n'est pas nécessaire de compromettre un site pour utiliser son adresse abusivement, et cela, entre autres grâce aux redirections d'URLs.

5.1 De quoi s'agit-il ?

La redirection d'adresses consiste à rediriger automatiquement un internaute vers une destination passée en paramètre d'une requête. Dans l'exemple suivant l'internaute se retrouvera automatiquement sur le site

www.une_autre_adresse.tld alors qu'il interrogeait le domaine *www.monsite.tld* :
`http://www.monsite.tld?redirection_vers=www.une_autre_adresse.tld`

Les redirections peuvent être utilisées dans de nombreux cas dont :

- à la place d'un lien direct (*monsite.tld?go=destination.tld*) ;
- à des fins statistiques (*monsite.tld?go=destination.tld&compteur=PlusUn*) ;
- afin d'offrir une fonctionnalité de serveur mandataire (*www.proxy.tld?=destination.tld*) ;
- ou comme contrôle de sortie permettant d'avertir l'utilisateur qu'il quitte le site au moyen d'une page intermédiaire (*monsite.tld?out=destination.tld*) ;

La redirection d'URLs a de nombreuses utilisations légitimes qui apportent des fonctionnalités intéressantes et simples à mettre en oeuvre. Cela rend son utilisation très attractive, parfois au détriment de la sécurité.

5.2 Mon site est-il utilisé à mon insu ?

Si une redirection est présente sur un site, il est important de vérifier qu'elle n'est pas utilisée à des fins détournées. Voyons ici quelques axes d'analyse possibles. Il peut être intéressant de lister dans un moteur de recherche les résultats associés à l'adresse du site et vérifier qu'il n'y a rien d'anormal (par exemple la recherche *jardinage.tld* & *viagra* ne devrait rien retourner).

L'approche inverse, à savoir regarder les mots clefs recherchés qui ont amené les visiteurs sur le site, est aussi très utile. Si dans la liste de ces mots il y a des sujets qui n'ont rien à voir avec le site, il y a probablement un problème.

Dans les journaux du serveur il faut être attentif aux pics de requêtes contenant `=http` ou `=//` et voir vers quoi elles redirigent.

Enfin, il faut prendre en compte, et cela quel que soit le sujet, les remarques qui peuvent être faites. Si quelqu'un se plaint que vous essayez de lui vendre des médicaments, cela peut être dû à une redirection d'URL malveillante.

5.3 Que faire pour l'éviter

Si la redirection d'adresses est nécessaire, il est possible de limiter son utilisation malveillante. Voyons quelques précautions qu'il est possible de prendre :

- n'autoriser que les redirections en provenance du site en contrôlant le *referer* ;
- si la redirection ne sert que pour des fichiers locaux, interdire toutes les redirections externes ;
- si les destinations sont connues, utiliser un système de listes *blanches* ;
- signer les redirections pour limiter leur utilisation.

Il est aussi important de configurer le fichier `robots.txt` afin que les redirections ne soient pas indexées. En effet, bien que cela ne change rien au problème, cela les rend moins visibles et donc moins attractives pour les attaquants. Si elles sont utilisées, alors elles le sont certainement au travers de liens malveillants postés sur l'Internet. Il convient alors de contacter les responsables afin de les faire retirer. Et bien sûr, si les redirections ne sont pas utilisées, il faut les désactiver.

5.4 Documentation

- Bulletin du CERTA du 17 octobre 2008 traitant du sujet :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-042.pdf>
- Article de Google du 30 janvier 2009 :
<http://googlewebmastercentral.blogspot.com/2009/01/open-redirect-urls-is-your-site-being.html>

6 Mises à jour Microsoft de février

Cette semaine, Microsoft a publié ses prévisions de mises à jour qui seront disponibles le 10 février 2009. Pour le moment, quatre bulletins sont ainsi prévus, l'impact maximum étant l'exécution de code arbitraire à distance pour chacun. Les systèmes ou applications suivants sont concernés :

- Internet Explorer 7 ;
- Exchange 2000 Server, Exchange Server 2003, et Exchange Server 2007 ;
- SQL Server 2000, SQL Server 2005 ;
- Visio 2002, Visio 2003, Vision 2007.

Les vulnérabilités sont jugées critiques par Microsoft pour Internet Explorer et Exchange, et importantes pour SQL Server et Visio.

S'il y a de fortes chances pour que l'alerte CERTA-2008-ALE-017 soit corrigée par ce lot de mises à jour, on remarquera que la vulnérabilité concernant le convertisseur de texte de Wordpad (CERTA-2008-ALE-015) reste toujours non corrigée.

6.1 Documentation

- Préavis Microsoft pour les bulletins de février 2009 :
<http://www.microsoft.com/technet/security/Bulletin/ms09-feb.msp>
- Bloc-notes de Pascal Saulière :
<http://blogs.technet.com/pascals>

7 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 29 janvier et le 05 février 2009.

