Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 mars 2007
N° CERTA-2007-ACT-013

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-13

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-2007-ACT-013`

Gestion du document

Référence	CERTA-2007-ACT-013
Titre	Bulletin d'actualité 2007-13
Date de la première version	30 mars 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-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-2007-ACT-013/

1 Activités en cours

1.1 Alerte CERTA-2007-ALE-008 sur Windows Explorer

Le CERTA a publié jeudi une alerte concernant Microsoft Windows. Elle concerne notamment les fichiers de rendu animé des curseurs (format `.ani`), qui peuvent être imposés lors de la navigation sur certains sites ou à l'ouverture d'un courrier électronique au format HTML. Les informations détaillées sont fournies dans l'alerte, ainsi que quelques contournements provisoires.

Cette vulnérabilité est exploitable par des applications largement déployées, et ne nécessite aucune action particulière de l'utilisateur. Le CERTA invite donc vivement ses correspondants à prendre connaissance du problème.

1.2 Importance du *Google hacking*

L'analyse par le CERTA d'un serveur Web compromis montre la multitude d'intrusions et de tentatives dont le site a été victime. Les intrusions ne ciblaient pas le site en particulier mais relèvent plus d'une technique opportuniste. En d'autres termes, l'analyse a montré l'importance des moteurs de recherche dans la quête de sites vulnérables par des personnes malveillantes.

Les constatations sont les suivantes :

Les informations sur le manque de robustesse de l'application `PhpmyBibli` (ou `PMB`) qui circulent sur l'Internet sont accompagnées de moyens de détection de cibles potentielles. La détection consiste à faire des requêtes particulières sur des moteurs de recherche. Cette méthode est très prisée par les délinquants de l'Internet et peut être utilisée avec le moteur de recherche `Google`, d'où son nom, le *Google hacking*. Elle tire partie de certaines fonctionnalités offertes pour aider les recherches, en ajoutant des opérations de filtrage telles que :

- limiter la recherche à certains sites (opérateur `site:` sous Google) ;
- limiter la recherche aux pages contenant dans leur adresse réticulaire certaines chaînes de caractères (opérateurs `inurl:` et `allinurl` sous Google) ;
- limiter la recherche à certains types de fichiers (opérateur `filetype:` sous Google) ;
- limiter la recherche au contenu texte des pages Web (opérateur `intext:` et `allintext:` sous Google) ;
- etc.

C'est avec cette méthode que la plupart des intrus ont été identifiés dans le cas de l'incident traité. Un des problèmes de `PMB` concernait une page particulière dans un répertoire nommé `opac_css`. Le journal des connexions inscrit tout naturellement la recherche adressée au moteur dans le champ *referer*.

La requête la plus courante est reproduite ci-dessous :

```
http://www.google.*/search?q=allinurl:opac_css&hl=*&lr=&start=10&...
```

Les étoiles remplacent les indications de pays dans le nom du site *Google* utilisé et dans le paramètre `hl` qui est la langue utilisée. La valeur 10 du paramètre `start` permet de déduire que le site ciblé apparaît sur la deuxième page de réponse du moteur.

Ces requêtes ont permis à 45 intrus de se diriger sur le site en l'espace de deux jours.

Voici pour résumé le cheminement des actions :

1. une personne publie sur l'Internet une vulnérabilité concernant `PMB`. Elle donne les détails, et notamment l'information que `PMB` est souvent identifiable sur un site par l'existence d'un répertoire `opac_css`.
2. des personnes voulant exploiter cette vulnérabilité cherchent des sites utilisant `PMB`. Elles utilisent pour cela les méthodes de recherche précédemment citées, et obtiennent une liste de sites « candidats ».
3. les journaux de ces sites peuvent contenir les traces, dans le champ HTTP `referer` de telles requêtes ayant conduit à accéder aux pages hébergées. Dans le cas de l'incident traité, et deux jours après la publication de la vulnérabilité, les requêtes émises depuis 45 adresses IPs distinctes possèdaient cette caractéristique.

