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 avril 2007
N° CERTA-2007-ACT-015

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-15

Gestion du document

Référence	CERTA-2007-ACT-015
Titre	Bulletin d'actualité 2007-15
Date de la première version	13 avril 2007
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-2007-ACT-015.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-2007-ACT-015/

1 Vulnérabilité dans Microsoft DNS Server

Microsoft a émis un bulletin de sécurité concernant une vulnérabilité dans la gestion des procédures RPC (*Remote Procedure Call*) de *Windows DNS Server*. Les systèmes d'exploitation *Windows 2000 Server SP4*, *Windows Server 2003 SP1* et *Windows Server 2003 SP2* sont concernés, même si ce composant n'est pas activé par défaut. En revanche, les systèmes d'exploitation *Windows 2000 Professional SP4*, *Windows XP SP2* et *Windows Vista* ne sont pas affectés par cette vulnérabilité.

Il n'existe actuellement aucun correctif pour cette vulnérabilité, mais Microsoft propose deux contournements provisoires :

– désactiver l'administration à distance par RPC de *Windows DNS Server*. Ce contournement consiste à modifier la clé de registre suivante (se référer au bulletin de sécurité de Microsoft) :

```
\HKLM\SYSTEM\CurrentControlSet\DNS\Parameters
```

– filtrer les ports 1024 à 5000 (le protocole n'a pas été précisé). Si vous appliquez ce contournement provisoire, il est important d'ajouter des règles permissives en amont pour les services légitimes qui utilisent un de ces ports.

Documentation

- Bulletin de sécurité Microsoft 935964 du 12 avril 2007 :
  http://www.microsoft.com/technet/security/advisory/935964.mspx
- Référence CVE-2007-1748 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1748

2 Vulnérabilités concernant Microsoft Office 2007

Plusieurs vulnérabilités ont été découvertes sur Microsoft Office 2007 depuis sa sortie. La première, découverte fin février, concerne uniquement (*a priori*) Publisher 2007, et permettrait à une personne malintentionnée d'exécuter du code arbitraire à distance.

Plus récemment, trois nouvelles vulnérabilités sur Microsoft Word 2007 ont été découvertes au moyen d'un outil de *fuzzing* (série de tests à l'aveugle, ou avec certains paramètres choisis aléatoirement). Les deux premières causent un déni de service (processeur à 100% d'utilisation) lors de l'ouverture du fichier compromis. La dernière, plus problématique, provoque un débordement de mémoire et concerne la librairie `wwlib.dll`. Ceci engendre au moins un arrêt brutal du logiciel, mais pourrait éventuellement permettre l'exécution de code arbitraire. L'éditeur Microsoft n'a pour le moment pas publié de correctif pour ces quatre failles.

A la date de rédaction de cet article, aucun code d'exploitation n'a été diffusé publiquement pour la vulnérabilité sur Publisher 2007. De même, aucun code d'exploitation lançant du code arbitraire pour la vulnérabilité concernant `wwlib.dll` ne semble circuler sur l'Internet. Toutefois, l'existence de telles vulnérabilités impose à chacun une vigilance particulière lors de l'ouverture de documents sous Office 2007.

Les documents Office 2007 suspects ou ayant entraîné un comportement anormal peuvent être signalés au CERTA, afin de procéder à une analyse.

3 *FolderShare*

`FolderShare` est un service `Windows Live` qui permet d'accéder à distance aux fichiers contenus sur une machine et de les partager. Il agit en complément logiciel de `Microsoft Desktop Search`.

Le fonctionnement de `FolderShare` repose sur une authentification sur le site `http://www.foldershare.com` (couple adresse de messagerie/mot de passe). Il permet notamment de « synchroniser » (copier) et de partager des fichiers entre plusieurs ordinateurs. Il utilise le port 443/tcp (`HTTPS`) pour les communications.

Ce service pose de nombreux problèmes de sécurité :

- les informations transitent *a priori* par les serveurs de `FolderShare` et sortent donc du périmètre de sécurité. La confidentialité des données ne peut plus être assurée ;
- le fonctionnement de `FolderShare` repose sur l'utilisation de mots de passe qui sont éventuellement partagés entre plusieurs machines ;
- `FolderShare` accède aux fichiers dans le contexte de sécurité de l'utilisateur. Par conséquent, les fichiers ne sont plus protégés par le chiffrement EFS (*Encrypting File System*) ;
- un utilisateur de `FolderShare` aura accès à tous les fichiers de tous les ordinateurs participant au réseau de partage créé.

