Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 mars 2007
N° CERTA-2007-ACT-012

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-12

Gestion du document

Référence	CERTA-2007-ACT-012
Titre	Bulletin d'actualité 2007-12
Date de la première version	23 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-012.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-012/

1 Activités en cours

1.1 Installation d'un site de filoutage (*phishing*) suite à une défiguration

Le CERTA a traité cette semaine un cas de site de filoutage (*phishing*). Ce site de filoutage a été mis en place près de 10 jours après une défiguration. Suite à la découverte de la défiguration, le webmestre du site s'était contenté de supprimer la page de défiguration et de mettre à jour l'application vulnérable attaquée, à savoir *pmb*. Le webmestre n'a pas vu que les intrus avaient également installé un interpréteur de commandes écrit en `php` (*phpshell*). Celui-ci pouvait être utilisé par n'importe quel internaute et permettait la télé-administration du site web, tout en donnant des droits limités sur le serveur.

Le CERTA rappelle que les incidents de défiguration ne se limitent pas toujours à l'ajout ou la modification d'une page web, mais que du code malveillant peut également être déposé. La modification de pages Web doit toujours faire l'objet d'une analyse pour chercher si elle cache des choses plus graves. Des recommandations sont indiquées dans la note d'information CERTA-2002-INF-002 (*Les bons réflexes en cas d'intrusion sur un système d'information*) disponible à l'adresse :
http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/

1.2 Autre cas de *phishing*

Le CERTA a traité un autre cas de site de *phishing* détecté suite à l'envoi massif de messages électroniques pointant vers ce serveur. L'analyse de ce serveur montre qu'aucun site de *phishing* n'est installé, mais qu'une page contenant une redirection vers le vrai site de *phishing* avait été ajouté.

2 Le mois PHP

2.1 Introduction

Le CERTA mentionnait dans un précédent bulletin l'existence du projet `MoPB` (pour *Month of PHP Bug*). Il s'agit de publier, au mois de mars 2007, quotidiennement, une nouvelle vulnérabilité concernant PHP. La fin du mois étant proche, le CERTA se propose d'établir un premier bilan de celles-ci dans les paragraphes suivants. Comme de nombreux incidents traités sont liés à des applications développées avec le langage PHP, le CERTA a également publié cette semaine une note d'information CERTA-2007-INF-002 plus générale rappelant quelques bons usages associés au langage PHP.

http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/

2.2 Présentation générale des vulnérabilités PHP du *MoPB*

A la date de rédaction de ce document, le projet `MoPB` a publié sur son site 29 vulnérabilités, dont 16 qui ne sont pas encore officiellement corrigées. Elles impliquent aussi bien la branche PHP 4.x que 5.x et certaines ont été corrigées dans les mises à jour de PHP sorties il y a quelques semaines (version 5.2.1 publiée le 14 février 2007, et version 4.4.6 le 01 mars 2007). D'autres font l'objet de discussion entre les développeurs dans le forum du CVS de PHP :

http://marc.info/?l=php-cvs&r=1&b=200703&w=2

La première remarque concerne les vulnérabilités qui ont été corrigées. Celles-ci n'avaient pas été annoncées publiquement par les développeurs de PHP au moment de la mise en ligne de la nouvelle version. Cette approche est criticable, dans la mesure où les utilisateurs, s'ils ne sont pas tenus informés des corrections apportées, ne peuvent pas percevoir l'impact réél d'une mise à jour plus « tardive ».

Comme seconde remarque, il est important de comprendre que ces vulnérabilités n'impliquent pas, comme souvent, un mauvais usage du langage, mais bien des erreurs intrinsèques à l'implémentation PHP. Tout serveur ayant installé celui-ci peut-être concerné par ces vulnérabilités.

Le CERTA invite donc ses correspondants à :

- mettre à jour les versions PHP actuellement utilisées ;
- limiter autant que possible l'insertion de pages PHP sur le serveur Web ;
- consulter les vulnérabilités publiées sur le site http://www.php-security.org ;
- lire la note d'informations CERTA-2007-INF-002 sur quelques bonnes pratiques dans l'emploi de PHP.