8 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/>

9 Rappel des avis émis

Dans la période du 30 janvier au 06 février 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-038 : Vulnérabilité dans Sun Java System Access Manager
- CERTA-2009-AVI-039 : Vulnérabilité des serveurs SunFire X2100 M2 et X2200 M2
- CERTA-2009-AVI-040 : Vulnérabilité dans Sun Solaris
- CERTA-2009-AVI-041 : Vulnérabilité dans FFmpeg

- CERTA-2009-AVI-042 : Vulnérabilité dans AIX
- CERTA-2009-AVI-043 : Vulnérabilité dans VMware ESX et ESXi
- CERTA-2009-AVI-044 : Multiples vulnérabilités dans Novell GroupWise
- CERTA-2009-AVI-045 : Vulnérabilité du serveur Web de Xerox WorkCentre
- CERTA-2009-AVI-046 : Vulnérabilités de Bugzilla
- CERTA-2009-AVI-047 : Vulnérabilité dans Squid
- CERTA-2009-AVI-048 : Multiples vulnérabilités dans Mozilla Firefox
- CERTA-2009-AVI-049 : Vulnérabilité dans HP-UX
- CERTA-2009-AVI-050 : Vulnérabilité dans Sun Java System Application Server

10 Actions suggérées

10.1 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.

10.2 Concevoir une architecture robuste

À 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.

10.3 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.

10.4 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.

10.5 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.

10.6 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.

10.7 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/>

11 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.

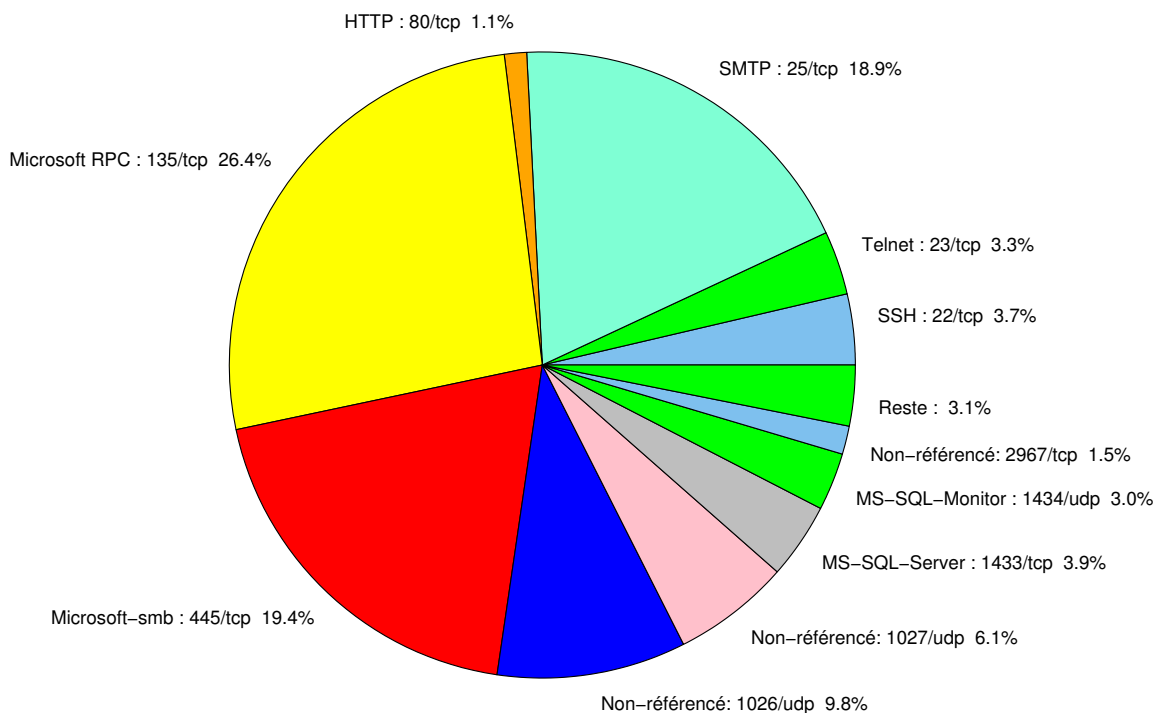


FIG. 1: Répartition relative des ports pour la semaine du 29.01.2009 au 05.02.2009

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	26.37
445/tcp	19.37
25/tcp	18.85
1026/udp	9.76
1027/udp	6.05
1433/tcp	3.91
22/tcp	3.65
23/tcp	3.28
1434/udp	2.97
2967/tcp	1.46
80/tcp	1.14
139/tcp	0.93
4899/tcp	0.88
21/tcp	0.83
137/udp	0.2
3389/tcp	0.15
2100/tcp	0.1

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	9
3	Paquets rejetés	10

Gestion détaillée du document

06 février 2009 version initiale.