Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 mars 2007
N° CERTA-2007-ACT-011

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-11

Dernière version de ce document : http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-011

Gestion du document

Référence	CERTA-2007-ACT-011
Titre	Bulletin d'actualité 2007-11
Date de la première version	16 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-011.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-011/

1 Activités en cours

1.1 Compromissions en exploitant des vulnérabilités de PMB

Le CERTA a traité cette semaine plusieurs incidents concernant des serveurs web, suite à l'exploitation de vulnérabilités du logiciel *PMB* (appelé également *PhpMyBibli*).

Ce logiciel libre français de gestion de bibliothèque a fait l'objet de deux avis du CERTA cette semaine (CERTA-2007-AVI-117 et CERTA-2007-AVI-128).

Historique rapide :

Le 9 mars 2007, des sites Internet publient des informations permettant :

– d'exploiter des vulnérabilités de la version 3.0.13 de PMB ;

– de trouver des sites utilisant ce logiciel.

Quelques heures après, des sites web d'administrations nationales et locales sont défigurés. Le traitement de l'une de ces défigurations a révélé une compromission plus grave, avec l'installation de plusieurs outils sur le serveur, destinés à :

– attaquer le réseau local du serveur compromis ;

– exécuter des dénis de services (flood) ;
– inclure le serveur dans un réseau de machines compromises (botnet).

Un autre incident, remonté par un correspondant du CERTA, a montré que le serveur compromis a servi à transmettre des courriels à des internautes pour les inciter à se connecter à un site frauduleux.

La connexion à ce dernier provoquait le chargement sur le poste de l'internaute d'un cheval de Troie, reconnu par peu d'antivirus, et la possible intégration du poste infecté à un botnet.

Le CERTA a émis un premier avis (CERTA-2007-AVI-117), l'éditeur ayant corrigé une vulnérabilité. Ce correctif s'est révélé insuffisant. Le travail concerté avec un ministère et avec l'éditeur a conduit à colmater d'autres brèches dans le logiciel. Un second avis (CERTA-2007-AVI-128) indique la version qui pare aux attaques utilisées cette semaine.

D'autres attaques plus discrètes, avec utilisation des serveurs compromis, ont pu avoir lieu.

Ces incidents prouvent une fois encore que :
– le mécanisme d'inclusion de PHP est intrinsèquement dangereux ;
– la défiguration d'un site est la partie visible de l'iceberg, la compromission pouvant être plus grave.

Recommandations :

– Vérifier l'intégrité des serveurs utilisant PMB et analyser les journaux des 7 derniers jours ;
– en cas de défiguration, toujours penser que l'intrusion peut être plus grave ;
– en cas de découverte de compromission, préserver les traces et alerter le responsable SSI (CERTA-2002-INF-002) ;
– migrer vers la version 3.0.17 indiquée dans l'avis CERTA-2007-AVI-128 ;
– respecter le principe de défense en profondeur :
  – appliquer les mises à jour du système et des logiciels ;
  – supprimer les services inutiles ;
  – filtrer les accès entrant selon la finalité du serveur ;
  – filtrer les accès sortant du serveur ;
– analyser régulièrement les journaux de connexion aux serveurs et le trafic du réseau.

1.2 Infections SpamThru

Le CERTA a été informé de l'infection de nombreuses machines par un code malveillant appelé SpamThru par certains éditeurs d'antivirus. Ce code malveillant a pour effet, entre autres, de transformer la machine infectée en robot de spam. La détection des machines infectées se fait essentiellement par l'analyse du trafic réseau. En effet, celles-ci tentent de se connecter par HTTPS (port 443/tcp) à quelques serveurs spécifiques afin de télécharger d'éventuelles mises à jour et les messages à propager (spam).

Les machines infectées sont également susceptibles d'engendrer un important trafic SMTP.

Recommandations :

Il est recommandé de vérifier qu'aucune connexion ne s'effectue vers des serveurs de messagerie non légitimes (trafic SMTP) et qu'aucune machine n'est à l'origine d'un envoi massif de messages électroniques.