Quelques vulnérabilités sont détaillées, à valeur d'illustration, dans les sections suivantes.

2.3 Faille PHP concernant les URL de type *zip://* et *bzip2://*

Une vulnérabilité dans la gestion des adresses réticulaires de type *zip://* et *bzip2://* a été publiée par le projet `MoPB` et n'est pas corrigée à la date de parution de ce bulletin. En effet, la mise en œuvre de ces liens dans PHP ne fait pas l'objet d'un contrôle assez strict. Ceci permettrait à une personne malintentionnée de lire ou d'altérer des fichiers qui lui sont normalement refusés par le biais d'une archive particulière pointée par ce type de lien.

2.4 Vulnérabilité de *mod_security*

Le module `mod_security` est un pare-feu applicatif orienté HTTP. Il offre un certain nombre de protections contre les attaques à l'encontre des applications Web. Il fonctionne avec le serveur `Apache` et souvent avec `PHP`.

Le caractère ASCIIZ (caractère NULL, parfois appelé « Zéro ») est utilisé comme signe de fin d'une chaîne de caractères dans certaines représentations. Une vulnérabilité concernant `mod_security` a récemment été rendue publique, et implique ce caractère particulier. L'exploitation de celle-ci permet de contourner certaines règles de sécurité. Elle nécessite les conditions suivantes :

- les paramètres doivent être transportés dans le corps d'une requête `applicationx-www-form-urlencoded` ;

– un octet NULL (ASCIIZ) non-encodé doit être envoyé ;

Le module `mod_security` ne traite pas les caractères situés à droite du caractère ASCIIZ, ce qui n'est pas le cas des différents langages de script comme `Perl`, `Python`, etc. Le langage `PHP` interprète également tout ce qui se trouve à droite du caractère ASCIIZ, depuis la version 5.2.0.

Ce problème est détaillé à l'adresse suivante :
http://www.modsecurity.org/blog/archives/2007/03/modsecurity_asc.html
Un contournement y est proposé, en l'attente d'un correctif.

2.5 Vulnérabilité de la fonction `substr_compare()`

La fonction `substr_compare()` est normalement utilisée pour comparer deux chaînes de caractères en spécifiant un décalage ou *offset* pour la première chaîne (à partir d'où il faut comparer) et une longueur de comparaison. Ainsi, en appelant `substr_compare("abcd", "efgh", 2, 2)`, les chaînes "cd" et "ef" sont comparées. La fonction retourne 1 si la première chaîne est plus grande 0 si les deux chaînes sont égales, et -1 sinon.

Certains filtres empêchent de spécifier des *offsets* et longueurs de manière à comparer des valeurs en dehors des chaînes en paramètre. Cependant, le dépassement d'entier n'est pas pris en compte et permet de réaliser ceci.

En se servant de cette vulnérabilité, un attaquant peut lire des informations en mémoire.

Cette vulnérabilité ne touche pas les applications se servant de la fonction `substr_compare()`, mais est utile à une personne malintentionnée : elle lui permet notamment de trouver des adresses pour exécuter du code arbitraire avec un débordement de tampon.

3 Un exemple d'actualité : l'application W-Agora, ou Web Agora

Plusieurs vulnérabilités ont été publiées cette semaine, concernant l'application `w-agora`, ou `Web Agora`. Il s'agit d'un logiciel français de gestion de forums et de publications, disponible sur le site :
http://www.w-agora.net

Les problèmes sont nombreux :

