Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 mars 2008
N° CERTA-2008-ACT-013

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-13

Gestion du document

Référence	CERTA-2008-ACT-013
Titre	Bulletin d'actualité 2008-13
Date de la première version	28 mars 2008
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-2008-ACT-013.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-2008-ACT-013/

1 Incidents de la semaine

1.1 Journaux d'administration et gestion des incidents

Le CERTA a traité cette semaine un incident lié à l'indisponibilité d'un serveur web pendant une période relativement longue. Une hypothèse envisageable est celle d'un dysfonctionnement au niveau du réseau. Malheureusement, l'administrateur n'a, à sa disposition, que les traces suivantes :

– les graphes de l'occupation de la bande passante, construits à partir d'un échantillonnage effectué toutes les dizaines de minutes par flux ;
– les données ponctuelles de l'état du système, fournies par l'utilitaire `sysstat` installé sur les machines.

Ces traces sont intéressantes dans le cadre de l'administration, afin de détecter une surcharge éventuelle des « tuyaux » ou un dysfonctionnement matériel (surchauffe, panne matériel, etc.).

Cependant, dans le cas présent, il s'agit des seuls journaux à disposition pour traiter l'incident. Cela est clairement insuffisant, car ils ne permettent pas de comprendre le problème. D'une part ceux-ci sont déjà une interprétation de données brutes indisponibles, mais ils ne permettent également pas de comprendre les dysfonctionnements réseau ou applicatifs.

Il est important de ne pas confondre des traces indicatives pour la maintenance opérationnelle d'un réseau, et la politique de journalisation, qui doit, elle, être la plus complète et la plus rigoureuse possible afin de traiter au mieux un incident. Dans le cas contraire, les problèmes seront difficilement expliqués s'ils sont déjà détectés.

1.2 Détournement des outils de statistique

Certains sites Internet laissent volontairement ou non l'accès aux pages de leurs outils de statistiques. La plupart de ces outils (exemple : *Webalyzer*) permettent, dans leur configuration par défaut, d'afficher les adresses réticulaires (*URL*) référençant le site web. Ces informations, et bien d'autres, sont collectées par le serveur web lors de l'arrivée d'un visiteur provenant d'un site référant.

Certains individus malintentionnés se servent de cette fonctionnalité pour promouvoir leur site et améliorer leur référencement dans les moteurs de recherche. Ces derniers référençant les pages des outils de statistiques deviennent alors la cible de programmes automatisés recherchant les sites utilisant des outils de statistiques connus. Sur chaque site retourné, le programme va ensuite engendrer un nombre important de requêtes bien souvent erronées mais avec un champ *Referer* spécifiquement construit.

Voici un exemple d'un tel comportement dans un journal de connexions `Apache` ; il peut y avoir plusieurs centaines de ces lignes par seconde. Dans cet exemple, l'adresse IP malveillante cherche à promouvoir un site pour adulte :

```
<IP malveillante> - - [20/Mar/2008:18:01:00 +0001] "POST / HTTP/1.1" 404
301 "<URL d'un site pour adulte>" "Mozilla/5.0 (X11; U; Linux i686;
en-US; rv:1.2.1) Gecko/20021204"
<IP malveillante> - - [20/Mar/2008:18:01:00 +0001] "POST / HTTP/1.1" 404
301 "<URL d'un site pour adulte>" "Mozilla/5.0 (X11; U; Linux i686;
en-US; rv:1.2.1) Gecko/20021204"
<IP malveillante> - - [20/Mar/2008:18:01:00 +0001] "POST / HTTP/1.1" 404
301 "<URL d'un site pour adulte>" "Mozilla/5.0 (X11; U; Linux i686;
en-US; rv:1.2.1) Gecko/20021204"
<IP malveillante> - - [20/Mar/2008:18:01:00 +0001] "POST / HTTP/1.1" 404
301 "<URL d'un site pour adulte>" "Mozilla/5.0 (X11; U; Linux i686;
en-US; rv:1.2.1) Gecko/20021204"
<IP malveillante> - - [20/Mar/2008:18:01:00 +0001] "POST / HTTP/1.1" 404
301 "<URL d'un site pour adulte>" "Mozilla/5.0 (X11; U; Linux i686;
en-US; rv:1.2.1) Gecko/20021204"
```