1.3 Externaliser les fichiers journaux

Cette semaine, le CERTA a traité une compromission de site internet. Le site était hébergé dans un serveur web mutualisé sur lequel il n'y avait pas suffisament de cloisonnement. L'un des sites des clients de ce serveur était vulnérable à des attaques de type PHP INCLUDE. La personne malveillante, ayant réussi à avoir accès au serveur, a pu compromettre l'ensemble des sites hébergés sur la machine. De plus, les fichiers journaux de chaque site web étaient stockés dans la même arborescence. Le malfaiteur, avant de quitter le serveur, a pu sans difficulté supprimer tous les fichiers journaux de la machine.

Le CERTA rappelle à cette occasion le besoin de déporter régulièrement les fichiers journaux sur une autre machine afin de ne pas risquer de perdre l'ensemble des informations en cas de panne ou de compromission.

2 Vulnérabilité dans Internet Explorer 7

2.1 Présentation

Une vulnérabilité a été publiée cette semaine, à propos d'Internet Explorer 7. Elle n'est pas encore corrigée, mais pourrait être utilisée dans le cadre d'attaques par filoutage (*phishing*). En voici les détails :

Lorsqu'une tentative d'accès à une page Web, par exemple *http://www.certa.ssi.gouv.fr* échoue, le navigateur affiche une page par défaut, avec un lien vers la page inaccessible pour réessayer ultérieurement. Cela se présente alors sous la forme :

```
res://ieframe.dll/navcancl.htm#http://www.certa.ssi.gouv.fr
```

Internet Explorer 7 n'affichera que `http://www.certa.ssi.gouv.fr` dans la barre d'adressage. Cette technique peut donc être utilisée pour une attaque par filoutage. Le site de filoutage se trouve localement sur la machine. Il suffit alors de forcer la personne à cliquer sur un lien de type `res://ieframe.dll/navcancl.htm#`, pour la rediriger vers une page d'erreur, puis la page falsifiée du site de filoutage.

Cette attaque nécessite plusieurs conditions, comme une modification de la page `navcancl.htm` et des actions de l'utilisateur. Cependant, le scénario peut très bien survenir dans un environnement qui n'est pas de confiance, sur une machine tierce (cyber-café, ordinateurs partagés, etc.).

2.2 Recommandations

Dans l'attente d'un correctif pour Internet Explorer 7, il est recommandé de :

- filtrer les liens de type `res://` pour récupérer des ressources personnalisées sous Windows. Leur utilisation dans le corps d'un courrier électronique ou sur une page Web externe est peu courante, voire très suspecte.
- ne pas faire confiance à la touche 'rafraichir' en cas d'erreur. Il vaut mieux retaper directement l'adresse du site demandé.
- comparer l'empreinte (MD5 par exemple) de la page `navcancl.htm` avec celle d'un système sein.

3 Les acteurs de filoutage veulent en savoir plus

Le CERTA a été informé de nouvelles variantes dans les arnaques par filoutage (ou *phishing*) sur Internet. Le principal intérêt du filoutage est de récupérer des informations confidentielles, notamment bancaires à l'insu des victimes. Des variantes peuvent exister, par exemple une victime reçoit dans sa messagerie électronique un courrier de confirmation de son inscription payante à un site pour adultes. Le courrier l'informe du montant de son inscription, de ses identifiants de connexions (nom d'utilisateur et mot de passe) ainsi que du moyen de stopper les prélèvements sur son compte bancaire (en entrant ses coordonnées bancaires sur le site frauduleux). Par ce moyen, les auteurs de cette arnaque espèrent que des victimes rentreront leur coordonnées bancaires mais également que certaines d'entre elles essayeront de se connecter sur le site pour adulte avec les identifiants fournis. Si des victimes s'exécutent, il est à parier qu'elles recevront dans les prochains jours des courriers non solicités (*SPAM*) concernant des sites pour adultes.

4 Filtre anti-filoutage sous Firefox

Depuis la version 2.0 de Mozilla Firefox, le navigateur permet d'alerter l'utilisateur, au moyen d'un message visuel, lorsqu'il navigue sur un site suspecté d'être un site de phishing.