– les scripts `delete_forum.php`, `rss.php`, `profile.php`, `search.php` et `index.php` ne gèrent pas correctement les valeurs de certains paramètres, ce qui peut permettre à une personne malveillante de récupérer le chemin complet d'installation de l'application ;
– lorsque l'option `register_globals` est activée, il est possible pour une personne malveillante, par le biais d'une simple requête, d'accéder aux informations contenues dans le fichier `global.inc` ;
– il est possible de copier et d'exécuter sur le serveur vulnérable du code PHP arbitraire, au moyen d'un message mis sur le forum, ou en utilisant le script `browse_avatar.php` ;
– une personne malveillante peut lancer différentes attaques d'injection de code indirecte (ou *cross-site scripting*), via certaines variables mal contrôlées dans les scripts `profile.php`, `search.php` ou `change_password.php` ;
– le script `search.php` ne contrôlerait pas correctement certains champs, pouvant conduire à des attaques de type « injection SQL ». Une personne malveillante pourrait utiliser cette méthode pour récupérer des informations confidentielles stockées dans la base de données utilisée.

Les références suivantes mentionnent certaines de ces vulnérabilités.
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0606
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0607
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1604
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1605
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1606
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1607

Dans l'attente d'une mise à jour de l'application, il est préférable de chercher une solution alternative et de surveiller attentivement les journaux, si celle-ci est déjà installée.

4 Commentaires sur les vulnérabilités de *libwpd*

Le CERTA a publié cette semaine l'avis CERTA-2007-AVI-135 concernant plusieurs vulnérabilités affectant la bibliothèque `libwpd` (versions 0.8.8 et antérieures). Cette bibliothèque permet le traitement de documents

au format *WordPerfect*. Elle est utilisée en tant que module par des applications telles que *OpenOffice* depuis la version 2.0, *Koffice* depuis la version 1.4 et *AbiWord* depuis la version 1.4. D'autres applications peuvent faire appel à cette bibliothèque, et donc l'installer.

L'exploitation de ces vulnérabilités permet l'exécution de code arbitraire au moment de l'ouverture d'un document *WordPerfect*.

Il est possible que la mise à jour de cette bibliothèque soit intégrée dans les derniers paquetages des applicatifs sus-mentionnés, comme c'est le cas pour *OpenOffice*. Il est tout de même conseillé de vérifier la version de `libwpd`, après application des dernières mises à jour (attention, certaines distributions ne respectent pas les numéros de version).

5 Les publicités et les techniques de *web spamming*

5.1 Introduction

De nombreuses techniques sont utilisées pour faire apparaître des liens Web pointant vers des sites douteux. Une méthode, nommée *search spamming* ou *web spamming*, consiste à utiliser des techniques d'optimisation des moteurs de recherche pour améliorer le rang des pages Web dans les résultats de recherche. L'idée est bien sûr de les faire apparaître dans les premières lignes retournées.

Les moyens ont d'abord consisté à tricher sur les mots-clés qualifiant les pages (*keywords*). Puis, comme certains moteurs de recherche s'appuient également sur les informations des liens eux-mêmes pour établir une classification, des associations de sites se sont créées pour s'entre-aider. Les deux solutions les plus fréquentes sont :

- ajouter sur une page donnée de nombreux liens vers des pages populaires et visitées, espérant ainsi que la page serve de passerelle pour accéder à ces sites ;
- parvenir à rediriger plusieurs liens légitimes vers le site tricheur, par des opérations comme :
  - copier des pages intéressantes et utiles (manuels ou pages de documentation par exemple), afin d'être largement cité ;
  - s'introduire frauduleusement sur un serveur et ne rien faire d'autre qu'ajouter quelques liens vers les sites douteux ;
  - inonder les espaces de discussion (forum) administrés de manière laxiste par des liens pointant vers les sites tricheurs ;
  - acheter des noms de domaine qui arrivent à expiration, ou qui utilisent des techniques de fautes de frappe opportunistes (*typosquatting*). La note CERTA-2007-INF-001 aborde ce problème.
  - etc.