Recommandations du CERTA

Il n'est pas simple d'éviter ce genre d'activité. Une bonne pratique, en revanche, serait, pour l'administrateur, d'avoir conscience des informations qui peuvent être accessibles par de telles requêtes et concernant son site. Il est aussi possible de s'adresser aux moteurs de recherche, pour leur demander de retirer certaines données indexées. Par exemple, sous Google, cela peut se faire via l'adresse :

http://www.google.com/remove.html

Il est important de maintenir certaines bonnes pratiques :

- mettre à jour les applications Web utilisées ;
- éviter de garder toutes les configurations par défaut (noms de fichiers, noms de variables, chemins d'accès) ;
- désactiver les fonctions dangereuses, comme le parcours des répertoires (*directory browsing*).

2 Administrations des forums et des bloc-notes

Le CERTA a mentionné dans son précédent bulletin d'actualité (CERTA-2007-ACT-012) que le fonctionnement des publicités Web envahissantes (*web spamming*) était un phénomène réel, et bien organisé. Certains groupes d'individus se chargent ainsi de diffuser l'information, en maintenant par exemple une liste d'endroits où les liens publicitaires peuvent être affichés.

Voici quelques exemples possibles :

- les bloc-notes permettent souvent aux lecteurs de formuler des commentaires. Le message publicitaire peut donc envahir ceux-ci ;
- les forums permettent à chacun de participer aux conversations, et donc d'insérer liens et messages publicitaires ;

– certains sites Web sont suffisamment permissifs pour permettre à des personnes d'insérer (de façon légitime ou pas) des images ou des documents. Cette permissivité est ensuite utilisée pour y déposer des données publicitaires ;
– etc.

Les impacts sont variés. Outre la mauvaise image que cela peut apporter au site, voire à l'institution elle-même, il existe quelques aspects légaux qu'il faut prendre en considération. Sans avoir la prétention de fournir tous les éléments, voici les grandes lignes des problèmes rencontrés :

– le site/forum/bloc-notes sert à diffuser des messages violents, pornographiques qui ne devraient pas être vus ou perçus par des mineurs ;
– le site/forum/bloc-notes sert à inciter à la diffamation, la discrimination ou la haine.
– le site/forum/bloc-notes sert à l'apologie ou la contestation de crimes graves (contre l'Humanité).
– le site/forum/bloc-notes est un moyen de provocation de crime ou de délit par voie écrite et publique.
– le site/forum/bloc-notes peut servir de diffusion de pornographie enfantine ou de procédés de fabrication d'explosifs.
– le site/forum/bloc-notes peut provoquer les mineurs à la consommation de stupéfiants.

Il ne s'agit pas de restreindre la liberté d'expression , mais tous ces points peuvent être considérés comme des infractions et doivent donc être pris avec le plus grand sérieux.

Recommandations

Quelques bonnes pratiques peuvent éviter au site, ou forum, ou bloc-notes, de diffuser de l'information douteuse :

– n'utiliser ces applications que si elles sont nécessaires, et pas pour un unique but cosmétique du site ;
– maintenir à jour les applications utilisées ;
– consulter régulièrement les messages qui circulent, et réguler les informations qui y sont déposées (désigner un ou plusieurs modérateurs);
– utiliser des règles simples en fonction des utilisations, comme bloquer les adresses réticulaires (URLs) si elles ne sont pas indispensables ou restreindre l'insertion d'images ;
– etc.

3 Problèmes sur Windows Vista

3.1 Vulnérabilité dans Windows Mail

Windows Mail est l'application de courrier électronique, qui remplace Outlook Express et qui est installée par défaut sur Microsoft Windows Vista.