Une vulnérabilité non corrigée permet à un utilisateur malintentionné de contourner cette protection en ajoutant dans l'adresse réticulaire des caractères slash ('/') multiples. Le message d'alerte visuel n'apparaît alors plus à la victime.

Exemple : http://example.phishing.dot////sitefraduleux/

Il est donc important de vérifier, dans l'attente d'un correctif, que de telles URL n'apparaissent pas au niveau de serveurs `proxy`.

5 Retour sur les vulnérabilités IPv6 de cette semaine

5.1 OpenBSD sous les projecteurs

Le CERTA a publié l'avis CERTA-2007-AVI-113 concernant OpenBSD. Le problème provient initialement d'une vulnérabilité au niveau d'un tampon (`mbuf`). Ce dernier est utilisé pour manipuler les données IPv6, et un code d'exploitation a démontré qu'il était possible, en adressant un paquet spécialement construit au système vulnérable, d'exécuter du code arbitraire à distance sur celui-ci. Plus précisément, le débordement de tampon survient après la réception de paquets `ICMPv6` fragmentés.

Cette vulnérabilité a fait grand bruit pour plusieurs raisons, la principale étant la configuration par défaut d'un système OpenBSD : le noyau dit `GENERIC` active IPv6, et le pare-feu `pf` d'OpenBSD ne filtre aucun paquet IPv6 arrivant sur les interfaces du système.

Cette vulnérabilité, qui ne serait pas toute récente, a poussé les développeurs d'OpenBSD à modifier leur fameuse phrase de bienvenue sur leur site : "*Only one remote hole in the default install, in more than 10 years!*" par "*Only two remote holes in the default install, in more than 10 years!*"

Un correctif provisoire est actuellement disponible, ainsi que des contournements pour filtrer le trafic IPv6.

http://www.coresecurity.com/?action=item&id=1703

ftp://ftp.openbsd.org/pub/OpenBSD/patches/4.0/common/010_m_dup1.patch

5.2 Le noyau Linux

Le CERTA a également publié cette semaine l'avis CERTA-2007-AVI-120, concernant une vulnérabilité de la fonction `ipv6_getsockopt_sticky`, qui se trouve dans les noyaux Linux (`net/ipv6/ipv6_sockglue.c`). Tout noyau ayant une version antérieure à la 2.6.20.2 serait potentiellement vulnérable. L'exploitation, qui peut se faire localement, permet à une personne malveillante d'accéder à une partie de la mémoire et d'élever ses privilèges.

Le code d'exploitation est disponible publiquement. Le problème vient du fait qu'IPv6 est activé par défaut dans la plupart des distributions Linux récentes.

5.3 Les recommandations du CERTA

Les évènements de cette semaine montrent bien toute l'ambiguïté d'IPv6. Les nouveaux protocoles s'imposent d'eux-même dans les systèmes d'exploitation récents, alors que deux problèmes subsistent :

– les administrateurs ne sont pas encore formés à cette technologie ;

– cette technologie continue d'évoluer, et les mises en œuvre ne sont pas nécessairement très fiables.

Le CERTA avait publié en 2006 une note d'information concernant IPv6. La section 6.2 a été enrichie cette semaine, pour apporter quelques méthodes de désinstallations. Des règles de filtrage sont également explicitées.

6 Le Javascript est omniprésent

Quand l'occasion se présente, le CERTA conseille de désactiver par défaut l'exécution de codes (scripts, applets, ActiveX, etc.). Cela est valable pour les codes Javascript interprétés dans les navigateurs les plus courants (Firefox, Internet Explorer).

Le CERTA tient à attirer l' attention sur le fait que Javascript est de plus en plus utilisé et intégré à d'autres formats de données que les pages HTML. Ainsi, le bulletin d'actualité du CERTA de la semaine dernière (CERTA-2007-ACT-010) mentionnait l'interprétation du javascript par Adobe Acrobate Reader, ce qui a induit une faille dans ce logiciel, exploitée par un code disponible sur l'Internet.