Les techniques sont nombreuses et variées. Les plus récentes consistent à tromper les outils automatiques qui parcourent les sites (*web crawlers*) en ne leur fournissant pas la même page qu'une personne arrivant sur le site douteux depuis le résultat d'un moteur de recherche. Cette décision peut se faire, par exemple, après consultation de l'en-tête HTTP et de ces champs `user-agent` et `referer`. La personne subit une redirection dès que la page est chargée. Le scénario implique une chaîne d'acteurs, qui sont identifiés comme suit :

- les créateurs et mainteneurs de sites douteux ;
- les personnes qui se chargent de faire la publicité de ces sites (les fédérateurs) ;
- les personnes qui vendent du 'trafic', en créant les domaines de redirection ;
- les personnes qui créent des pages attractives, qui sont affichées dans les résultats de recherche.

Ce bulletin d'actualité n'a pas la prétention d'expliquer tout le fonctionnement de ces activités complexes. Il cherche uniquement à mettre en valeur le fait suivant : le *web spamming* est un phénomène répandu, et très organisé. Les moyens techniques pour s'en protéger existent, mais ne sont pas parfaits. A valeur d'illustration, la redirection peut se faire au moyen d'un script Javascript sur la page visitée :

```
<_script language="javascript">
        location.replace("Nouvelle_Page.html")
</_script>
```

Cependant, même si le Javascript, comme il faudrait, reste désactivé par défaut, il reste possible d'abuser de la propriété de rafraichissement des pages, en ajoutant dans l'en-tête HTML :

```
<_meta http-equiv="refresh" content="0; url=Nouvelle_Page.html">
```

5.2 Recommandations du CERTA

Pour éviter de naviguer dans les pages précédemment citées, il est préférable de :
- ne visiter que des sites de confiance ;
- se méfier des redirections abusives, ou successives. Celles-ci peuvent être visibles au niveau de la barre d'état du navigateur ;
- utiliser si possible un proxy Web qui normalisera proprement les en-têtes HTTP ;
- naviguer par le biais d'un navigateur correctement configuré ;
- évaluer raisonnablement les résultats d'une recherche, et faire une requête suffisamment précise (se reporter à la documentation Google par exemple).

5.3 Documentation associée

- Z. Gyongyi, H. Garcia-Molina, "Web Spam Taxonomy" :
  http://airweb.cse.lehigh.edu/2005/gyongyi.pdf
- Projet de recherche Microsoft SearchRanger :
  http://research.microsoft.com/SearchRanger
- Les principes de base de la recherche Google :
  http://www.google.fr/support/bin/static.py?page=searchguides.html&ctx=basics
- Documentation pour une recherche avancée avec le moteur de recherche Exalead :
  http://www.exalead.fr/search

6 Cheval de Troie : *Gozi*

Une analyse inverse d'un code malveillant, de type cheval de Troie (surnommé « Gozi ») a été publiée sur l'Internet. Il existe beaucoup de variantes de chevaux de Troie, mais celui-ci présente une caractéristique qui n'est pas, *a priori* très courante.

Ce code malveillant embarque des fonctions qui permettent la capture d'informations sensibles. Ce code exploite des fonctions avancées de la bibliothèque de fonctions (DLL) "`ws2_32.dll`" afin de créer sur le système compromis un "*Layered Service Provider*" (LSP). Ainsi, le code malveillant se place entre le navigateur Internet Explorer et un tunnel SSL/TLS en cours d'utilisation. En pratique, un utilisateur connecté à un site à travers un tunnel SSL/TLS (consultation en HTTPS) verra ses informations capturées par le code malveillant avant d'être transférées dans le tunnel SSL/TLS.

De plus, le code en question embarque des fonctions de dissimulation ("*rootkit*") qui rendent sa détection sur un système en fonctionnement délicate. Cependant, la mise en place de filtrages sur les équipements périmétriques (serveurs mandataires, pare-feu, ...) et la lecture régulière des journaux d'événements permettraient de découvrir de telles compromissions.

Ce code malveillant donne l'occasion de rappeler que, même si le canal de communication et le serveur destinataires sont convenablement sûrs, la sécurité de la transaction impose aussi la salubrité des postes clients.

