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 décembre 2007
N° CERTA-2007-ACT-052

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-52

Gestion du document

Référence	CERTA-2007-ACT-052
Titre	Bulletin d'actualité 2007-52
Date de la première version	28 décembre 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-052.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-052/

1 Vulnérabilités dans Dokeos

Plusieurs vulnérabilités affectant *Dokeos* (versions 1.8.4 et antérieures) ont été récemment rendues publiques. Elles se déclinent en deux catégories :

– des vulnérabilités de type *cross-site scripting*. Ces problèmes sont généralement liés à un mauvais filtrage des données envoyées par des utilisateurs, par exemple dans des formulaires. Elles affectent généralement les internautes qui visitent le site. Leurs conséquences peuvent varier, allant du simple affichage d'un mot de passe à des vols de *cookie*. Si l'on considère que le webmestre est susceptible de visualiser ces pages, alors ce genre de risques est à prendre au sérieux ;
– une vulnérabilité qui permet l'exécution de code arbitraire à distance. Ce problème vient du fait qu'un utilisateur légitime (c'est-à-dire disposant d'un compte *Dokeos*) du site peut installer un fichier (*upload*) dans une zone dédiée. Il est possible, par le biais d'une double extension, de contourner certains paramétrages de sécurité et de télécharger un fichier contenant du code `PHP` (par exemple). Ce fichier pourra ensuite être appelé (et donc exécuté par le serveur).

Ces vulnérabilités ont été évoquées dans l'avis CERTA-2007-AVI-564 et ont fait l'objet d'un correctif de sécurité de la part des développeurs de *Dokeos*. Elles seront également corrigées dans la future version 1.8.5.

En guise de contournement provisoire, il est possible, pour la vulnérabilité concernant le téléchargement de fichiers portant une double extension, de mettre en place un fichier `.htaccess` dans le répertoire `main/upload/user/`, avec le contenu suivant :

```
AddHandler cgi-script .php .pl .py .jsp .asp .htm .shtml .sh .cgi .phps .bash
Options -ExecCGI
```

Documentation :

- Avis CERTA-2007-AVI-564 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-564/

2 Je reçois des cartes de vœux !

Comme chaque année à la même période les boites à lettres sont envahies de courriels intitulés par exemple "*Happy new Year*" ou "*New Year Ecard*" et autres "cartes de vœux". Ces prétendus messages de vœux peuvent contenir des pièces jointes malveillantes ou inviter les destinataires à cliquer sur un lien pour télécharger une carte de vœux virtuelle qui tentera d'infecter l'ordinateur.

Que le réseau de machines compromises dénommé Storm présenté dans le bulletin CERTA-2007-ACT-034 soit ou non à l'origine de ces messages malveillants, les bonnes pratiques pour se protéger de ce type d'attaque restent d'actualité:

- mettre à jour régulièrement et systématiquement toutes les applications ;
- ne jamais répondre aux pourriels ;
- se méfier des courriels dont on ne reconnaît ni la langue ni l'émetteur ;
- ne pas faire spontanément confiance dans le champ émetteur d'un courriel ;
- ne jamais cliquer sur un lien inséré dans un message sans un minimum de précaution.

Les recommandations du CERTA restent également d'actualité :

- Mise en garde au sujet des cartes de vœux :
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-REC-002/
- Les canulars par messagerie :
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-005/
- Limiter l'impact du spam :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-004/

3 Cadeaux de Noël, et codes multi plates-formes

3.1 La problématique

Des codes malveillants étaient déjà connus pour se propager sur différentes plates-formes, comme le ver W32/Mobler qui installe SymbOS/MultiDropper.CC sur les systèmes Windows et SymbOS/MultiDropper qui installe W32/Mobler sur les cartes mémoires amovibles qui sont connectées à l'ordinateur. Depuis quelques mois, il apparaît donc des vulnérabilités qui offrent la possibilité d'être utilisées sur différentes plates-formes. Cela a été constaté, par exemple, avec la vulnérabilité dans *libTIFF* qui a permis aux accros de la console de jeux `PSP` (*Playstation Portable*) de *Sony* d'installer les applications qu'ils avaient développées. L'exploit utilisé a été publié et a ainsi permis son étude et son adaptation. Cette même exploitation de vulnérabilité est réapparue pour contourner les protections mises en place par *Apple* dans son téléphone mobile multifonctions l'`iPhone`. Le fait de pouvoir porter des codes d'exploitation sur différentes plates-formes permet aux attaquants de capitaliser leurs recherches et d'accélérer la sortie de nouveau code exploitant les mêmes vulnérabilités. Il apparaît depuis quelques jours qu'une vulnérabilité semble offrir ces même possibilités grâce à une vidéo au format *MP4* provoquant un dépassement de mémoire tampon dans plusieurs lecteurs multimédia. Cette vidéo spécialement conçue pourrait être portée sur des systèmes de téléphones mobiles et avoir les mêmes conséquences.

