Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 mai 2008
N° CERTA-2008-ACT-018

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-18

Gestion du document

Référence	CERTA-2008-ACT-018
Titre	Bulletin d'actualité 2008-18
Date de la première version	02 mai 2008
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-018.pdf
Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-018/

1 Les incidents traités cette semaine

1.1 Compromissions successives

Cette semaine, le CERTA a participé au traitement d'un incident relatif à la compromission d'un site internet. Lors de cet incident, la prise de contact a été très rapide car ce site avait hébergé des pages de filoutage (*phishing*) quelques jours plus tôt. Le propriétaire du site n'étant pas familier de l'administration Web pensait s'appuyer naturellement sur son hébergeur pour résoudre le problème. Or le contrat qui le liait à celui-ci ne mentionnait pas d'assistance ni de diagnostic en cas de compromission.

Le CERTA rappelle que les sites internet nécessitent des applications qui évoluent dans le temps. Des correctifs de sécurité sont régulièrement publiés afin de corriger des vulnérabilités qui peuvent être triviales à exploiter par des attaquants.

Le CERTA rappelle également que, lors de la signature d'un contrat d'hébergement, il ne faut pas négliger les aspects de sécurité ; certaines clauses peuvent être ajoutées afin d'obtenir un niveau de service et une bonne réactivité de son hébergeur en cas d'incident.

Documentation associée

– Note d'information sur les bonnes pratiques concernant l'hébergement mutualisé :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/

1.2 Actions et réactions

Cette semaine, le CERTA a informé le responsable d'un site web de la compromission de ce dernier. Le propriétaire n'a pas pris de mesure particulière malgré des problèmes évidents :

– ajout de fichiers et création de dossiers ;

– utilisation d'une version ancienne et vulnérable de `Joomla!`.

Le responsable du site préférait reporter la faute sur son hébergeur, étant persuadé que la compromission venait de celui-ci.

Ce comportement peut mettre en péril l'intégralité du serveur ainsi que tous les éventuels sites co-hébergés. Il est donc important de comprendre les raisons techniques qui ont conduit à la compromission et de prendre les mesures nécessaires pour éviter que cela ne se reproduise.

L'administrateur du site compromis a dans le cas présent accepté de revoir la sécurité de son site.

2 Alerte CERTA-2008-ALE-005

Des codes malveillants exploitant une vulnérabilité non corrigée de Microsoft portant sur le moteur de base de données Jet Database Engine se propagent sur l'Internet. Ces codes se présentent sous la forme d'un fichier au format Word auquel est associé un fichier de base de données caché sous une extension .doc. Cette propagation s'effectue via des courriels comportant en pièce jointe les fichiers infectés.

Dans la version rencontrée, ces courriels contiennent une pièce jointe au format `.rar`. Une fois ouverte, celle-ci révèle plusieurs fichiers semblant être au format « word » : certains le sont effectivement (par exemple `questions.doc`) et d'autres sont les bases de données associées (par exemple `~$questions.doc`) qui est en réalité un fichier `.mdb` (*Microsoft Access Database*). Ce type de fichiers fait partie de ceux référencés par Microsoft comme « non sécurisés ».

Les codes malveillants rencontrés sont mal reconnus par les antivirus mais nécessitent des droits d'administrateur pour s'exécuter correctement.

Le CERTA préconise d'appliquer les mesures de contournement proposées dans l'alerte du 26 mars 2008 dans l'attente d'un correctif.

Documentation

– Alerte CERTA-2008-ALE-005 du 25 mars 2008, « Vulnérabilité dans Microsoft Jet Database Engine » :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-005/

– Avis de sécurité Microsoft 950627 du 21 mars 2008 :
http://www.microsoft.com/technet/security/advisory/950627.mspx

– Bloc-Notes de Microsoft, « Update Microsoft Security Advisory (950627) » du 24 mars 2008 :
http://blogs.technet.com/msrc/archive/2008/03/24/update-msrc-blog-microsoft-security-advisory-950627.aspx

– Note Microsoft, « Vue d'ensemble des types de fichiers non sécurisés dans les produits Microsoft » :
http://support.microsoft.com/kb/925330

– Note Microsoft, *Jet Expression can execute unsafe Visual Basic for Applications fonctions* :
http://support.microsoft.com/kb/239104

3 Bandeau de publicité et niveau de confiance

Un expert en sécurité a récemment détaillé la problématique de l'utilisation de bandeaux de publicité dans des sites officiels.

