Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 janvier 2007
N° CERTA-2007-ACT-004

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-04

Gestion du document

Référence	CERTA-2007-ACT-004
Titre	Bulletin d'actualité 2007-04
Date de la première version	26 janvier 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-004.pdf
Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-004/

1 Activité en cours

1.1 Incidents

Le CERTA a traité cette semaine de nombreux cas de défiguration. Pour la plupart d'entre eux, la faille exploitée était de type `php include` et concernait un module optionnel du logiciel de gestion de contenu `Mambo`. Les attaques de ce type sont rendues possibles par des erreurs de programmation. Quand il existe un correctif, il est conseillé de l'appliquer. Toutefois, il arrive parfois que les applications vulnérables n'aient pas de correctif car leur développement a été abandonné. Il reste possible de bloquer les attaques de type `php include` en modifiant la configuration `php` du serveur web (par exemple en désactivant la variable `REGISTER_GLOBALS`) mais ceci peut avoir des conséquences sur le bon fonctionnement des serveurs. Il est aussi nécessaire de filtrer au niveau du pare-feu les connexions sortantes issues du serveur Web mettant en œuvre Mambo.

1.2 Le nettoyage du code source des pages Web

Le CERTA a traité cette semaine un incident concernant un site Web. Au cours de l'analyse, il est apparu que le code source des pages Web contenaient des informations facilitant d'éventuelles attaques contre ce site.

Le code source des pages Web est une information qui est généralement accessible par toute personne qui peut visualiser la page dans le navigateur.

Cependant, ce même code peut contenir, outre les données nécessaires, des indications sur la mise en œuvre du site, souvent incorporées dans des zones de commentaires.

La *sécurité par l'obscurité*, qui consiste à tout cacher en estimant qu'il s'agit d'une mesure de sécurité suffisante, n'est souvent pas la meilleure solution. Mais, dans le cas présent, il est aussi important d'éviter de tendre un bâton aux personnes malveillantes...

Les outils de développement de site (par exemple les systèmes de gestion de contenu, ou `CMS`), ne sont pas toujours bien maintenus et/ou mis à jour. Le fait de ne pas communiquer de manière triviale dans les commentaires du code source des pages le produit utilisé revient donc à réduire les risques, ou du moins, à rendre plus difficile une action malveillante.

Il est important de vérifier que de telles informations n'apparaissent pas, et de signaler cette exigence aux développeurs du site.

2 Des vulnérabilités non corrigées concernant Microsoft Visual Studio

2.1 Présentation

Des vulnérabilités sont apparues cette semaine, concernant Microsoft Visual Studio, mais ne sont pas encore corrigées. Compte tenu de l'application visée et de la mise en œuvre de l'attaque, elles ne font pas l'objet d'une alerte, mais en voici les détails, dans l'attente d'un avis du CERTA qui annoncera la disponilibité des correctifs. Elles concernent des fichiers avec des extensions bien précises :

- les fichiers d'extension `.RC`, contenant diverses informations sur un projet de Visual Studio : un champ trop long dans le fichier pourrait provoquer un débordement de tampon. Une personne malveillante qui parviendrait à inciter un utilisateur à ouvri r un tel fichier pourrait exécuter des commandes arbitraires sur le système à l'insu de ce dernier ;
- les fichiers d'extension `.CNT`, contenant les informations sur les fichiers d'aide (`Help File Contents`) : une corruption de la mémoire est possible, quand l'application interprète certaines lignes du fichier qui devraient être dans un format bien déterminé (`'%d%s'` : *1 DescriptionDuContenu*).
- les fichiers d'extension `.HPJ`, contenant des informations d'*aide contextuelle* associée à un projet Visual Studio : une variable du fichier ne serait pas correctement contrôlée. Une personne malveillante pourrait profiter de ce problème pour provoquer un débordement de la pile mémoire et exécuter du code arbitraire sur le système vu lnérable.