Les outils d'analyse présenteront alors l'adresse réticulaire (*URL*) ci-dessus dans la liste des meilleurs adresses référençant le site web. Cette liste étant également indexée dans les moteurs de recherche, les sites envoyés par ces programmes automatisés voient leur référencement et leur notation augmenter dans les moteurs de recherche.

Pour éviter de contribuer à ce genre de comportement le CERTA recommande :

- de ne pas mettre les outils de statistiques sur des serveurs externes, d'autres informations pouvant être exploitées à l'insu des internautes ;
- de limiter l'accès aux pages de statistiques ;
- d'interdire le référencement de ces pages à l'aide d'un fichier *robots.txt* ;
- de configurer l'outil de statistiques pour ne pas afficher d'information sur les liens référants.

1.3 Un nettoyage presque parfait

Cette semaine, le CERTA a participé au traitement d'un incident relatif à la compromission d'un serveur web. Suite à la découverte d'un site de *phishing* déposé sur un serveur compromis, le CERTA a contacté l'administrateur de ce serveur afin qu'il prenne les mesures nécessaires pour interdire l'accès aux pages frauduleuses. L'administrateur a immédiatement empêché l'accès aux fichiers signalés par le CERTA afin de limiter le nombre de victimes potentielles de cet incident. Cette mesure n'était pas suffisante car les attaquants avaient également déposé un fichier dont le nom n'attirait pas l'attention. Le but de ce fichier, qui ne contenait qu'une seule ligne de code, était de rediriger les victimes vers un autre site malveillant situé dans un autre pays.

Le CERTA rappelle que lors d'une compromission, quelle qu'elle soit, il convient de repartir sur des bases saines en appliquant les recommandations de la note d'information sur les bon réflexes en cas d'intrusion sur un système d'information. Les nettoyages rapides et manuels risquent de ne pas être exhaustifs, de perturber une analyse postérieure et de laisser des portes dérobées, des traces ou bien encore des signatures pour les attaquants.

Documentation

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

2 Configuration de PHP

Le CERTA revient cette semaine sur la configuration de PHP et plus particulièrement sur la variable `expose_php`. La recherche de vulnérabilité étant de plus en plus automatisée, il est important de limiter les informations directement accessibles depuis l'Internet qui décrivent le système . Cette variable permet de contrôler les détails transmis par PHP en réponse à toutes les requêtes et elle est configurable dans le fichier `php.ini`.

Dans l'exemple suivant le fichier inexistant *inexistant.html* est demandé. Avec la configuration par défaut (`expose_php=On`) on obtient la réponse suivante :

```
Not Found
The requested URL /inexistant.html was not found on this server.
Apache/2.2.3 (Debian) PHP/5.2.0-8+etch5~pu1 Server at localhost Port 80
```

En désactivant cette variable (`expose_php=Off`) on obtient la réponse suivante :

```
Not Found
The requested URL /inexistant.html was not found on this server.
Apache/2.2.3 (Debian) Server at localhost Port
```

Dans le premier cas, la simple demande d'un fichier *html* permet de savoir si `PHP` est installé ainsi que sa version. Il est intéressant de remarquer que cette variable contrôle aussi l'accès aux données cachées par les développeurs (*easter egg*) telles que les remerciements, accessibles en passant l'argument "?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000" à n'importe quel fichier PHP existant.

2.1 Conclusion

Transmettre des informations concernant la présence de logiciels et leur numéro de version est un élément important dans la recherche de vulnérabilités. Afin de limiter ce type de divulgation, le CERTA recommande de désactiver cette variable.