Cette pratique très courante consiste à placer dans un site un cadre (ou *frame*) pointant vers un bandeau hébergé sur un serveur tiers.

Le problème est qu'il est tout à fait possible d'inclure dans ce cadre publicitaire, en plus de l'image, du javascript ou bien une *applet* flash (cf. le bulletin d'actualité CERTA-2008-ACT-016). Dès lors, on comprend que le niveau de confiance d'un site officiel repose en partie sur celui qui héberge le bandeau de publicité.

Or le chercheur a observé que de nombreux bandeaux étaient hébergés par un nombre restreint de sociétés spécialisées dans le domaine. Malheureusement, elles sont parfois peu regardantes sur la sécurité et la qualité du contenu hébergé. Une faille a d'ailleurs été identifiée par le chercheur, mettant en évidence qu'il était possible d'injecter via ces bandeaux du code malveillant dans le contexte d'un site tout à fait officiel.

Une autre technique dangereuse a également été mise en évidence : certains fournisseurs d'accès configurent leurs serveurs de résolution de nom (`DNS`) pour que, lorsqu'un domaine n'est pas trouvé par un client, soit affichée une page de publicité plutôt qu'une erreur disgracieuse. Là encore, ce type de comportement est à risque car ces pages de publicité sont fournies par le même genre d'hébergeurs que les bandeaux précédemment cités. Une simple erreur de frappe dans une barre d'adresse pourrait donc conduire à une injection de code dans le contexte du navigateur de la victime. On peut également imaginer que la page de publicité soit remplacée par une page de filoutage (*phishing*).

Recommandations:

Dans ce contexte, il est assez difficile de se protéger de ce type de menaces puisque l'attaque peut être conduite alors que l'utilisateur navigue sur un site officiel. Le niveau de sécurité est fixé par le serveur hébergeant la publicité.

Il existe des outils filtrant la publicité, certains sont même intégrés aux navigateurs mais le plus sûr reste encore la désactivation du support des langages comme javascript, flash, ActiveX,... dans les navigateurs. Ceux-ci sont souvent indispensables à la conduite de ce type d'attaques.

4 Les consoles retro-connectées

Entre l'exploitation d'une vulnérabilité permettant l'exécution de code arbitraire et le contrôle à distance d'une machine, il y a souvent une étape consistant à ouvrir un canal avec une console (*shell*) utilisable à distance. Plusieurs façons de faire sont déjà bien connues. Il est possible d'utiliser `netcat`, de charger un programme à l'aide de `wget` ou de recompiler localement un programme injecté en texte. Dans tous les cas, il s'agit de mettre quelque chose en écoute sur un port et d'attendre que la connexion soit établie depuis l'exterieur. Ces « services » en écoute sont identifiables avec la commande `netstat`.

Dans le cas suivant, le processus *nc* écoute sur le port 20000/tcp

```
#nc -l -p20000
#netstat -l -t tcp
tcp 0 0 *:20000 *:* LISTEN
```

Le principe peut etre inversé en faisant initialiser les connexions par la machine compromise, à destination de la machine de l'attaquant, et cela avec les mêmes outils.

Même si, la plupart du temps, ces rétro-connexions sont directement effectuées à partir des fonctions embarquées dans le code d'exploitation, il est possible de mener cette pratique à partir de commandes simples du système. Par exemple les commandes sous Linux `nc MonSite.tld 13` ou `cat </dev/tcp/MonSite.tld/13` établissent une connexion avec le serveur *MonSite.tld* sur le port 13/tcp. (la seconde nécessite cependant l'utilisation d'un *bash* compilé avec l'option *–enable-net-redirections* et ne fonctionne pas par défaut sur toutes les distributions).