Les versions affectées par ces vulnérabilités sont les suivantes :

- Microsoft Help Workshop version 4.03.0002 ainsi que celles antérieures ;
- Microsoft Visual Studio 6.0 SP6 ;
- Microsoft Visual Studio 2003 (.NET).

2.2 Recommandations du CERTA

Dans l'attente d'un correctif, il est préférable :

- de manipuler des fichiers avec les extensions `.RC`, `.CNT` et `.HPJ` dans un environnement de confiance ;
- de filtrer éventuellement ces extensions de fichiers au niveau des passerelles de messagerie ;
- de contacter le CERTA s'il y a le moindre doute.

3 Du risque associé à certains services paradoxaux

On peut rencontrer sur l'Internet un certains nombre de sites proposant de vérifier pour le client d'un service s'il aurait été victime d'un vol d'identité. Cependant les méthodes employées sont souvent des plus douteuses. Le mode opératoire de ces sites pour une telle vérification consiste dans un premier temps à demander la saisie de l'identifiant qui aurait pu être dérobé.

Le site de vérification peut alors indiquer que cet identifiant a bien été dérobé et qu'il convient pour s'en assurer de donner en complément ses coordonnées bancaires... Le site promet alors de contacter la banque pour l'informer de cet état de fait.

Ce genre de pratique s'apparente plus à du *phishing* qu'à un réel service. Il est donc recommandé de proscrire l'usage de ce genre de sites.

4 Filtrage et syntaxe d'URL

4.1 Principes

Une URL est de la forme suivante, où les éléments entre crochets sont très souvent omis :

`protocole://[utilisateur:[mot-de-passe]@]hote[:port]/chemin?requete#etiquette`

Par exemple, sans utilisateur, ni port, ni étiquette :

`http://www.premier-ministre.gouv.fr/fr/p.cfm?ref`

La représentation est définie dans le standard RFC3986. En l'occurrence, celle de l'hôte peut être faite par adresse IP numérique ou par nom. Les nombreuses variantes, permises ou tolérées par les implémentations, peuvent être source d'inefficacité du filtrage d'URL.

A titre d'exemple, si l'hôte est désigné par une adresse IP numérique, des mises en œuvre autorisent la représentation avec 1 à 4 entiers, séparés par des points. Le dernier entier représente les derniers octets de l'adresse (sa taille est donc variable). Chaque entier peut lui-même être représenté en décimal, en octal, s'il commence par 0, ou en hexadécimal, s'il est précédé par 0x ou 0X. La représentation de ces entiers peut ne pas être uniforme.

Voici un exemple, avec l'adresse du site http://www.certa.gouv.fr et l'adresse IP utilisée à la date de parution de ce bulletin d'actualité :

- http://www.certa.ssi.gouv.fr/
- http://213.56.176.2/
- http://3577262082/
- http://0325.0070.0260.0002/
- http://0xD5.0x38.0xB0.0x02/

Il est également possible de faire des combinaisons de ces représentations.

Enfin, dans les noms d'hôtes, un caractère non ASCII peut être représenté en UTF-8 par une chaîne d'octets. Chacun de ces octets est inclus dans l'URL sous forme `%HL` ou `H` et `L` sont les caractères désignant les chiffres hexadécimaux de l'octet, comme `%7B`. La représentation IDNA (RFC3490) est recommandée pour les recherches DNS.

4.2 Recommandations

Compte tenu des remarques précédentes, il est important de :

- prendre le temps de vérifier le sens et la validité d'un lien présenté dans un courrier électronique ou d'une autre manière quelconque ;
- tester que la politique de filtrage d'URL considère ces différentes représentations, et que le filtre transforme les URL sous une forme canonique.

5 Vulnérabilité de certains téléphones portables *Bluetooth*

Cette semaine, plusieurs fabricants de téléphonie mobile ont communiqué sur des vulnérabilités de type déni de service affectant leurs produits équipés d'une interface *Bluetooth*. Ces vulnérabilités peuvent être exploitées à distance pour provoquer un déni de service. A ce jour, un code destiné à prouver l'exploitation de ces vulnérabilités est disponible sur l'Internet.

