Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 novembre 2009
N° CERTA-2009-ACT-045

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-45

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-045`

Gestion du document

Référence	CERTA-2009-ACT-045
Titre	Bulletin d'actualité 2009-45
Date de la première version	06 novembre 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-045.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-045/

1 Contrôle des ordinateurs par les réseaux sociaux

De nos jours, les *botnet* sont une des principales menaces en sécurité informatique. Pour rappel, un *botnet* est un ensemble de machines contrôlées par une entité malveillante (le plus souvent à la suite d'une infection massive sur l'Internet). On appelle zombis ces machines infectées.
La taille de ces *botnet* varie de quelques dizaines de machines à plusieurs centaines de milliers de zombis.

Un des points stratégiques de ces énormes réseaux est le canal de commandement. Il faut trouver un moyen efficace de contrôler et de maintenir cet énorme réseau de machines. Les zombis reçoivent leurs instructions (déni de service sur une cible donnée, exploitation d'une faille de sécurité, envois de spam, etc.) par le biais de ce canal de commandement. La technique historique la plus utilisée repose sur le protocole `IRC`, mais cela peut aussi se faire via des pages Web, les *newsgroups*, ou encore à l'aide de protocoles propriétaire.

Dernièrement, ce sont les réseaux sociaux qui ont été dévoyés pour servir de canal de contrôle. En particulier *Facebook* et *Twitter*. À titre d'exemple, un code malveillant récent utilise la fonction `Notifications` de la version mobile de *Facebook* pour relayer des instructions à des zombis. La version mobile du site est utilisée certainement pour des raisons pratiques, en effet, le code HTML est plus léger, et donc plus facile à télécharger et

à traiter.

2 Nouvelles imprimantes et dangers associés

Les imprimantes les plus récentes ont beaucoup plus de fonctionnalités que leurs ancêtres rustiques. Elles font désormais aussi office de scanner, de fax et sont connectées sur le réseau. Certaines d'entre elles embarquent des systèmes d'exploitation bien connus (comme `Linux` par exemple) ou des dérivés de ces derniers. Elles proposent aussi des services réseau, la plupart du temps pour faciliter leur utilisation standard. L'un des services les plus fréquemment employés sur les imprimantes repose sur une interface Web afin de configurer la machine.

C'est là où le bât blesse. Les imprimantes ne sont pas toujours considérées comme des ordinateurs et échappent parfois à la politique de sécurité du système d'information. Or, ces appareils ne sont pas systématiquement accompagnés d'une documentation claire. En particulier, l'administrateur du réseau ne sait pas forcément quel est le système d'exploitation installé, ni ne connait les versions de logiciel (notamment pour le serveur Web), et peut donc légitimement se demander si les vulnérabilités publiées chaque jour affectent leur matériel.

Outre la problématique des failles logicielles, les propriétaires des imprimantes sont confrontés à un souci de confidentialité. En effet, certains de ces matériels exposent, via l'interface Web, leur configuration ainsi que certains journaux. Les machines possédant une adresse IP routable sont donc accessibles depuis l'Internet si aucune règle de filtrage n'est mise en place. Parmi les informations ainsi rendues publiques peuvent se trouver des numéros de téléphone (fax) appelés, des éléments du réseau, etc. Certains matériels sont accessibles via le wifi, ce qui rend le filtrage particulièrement complexe.

3 iPhone, iPod touch et Jailbreak

Les `iPhone` et `iPod Touch` sont des plateformes reposant sur un système d'exploitation dérivé de Mac OS X et sont finalement de réels petits ordinateurs de poche. On y retrouve naturellement le principe d'utilisateur et de gestion des droits (accès en lecture/ecriture/exécution des fichiers). Par défaut le possesseur d'un `iPhone` (ou `iPod`) est identifié sur son appareil comme « utilisateur aux droits restreints ». Les applications ont elles aussi des droits limités par rapport au système, elles sont en « cage » (*jail*).