Microsoft a émis un bulletin de sécurité rappelant les bonnes pratiques quant à l'utilisation de `FolderShare`. En particulier, pour bloquer le trafic `FolderShare`, il faut filtrer les connexions à destination de la machine `redir1.foldershare.com` sur le port 443/tcp.

Documentation :

- Bulletin de sécurité Microsoft 925077 du 21 novembre 2006 :
  http://support.microsoft/kb/925077
- Note d'information du CERTA « Outils d'indexation et de recherche » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/
- Note d'information du CERTA « Les mots de passe » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/

4 Des documents corrompus qui trichent lors de la restauration

Plusieurs vulnérabilités ont affecté, et affectent encore certaines applications de bureautique. Pour les exploiter, il faut que l'utilisateur ouvre sur son poste de travail, avec l'application vulnérable, un document spécialement construit. Il peut l'avoir obtenu par différents moyens :

- téléchargement sur un site Web ;
- pièce jointe à un courrier électronique ;
- document récupéré depuis un support amovible (clé USB, disque dur externe, etc.).

Quand un tel document est ouvert, il provoque régulièrement une erreur de l'application. Cela peut être vu comme un effet secondaire de la compromission.

Certains codes malveillants actuels trichent à ce niveau, en profitant des fonctionnalités de restauration des applications. Quand la compromission a lieu, elle fait tout d'abord fermer inopinément l'application visée. Puis, dans un second temps, elle remplace le fichier malveillant par un autre inoffensif et contenant éventuellement des informations valables. La fonction de réparation ouvrira cette dernière version, et l'utilisateur ne comprendra pas que le document récemment ouvert a posé problème.

Néanmoins, dans plusieurs cas récemment rencontrés, le document qui sera réouvert peut avoir un nom différent (visible dans le titre de la fenêtre de l'application).

Un exemple de tel code malveillant est décrit à l'adresse suivante :
http://www.avertlabs.com/research/blog/?p=251

Il s'agit d'une méthode parmi d'autres pour essayer de dissimuler la présence de la compromission aux yeux de l'utilisateur. Il convient donc de prendre quelques précautions pour limiter ces risques :

- être méfiant vis-à-vis des documents transférés, en ne les obtenant que de sources de confiance ;
- utiliser des outils de sécurité pour vérifier si les documents échangés ne contiennent pas des éléments de signatures connues, comme par exemple :
  - un filtrage au niveau de la messagerie électronique
  - l'utilisation d'un antivirus à jour
- être circonspect concernant la fermeture inopinée d'une application, ou un comportement anormal de celle-ci ;
- regarder par curiosité les informations du document, comme son titre, qui peuvent changer.

5 *UPnP*

Le CERTA a publié cette semaine l'avis CERTA-2007-AVI-166 sur une vulnérabilité relative à la mise en œuvre du protocole `UPnP` dans Microsoft Windows. Ce protocole a pour but de faciliter l'échange d'informations entre différents équipements ou ordinateurs. En particulier, il permet de signaler les ressources partagées ou mises à disposition sur le réseau. Le support de ce protocole est souvent activé par défaut dans certains équipements communiquants comme des imprimantes en réseau, des `NAS` (espace de stockage en réseau) ou bien encore des routeurs. Ce protocole n'est en général pas indispensable au bon fonctionnement de ces différents équipements.

Dans ce contexte, une désactivation de ce protocole suppléée à une configuration manuelle mieux maîtrisable est donc plutôt recommandée.

Enfin, `UPnP` est un protocole transverse : c'est à dire qu'il peut se baser pour fonctionner avec plusieurs autres protocoles comme `SSDP` (1900/UDP), `Windows Media Connect` (10243/TCP) ou encore plus simplement `HTTP` (80/TCP). Il est donc recommandé de contrôler ces différents protocoles et de bien vérifier la politique de filtrage.

