

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-04

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-004>

Gestion du document

Référence	CERTA-2009-ACT-004
Titre	Bulletin d'actualité 2009-04
Date de la première version	23 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-004.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-004/>

1 MS08-067...

1.1 Des problèmes

Le CERTA a alerté ses correspondants à de très nombreuses occasions à propos des risques liés à la vulnérabilité Windows MS08-067. En effet, cette vulnérabilité affectant une fonction de `netapi32.dll` a fait l'objet des publications suivantes :

- Bulletin d'actualité CERTA-2008-AVI-523 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-523/>
- Bulletin d'actualité CERTA-2008-ACT-43 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-043.pdf>
- Bulletin d'actualité CERTA-2008-ACT-45 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-045.pdf>
- Bulletin d'actualité CERTA-2008-ACT-48 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-048.pdf>

- Bulletin d'actualité CERTA-2009-ACT-002 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-002.pdf>

Comme annoncé, cette vulnérabilité est exploitée par des vers parfois dénommés *conficker* ou *downadup*. Comme toujours, la première mesure efficace de défense consiste à appliquer à temps les correctifs de sécurité (dans le cas présent, disponible depuis octobre 2008). Si cela se révèle impossible pour des raisons organisationnelles ou techniques, il est indispensable de bien mesurer le risque pris et de prendre les mesures de précaution afin d'en limiter l'impact.

Les correctifs de sécurité ne sont parfois pas appliqués à cause du risque de dysfonctionnement que cela provoquerait sur des applications métiers sensibles. On se retrouve donc dans une situation paradoxale dans laquelle on n'applique pas une mesure de sécurité afin de protéger une application sensible ! Le risque est-il bien apprécié ? La situation n'est pas triviale pour les administrateurs mais il conviendrait sans doute d'améliorer la gestion du risque :

- les tests de non régression ou d'incompatibilité sont-ils réellement faits ou se contente-t-on de ne pas vouloir modifier une « plate-forme qui marche » ?
- existe-t-il une gestion du risque tout au long du cycle de vie des applications ?
- dans le cas présent de la vulnérabilité MS08-067, des mesures de défense en profondeur ont-elles été prises si l'application du correctif s'avérait impossible ?
- existe-t-il une politique de filtrage adaptée (cf. note d'information CERTA-2006-INF-001, « Filtrage et pare-feux ») ?
- les interconnexions sont-elles correctement gérées, y compris via des clefs USB (cf. note d'information CERTA-2006-INF-006, « Risques associés aux clés USB ») ?
- quelle est la qualité des mots de passe d'accès à ces applications sensibles ?
- etc.

Si les applications ne peuvent être mises à jour pour des raisons de sûreté de fonctionnement, il ne faudrait pas que cet argument légitime soit affirmé sans mise en oeuvre de mesures de sécurité conformes à la sensibilité de l'application. Sûreté et sécurité ne devraient jamais être en opposition et c'est une saine gestion des risques qui aidera à discerner les impératifs.

1.2 Liens complémentaires

L'actualité a repris plusieurs fois cette semaine des chiffres importants concernant principalement la propagation d'un des codes exploitant la vulnérabilité corrigée par MS08-067. Les liens ci-dessous permettent de trouver toute l'information utile et nécessaire aux mesures de détection et au nettoyage de ce code en particulier :

- Bloc-Notes Microsoft MMPC, article du 22 janvier 2009 :
<http://blogs.technet.com/mmpc/archive/2009/01/22/centralized-information-about-the-conficker-worm.aspx>
- Article Microsoft KB 962007, « Alerte concernant le ver Win32/Conficker.B » :
<http://support.microsoft.com/kb/962007>
- Outil de suppression de logiciels malveillants Microsoft Windows :
<http://support.microsoft.com/?kbid=890830>
<http://www.microsoft.com/france/securite/malwareremove/default.aspx>
- Déploiement de l'outil de suppression de logiciels malveillants Microsoft Windows dans un environnement d'entreprise :
<http://support.microsoft.com/kb/891716>
- Bloc-notes de Mathieu Malaise, « Instructions pour la suppression de Conficker », 23 janvier 2009 :
<http://blogs.technet.com/mathieum/archive/2009/01/12/instructions-pour-la-suppression-de-conficker.aspx>
- Outil de nettoyage proposé par F-Secure :
<http://www.f-secure.com/weblog/archives/00001588.html>
<ftp://ftp.f-secure.com/anti-virus/tools/beta/f-downadup.zip>
- Forum et bloc-notes de Symantec :
<https://www.symantec.com/stn/blogs/index.jsp>
http://www.symantec.com/business/security_response/weblog/index.jsp
- Outil de nettoyage Symantec :
http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-011316-0247-99

Ces informations sont données à titre indicatif. D'autres solutions sont également proposées par les diverses sociétés offrant des services de sécurité.