Cette semaine, le logiciel Quicktime est à l'honneur. Un cheval de Troie nommé `JS/SpaceTalk Trojan` a été découvert, se présentant sous la forme d'un fichier vidéo au format `.mov`. Il rappelle brutalement que ce format peut intégrer du code Javascript. Cette propriété se nomme `HREF track` chez Apple et sera également reconnue sous iTunes.

Ces trois logiciels ne semblent pas être les seuls à interpréter ce langage, qui peut aussi être intégré insidieusement dans des formats `flash` ou `MP3`. Il semblerait que d'autres logiciels interprétent le Javascript : lecteurs audio, lecteurs videos, lecteurs Flash, lecteurs PDF, ... Plus important, certains logiciels ne proposent même pas à l'utilisateur de désactiver l'interprétation automatique de ce langage.

Face à ce problème, le CERTA recommande à ses lecteurs la plus grande vigilance envers les logiciels qu'ils emploient. Il convient de désactiver le support du javascript quand c'est possible, et de migrer vers un logiciel alternatif lorsque la désactivation n'est pas possible.

Une bonne pratique consiste à regarder attentivement les options de configuration, avant toute utilisation d'une nouvelle application, aussi réputée soit-elle.

7 Publications Microsoft de cette semaine

Les versions anglaises des services packs 2 pour Windows Server 2003 version 32 bits et Windows XP Professionel version 64 bits ont été publiés respectivement le 12 et 13 mars 2007. Les versions françaises ne sont pas encore disponibles.

Cette mise à jour comporte de nombreux correctifs, dont 51 de sécurité, et quelques améliorations, parmi lesquelles :

- le « Scalable Networking Pack » (SNP), qui permet une gestion du réseau moins coûteuse pour le processeur ;
- le support du WPA2 qui permet une meilleure sécurité du sans-fil Wi-Fi ;
- les « Windows Deployment Services » (WPS), qui permettent notamment de déployer des machines sous Windows Vista plus facilement ;
- des améliorations pour IPSEC, le pare-feu de Windows, la virtualisation, les performances de SQL-Server, etc.

Attention toutefois, cette mise à jour désinstalle certains « *hotfixes* » précédemment installés qu'il faudra réinstaller par la suite. Un utilitaire développé par Microsoft est disponible pour les identifier avant ou après la mise à jour.

8 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 08 et le 15 mars 2007.

9 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/

10 Rappel des avis émis

Durant la période du 08 au 15 mars 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-115 : Vulnérabilité de Computer Associates eTrust Admin
- CERTA-2007-AVI-116 : Vulnérabilité dans Novell NetMail
- CERTA-2007-AVI-117 : Vulnérabilité de PMB
- CERTA-2007-AVI-118 : Vulnérabilité dans MySQL
- CERTA-2007-AVI-119 : Vulnérabilité dans Wordpress
- CERTA-2007-AVI-120 : Vulnérabilité du protocole IPv6 dans le noyau Linux
- CERTA-2007-AVI-121 : Vulnérabilité de la machine Java sous HP-UX
- CERTA-2007-AVI-122 : Vulnérabilité dans MPlayer et Xine-lib
- CERTA-2007-AVI-123 : Vulnérabilités dans le noyau Linux
- CERTA-2007-AVI-124 : Vulnérabilités dans MacOS X
- CERTA-2007-AVI-125 : Vulnérabilité dans Adobe JRun et ColdFusion MX
- CERTA-2007-AVI-126 : Vulnérabilité dans Sun Java System Web Server
- CERTA-2007-AVI-127 : Vulnérabilité dans les produits Trend Micro
- CERTA-2007-AVI-128 : Vulnérabilités dans PMB
- CERTA-2007-AVI-129 : Vulnérabilité dans CUPS

