Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 janvier 2009
N° CERTA-2009-ACT-005

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-05

Conditions d'utilisation de ce document : http://www.certa.ssi.gouv.fr/certa/apropos.html
Dernière version de ce document : http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-005

Gestion du document

Référence	CERTA-2009-ACT-005
Titre	Bulletin d'actualité 2009-05
Date de la première version	30 janvier 2009
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-2009-ACT-005.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-2009-ACT-005/

1 TYPO3 et ses vulnérabilités

1.1 Présentation

Les éditeurs de *TYPO3* ont récemment annoncé que les correctifs fournis par les versions 4.0.10, 4.1.8 et 4.2.4 contenaient des régressions. Depuis le 24 janvier 2009, de nouvelles versions de *TYPO3* sont disponibles en téléchargement (versions 4.0.11, 4.1.9 et 4.2.5). Ces nouvelles versions ne sont pas considérées comme des correctifs de sécurité mais remédient à ces régressions.

Nous avions évoqué, dans le bulletin d'actualité CERTA-2009-ACT-004, l'importance de changer la clé de chiffrement après application des correctifs de sécurité. Le « découvreur » de la vulnérabilité concernant le chiffrement a récemment publié une vidéo ainsi qu'un outil permettant d'exploiter cette faille. Celle-ci permet notamment d'injecter du script (et donc d'insérer des liens vers des codes malveillants) sur les sites Web ayant une clé faible. Ces attaques sont particulièrement faciles à réaliser, et nous insistons donc sur la nécessité de créer de nouvelles clés de chiffrement pour les sites fonctionnant avec *TYPO3*.

1.2 Documentation

- Annonce des développeurs de *TYPO3* :
  http://typo3.org/news-single-view/?tx_newsimporter_pi1[showItem]=0&tx_newsimporter_pi1[feed]=10&cHash=c5554a06e2

2 Sans-fil... et sans reproche ?

2.1 Vulnérabilités des pilotes

Le CERTA a évoqué à plusieurs reprises dans ses bulletins d'actualité la problématique des vulnérabilités de pilotes pour les interfaces sans-fil. Outre les conséquences d'une exploitation réussie sur le système (accès aux droits noyau) se posent les questions de la disponibilité et de l'application des mises à jour.

Une vulnérabilité a ainsi été identifiée récemment pour les pilotes `Ralink`. Elle concernerait plusieurs types de cartes (rt73, rt2400, rt2500, rt2570 et rt61).

La vulnérabilité reste relativement simple. Les requêtes de sondage (*probe*) ne sont pas correctement interprétées, en particulier quand le champ caractérisant l'identifiant SSID a une longueur excessive. Une variable non signée dont la valeur est comprise entre 128 et 255 sera en réalité traitée comme une valeur de -128 à -1, contournant ainsi l'un de contrôles.

La carte doit cependant être en mode *ad-hoc* (communication de machine à machine sans infrastructure avec point d'accès) pour être vulnérable.

La société soutient le portage des pilotes pour différents systèmes d'exploitation. Aucune mise à jour officielle n'est cependant diffusée à la date de rédaction de cet article.

La vulnérabilité peut toucher aussi bien des environnements Windows que Linux ou Macintosh. Des correctifs sont apportés par quelques initiatives de développeurs (sous Debian par exemple).

Cet exemple donne l'occasion au CERTA de rappeler l'un des risques intrinsèques majeurs au sans-fil : les interfaces peuvent être atteintes par tout signal sans aucun contrôle a priori de l'interprétation qui en est faite. Une vulnérabilité au niveau des pilotes rend caduques les solutions de sécurité mises en place à des couches supérieures (IPsec, VPN, WPA...).

Il est donc important :

- de ne pas utiliser d'équipements avec des interfaces sans-fil quand cela n'est pas nécessaire ;
- de désactiver physiquement les interfaces quand elles ne sont pas utilisées ;
- de vérifier régulièrement auprès des constructeurs si des nouvelles versions de pilotes sont disponibles ;
- de mettre en place des tunnels chiffrants de confiance en amont ;
- de sensibiliser les utilisateurs à ces risques souvent méconnus.