Le CERTA a eu l'occasion d'analyser et de tester certains de ces codes. L'attaque consiste à envoyer de façon ininterrompue un élément (fichier, contact, etc.) vers le profil `Obex Push` du périphérique vulnérable, qui se traduit par un consommation excessive des ressources de l'appareil. Cela provoque un déni de service de la pile Bluetooth et/ou de l'appareil. A la date de rédaction de ce document, la liste des périphériques vulnérables est limitée à 5 téléphones mobiles équipés d'une interface Bluetooth. Il s'agit de :

- Motorola MOTORAZR V3
- Sony Ericsson K700i
- Sony Ericsson W810i
- Nokia N70
- LG Chocolate KG800

Il est cependant fort probable que cette liste ne soit pas exhaustive.

5.1 Documentation

- Référence CVE CVE-2007-0521 :
  http://nvd.nist.gov/nvd.cfm/?cvename=CVE-2007-0521
- Référence CVE CVE-2007-0522 :
  http://nvd.nist.gov/nvd.cfm/?cvename=CVE-2007-0522
- Référence CVE CVE-2007-0523 :
  http://nvd.nist.gov/nvd.cfm/?cvename=CVE-2007-0523
- Référence CVE CVE-2007-0524 :
  http://nvd.nist.gov/nvd.cfm/?cvename=CVE-2007-0524

5.2 Recommandations

Les mises à jour sur les téléphones portables n'existent pas ou ne sont pas faciles à appliquer.

Le CERTA recommande donc vivement de vérifier que l'activité bluetooth est bien désactivée par défaut sur tout appareil commmuniquant. Quand une communication via cette technologie doit avoir lieu, elle doit se faire entre dispositifs jumelés (partageant un secret), et dans un enviromment de confiance. Les risques associés doivent être considérés.

6 La liste noire maintenue par Google

6.1 Présentation

A la date de publication de ce bulletin, le navigateur `Mozilla Firefox 2` ainsi que la barre de navigation `Google` pour `Firefox` contiennent un module (`Safebrowsing`) permettant de vérifier que le site visualisé par l'internaute n'est pas présent dans une liste noire de `Google`. Si tel est le cas, un message d'avertissement prévient l'utilisateur des risques potentiels à visiter cette page. Afin de ne pas surcharger ces contrôles, `Google` maintient également une liste blanche de domaines qui sont censés ne pas héberger de sites frauduleux.

Le fait de pouvoir consulter cette liste noire apporte également l'intérêt de contrôler la présence ou non d'un site (ou d'une adresse y faisant référence) dans cette liste. Ainsi, le `CERTA` vérifie régulièrement dans ce genre de liste l'absence de sites relatifs à l'administration française.

D'autres sociétés, comme `Microsoft`, maintiennent également des listes noires et blanches utilisables par certains navigateurs comme `Microsoft Internet Explorer 7`.

Attention toutefois à ne pas accorder une trop grande confiance dans ces listes, elles ne sont pas exhaustives et chacun se doit de rester vigilant. Par ailleurs, la manière dont ces listes sont maintenues n'est pas toujours publique, et vérifiable.

6.2 Documentations

- Signaler une page de phishing chez Google :
  http://www.google.com/safebrowsing/report_phish
- Signaler une erreur dans les alertes d'usurpation d'identité :
  http://www.google.com/safebrowsing/report_error

7 Retour sur les récentes vulnérabilités CISCO

Cisco a publié cette semaine trois mises à jour distinctes, qui ont été présentées dans l'avis CERTA-2007-AVI-050.

Les éléments d'un réseau sont sensibles, et les vulnérabilités corrigées peuvent être exploitées pour provoquer un dysfonctionnement de ceux-ci, voir en prendre le contrôle total.

Le CERTA recommande donc vivement d'appliquer les mises à jour, et de surveiller avec attention le comportement des éléments CISCO vulnérables.