3.2 Les recommandations

Le CERTA tient à rappeler que ces systèmes multimédia, qu'ils se présentent sous la forme de consoles de jeux (portables ou de salon), de téléphones mobiles ou d'agendas personnels, sont des ordinateurs à part entière et présentent bien des opportunités pour des personnes malveillantes notamment grâce à leurs possibilités de communication ou leurs puissances de calcul. Il est donc nécessaire d'apporter la même attention et les mêmes précautions que pour un poste classique lorsque des supports amovibles ou des périphériques y sont connectés ou bien lorsque que ces systèmes sont connectés à un réseau.

4 Détournement de l'indexation des moteurs de recherche

4.1 Présentation des faits

Un correspondant du CERTA a signalé cette semaine que le moteur de recherche Google n'indexait plus directement son site, mais plutôt une adresse « étrange » de la forme :

```
http://www.Adresse_Legitime/?ref=Autre_URL_inconnue
```

En réalité, des personnes malveillantes ont profité de la notoriété de certaines pages sur d'autres sites pour augmenter la cote de popularité de l'adresse ci-dessus. L'insertion de cadres (`IFRAME`) dans des sites est un moyen d'y parvenir.

Cette adresse « étrange » est consultée par le robot du moteur de recherche, ici `googlebot`. Si ce dernier reçoit une réponse positive (code HTTP 200) du serveur légitime, la page est bien indexée, mais avec cette URL « étrange ».

Les impacts sont variés, mais le premier est celui sur l'image du site légitime, associé contre son gré par le moteur de recherche à une autre adresse. Pour les personnes malveillantes, cette méthode qui consiste à détourner le principe d'indexation actuellement utilisé, permet aussi de diffuser rapidement des adresses, et de complexifier le système publicitaire mis en place.

4.2 Des mesures possibles

Il ne s'agit dans le cas présent pas d'une vulnérabilité directe du site. Cependant, afin de se prémunir d'un tel désagrément, quelques actions sont envisageables :

- modifier le fichier `robots.txt`. La syntaxe de ce dernier n'est pas très souple, mais il est possible d'écrire des règles spécifiques pour les champs `User-Agent` caractéristiques des robots ;
- construite une carte du site, pour la communiquer ensuite directement au moteur de recherche. Google détaille par exemple la réalisation de cette carte à l'adresse :
  http://www.google.com/webmasters/tools/docs/fr/about.html
- signaler le problème via l'interface dédiée du moteur de recherche. Sous Google, il faut préalablement créer un compte *webmaster*.

5 Mise à jour de Perl

Le 18 décembre 2007 est sortie une nouvelle version du langage de programmation `Perl`. La version 5.10, qui est maintenant la version en cours, est la première mise à jour depuis plus de cinq ans. Cette nouvelle version améliore les performances de l'interpréteur, garantit une meilleure portabilité ainsi qu'une moindre consommation de la mémoire. Il est également à noter un nouvel opérateur de comparaison –. Une documentation complète des changements apportés est disponible via le *perldelta*.

5.0.1 Documentation

- La documentation des évolutions apportées dans Perl 5.10 (*perldelta*) :
  http://search.cpan.org/dist/perl-5.10.0/pod/perl5100delta.pod
- La page de téléchargement des sources Perl 5.10 :
  http://www.cpan.org/authors./id/R/RG/RGARCIA/perl-5.10.0.tar.gz

6 Modification des fichiers `hosts`

6.1 Présentation

La plupart des systèmes d'exploitation maintiennent un fichier dans lequel il est possible d'entrer statiquement la correspondance entre un nom de machine et une adresse IP. Cette solution permet de ne pas chercher à résoudre la correspondance par des protocoles réseaux, comme DNS permet de faire par exemple.

Sous Linux ou Mac OS, il est donc possible de trouver le fichier `/etc/hosts`, dont le contenu est sous la forme :

```
Adresse_IP_1      nom_de_la_machine_1         alias_possibles
Adresse_IP_2      nom_de_la_machine_2         alias_possibles
```

Sous Windows 2000/XP/Vista, un fichier très similaire existe :

`C:%windir%\system32\drivers\etc\hosts`

Ce fichier peut être modifié par des codes malveillants ayant obtenu un accès privilégié au système (administrateur).