Pour les machines ayant une utilisation définie, il est important de se limiter aux flux utiles. Un serveur n'a pas de raison *a priori* d'établir des connexions vers l'exterieur (à voir en fonction de la PSSI locale), et un poste client ne devrait pas recevoir de requêtes de connexion. Mais cela n'est pas suffisant ; les exemples ci-dessus montrent qu'une machine compromise peut initialiser une connexion vers une adresse malveillante en utilisant un port autorisé et ainsi être discrètement contrôlée à distance.

Pour détecter ce genre d'incident le CERTA recommande l'analyse régulière des flux, en plus de leur limitation. Cette analyse peut reposer sur la bonne configuration des journaux existants et sur le déploiement d'équipement dédiés.

4.1 Documentation

– Le manuel de *bash* :
http://www.gnu.org/software/bash/manual/html

– Site du programme *netcat* :
http://netcat.sourceforge.net

5 Les redirections *Google* au service de codes malveillants

Il apparaît dans l'actualité de nombreux codes malveillants détournant des fonctionnalités du moteur de recherche à des fins malveillantes. En effet *Google* offre plusieurs services annexes à son moteur de recherche que des individus malveillants ne manquent pas d'utiliser et de détourner afin de tromper la vigilance des utilisateurs.

Parmi les fonctionnalités offertes par *Google*, il existe le service *Google Adwords/Adsense* qui permet de créer des liens publicitaires et commerciaux afin que le moteur de recherche les affiche lors de la recherche d'un ou plusieurs mots clés. Ces liens, plus particulièrement ceux de *AdSense for domains*, ont une forme assez spécifique car ils se présentent comme ceci :

```
http://www.google.com/pagead/iclk?sa=l&ai=YYYYYYY&num=XXXXX&
                                    adurl=http://monsite/mapage.php
```

Des personnes malintentionnées se servent de ce service afin de rediriger les personnes vers des sites malveillants. Les utilisateurs ne prêtant pas davantage attention au lien, voient un lien *Google* qu'ils considèrent de confiance et cliquent sans vérifier l'intégralité du lien. Ce lien redirige en fait vers une page malveillante. Ces lignes peuvent aussi amener les utilisateurs à consulter les pages du lien sans action spécifique de leur part, grâce à un *iframe* ou un *wget*.

Les liens de ce type présentent au moins deux avantages pour quelqu'un désirant commettre des actions malveillantes :

– il permet de contourner certains filtrages d'adresses réticulaires en s'appuyant sur l'éventuelle confiance qu'un filtre accorde aux adresses associées *google.com* ;
– les utilisateurs finaux ne vérifient pas systématiquement l'intégralité de l'adresse, surtout si le lien est très long.

Le CERTA recommande donc une grande vigilance avant de cliquer sur un lien, même si celui-ci est fourni par une personne ou un site supposé de confiance. Cette technique est, entre autres, utilisée par des codes malveillants se répandant via les messageries instantanées. Par exemple, cela peut se faire sous la forme d'une demande à la liste des contacts de la personne compromise de cliquer sur un lien. Il est également possible de mettre en place une politique de filtrage en sortie, par exemple sur le serveur mandataire (qu'il soit sur l'intranet ou local sur un poste), afin de ne pas donner suite à ce type de requête de la forme *http://....=http://.....*

Enfin, il est recommandé d'inspecter régulièrement les journaux d'événements afin de repérer des requêtes de type *http://....=http://....* signe d'une redirection qui peut être suspecte.

6 Interprétation d'URI

Les protocoles associés aux URI (*Uniform Resource Identifier*) les plus fréquentes que nous utilisons sont : `http://`, `mailto://` ou `ftp://`.

Le standard RFC 4395 maintient les directives que des nouvelles URI doivent ou peuvent respecter. Il ne fournit cependant aucune liste des préfixes actuellement utilisé.