8 Le *Month of Apple Bug* : épisode 4

Voici, pour cette semaine, les vulnérabilités sur les produits Apple publiées par le projet « *Month Of Apple Bugs* » :

- une vulnérabilité dans le logiciel iChat et sa mise en œuvre du protocole AIM (AOL Instant Messaging) permettant de provoquer un déni de service ou l'exécution de code arbitraire sous certaines conditions ;
- des erreurs de conception dans un composant du panneau de configuration et dans l'agent de notification de Apple MacOS X permettant un utilisateur local d'élever ses privilèges ;
- une vulnérabilité dans l'application Apple QuickDraw et sa mise en œuvre des images au format PICT ;
- une erreur dans le système de mise à jour logiciel permettant d'effectuer un déni de service.

9 Interprétation de l'élément HTML *TITLE* par les navigateurs

Dans le standard HTML 4.0 (http://www.w3.org/TR/html4/html40.txt), il est dit que :

```
7.4.2  The TITLE element
Titles may contain character entities (for accented characters, etc.),
but may not contain other markup (including comments).
```

Il y a donc une imprécision, donc une interprétation différente selon les navigateurs.

Certains considèrent que les commentaires n'ont pas lieu d'être dans le champ TITLE, et prennent tout le contenu comme du texte, qui sera affiché. Cela inclut les balises de commentaires.

D'autres, en revanche, adoptent un comportement inattendu. Ils peuvent par exemple ignorer simplement les balises de commentaires, et interpréter d'autres balises comme <SCRIPT> au sein même du champ TITLE.

Certains filtres HTML bloquent les balises de script, mais ne vont pas vérifier si de telles balises se trouvent dans les champs commentaires. Dans ces conditions, une personne malveillante peut insérer un script dans un commentaire, se trouvant lui-même entre les balises <TITLE> et </TITLE>. Le script sera interprété par cette famille de navigateurs.

La politique de sécurité appliquée par les filtres HTML est alors contournée.

Dans le cas où des filtres sur le contenu HTML sont mis en place, il est important qu'ils vérifient correctement le contenu TITLE.

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 18 et le 25 janvier 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-008 sur les outils d'indexation et de recherche :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-008/

12 Rappel des avis émis

Durant la période du 19 au 25 janvier 2007, le CERTA a émis les avis suivants :
– CERTA-2007-AVI-038 : Vulnérabilités dans IBM WebSphere
– CERTA-2007-AVI-039 : Vulnérabilité dans les produits Cisco CS-MARS et ASDM
– CERTA-2007-AVI-040 : Vulnérabilité IPv6 sur OpenBSD
– CERTA-2007-AVI-041 : Vulnérabilité de Xpdf et ses dérivés
– CERTA-2007-AVI-042 : Vulnérabilité de BitDefender Client Professional Plus
– CERTA-2007-AVI-043 : Vulnérabilité de Check Point Connectra
– CERTA-2007-AVI-044 : Multiples vulnérabilités de BEA WebLogic
– CERTA-2007-AVI-045 : Vulnérabilité dans Cahier de Texte
– CERTA-2007-AVI-046 : Vulnérabilité dans Sun Solaris
– CERTA-2007-AVI-047 : Multiples vulnérabilités dans les produits BrightStor ARCserve Backup
– CERTA-2007-AVI-048 : Vulnérabilité de Sun Ray Server Software
– CERTA-2007-AVI-049 : Vulnérabilité dans Linux-PAM
– CERTA-2007-AVI-050 : Vulnérabilités de certaines couches protocolaires dans Cisco IOS
– CERTA-2007-AVI-051 : Vulnérabilités dans Apache sur HP-UX
– CERTA-2007-AVI-052 : Vulnérabilité dans Citrix Metaframe Presentation Server
– CERTA-2007-AVI-053 : Vulnérabilité de Symantec Web Security
– CERTA-2007-AVI-054 : Vulnérabilités du module Project de Drupal
– CERTA-2007-AVI-055 : Vulnérabilité de GTK2