L'objectif du *Jailbreak* est de contourner les mécanismes de sécurité. Des outils « automatiques » permettent d'installer principalement deux choses. Un *installeur* qui permettra ensuite à l'utilisateur de piocher dans des bibliothèques d'applications et un serveur `SSH` avec un compte ayant un mot de passe par défaut. Plusieurs problèmes apparaissent. En premier lieu, les utilisateurs inexpérimentés ne pensent pas souvent à changer le mot de passe par défaut du `SSH` ou à désactiver le service. Un article a été publié cette semaine à propos d'une personne qui ayant pris le contrôle d'appareils en s'identifiant via ce service avec les identifiants par défaut, a fait afficher un message demandant une participation financière. Ensuite, toutes les applications récupérées via l'*installeur* s'exécutent hors de la cage et ont accès à tout le système. Si les logiciels disponibles via l'`AppStore` subissent normalement un certain nombre de contrôles, qu'en est-il de ceux téléchargés ? Ils peuvent être malveillants ou vulnérables, et comme ils peuvent avoir tous les droits sur l'appareil, on pourrait imaginer qu'ils puissent par exemple telephoner à des numéros surtaxés, enregistrer les conversations, faire suivre le courrier électronique... Bref, cela revient à télécharger et installer un peu n'importe quoi, avec les droits administrateur sur un ordinateur sans anti-virus.

Le CERTA recommande bien sur la plus grande prudence avec ce type de manipulation.

4 Des jeux pas si amusants que ça...

La presse a récemment relayé une information à propos d'un mini-jeu pour `Mac OS X` imitant ce qu'on pouvait trouver sur les bornes d'arcade dans les années 80. Ce programme, mis à disposition sur un *blog*, est accompagné d'une mise en garde. En effet, le principe consiste à détruire des envahisseurs à l'aide de son vaisseau spatial. Toutefois, à chaque ennemi détruit, un fichier d'un répertoire bien précis sera effacé.

Une mise en garde accompagne la distribution de ce jeu. Elle apparaît également au lancement de celui-ci. Néanmoins, les internautes ont souvent de mauvaises pratiques. En particulier, il est fréquent de partager un fichier à ses amis parce qu'il semble amusant. De plus, les utilisateurs ne prennent pas toujours le temps de lire les notices d'accompagnement. Par conséquent, il est possible que ce code malveillant soit volontairement distribué entre amis, ce qui incite davantage à l'exécuter.

Les risques de voir se développer des codes malveillants de ce genre est élevé. D'autant plus que ces programmes sont particulièrement adaptés pour fonctionner avec les téléphones portables. Le meilleur moyen de prévention contre ce phénomène reste la sensibilisation des utilisateurs.

5 Les expressions régulières. Faut-il les dénigrer ?

5.1 Des usages très variés

Les expressions régulières sont un moyen d'expression puissant, pratique et utile, qui se retrouve utilisé dans de très nombreuses situations :

- la gestion des requêtes pour les moteurs de recherche ;
- les recherches dans des bases de données textuelles ;
- le filtrage de flux applicatifs et réseaux, comme les passerelles Web (*proxies*), les anti-spam ou les systèmes de détection d'intrusion ;
- les contrôles de variables d'entrée adressées à un serveur Web ;
- etc.

5.2 Des limites algorithmiques

Il existe plusieurs algorithmes pour la reconnaissance d'expressions régulières. Ces différents algorithmes ont leurs avantages et leurs inconvénients : temps moyen de calcul, temps de calcul dans le pire des cas, temps de calcul pour l'initialisation. Selon les expressions régulières utilisées et le texte cherché, les meilleures performances ne seront pas toujours obtenues par le même algorithme. Il est bon de noter que dans le cas de motifs fixes et non d'expressions régulières, des algorithmes plus performants existent tels que Aho-Corasick. Il est donc souhaitable de différencier les cas où un motif fixe suffit des cas où on a besoin des expressions régulières.