Plusieurs préfixes existent comme :

– `firefoxurl`://
– `acrobat`://
– `aim`://
– `picasa`://
– `gtalk`://
– etc.

Ces préfixes sont ajoutés au cours de l'installation de certains logiciels. L'installation modifie par exemple la base de registres sous Windows pour faciliter l'accès à l'application via le navigateur. Le préfixe est alors associé à une ligne de commandes permettant d'exécuter l'application avec des paramètres par défaut.

Ces fonctionnalités sont largement utilisées par plusieurs systèmes d'exploitation, parmi lesquels Windows, Mac OS X ou Linux. Cela inclut également des systèmes comme Windows Mobile ou Symbian pour les téléphones portables ou les assistants personnels.

Les attaques par injection de code indirecte peuvent profiter de ces fonctionnalités. En effet, ces liens donnent un accès direct aux applications et peuvent donc permettre d'atteindre ces dernières. Ce lien peut éventuellement comprendre des options complémentaires ou profiter d'erreurs du contrôle des paramètres fournis dans la ligne de commande.

Le CERTA rappelle à cette occasion les récentes vulnérabilités qui ont impliqué, avant corrections, le protocole `res://`, et ayant fait l'objet du bulletin de sécurité Microsoft MS07-035. Le bulletin d'actualité CERTA-2007-ACT-045 mentionnait également les préfixes `data:` et `jar:`.

Sans reprendre dans le détail les problèmes associés à chacun de ces préfixes, le lecteur comprendra qu'ils offrent un moyen indirect d'accéder à des applications et de nouvelles vulnérabilités potentielles par le biais d'une page Web.

Le CERTA recommande donc de contrôler ces interprétations de préfixes et de les supprimer si elles ne sont pas nécessaires. De manière générale, il faut éviter que des applications n'ayant pas de raison de communiquer puissent interagir simplement entre elles. Cela est d'autant plus important quand ces applications interagissent et interprètent des données issues de l'internet.

Documentation

- RFC 4395, "Guidelines and Registration Procedures for New URI Schemes", février 2006 : http://www.apps.ietf.org/rfc/rfc4395.html
- RFC 2368, "The mailto URL scheme", juillet 1998 : http://www.apps.ietf.org/rfc/rfc2368.html
- RFC 3986, "Uniform Resource Identifier (URI): Generic Syntax", janvier 2005 : http://www.apps.ietf.org/rfc/rfc3986.html

7 Nouvelle version d'*OpenBSD*

La version 4.3 du système d'exploitation *OpenBSD* est sortie le 1er mai 2008, à la suite de son traditionnel cycle de 6 mois pour une nouvelle version. Cette sortie apporte son lot de nouveautés et de modifications.

La liste de l'ensemble des changements est disponible sur le site de la distribution, mais voici les principales :

- le support des serveurs de type *hppa K-class* et des processeurs *88110* ;
- ajout de *SMP* pour les plates-formes *sparc64* et *mvme88k* ;
- l'intégration de nombreux nouveaux pilotes réseau, notamment de cartes WiFi :
- application dans la nouvelle version stable du correctif empêchant l'exploitation d'un dépassement de mémoire tampon dans le protocole *ppp* ;
- intégration du correctif *OpenSSL* ;
- correction du serveur *DHCP* afin de se protéger d'une corruption par un client malveillant.

Pour de plus amples informations, les liens vers la liste complète des modifications et la page de téléchargement sont disponibles dans la documentation.

Documentation

- Liste de apports entre *OpenBSD* 4.2 et *OpenBSD* 4.3 : http://www.openbsd.org/plus43.html
- Pour télécharger *OpenBSD* 4.3 : http://www.openbsd.org/ftp.html

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 24 avril et le 01 mai 2008.

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 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'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel règlementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

Quoique puisse suggérer ce document, la politique de sécurité en vigueur dans votre service doit primer.

Cette section précise néanmoins quelques mesures générales de nature à vous prémunir contre les agressions décrites dans ce document. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

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 oeuvre (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 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.