Cette méthode est différente d'une modification de la configuration DNS du système par un cheval de Troie, que le CERTA a mentionné dans le bulletin CERTA-2007-ACT-044. Ce cheval de Troie se présente sous la forme d'un codec vidéo à installer pour visionner gratuitement certaines catégories de films. Ce cheval de Troie, aussi appelé DNSChanger, vise les postes MacOS et modifie le serveur DNS utilisé, afin de détourner les requêtes Web vers des pages de filoutage. Il ne s'agit donc pas d'une modification du fichier `hosts`, mais de la configuration même du DNS.

6.2 Une motivation

La modification du fichier `hosts` peut se faire par un code malveillant pour les mêmes raisons :

- diriger certaines requêtes vers des serveurs particuliers, ou des machines relais dédiées, afin de jouer un rôle d'intermédiaire (voyeur).
- afficher des contenus publicitaires dédiés, voire générer des revenus à partir de cette fraude.

La modification du fichier `hosts` sous Windows par le cheval de Troie Trojan.Qhost.WU est de la forme :

```
X.X.X.X          page2.googlesyndication.com
```

Cette modification permet, lorsque l'utilisateur navigue sur des pages, de changer les informations textuelles publicitaires initialement prévues. On pourrait également imaginer d'autres scénarios, comme ajouter du contenu malveillant à certaines pages.

6.3 Recommandations

Plusieurs mesures peuvent être entreprises pour ne pas subir ce genre de modification :

- vérifier régulièrement l'intégrité des fichiers système et de configuration ;
- naviguer avec des droits limités ;
- ne pas installer de logiciels ne provenant pas de source de confiance. Tout logiciel installé avec des droits d'administration du système a la capacité de modifier les fichiers du système ;
- surveiller les flux réseau afin de déterminer une quelconque anomalie.

7 Ce n'est qu'un au revoir...

L'année 2007 s'achève. Le CERTA profite donc de ce dernier numéro pour souhaiter d'excellentes fêtes à ses lecteurs.

Au cours de cette année, le CERTA a eu l'occasion de publier un peu plus de 300 articles différents dispersés dans ses bulletins d'actualité. Voici ci-dessous une liste, non exhaustive, de certains d'entre eux, qui peuvent faire l'objet de relecture, en ces fêtes de Noël :

- « Les logiciels gratuits pseudo-miracles », CERTA-2007-ACT-003 du 19 janvier 2007 : http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-003.pdf
- « Du risque associé à certains services paradoxaux », CERTA-2007-ACT-004 du 26 janvier 2007 : http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-004.pdf

– « Filtrage et syntaxe d'URL », CERTA-2007-ACT-004 du 26 janvier 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-004.pdf
– « Règles de filtrage pour les serveurs », CERTA-2007-ACT-008 du 23 février 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-008.pdf
– « Fuite d'informations », CERTA-2007-ACT-010 du 09 mars 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-010.pdf
– « Réservation des noms de domaine », CERTA-2007-ACT-17 du 27 avril 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-017.pdf
– « Des problèmes de codage/décodage pour les outils de sécurité », CERTA-2007-ACT-020 du 18 mai 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-020.pdf
– « Les outils de travail à distance », CERTA-2007-ACT-021 du 25 mai 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-021.pdf
– « Les documents Office : conversions », CERTA-2007-ACT-023 du 08 juin 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-023.pdf
– « Mots de passe et incidents », CERTA-2007-ACT-025 du 22 juin 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-025.pdf
– « Les activités de l'Internet et les interprétations de données », CERTA-2007-ACT-027 du 06 juillet 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-027.pdf
– « Les affichages dissimulés à l'intérieur de pages Web », CERTA-2007-ACT-033 du 17 août 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-033.pdf
– « Connaître la boîte, pour mieux déterminer ses vulnérabilités », CERTA-2007-ACT-036 du 07 septembre 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-036.pdf
– « Déménager un site Web : des précautions à prendre », CERTA-2007-ACT-037 du 14 septembre 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-037.pdf
– « Les messageries instantanées, risques immédiats ? », CERTA-2007-ACT-038 du 21 septembre 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-038.pdf
– « Les attaques en déni de service », CERTA-2007-ACT-039 du 28 septembre 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-039.pdf
– « Il n'y a rien d'intéressant sur la machine ! », CERTA-2007-ACT-047 du 23 novembre 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-047.pdf

8 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 décembre 2007.