- Site de téléchargement des pilotes Ralink :
  http://www.ralinktech.com/ralink/Home/Support.html
- Avis de sécurité Debian, rt2400 :
  http://www.debian.org/security/2009/dsa-1712
- Avis de sécurité Debian, rt2500 :
  http://www.debian.org/security/2009/dsa-1713
- Avis de sécurité Debian, rt2570 :
  http://www.debian.org/security/2009/dsa-1714
- Référence CVE associée CVE-2009-0282 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0282
- Projet rt2x00 pour le développement des pilotes sous Linux :
  http://rt2400.sourceforge.net/
- Portail de la Securité Informatique, « La problématique générale des réseaux sans-fil » :
  http://www.secinfo.gouv.fr/gp_article88.html

2.2 Services Bluetooth

Une vulnérabilité a été publiée cette semaine, concernant le service OBEX FTP avec Windows Mobile 6, pour les appareils utilisant la pile Bluetooth de Microsoft. La vulnérabilité ne fonctionne qu'après appariement (*pairing*) entre équipements et permet un accès à toute l'arborescence de l'équipement victime par traversée de répertoires.

Cette vulnérabilité peut donc être importante, dans le cas où l'attaquant remplace un exécutable existant ou l'installe à un endroit afin d'être sollicité au prochain redémarrage. Autoriser un accès FTP ne doit pas être équivalent à donner un accès à tout le système !

Il est donc important de maîtriser au mieux sa connexion Bluetooth, et en particulier :

- n'activer l'interface que quand cela est nécessaire ;
- s'apparier avec des équipements de confiance uniquement ;
- désactiver les options inutiles, comme le partage de fichiers dans les paramètres de configuration Bluetooth FTP.

3 Des activités DNS surprenantes

Plusieurs correspondants ont signalé au CERTA d'étranges traces visibles dans les journaux de leur serveur DNS. Avant toute chose, cette démarche de surveillance des journaux DNS est une excellente pratique qui a le mérite d'être ici soulignée.

Les traces en question sont les résidus d'une attaque en déni de service. Le serveur victime a pour adresse IP W.X.Y.Z.

Une personne malveillante émet alors depuis une ou plusieurs machines (botnet) plusieurs trames en UDP afin d'usurper l'adresse émettrice W.X.Y.Z à destination de plusieurs serveurs DNS. La requête envoyée demande de répondre à la question "NS .", i.e. de fournir la liste des serveurs de noms racines.

La liste est relativement longue et si une réponse est retournée, elle est contenue dans une trame de taille bien supérieure à la requête initiale. La réponse est adressée à W.X.Y.Z.

Cette forme d'attaque, dite d'amplification ou de concentration, utilise donc des serveurs quelconques pour aboutir. Ces serveurs n'ont pas besoin d'être récursifs ouverts. Il suffit qu'ils acceptent de répondre à la question "NS .".

Il est possible de tester son serveur depuis l'extérieur de son réseau, en l'interrogeant par exemple de la forme :

```
$dig @ADRESSE_VOTRE_SERVEUR NS .
```

Les tentatives rejetées par le serveur devraient être visibles dans les journaux du serveur. L'adresse qui interroge le serveur est celle de la machine réellement victime de l'attaque, soit W.X.Y.Z.

Si le serveur retourne une liste de serveurs racines, des modifications sont envisageables sur le serveur. Dans le cas contraire, il peut contribuer, sans autre mesure, aux attaques précédemment citées. Cette position n'est cependant pas obligatoire et correspond à un flou des standards. Néanmoins, la liste des serveurs racines est normalement connue par défaut (par où commencer l'interrogation DNS sinon ?).

Sous BIND, la correction consiste à modifier, pour les serveurs non récursifs, l'option globale suivante :

```
additional-from-cache no;
```

Cette option n'est pas disponible dans les versions les plus anciennes de BIND.

Il est également possible de mettre en place des politiques d'accès strictes par zone et de refuser toute requête dans la politique par défaut.