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

– CERTA-2007-AVI-013-001 : Plusieurs vulnérabilités dans le navigateur Opera
(ajout des références CVE, Gentoo et Suse)
– CERTA-2007-AVI-037-001 : Vulnérabilités de BEA AquaLogic
(ajout des références CVE) item CERTA-2007-AVI-050-001 : Vulnérabilités de certaines couches protocolaires dans Cisco IOS
(ajout des références CVE et modification des risques)

Et les alertes suivantes ont été modifiées :

– CERTA-2006-ALE-013 : Vulnérabilités de MacOS X
– CERTA-2007-ALE-001 : Vulnérabilité dans Apple Quicktime
– CERTA-2007-ALE-003 : Filoutage contre le site voyages-sncf.com

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.

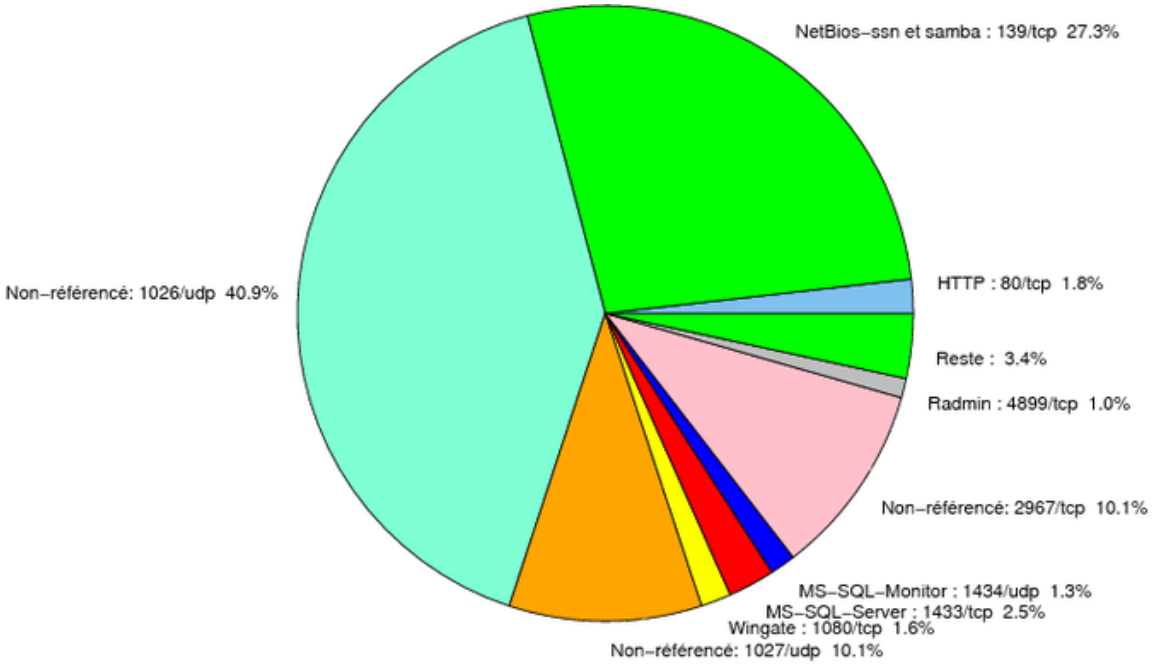

FIG. 1: Répartition relative des ports pour la semaine du 18.01.2007 au 25.01.2007

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	40.87
139/tcp	27.29
2967/tcp	10.13
1027/udp	10.11
1433/tcp	2.45
80/tcp	1.78
1080/tcp	1.58
1434/udp	1.33
4899/tcp	1.01
137/udp	0.99
22/tcp	0.64
3128/tcp	0.59
25/tcp	0.27
3306/tcp	0.17
15118/tcp	0.14
2100/tcp	0.09
3389/tcp	0.07
143/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

26 janvier 2007 version initiale.