1.3 Conclusion

Cette propagation met à nouveau en évidence l'impérative nécessité d'appliquer les correctifs de sécurité, d'utiliser des systèmes d'exploitation maintenus à jour par les éditeurs (cf. note d'information CERTA-2005-INF-003, « Les systèmes et logiciels obsolètes »), de mettre en oeuvre une réelle politique de filtrage et une gestion adéquate des journaux d'événements.

2 Envois de pourriels

2.1 Présentation

Une administration a informé le CERTA que son *webmail* avait été utilisé pour envoyer près de 200 000 messages indésirables, certains étant des arnaques ou escroqueries.

Après l'analyse des journaux faite par l'administrateur de ce serveur, il est apparu qu'un compte légitime avait été utilisé frauduleusement pour émettre ces messages. Le CERTA soupçonne les attaquants d'avoir obtenu les identifiants de connexion au *webmail* suite à une campagne d'ingénierie sociale similaire à celle évoquée dans le bulletin d'actualité CERTA-2008-ACT-028.

Dans la gestion des incidents de ce type, le CERTA recommande aux administrateurs de vérifier auprès des propriétaires légitimes des comptes exploités s'ils ont reçu une demande de mise à jour de leur mot de passe par messagerie. Le cas échéant, il est important de sensibiliser tous les utilisateurs à ce type de menace et de rappeler qu'il ne faut jamais fournir ses identifiants de connexion. Par ailleurs, il est nécessaire de rappeler que l'obtention des identifiants de connexion peut se faire par d'autres biais :

- utilisation d'un enregistreur de frappes clavier (*keylogger*) ;
- écoute du réseau (*sniffing*) ;
- adresses de messagerie sont parfois disponibles sur l'Internet (ainsi que les mots de passe dans de rares cas) ;
- mot de passe utilisé trop faible.

2.2 Documentation

- Bulletin d'actualité CERTA-2008-ACT-028 du 11 juillet 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-028/>

3 Vulnérabilités dans TYPO3

Le CERTA a publié cette semaine l'avis CERTA-2009-AVI-024 concernant *TYPO3*. Cet avis couvre plusieurs vulnérabilités de ce gestionnaire de contenu dont l'une concerne la clé de chiffrement créée lors de l'installation. Le problème avec cette clé est que le tirage de la graine n'est pas suffisamment aléatoire, ce qui diminue l'entropie.

L'application du correctif de sécurité corrige bien les vulnérabilités mais il est néanmoins nécessaire de créer une nouvelle clé de chiffrement. Cela se fait de la façon suivante :

- vider le cache de configuration ;
- ouvrir l'outil d'installation ;
- choisir le menu *Basic Configuration* ;
- aller en bas de la page et appuyer sur le bouton *Generate random key* ;
- valider en sélectionnant *Update localconf.php* ;
- vider de nouveau le cache de configuration et de page.

Il est important de préciser que certaines vulnérabilités, et notamment celles concernant des clés de chiffrement ou les mots de passe, ne disparaissent pas toujours après l'application d'un correctif de sécurité. Il est parfois nécessaire, comme ici avec *TYPO3* ou récemment avec *Debian*, de procéder à un certain nombre d'opérations manuelles.

4 Rappel sur l'alerte en cours CERTA-2008-ALE-015

4.1 Codes malveillants en circulation

Le CERTA a publié le 10 décembre 2008 une alerte concernant une vulnérabilité du convertisseur de texte WordPad. Celle-ci n'est pas actuellement corrigée par un bulletin de sécurité Microsoft. En revanche, plusieurs courriels malveillants circulent actuellement avec une pièce jointe cherchant à exploiter cette vulnérabilité. L'extension qui sollicite par défaut l'application WordPad est le .WRI, mais des extensions .DOC ou .RTF peuvent également le faire selon la configuration du système et en l'absence de l'application Microsoft Office sur le PC du destinataire.

Comme pour d'autres codes d'exploitation, il est fort possible qu'à l'ouverture de la pièce jointe malveillante, une version propre du document soit affichée à l'utilisateur puis stockée sur le disque après contamination de l'ordinateur.

4.2 Gestion des extensions sous Microsoft Windows

Il existe quelques manipulations possibles pour connaître et modifier les associations qui existent sous Windows entre les applications et les extensions de fichiers. Elles se retrouvent également dans la base de registre. Des commandes intéressantes sont :

- ASSOC : la commande affiche pour chaque extension le type de fichier associé
- FTYPE : la commande affiche ou modifie les associations entre types de fichiers et applications

Plusieurs extensions peuvent être associées au même type de fichier (ex. : .jpg et .jpeg associés au même type jpegfile).