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 15 et le 22 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 15 au 22 mars 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-130 : Vulnérabilité de Websphere
- CERTA-2007-AVI-131 : Vulnérabilité dans Horde IMP
- CERTA-2007-AVI-132 : Vulnérabilités dans Horde Application Framework
- CERTA-2007-AVI-133 : Vulnérabilités dans BrightStor ARCserve
- CERTA-2007-AVI-134 : Multiples vulnérabilité du logiciel McAfee ePolicy Orchestrator
- CERTA-2007-AVI-135 : Vulnérabilités dans libwpd
- CERTA-2007-AVI-136 : Multiples vulnérabilités dans OpenOfficeorg

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

- CERTA-2007-AVI-126-001 : Vulnérabilités dans Sun Java System Web Server
  (ajout d'une vulnérabilité)

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.

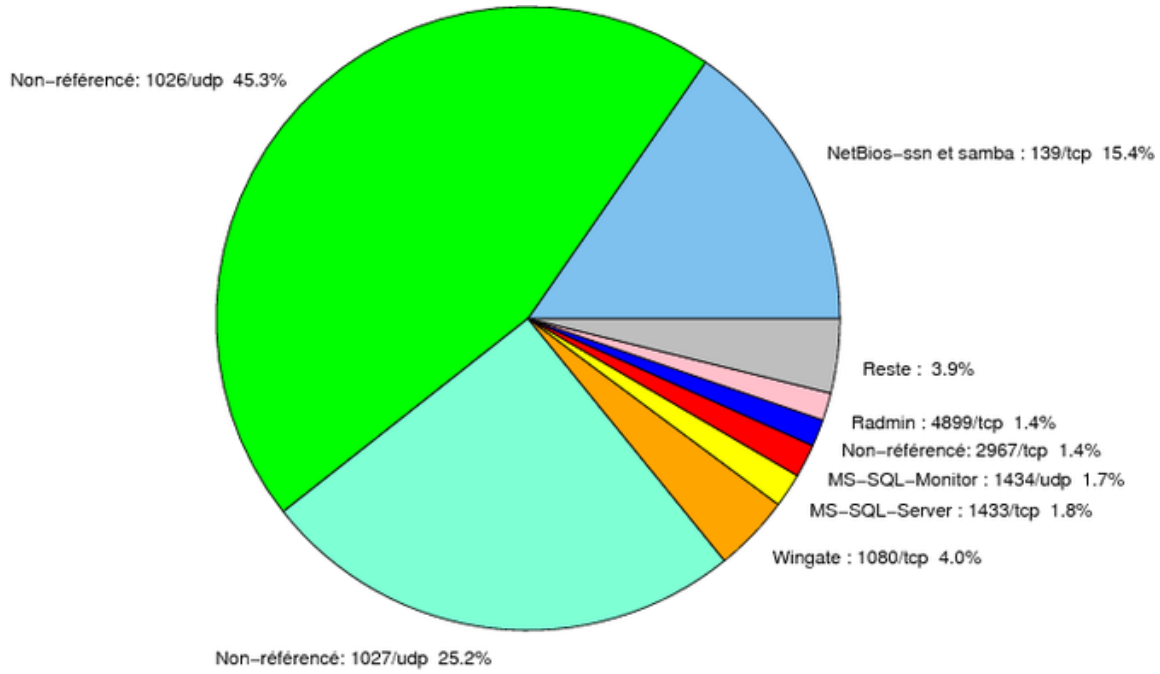

FIG. 1: Répartition relative des ports pour la semaine du 15.03.2007 au 22.03.2007

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	45.27
1027/udp	25.21
139/tcp	15.35
1080/tcp	3.97
1433/tcp	1.76
1434/udp	1.71
4899/tcp	1.42
2967/tcp	1.4
3128/tcp	0.94
137/udp	0.84
25/tcp	0.46
80/tcp	0.33
3306/tcp	0.31
443/tcp	0.21
15118/tcp	0.09
3389/tcp	0.07
143/tcp	0.04
111/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

23 mars 2007 version initiale.