6 Remarque sur la gestion des favoris

Il est de bon usage de limiter le stockage intempestif d'informations personnelles sur l'ordinateur, suite à la navigation sur Internet. Les pratiques souvent mentionnées sont :

- l'effacement régulier de l'historique de navigation, voire une désactivation de ce dernier ;
- l'effacement des données entrées par certains formulaires. De manière générale, il ne faut pas que l'action de remplir un formulaire soit effectuée automatiquement par le navigateur ;
- nettoyer à chaque fermeture du navigateur les sessions d'identification et les *cookies*, et regarder leur contenu ;
- ne pas enregistrer de mots de passe dans le trousseau du navigateur ;

– vider le cache, ou ne pas utiliser cette fonctionnalité ;
– supprimer l'historique de téléchargement fourni par certains navigateurs ;
– etc.

Si la machine est accessible par plusieurs personnes, ou est compromise d'une certaine façon, il est préférable de limiter l'accès aux données personnelles liées à la navigation.

Un point est cependant fréquemment oublié. Il s'agit des `marque-pages`, ou `favoris`. L'utilisateur peut enregistrer, au cours de sa navigation l'adresse réticulaire (`URL`) d'une page visitée, afin de pouvoir rapidement y accéder ultérieurement. Le problème réside dans le fait que cette URL est souvent oubliée, au profit du nom associé à la page par l'utilisateur, et la gestion des liens dans les fichiers. L'`URL` peut cependant être de la forme :

– `Nom` : MonMoteur, `adresse` : http://www.SiteMonMoteurDeRecherche/maRecherche=info1
– `Nom` : MesMails, `adresse` : http://www.MonSiteDeMessagerie/login=info2&lang=fr
– `Nom` : MonSite, `adresse` : http://www.SiteQuelconque/script?param1=info3&param2=info4

Ce sont les URLs précédentes qui sont stockées sur le système, y compris les données `info1`, `info2`, `info3` ou `info4`. Il faut donc ajouter aux bonnes pratiques précédemment listées une vérification régulière des favoris enregistrés. Les navigateurs offrent les moyens de modifier les URLs enregistrées. Par exemple :

– Sous Firefox, « Marque-Pages », « Organiser les marque-pages... » : « Propriétés » de chaque entrée.
– Sous Internet Explorer, « Favoris », « Organiser les favoris... » : cliquer sur le lien à modifier avec le bouton droit de la souris, pour obtenir les propriétés.

7 Correctifs d'Oracle

Oracle a publié cette semaine sur son site Internet l'annonce de correctifs de sécurité, qui seront disponibles la semaine prochaine. Ces derniers devraient impliquer 37 vulnérabilités distinctes, et jugées critiques par l'éditeur. Ils concernent la plupart des produits, dont :

– Oracle Database : 13 vulnérabilités annoncées ;
– Oracle Application Server : 5 vulnérabilités annoncées ;
– Oracle Collaboration Suite : 1 vulnérabilité annoncée ;
– Oracle E-Business Suite and Applications : 11 vulnérabilités annoncées ;
– Oracle Enterprise Manager : 2 vulnérabilités annoncées ;
– Oracle PeopleSoft Enterprise et JD Edwards EnterpriseOne : 2 vulnérabilités annoncées.

L'adresse est la suivante :

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html

Le CERTA publiera la semaine prochaine un avis de sécurité concernant ces correctifs. Dans l'attente de ceux-ci, il est aussi recommandé de renforcer la vigilance concernant les applications impliquées, notamment par une analyse détaillée des journaux.

8 Microsoft Windows DEP

La Fonction `DEP` (`Data Execution Prevention` pour « prévention d'exécution de données » a été mise en place dans les systèmes Windows depuis le Service Pack 2 de Windows XP. Elle a pour but de prévenir l'exécution par l'ordinateur de zones en mémoire normalement allouées pour des données. En effet, il doit être anormal pour un système d'exploitation d'aller exécuter une zone prévue pour le stockage d'informations. Or, sur les processeurs de type `x86`, et jusqu'à un passé très récent, rien n'interdisait ce type d'opération. C'est typiquement ce défaut qui conférait un caractère relativement facile à l'exploitation de vulnérabilités de type « débordement de tampon ».