- Note d'information CERTA-2008-INF-002, « Du bon usage du DNS » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-002/
- Article de S. Bortzmeyer, « Attaque DNS par amplification en demandant 'NS .' », 24 janvier 2009 :
  http://www.bortzmeyer.org/dns-attaque-ns-point.html
- Article ISC SANS, « DNS queries for », 18 janvier 2009 :
  http://isc.sans.org/diary.html?storyid=5273
- Page Web de test proposée par l'ISC SANS :
  http://isc1.sans.org/dnstest.html
- Article de l'OARC-DNS, « Upward Referrals Considered Harmful », 22 janvier 2009 :
  https://www.dns-oarc.net/oarc/articles/upward-referrals-considered-harmful
- Liste de discussion NANOG :
  http://www.merit.edu/mail.archives/nanog/msg14428.html

4 Vulnérabilité dans FFmpeg

Cette semaine, le CERTA a émis l'avis CERTA-2009-AVI-041 concernant la bibliothèque `FFmpeg`. La vulnérabilité permet à une personne malintentionnée d'exécuter du code arbitraire sur le poste d'une victime ayant ouvert un fichier spécialement conçu au format `4xm`.

Des détails précis concernant la vulnérabilité sont disponibles sur l'Internet. Il est donc possible que des codes d'exploitation apparaissent bientôt. La faille est corrigée dans la version courante de `FFmpeg`, disponible dans le répositoire `SVN`.

`FFmpeg` est une bibliothèque très utilisée par les applications vidéo (*libavcodec*). Une liste non exhaustive est disponible sur le site de la bibliothèque (cf. section Documentation). On peut citer par exemple `VLC` et `Mplayer`. Il est donc très important de mettre à jour cette bibliothèque, soit manuellement soit via une mise à jour de l'application en question si elle est disponible.

4.1 Documentation

- Avis CERTA-2009-AVI-041 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-041/index.html
- Liste non exhaustive des applications utilisant FFmpeg :
  http://ffmpeg.mplayerhq.hu/projects.html

5 Fin du support du service pack 1 de Windows Serveur 2003

Le 14 avril 2009, Microsoft arrête le support du service pack 1 de Windows Serveur 2003. Ceci signifie qu'à cette date aucune mise à jour de sécurité ne fonctionnera sur un Windows Server 2003 qui n'est pas en Service Pack 2. Il est donc urgent d'installer le dernier service pack dès que possible sur tous les systèmes encore en Service Pack 1.

À cette occasion, le CERTA rappelle que le support pour les systèmes d'exploitation Windows 2000 prend fin le 13 juillet 2010 et que les organisations n'ayant pas encore envisagé de migration doivent le faire sans plus tarder.

5.1 Documentation

- Bloc-notes de Pascal Saulière :
  http://blogs.technet.com/pascals/default.aspx
- Politique de support des produits Microsoft :
  http://support.microsoft.com/gp/lifeselect

6 Le problème des scripts *inter-sites*

Dans le cadre de cet article, la dénomination de scripts *inter-sites* décrit les scripts contenus dans une page Web qui font des appels bloquants à du code situé sur un autre site.

Dans les faits voyons comment cela se traduit pour les utilisateurs. Ces derniers peuvent choisir de n'autoriser que les scripts nécessaires en utilisant par exemple des outils tels que *NoScript*. Lors de la visite d'une page, l'outil annonçant qu'il bloque l'exécution de plusieurs codes, l'utilisateur autorise alors ceux qui lui semblent légitimes, souvent ceux contenus sur le même site, espérant ainsi obtenir le fonctionnement nominal de la page. Si cela ne suffit pas et qu'il est nécessaire d'autoriser des scripts externes, c'est qu'il y a certainement des appels bloqués à du code tiers. Cela veut donc dire que le site utilise du code dont il n'est pas maître, avec tous les risques que cela implique, et que l'utilisateur ne peut pas accorder un niveau de confiance au site sans être obligé d'accorder le même niveau à l'hébergeur du code tiers.

Pour contourner le problème, des outils commencent à proposer des fonctionnalités de substitution de code à la volée. Si la fonction externe appelée est clairement identifiée, l'utilisateur aura un troisième choix, en plus d'autoriser et d'interdire, celui de substituer par une version locale qui s'exécutera dans le contexte de la page visitée. Cette solution permet de s'affranchir du problème d'autorisation, mais n'est qu'une méthode de contournement qui repose encore sur du code tiers.