Récemment, une vulnérabilité non corrigée a été identifée sur Windows Mail, permettant à une personne malintentionnée d'exécuter certains fichiers présents sur l'ordinateur de la victime. Ceci nécessite une action de l'utilisateur, qui doit cliquer sur un lien dans le courrier électronique qui pointe sur le fichier local à exécuter. Le fichier local doit cependant vérifier certains prérequis pour être directement exécutable.

Cette vulnérabilité n'est pas critique, mais montre une fois de plus qu'il est important de vérifier et de taper manuellement les liens contenus dans les courriers électroniques.

3.2 Problèmes recontrés lors de copies de fichiers

Certains utilisateurs de Windows Vista ont rencontré des problèmes lors de la copie de fichiers anodins depuis ou vers leur disque dur. Le problème a été reconnu par Microsoft qui propose un correctif après avoir pris contact auprès de leur support technique. Certains symptômes de ce problème sont une lenteur anormale ou surtout un blocage du processus de copie (avec un temps restant nul).

Il est recommandé de n'appliquer ce correctif que si des problèmes de ce type ont été rencontrés. Une version officielle de celui-ci (*hotfix*) devrait être disponible dans le premier *service pack* de Windows Vista.

3.3 Liens utiles

– Article 931770 de la base de connaissances Microsoft :
http://support.microsoft.com/kb/931770/en-us

4 Les moteurs d'antivirus

Choisir un outil de sécurité n'est pas chose aisée. Plusieurs paramètres font pencher la balance vers un éditeur plutôt qu'un autre : certification (CC), performance, confiance envers le pays de l'éditeur, maintenance, ... Parfois, même, il est de bon ton d'accumuler des équipements et des technologies variés, suivant le principe de défense en profondeur.

Cependant, l'opacité des produits fait qu'il est difficile de s'apercevoir des liens étroits entre un éditeur à qui on accorde sa confiance, et un autre qui n'a pas la même faveur. Par exemple, plusieurs antivirus utilisent un moteur développé, maintenu et enrichi par d'autres éditeurs. Ceci pose plusieurs problèmes :

- confiance envers l'éditeur du moteur ,
- répercution de vulnérabilités et problèmes de mise à jour de base de signature ,
- monoculture allant à l'encontre du principe de défense en profondeur
- ...

Ainsi, le CERTA tient à rappeler qu'il est fortement recommandé de se renseigner sur les fonctionnalités sous-jacente d'un logiciel ou d'un matériel informatique avant de lui accorder sa confiance.

5 Virus IE7.0.exe

Depuis le 29 mars 2007, un pourriel, ou *spam*, circule sur l'Internet. Ce *spam*, se faisant passer pour microsoft (le champ indiquant la source d'émission `from` est : `admin[at]microsoft[dot]com`), est construit afin de faire croire à l'utilisateur qu'une mise à jour d'Internet Explorer 7 est disponible. En réalité, le lien contenu dans le courrier électronique renvoie vers un certain nombre de sites hébergeant un exécutable nommé IE7.0.exe.

Cet exécutable est en fait un code malveillant. Une fois exécuté, ce code se réplique sur le système en :

- se recopiant dans

  `\%temp%\winlogon.exe`

- ajoutant la valeur "Firewall auto setup =

  `\%temp%\winlogon.exe"`

  dans la clef

  `HKCU\Software\Microsoft\CurrentVersion\Run`

De plus, ce code malveillant embarque des fonctions de type `Rootkit`, permettant de dissimuler son activité propre sur la machine infectée.

Même si ce code est déjà reconnu par certains antivirus, le CERTA insiste sur le fait que, comme d'habitude, ce code utilise "le clic facile" comme moyen d'infection. Microsoft (comme beaucoup d'autres éditeurs de logiciels) n'envoie en aucun cas ses mises à jour par l'intermédiaire d'un courrier électronique. Il convient donc de supprimer tous les messages invitant à ce genre d'actions.