Documentation

– Note d'information CERTA-2007-INF-002, « Du bon usage de PHP » :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/

3 iTunes et mise à jour

Avec la dernière version de `Apple iTunes` pour `Microsoft Windows`, le système de mise à jour de la suite `iTunes et Quicktime` installera en plus par défaut le navigateur `Safari 3.1`. Le propos ici n'est pas de qualifier la qualité du dernier navigateur de `Apple` mais plutôt de s'interroger sur la pertinence d'une telle mise à jour. En effet, nous ne sommes pas, dans le cas présent, face à une correction de faille mais plutôt dans l'installation d'un logiciel supplémentaire optionnel. Il n'est pas essentiel de disposer de `Safari` pour écouter de la musique avec `iTunes`. Le problème n'est pas forcément la qualité du navigateur et, au contraire, il participerait plutôt à la diversité des logiciels de navigation. Mais l'installation d'un logiciel supplémentaire qui n'est pas désiré ne fait qu'accroître la surface d'attaque du système.

Recommandations :

Cette mise à jour lors de l'avertissement d'installation peut être tout à fait décochée pour que `Safari` ne soit pas installé. Si vous ne voulez pas utiliser ce navigateur, il est donc inutile de l'ajouter au nombre des logiciels à mettre à jour.

4 La méthode *TRACE*

4.1 Rappel sur la méthode

La méthode *TRACE* est définie dans le standard *RFC* 2616 définissant le protocole *HTTP/1.1*. Elle permet de journaliser les requêtes envoyées par un client à un serveur web et les réponses envoyées par ce dernier au client. Ainsi, la réponse à une requête TRACE contient en corps de message la requêtes initiale reçue par le serveur. Cette méthode est autorisée par défaut et est très utile pour effectuer des tests et corriger des erreurs lors du développement d'applications web.

http://www.ietf.org/rfc/rfc2616.txt

Pour vérifier si la méthode est activée :

```
$telnet LeSiteCible.tld

TRACE / HTTP/1.0
Host : test
A: toto
B: titi

HTTP/1.1 200 OK
Date Fri, 28 Mar 2008 10:40:24 GMT
Server: Apache
Connection: close
Content-Type: message/http

TRACE / HTTP/1.0
  Host : test
  A: toto
  B: titi
```

Les valeurs de la requêtes « toto » et « titi » sont inclus dans la réponse du serveur.

4.2 Les risques

Il est possible de dérober des données de session en forçant l'utilisateur à utiliser la méthode TRACE vers un site cible. Ces données peuvent être relatives aux *cookies*, à l'authentification, à la référence du navigateur...

Via des scripts, il est donc possible de récupérer ces informations outrepassant les politiques de restriction des domaines. Si un utilisateur visite des pages malveillantes, il peut être amené à charger ce type de script et ainsi dévoiler à son insu des données sensibles le concernant. Plusieurs scanners de vulnérabilités de sites web testent par défaut si cette méthode est autorisée. De plus ces tentatives ne sont pas toujours visibles dans les journaux applicatifs.

4.3 Les recommandations

Afin de limiter les risques liés à cette méthode, le CERTA recommande de :

- désactiver ou ne pas autoriser les requêtes utilisant la méthode *TRACE* sur les serveurs de production et plus généralement lorsqu'elles ne sont pas nécessaires ;
  - pour apache, il faut ajouter la directive suivante dans le fichier de configuration :

    ```
    TraceEnable "Off"
    ```
  - pour IIS, il faut filtrer les requêtes utilisant TRACE via URLScan.
- désactiver dans le navigateur l'exécution de scripts dynamiques ActiveX, *JavaScript*, *Flash*, *Java*, *VBScript*, etc.

5 Vulnérabilité sur Microsoft Jet Database Engine

5.1 Présentation

Cette semaine, le CERTA a publié l'alerte CERTA-2008-ALE-005 concernant une vulnérabilité dans *Microsoft Jet Database Engine*.