Elles permettent de modifier ou lire en ligne de commande ou via un script les différentes associations.

Sous Windows XP SP3 :

```
C:\>assoc .wri
.wri=wrifile
```

```
C:\>ftype wrifile
wrifile="C:\Program Files\Windows NT\Accessoires\WORDPAD.EXE" "%1"
```

```
C:\>
```

"%1" fait référence au nom de fichier (nom court), tandis que "%0" représente le programme exécutable.

L'archivage se fait de la manière assez prédictible :

- assoc > ASSOC_sauvegarde.txt
- ftype > FTYPE_sauvegarde.txt

Et la restauration se fait de la même manière :

- FOR /F "tokens=* delims=" %G IN (ASSOC_sauvegarde.txt) DO ASSOC %G
- FOR /F "tokens=* delims=" %G IN (FTYPE_sauvegarde.txt) DO FTYPE %G

Il est également recommandé de configurer le système d'exploitation pour afficher les extensions.

En remarque finale, le CERTA rappelle qu'il existe certaines subtilités concernant cette gestion d'association. L'une d'elle avait été par exemple évoquée dans un précédent bulletin d'actualité (CERTA-2008-ACT-043).

5 Firefox 3.0.5 et *clickjacking*

5.1 Présentation

Le CERTA a détaillé dans son bulletin d'actualité CERTA-2008-ACT-041 les attaques dites en « *clickjacking* ». Il s'agit de détourner certaines actions de l'utilisateur à des fins illicites. Cette semaine, un fonctionnement particulier de Firefox a été pointé comme facilitant ce type d'attaque. Le navigateur traitant les événements liés à un *onmouseover* avant la redirection due à un clic sur un lien (*HREF*), la destination affichée dans la barre d'état (en bas à gauche) n'est pas forcément celle qui sera effectivement atteinte.

En effet, pour cliquer sur le lien, le curseur est forcément dessus, et cela déclenche un événement *onmouseover* qui peut être utilisé pour changer la cible.

Le CERTA recommande :

- de ne pas avoir toute confiance dans les informations affichées dans la barre d'état ;
- de vérifier dans la barre d'adresse que la destination atteinte est bien celle désirée ;
- de n'activer le *javascript* qu'au besoin, et sur des sites de confiance.

5.2 Documentation

- Bulletin d'actualité CERTA-2008-ACT-041 du 10 octobre 2008, « Les attaques en Clickjacking » : <http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-041.pdf>

6 Indiscrétion via les fichiers de session

Cette semaine est apparue sur l'Internet un scénario original de fuite d'information qui mérite réflexion et recommandations.

6.1 Le scénario

Soit un site Internet *www.siteintranet.tld* et un site malveillant *www.sitemalveillant.tld* et le postulat suivant *www.siteintranet.tld* est vulnérable à une injection de code indirecte (XSS), n'utilise pas le protocole *HTTPS* et ne vérifie pas la cohérence de l'entête *Host* pour la consultation.

La personne malveillante en charge du site *www.sitemalveillant.tld* dépose, lors de la visite d'une victime, un fichier de session (*cookie*) contenant la charge utile à l'exploitation d'une injection de code indirecte. Après redémarrage du navigateur (soit manuellement, soit via un déni service), le *cookie* est toujours présent dans la plupart des configurations de navigateur. Si la victime visite de nouveau le site *www.sitemalveillant.tld* mais que, cette fois-ci, le site change son enregistrement DNS, il peut rediriger la victime vers l'adresse IP de *www.siteintranet.tld*. À cause du redémarrage du navigateur, le DNS n'est pas autorisé à rebondir vers la nouvelle adresse IP. Ainsi, lorsque la victime visite de nouveau *www.siteintranet.tld*, son navigateur envoie une requête dont l'en-tête *Host* est de la forme :

```
Host:www.sitemalveillant.tld
```

Dans le cas où le site *www.siteintranet.tld* ne vérifie pas cet en-tête, les requêtes sont tout de même interprétées, y compris le *cookie* envoyé. Même si l'attaquant ne peut pas usurper le compte de la victime, il peut via un *shell XSS* récolter des données sur la configuration du site *www.siteintranet.tld*.