6 Vulnérabilité dans le protocole WPAD sous Windows

Un poste client peut être configuré pour utiliser le protocole `WPAD` (*Web Proxy Automatic Discovery*) pour obtenir automatiquement un serveur mandataire `HTTP` (*proxy Web*). Dans ce cas, la machine cherche à contacter un hôte qui possède le fichier de configuration `wpad.dat`. Il existe plusieurs méthodes pour rechercher un tel hôte, parmi lesquelles deux reposent sur l'utilisation du `DNS` et de `WINS`.

Le protocole `WPAD` peut être détourné à des fins malveillantes en ajoutant un nom d'hôte *WPAD* dans le serveur `DNS` ou le serveur `WINS`. Cette manipulation est particulièrement accessible aux utilisateurs du réseau interne. Le principe de cette attaque est de proposer par la suite un fichier `wpad.dat` configuré pour router le trafic `HTTP` vers un serveur malveillant.

Microsoft propose un palliatif : il s'agit d'entrer manuellement le nom d'hôte *WPAD* de façon statique dans le serveur `DNS` et/ou le serveur `WINS`. Cette manipulation est décrite dans l'article 934864 de *Microsoft*, disponible à l'adresse :

http://www.microsoft.com/kb/934864

7 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 22 et le 29 mars 2007.

8 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

9 Rappel des avis émis

Durant la période du 23 au 29 mars 2007, le CERTA a émis l'alerte suivante :

- CERTA-2007-ALE-008 : Vulnérabilité dans Microsoft Windows

Pendant la même période, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-138 : Vulnérabilité dans file
- CERTA-2007-AVI-139 : Vulnérabilité de la bibliothèque ZZIPlib
- CERTA-2007-AVI-140 : Vulnérabilité dans HP OpenView Network Node Manager
- CERTA-2007-AVI-141 : VulnÃérabilité dans les téléphones CISCO 7940/7960
- CERTA-2007-AVI-142 : Vulnérabilités dans OpenAFS
- CERTA-2007-AVI-143 : Vulnérabilité dans Squid
- CERTA-2007-AVI-144 : Multiples vulnérabilités dans PHP
- CERTA-2007-AVI-145 : Vulnérabilité dans Evolution
- CERTA-2007-AVI-146 : Vulnérabilité dans Firefox
- CERTA-2007-AVI-147 : Vulnérabilité dans ulogd
- CERTA-2007-AVI-148 : Multiples vulnérabilités dans IBM Lotus Domino
- CERTA-2007-AVI-149 : Vulnérabilité de LDAP Account Manager
- CERTA-2007-AVI-150 : Vulnérabilités dans Cisco Unified CallManager et Presence Server

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

- CERTA-2007-AVI-020-003 : Multiples vulnérabilités dans Fetchmail
  (ajout des références aux bulletins de sécurité Debian et SuSE)
- CERTA-2007-AVI-056-006 : Vulnérabilité du serveur DNS BIND
  (ajout de la référence au bulletin de sécurité Avaya)
- CERTA-2007-AVI-069-002 : Multiples vulnérabilités sous PostgreSQL
  (ajout des références aux bulletins de sécurité Debian, Gentoo, Mandriva, Red Hat, Ubuntu et Avaya)
- CERTA-2007-AVI-102-003 : Multiples vulnérabilités de produits Mozilla
  (ajout des références aux mises à jour de sécurité Ubuntu, Gentoo, SuSE, Mandriva, Red Hat)
- CERTA-2007-AVI-108-001 : Vulnérabilité dans Apache Tomcat
  (ajout de la référence au bulletin de sécurité Gentoo)
- CERTA-2007-AVI-111-001 : Vulnérabilité de Webcalendar
  (ajout de la référence CVE et du bulletin de sécurité Debian)
- CERTA-2007-AVI-114-002 : Vulnérabilité dans GnuPG
  (ajout des références aux bulletins de sécurité Ubuntu et Debian)
- CERTA-2007-AVI-135-001 : Vulnérabilités dans libwpd
  (ajout des références aux bulletins de sécurité Debian, SuSE, Ubuntu)
- CERTA-2007-AVI-136-002 : Multiples vulnérabilités dans OpenOfficeorg
  (ajout de référence au bulletin de sécurité Ubuntu.)
- CERTA-2007-AVI-137-001 : Vulnérabilité de Zope
  (correction de la version affectée)

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'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.