En réalité, cette vulnérabilité de type débordement de mémoire était déjà connue et c'est seulement le vecteur d'attaque qui est nouveau. Les fichiers `mdb` sont en effet considérés comme non sûrs (au même titre que les fichiers exécutables), et l'exécution possible de code à leur ouverture est de toute façon - qu'il y ait une vulnérabilité ou non - reconnue par l'éditeur. Toutefois, dans le cas de cette alerte, c'est via l'ouverture d'un fichier `doc` que se fait l'exécution de code : le fichier *Word* ouvre à son tour le fichier `mdb` en utilisant la librairie `msjet40.dll` vulnérable.

Des cas d'exploitation ont été rapportés, ce qui a poussé le CERTA à publier une alerte. Ces exploitations reposent principalement sur le schéma suivant : la réception par courriel d'une archive `zip` contenant, dans un répertoire, un fichier `doc` et un fichier `db` (`mdb` renommé). L'ouverture du fichier `doc` provoque l'exécution de code arbitraire.

Le principal contournement est la désactivation de *Microsoft Jet Database Engine* en exécutant la commande suivante :

```
echo y| cacls "%SystemRoot%\system32\msjet40.dll" /E /P everyone:N
```

Ceci a pour effet de restreindre l'accès au fichier `msjet40.dll` à tout le monde.

La commande suivante remet les droits par défaut :

```
echo y|cacls "%SystemRoot%\system32\msjet40.dll" /E /R everyone
```

Les autres contournements sont plus ordinaires :

- utiliser un compte aux droits restreints ;
- utiliser un logiciel de traitement de texte alternatif ;
- n'ouvrir que des documents de confiance ;
- être circonspect à l'égard des pièces jointes de courriels.

Les systèmes d'exploitation *Windows Server 2003 Service Pack 2*, *Windows Vista* et *Windows Vista Service Pack 1* ne sont pas concernés par cette vulnérabilité car ils ont une nouvelle version de *Microsoft Jet Database Engine* (supérieure à 4.0.9505.0). Toutes les versions de *Word 2000* à *Word 2007 Service Pack 1* semblent touchées.

5.2 Documentation

- Alerte CERTA-2008-ALE-005 du 25 mars 2008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-005/

6 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 20 et le 27 mars 2008.

7 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/

8 Rappel des avis émis

Dans la période du 21 au 27 mars 2008, le CERTA a émis les avis suivants :

– CERTA-2008-AVI-151 : Vulnérabilité dans HP-UX StorageWorks
– CERTA-2008-AVI-152 : Multiples vulnérabilités dans WinRAR
– CERTA-2008-AVI-153 : Vulnérabilité dans bzip2
– CERTA-2008-AVI-154 : Multiples vulnérabilités dans Kerberos
– CERTA-2008-AVI-155 : Multiples vulnérabilités dans IBM Informix Dynamic Server
– CERTA-2008-AVI-156 : Vulnérabilité dans CUPS
– CERTA-2008-AVI-157 : Vulnérabilité dans VLC
– CERTA-2008-AVI-158 : Vulnérabilité dans Apple Aperture/iPhoto
– CERTA-2008-AVI-159 : Vulnérabilité de Novell eDirectory
– CERTA-2008-AVI-160 : Vulnérabilités dans Firefox
– CERTA-2008-AVI-161 : Vulnérabilité dans AirPort Extreme Base Station
– CERTA-2008-AVI-162 : Vulnérabilités dans MySQL
– CERTA-2008-AVI-163 : Multiples vulnérabilités dans Cisco IOS
– CERTA-2008-AVI-164 : Vulnérabilité dans Novell eDirectory

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

– CERTA-2008-AVI-108-001 : Vulnérabilités dans Wireshark
(ajout des références aux bulletins de sécurité Gentoo, Mandriva et SuSE)
– CERTA-2008-AVI-153-001 : Vulnérabilité dans bzip2
(ajout des références aux bulletins de sécurité Mandriva et Ubuntu)
– CERTA-2008-AVI-154-001 : Multiples vulnérabilités dans Kerberos
(ajout des références aux bulletins de sécurité Gentoo, Debian et Mandriva)
– CERTA-2008-AVI-156-001 : Vulnérabilité dans CUPS
(ajout d'une référence CVE et de références aux bulletins de distributions Linux)
– CERTA-2008-AVI-160-001 : Vulnérabilités dans Firefox
(ajout des bulletins de sécurité Ubuntu et Red Hat)

9 Actions suggérées

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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.