Le CERTA recommande aux développeurs de faire attention à cette problématique. Si des appels externes doivent être faits (*modules statistiques, compteurs...*) ils ne doivent par être bloquants afin de laisser le choix à l'utilisateur des niveaux de confiance qu'il accorde.

7 MS08-067 et les versions embarquées de Windows

Le CERTA a déjà, à plusieurs reprises, abordé le sujet de la vulnérabilité `MS08-067`, massivement exploitée par des vers comme `Conficker` ou `Downadup`. Le détail de son mode de propagation et son fonctionnement général précédement détaillés ne seront pas rappelés ici.

Il paraît cependant intéressant de s'attarder sur certaines versions particulières de `Microsoft Windows` qui peuvent ne pas avoir été prises en compte dans le plan de déploiement des mises à jour. Ainsi, on trouve dans divers secteurs d'activité des versions 'modifiées' du système d'exploitation `Windows XP` appelées `Microsoft Windows XP Embedded`. Ces versions peuvent être présentes dans divers équipements comme les bornes de paiement, des bornes d'informations ou certaines caisses automatiques. On peut aussi les trouver dans les consoles asservissant un équipement médical comme des *scanners*, des appareils d'`IRM` (Imagerie à Résonance Magnétique) ou des robots d'assistance à la chirurgie. Des autocommutateurs téléphoniques privés (PBX/IPBX) peuvent aussi en être pourvus.

Or, la mise à jour de certains de ces équipements est parfois délicate. En effet, le problème est de s'assurer que l'application du correctif n'induira pas d'effets indésirables sur le fonctionnement de l'équipement asservi ou sur les autres logiciels du terminal en question. De plus, ces équipements sont souvent sous la responsabilité du fabriquant pour la maintenance. L'utilisateur final comme une banque, un commerçant, une collectivité ou un hôpital ne dispose souvent pas du 'droit' d'intervenir sur l'équipement. Il lui est, alors, impossible d'assurer la sécurité du système embarqué. Les services présents dans un `Windows Embedded` particulier peuvent varier énormement en fonction du contexte d'utilisation. Ainsi le service « Server » ne sera pas forcement présent ou activé. Il n'en reste pas moins que ces versions particulières de `Windows Embedded` non mises à jour restent vulnérables.

Dans ce contexte, il est indispensable d'avoir pris les mesures palliatives adéquates :

- ne pas connecter la machine sur le réseau même pour des raisons d'interopérabilité ou d'échanges de données ;
- limiter les échanges de données par le biais de supports comme les clefs `USB` ;
- établir un contrat de maintenance clair dans lequel figure les mises à jours de la partie « système d'exploitation » au moins pour les cas critiques.

En tout état de cause et dans le cas présent, lorsque l'on dispose de ce type de produits, il est indispensable de prendre contact avec le fabriquant ou l'intégrateur pour décider avec lui d'une procédure permettant d'appliquer les correctifs indispensables.

- Bloc-notes Microsoft Windows Embedded Standard, « December 2008 Updates are Available » :
  http://blogs.msdn.com/embedded/archive/2008/12/26/december-2008-updates-are-available-including-for-xpe-sp3-and-standard.aspx

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 22 et le 29 janvier 2009.

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 23 au 30 janvier 2009, le CERTA a émis les avis suivants :

– CERTA-2009-AVI-030 : Vulnérabilité dans Cisco Unified Communications Manager
– CERTA-2009-AVI-031 : Vulnérabilité des Serveurs Sun Serie M
– CERTA-2009-AVI-032 : Multiples vulnérabilités dans CA Cohesion Application Configuration Manager
– CERTA-2009-AVI-033 : Multiples vulnérabilités dans CA Anti-Virus
– CERTA-2009-AVI-034 : Vulnérabilité dans Sun Solaris
– CERTA-2009-AVI-035 : Vulnérabilité dans VNC Viewer
– CERTA-2009-AVI-036 : Vulnérabilités dans Horde
– CERTA-2009-AVI-037 : Vulnérabilité dans IMP
– CERTA-2009-AVI-038 : Vulnérabilité dans Sun Java System Access Manager
– CERTA-2009-AVI-039 : Vulnérabilité des serveurs SunFire X2100 M2 et X2200 M2
– CERTA-2009-AVI-040 : Vulnérabilité dans Sun Solaris
– CERTA-2009-AVI-041 : Vulnérabilité dans FFmpeg

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'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.