9 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/

10 Rappel des avis émis

Dans la période du 21 au 27 décembre 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-557 : Vulnérabilité d'un module CISCO
- CERTA-2007-AVI-558 : Vulnérabilité dans les produits Computer Associates
- CERTA-2007-AVI-559 : Multiples vulnérabilités dans Wireshark
- CERTA-2007-AVI-560 : Vulnérabilités de serveur HTTP d'IBM
- CERTA-2007-AVI-561 : Vulnérabilité de Websense Enterprise
- CERTA-2007-AVI-562 : Vulnérabilité dans Asterisk
- CERTA-2007-AVI-563 : Plusieurs vulnérabilités de Sun Java System Web Proxy Server
- CERTA-2007-AVI-564 : Vulnérabilités dans Dokeos
- CERTA-2007-AVI-565 : Vulnérabilité dans Novell Groupwise
- CERTA-2007-AVI-566 : Multiples vulnérabilités dans Mambo
- CERTA-2007-AVI-567 : Vulnérabilité dans Novell Identity Manager
- CERTA-2007-AVI-568 : Multiples vulnérabilités dans VLC Media Player

11 Actions suggérées

11.1 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.

11.2 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.

11.3 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.

11.4 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.

11.5 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.

11.6 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.

11.7 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

12 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.

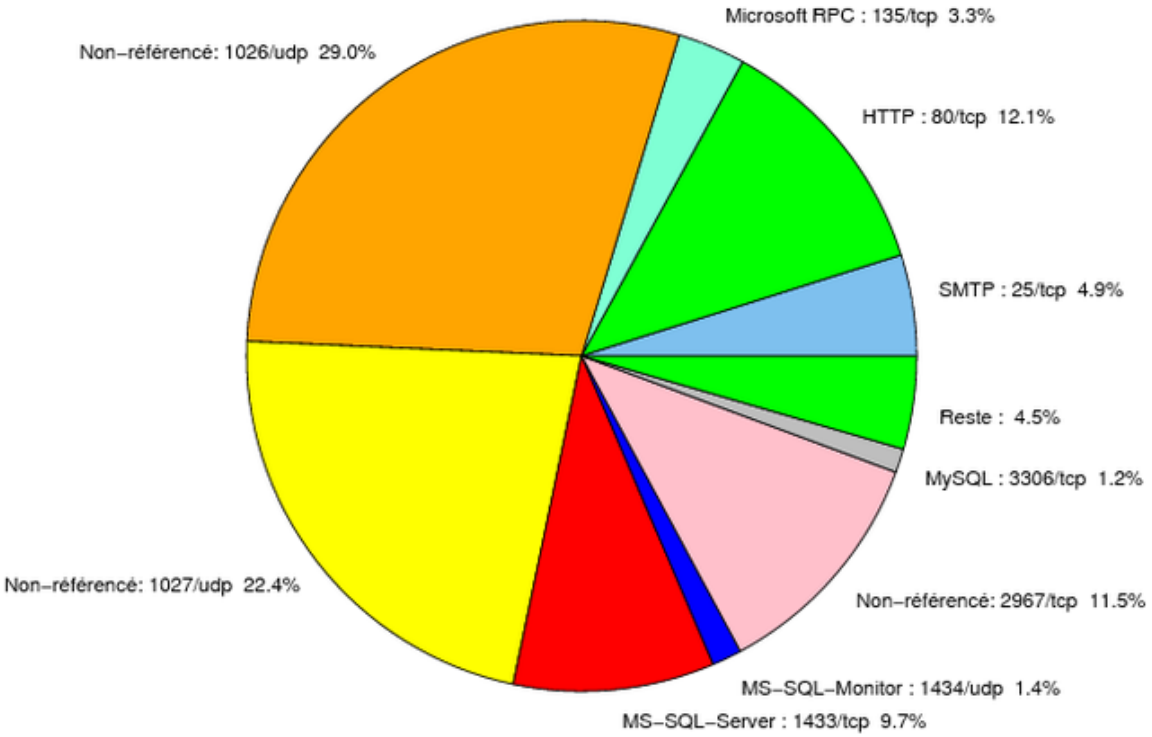

FIG. 1: Répartition relative des ports pour la semaine du au 20.12.2007 au 27.12.2007

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/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 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
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CERT
389	TCP	LDAP	–	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 http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CERT
443	TCP	HTTPS	–	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 http://www.certa.ssi.gouv.fr/site/CERT
445	TCP	Microsoft-smb	–	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 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 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	29.01
1027/udp	22.41
80/tcp	12.14
2967/tcp	11.5
1433/tcp	9.7
25/tcp	4.86
135/tcp	3.27
1434/udp	1.42
3306/tcp	1.15
4899/tcp	0.9
139/tcp	0.86
137/udp	0.3
15118/tcp	0.13
21/tcp	0.1
23/tcp	0.08
143/tcp	0.05
3389/tcp	0.04

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

28 décembre 2007 version initiale.