9.6 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.

9.7 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

10 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.

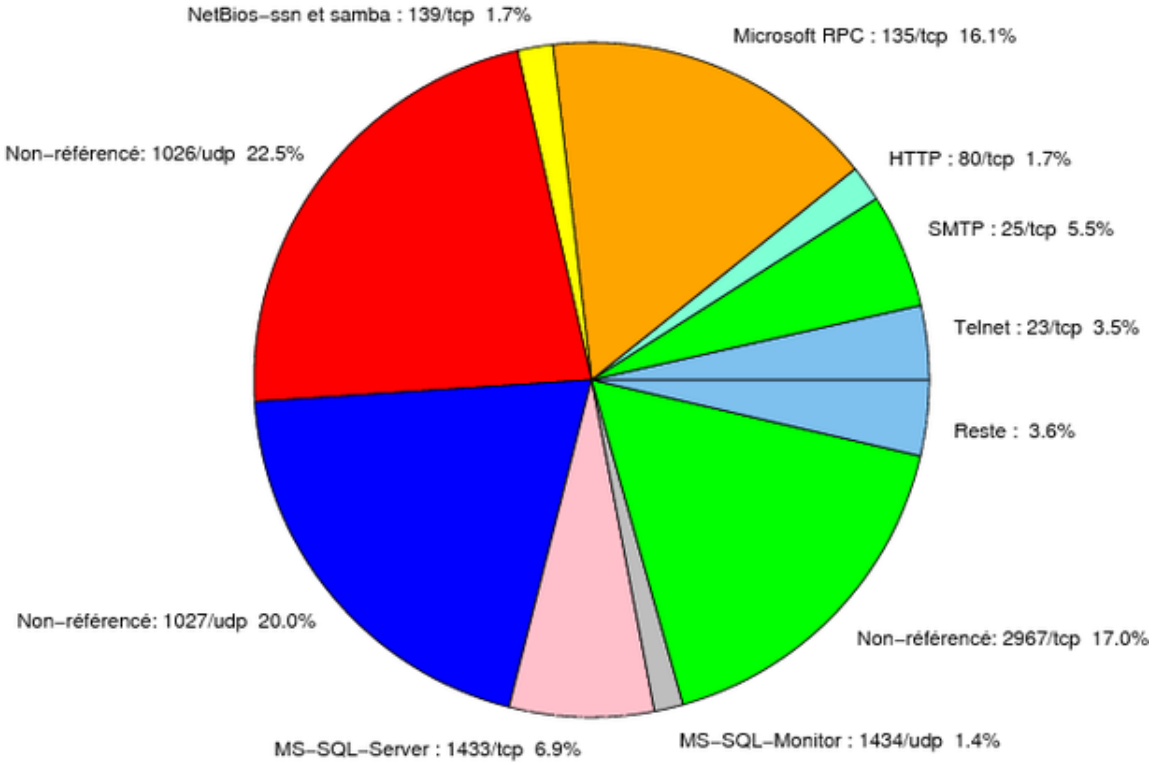

FIG. 1: Répartition relative des ports pour la semaine du 20.03.2008 au 27.03.2008

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

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

port	pourcentage
1026/udp	22.5
1027/udp	20.03
2967/tcp	17
135/tcp	16.09
1433/tcp	6.92
25/tcp	5.47
23/tcp	3.54
80/tcp	1.77
139/tcp	1.69
1434/udp	1.38
22/tcp	0.96
4899/tcp	0.66
445/tcp	0.6
21/tcp	0.54
3306/tcp	0.43
137/udp	0.29
143/tcp	0.13
1080/tcp	0.04
2100/tcp	0.03
3128/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

28 mars 2008 version initiale.