Pour combler ce manque de contrôle, Microsoft a donc mis en œuvre le système de `DEP`. Il utilise soit les fonctionnalités matérielles des derniers processeurs Intel ou AMD soit il émule celles-ci quand le processeur n'en est pas capable. Par défaut, cette fonctionnalité ne s'applique qu'aux composants Microsoft mais il est possible de l'activer pour tous les fichiers présents sur la machine. Microsoft signale tout de même que dans ce cas, certains logiciels pourront connaître des dysfonctionnements. Une documentation est disponible à l'adresse :

http://www.microsoft.com/france/technet/securite/prodtech/depcnfxp_PL.mspx

Celle-ci détaille les différentes façons de configurer `DEP`. Il est à noter que dans le cas de la vulnérabilité détaillée dans CERTA-2007-ALE-008 relative au fichier `ANI`, cette fonctionnalité aurait pu prévenir l'exécution arbitraire du code « embarqué » dans l'image. Cependant, ceci reste une solution imparfaite car il existe aujourd'hui des techniques éprouvées contournant ce type de protection.

9 Courriers malveillants...

Un envoi massif de courriers électroniques non sollicités porteurs de code malveillant est actuellement constaté par le CERTA, ainsi que certains éditeurs d'antivirus. En voici les détails des variantes, à la date de rédaction de ce bulletin :

Ce message se présente au destinataire après avoir usurpé le nom de l'expéditeur. Le message contient également deux pièces jointes ; un fichier image au format `GIF` et une archive au format ZIP. L'archive est protégée par un mot de passe qui se trouve dans le fichier image.

Les sujets utilisés par ce code malveillant sont les suivants :

- "Worm Alert!"
- "Worm Detected"
- "Virus Alert"
- "ATTN!"
- "Trojan Detected!"
- "Worm Activity Detected!"
- "Spyware Detected!"
- "Dream of You"
- "Virus Activity Detected!"

L'archive en pièce jointe est nommée de l'une des façon suivante :

- "patch-XXXXX.zip"
- "bugfix-XXXXX.zip"
- "hotfix-XXXXX.zip"
- "removal-XXXXX.zip"

La particularité de ce message électronique réside dans le fait qu'il protège son code malveillant dans une archive protégée, ce qui lui permet de contourner plusieurs analyses anti-virales des passerelles, tout en laissant la possibilité à la victime de décompresser l'archive et d'exécuter le code malveillant.

Toutes les informations concernant les bonnes pratiques liées à la messagerie, et permettant de se protéger de ce type de menace sont disponibles dans les documents suivants :

http://www.certa.ssi.gouv.fr/site/CERTA-2005-MEM-001.pdf
http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-007/index.html
http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-002/index.html

10 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 05 et le 12 avril 2007.

11 Liens utiles

- Mémento sur les virus :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
- Note d'information sur l'acquisition de correctifs :
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/index.html
- Note d'information sur les systèmes obsolètes :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html
- Note d'information sur les bonnes pratiques concernant l'hébergement mutualisé :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/index.html
- Note d'information sur les mots de passe :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html
- Note d'information sur la terminologie d'usage au CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/index.html
- Note d'information sur les enjeux de sécurité liés à une migration vers IPv6 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/index.html

- 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 CERTA-2006-INF-006, Risques associés aux clés USB : http://www.certa.ssi.gouv.f r/site/CERTA-2000-INF-006/
- Note d'information du CERTA CERTA-2006-INF-009 sur les outils d'indexation et de recherche : http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/
- Note d'information du CERTA CERTA-2007-INF-001 sur la gestion des noms de domaine : http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/
- Note d'information sur le bon usage de PHP : http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002

12 Rappel des avis émis

Durant la période du 06 au 12 avril 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-163 : Vulnérabilité dans Symantec Enterprise Security Manager
- CERTA-2007-AVI-164 : Multiples vulnérabilités dans SAP RFC Library
- CERTA-2007-AVI-165 : Vulnérabilités dans Microsoft Content Management Server (CMS)
- CERTA-2007-AVI-166 : Vulnérabilité dans le service UPnP de Microsoft Windows
- CERTA-2007-AVI-167 : Vulnérabilité de Microsoft Agent dans Windows
- CERTA-2007-AVI-168 : Multiples vulnérabilités de CSRSS dans Microsoft Windows
- CERTA-2007-AVI-169 : Vulnérabilité dans le noyau de Microsoft Windows

Pendant la même période, l'avis suivant a été mis à jour :

- CERTA-2007-AVI-068-001 : Multiples vulnérabilités de Samba
  (ajout des références aux bulletins de sécurité de Ubuntu, Mandriva, HP-UX, Gentoo, et SuSE)

13 Actions suggérées

13.1 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'inf ormation de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'orga nisme 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.