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 oeuvre (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 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.ssi.gouv.fr/fr/formation/

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.

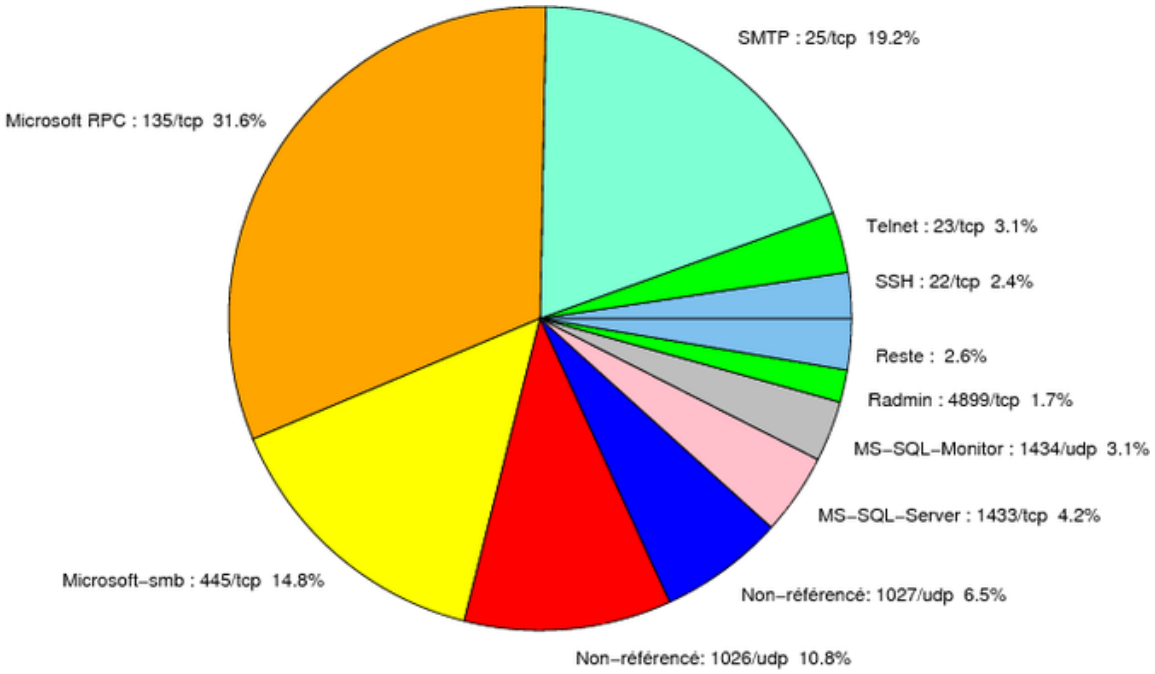

FIG. 1: Répartition relative des ports pour la semaine du 22.01.2009 au 29.01.2009

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/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 http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CER
389	TCP	LDAP	–	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
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CER
443	TCP	HTTPS	–	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
445	TCP	Microsoft-smb	–	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 http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CER
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CER
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CER
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CER
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	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
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CER
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER

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	31.72
25/tcp	19.18
445/tcp	14.75
1026/udp	10.75
1027/udp	6.48
1433/tcp	4.21
23/tcp	3.18
1434/udp	3.13
22/tcp	2.37
4899/tcp	1.67
80/tcp	1.18
139/tcp	0.59
137/udp	0.37
2967/tcp	0.27
3128/tcp	0.16
3389/tcp	0.05

TAB. 3: Paquets rejetés

Liste des tableaux

1 Gestion du document 1
2 Correctifs correspondant aux ports destination des paquets rejetés 10
3 Paquets rejetés 11

Gestion détaillée du document

30 janvier 2009 version initiale.