6.2 Les recommandations

Même si le scénario de cette attaque repose sur un certain nombre de conditions, ce dernier reste envisageable. Le CERTA recommande d'appliquer les protections suivantes :

- supprimer de manière systématique les fichiers de session à la fermeture du navigateur ;
- s'assurer pour les administrateurs de site Internet que leur site n'est pas vulnérable à une injection de code indirecte ;
- cloisonner les réseaux et leurs usages ;
- vérifier l'en-tête *Host* afin de s'assurer de la cohérence de cette dernière ;
- appliquer des mesures d'authentification, y compris pour les serveurs locaux.

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 15 et le 22 janvier 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 16 au 23 janvier 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-019 : Vulnérabilité dans Symantec AppStream
- CERTA-2009-AVI-020 : Vulnérabilité dans Sophos Anti-Virus
- CERTA-2009-AVI-021 : Vulnérabilité dans IBM HMC
- CERTA-2009-AVI-022 : Multiples vulnérabilités dans Sun Java System Access Manager
- CERTA-2009-AVI-023 : Multiples vulnérabilités dans Drupal
- CERTA-2009-AVI-024 : Multiples vulnérabilités dans TYPO3
- CERTA-2009-AVI-025 : Vulnérabilités dans des produits Horde
- CERTA-2009-AVI-026 : Multiples vulnérabilités dans Trend Micro OfficeScan
- CERTA-2009-AVI-027 : Multiples vulnérabilités dans HP OpenView
- CERTA-2009-AVI-028 : Vulnérabilité dans Cisco Security Manager
- CERTA-2009-AVI-029 : Multiples vulnérabilités dans Apple QuickTime

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

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.

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.

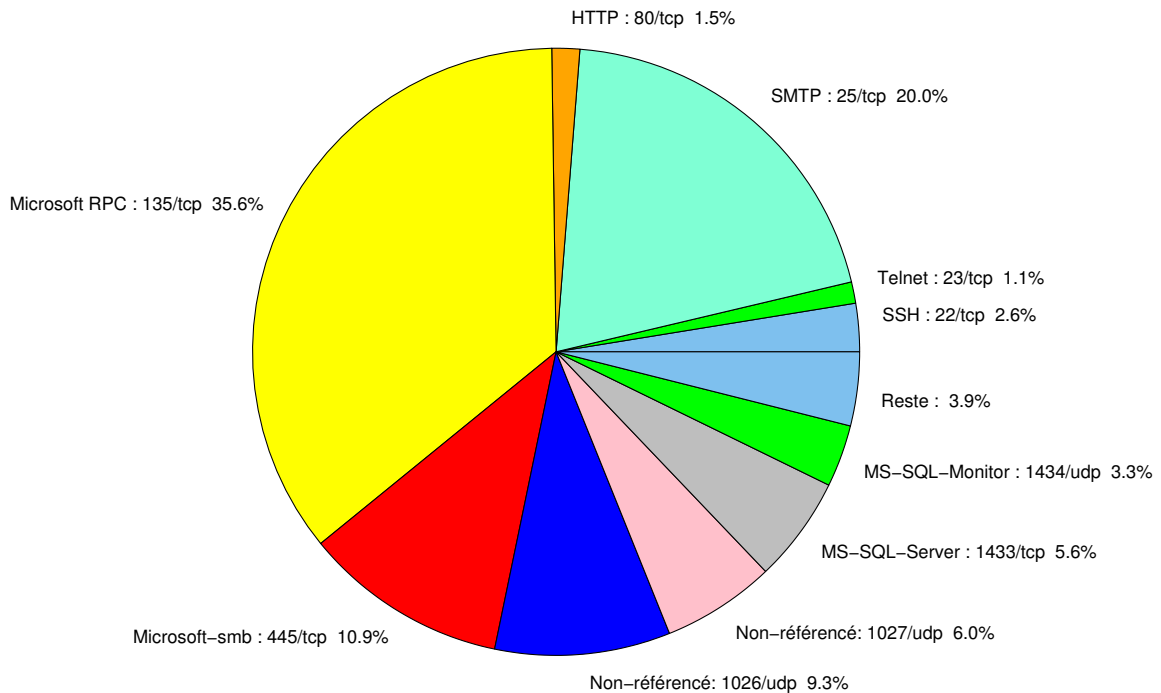


FIG. 1: Répartition relative des ports pour la semaine du 15.01.2009 au 22.01.2009

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	35.64
25/tcp	20.04
445/tcp	10.87
1026/udp	9.33
1027/udp	6.03
1433/tcp	5.63
1434/udp	3.3
22/tcp	2.56
80/tcp	1.48
23/tcp	1.25
4899/tcp	0.96
2967/tcp	0.56
137/udp	0.28
3128/tcp	0.22
3306/tcp	0.17
3389/tcp	0.05

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	10
3	Paquets rejetés	11

Gestion détaillée du document

23 janvier 2009 version initiale.