13.2 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 œuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

13.3 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.

13.4 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.

13.5 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 COSSI/CERTA peut vous aider dans ce travail d'analyse.

13.6 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.

13.7 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.formation.ssi.gouv.fr

14 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.

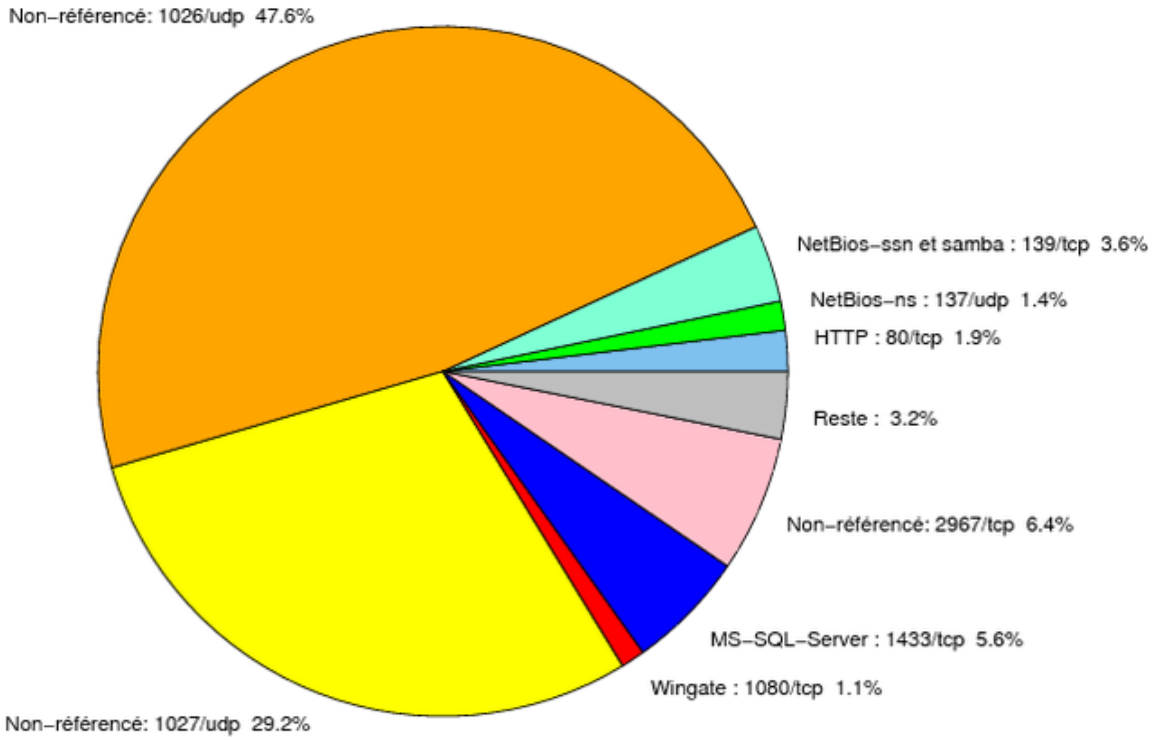

FIG. 1: Répartition relative des ports pour la semaine du 05.04.2007 au 12.04.2007

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CE
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
106	TCP	MailSite Email Server	–	–
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CE
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CE
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CE
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE

				http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CE
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CE
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CE
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CE
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CE
2381	TCP	–	HP System Management	http://www.certa.ssi.gouv.fr/site/CE
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CE
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CE
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CE
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CE
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
10080	TCP	Amanda	MyDoom	–
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CE
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CE

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

port	pourcentage
1026/udp	47.62
1027/udp	29.22
2967/tcp	6.39
1433/tcp	5.59
139/tcp	3.62
80/tcp	1.9
137/udp	1.36
1080/tcp	1.12
1434/udp	0.85
4899/tcp	0.68
22/tcp	0.34
3128/tcp	0.29
3306/tcp	0.15
15118/tcp	0.13
21/tcp	0.1
2100/tcp	0.09
443/tcp	0.07
143/tcp	0.02
9898/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

13 avril 2007 version initiale.