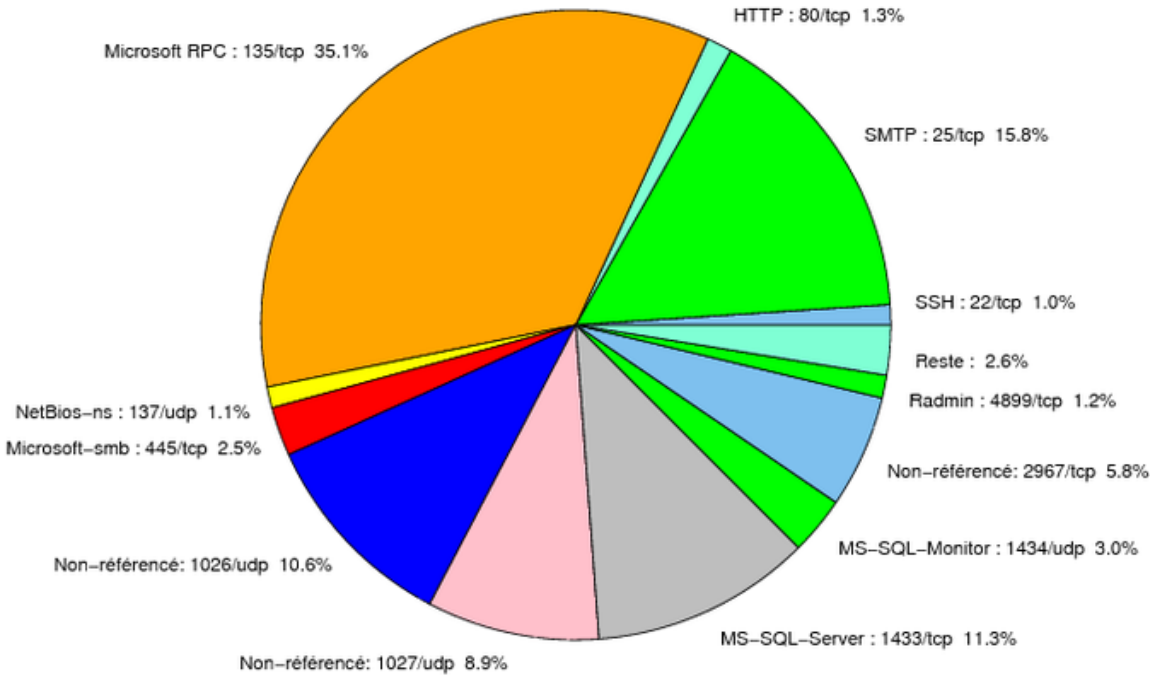

FIG. 1: Répartition relative des ports pour la semaine du 24.04.2008 au 01.05.2008

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	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
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT CERTA-2007-ALE-005-001
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CERT
69	UDP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CERT
80	TCP	HTTP	–	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
106	TCP	MailSite Email Server	–	– http://www.certa.ssi.gouv.fr/site/CERT
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERT
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CERT
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERT
139	TCP	NetBios-ssn et samba	–	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 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/CER
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6106	TCP	Symantec Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6502	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6503	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6504	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
8080	TCP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
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/CER
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CER
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CER
54345	TCP	HP Mercury	–	http://www.certa.ssi.gouv.fr/site/CER
65535	UDP	LANDesk Management Suite	–	http://www.certa.ssi.gouv.fr/site/CER

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

port	pourcentage
135/tcp	35.1
25/tcp	15.77
1433/tcp	11.32
1026/udp	10.56
1027/udp	8.85
2967/tcp	5.79
1434/udp	2.96
445/tcp	2.51
80/tcp	1.34
4899/tcp	1.16
137/udp	1.07
22/tcp	1.03
23/tcp	0.94
143/tcp	0.35
3306/tcp	0.17
42/tcp	0.13
6129/tcp	0.08
3389/tcp	0.04

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

02 mai 2008 version initiale.