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

- CERTA-2007-AVI-024-001 : Multiples vulnérabilités dans Adobe Acrobat
  (ajout des références à Red Hat, Sun, SuSE, Gentoo)
- CERTA-2007-AVI-076-003 : Multiples vulnérabilités dans php
  (ajout de la référence SuSE)
- CERTA-2007-AVI-093-002 : Multiples vulnérabilités dans ClamAV
  (ajout des références Debian, SuSE et Gentoo)
- CERTA-2007-AVI-094-001 : Vulnérabilité dans SpamAssassin
  (ajout des mises à jour de sécurité Gentoo, Fedora, Mandriva, Red Hat)
- CERTA-2007-AVI-095-001 : Vulnérabilité de Snort
  (ajout de la référence au correctif pour Gentoo)
- CERTA-2007-AVI-102-002 : Multiples vulnérabilités de produits Mozilla
  (ajout des références aux mises à jour de sécurité Ubuntu, Gentoo, SuSE, Mandri va)
- CERTA-2007-AVI-113-001 : Vulnérabilité dans OpenBSD
  (ajout du caractère distant de la vulnérabilité via un paquet `ICMPv6`)
- CERTA-2007-AVI-114-001 : Vulnérabilité dans GnuPG
  (ajout des références aux mises à jour de Fedora et Red Hat)

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.

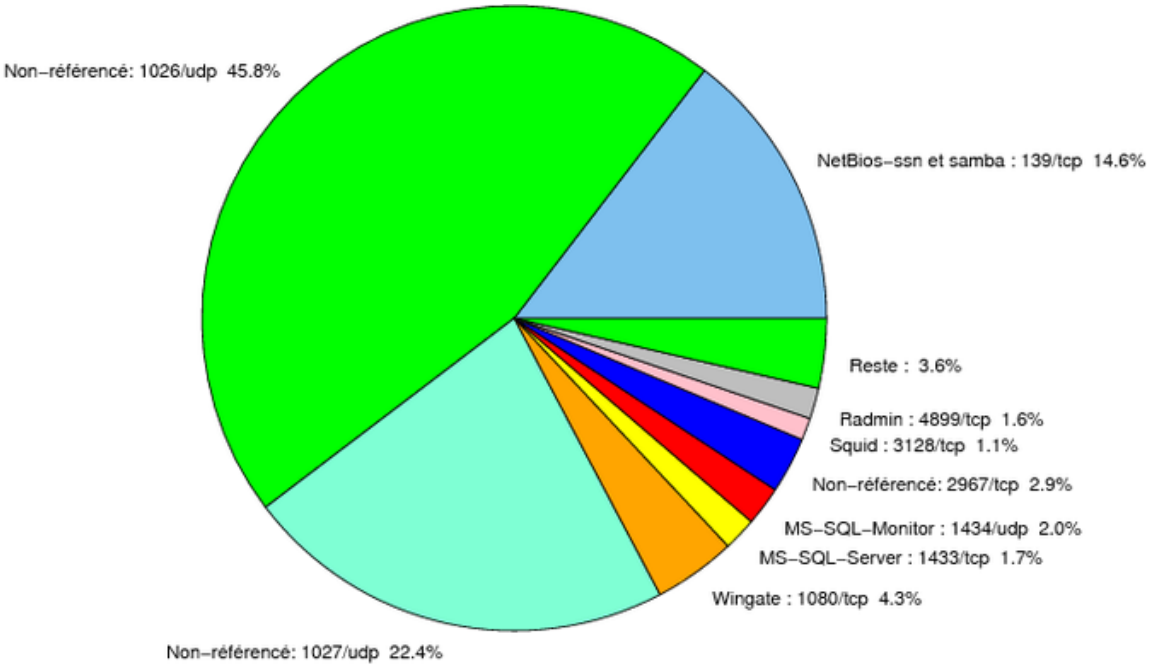

FIG. 1: Répartition relative des ports pour la semaine du 08.03.2007 au 15.03.2007

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	45.76
1027/udp	22.4
139/tcp	14.57
1080/tcp	4.26
2967/tcp	2.9
1434/udp	2.02
1433/tcp	1.72
4899/tcp	1.6
3128/tcp	1.14
137/udp	0.93
80/tcp	0.69
25/tcp	0.48
443/tcp	0.45
22/tcp	0.42
2100/tcp	0.18
21/tcp	0.15
143/tcp	0.06
3306/tcp	0.03

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

16 mars 2007 version initiale.