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 œuvre (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 COSSI/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 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.

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.formation.ssi.gouv.fr

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.

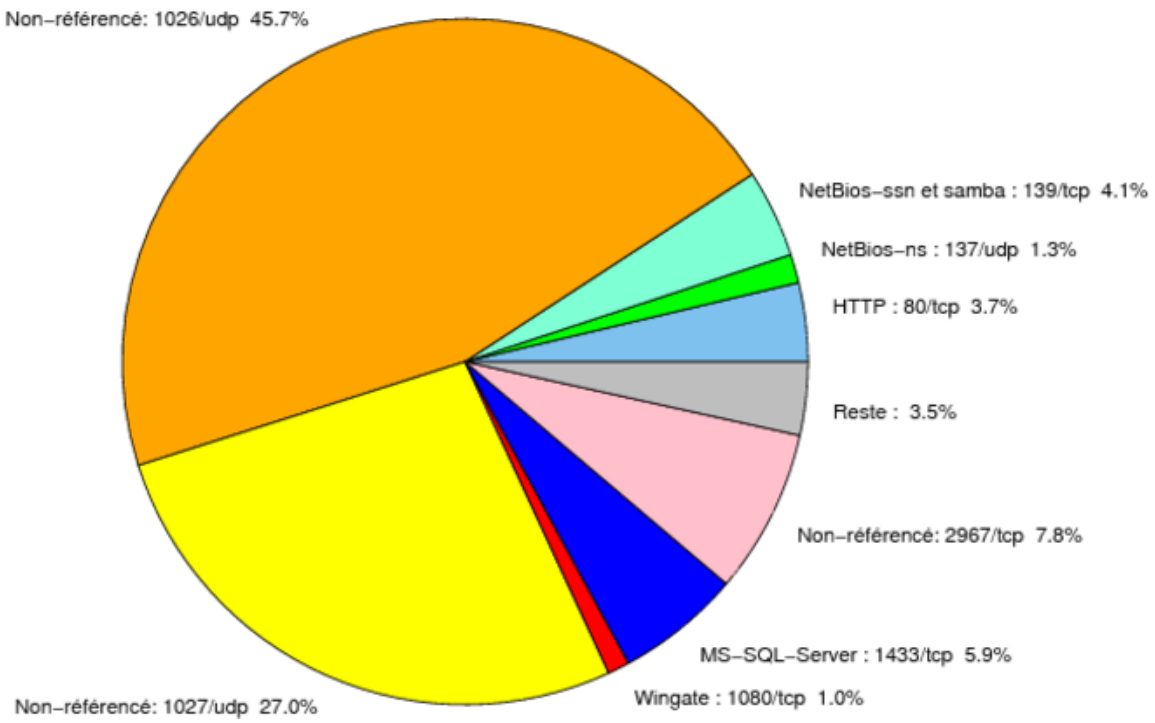

FIG. 1: Répartition relative des ports pour la semaine du 22.03.2007 au 29.03.2007

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	45.69
1027/udp	26.99
2967/tcp	7.75
1433/tcp	5.88
139/tcp	4.14
80/tcp	3.7
137/udp	1.34
1080/tcp	1.02
1434/udp	0.88
22/tcp	0.55
4899/tcp	0.5
25/tcp	0.31
21/tcp	0.27
23/tcp	0.24
3306/tcp	0.18
15118/tcp	0.1
3128/tcp	0.09
2100/tcp	0.06
3389/tcp	0.05
6129/tcp	0.04
11768/tcp	0.03
111/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

30 mars 2007 version initiale.