Le plus grand danger algorithmique est le cas où le temps de calcul dans le pire des cas diffère largement du temps moyen de calcul, par exemple un temps exponentiel en la taille de l'entrée dans le pire des cas contre un temps linéaire dans le cas moyen. Ceci est le cas pour certains algorithmes concernant les expressions régulières. Il faut en être conscient, et veiller dans ce cas à ce que celles-ci ne puissent pas être des cas pathologiques. Il faut notamment empêcher une personne malveillante de pouvoir contrôler ces entrées. Elle pourrait en profiter pour faire un déni de service sur le système en l'amenant dans les états les plus coûteux.

5.3 Des limites de syntaxe

Selon les implémentations, les expressions régulières sont exprimées dans des langages différents. Certains de ces langages définissent une extension des expressions régulières. Cela permet une plus grande exprissivité mais au prix de la robustesse des algorithmes qui les traitent (principe de *back-reference* par exemple).

Il faut de plus faire attention à l'interprétation des résultats. Selon les algorithmes, toutes les occurrences d'un motif sont cherchées, ou bien la plus longue, ou encore la première trouvée.

5.4 Des vulnérabilités dans les implémentations

Enfin, comme tout code qui manipule des données, le moteur d'expressions régulières peut être affecté par des vulnérabilités de développement et de conception.

Voici quelques exemples parmi ceux qui ont pu marquer ces dernières années :

- vulnérabilité dans la gestion de certificats dans les produits Mozilla (MFSA2009-43) ;
- vulnérabilité de la bibliothèque PCRE (CVE-2007-5116) ;
- vulnérabilité dans Perl (UTF-8) (CVE-2008-1927) ;
- vulnérabilité de l'interprétation des lignes de commande (CLI) de Cisco IOS (cisco-sr-20070912-regexp) ;
- vulnérabilité de la gestion de contenu XML par Xquery sous MacOS (indirectement bibliothèque PCRE CVE-2008-0674) ;
- etc.

Il faut noter que certaines bibliothèques sont massivement réexploitées dans différents contextes. La vulnérabilité de l'une d'elles peut donc se répercuter très largement sur plusieurs types de produits. Il faut donc bien maîtriser son parc mais également les briques sous-jacentes des produits utilisés, dans la mesure du possible et quand cela est renseigné.

5.5 Recommandations

L'objet de cet article n'est pas de décrire en détail toutes les vulnérabilités associées aux expressions régulières, mais de rappeler certaines problématiques de sécurité. Comme pour toute gestion de données venant du monde extérieur, le traitement de celles-ci par des expressions régulières doit être fait avec la plus grande précaution et doit être maîtrisé. Il faut bien prendre en compte toutes les entrées malveillantes envisageables et ne pas supposer a priori de leur bienveillance ou de leur bon aspect. Si le mécanisme, complexe, ne permet pas de résoudre simplement les faiblesses, alors des méthodes de « nettoyage » et de surveillance doivent être mises en place en amont. Ces mécanismes ne doivent bien évidemment pas souffrir des mêmes vulnérabilités...

5.6 Quelques références

- S.A. Crosby, D.S. Wallach, « Denial of Service via Algorithmic Complexity Attacks », Usenix 2003 :
  http://www.cs.rice.edu/~scrosby/hash/
- G. Navarro, M. Raffinot, « Flexible Pattern Matching in Strings, Practical on-line search algorithms for texts and biological sequences », 2002, Cambridge University Press.
- R. Cox, « Regular Expression Matching Can Be Simple And Fast (but is slow in Java, Perl, PHP, Python, Ruby, ...) », janvier 2007 :
  http://swtch.com/~rsc/regexp/regexp1.html
- The Open Group Base Specifications Issue 6, « Regular expressions », 2004 :
  http://www.opengroup.org/onlinepubs/009695399/basedefs/xbd_chap09.html
- R. Sedgewick, K. Wayne, cours Princeton University, avril 2009 :
  http://www.cs.princeton.edu/courses/archive/fall09/cos226/lectures/64PatternMatch.pdf
- CheckMarx, « ReDoS (Regular Expression Denial of Service) Revisited », 2009 :
  http://www.checkmarx.com/Upload/Documents/PDF/Checkmarx_OWASP_IL_2009_ReDoS.pdf

6 Problèmes avec la mise à jour MS08-054

Cette semaine, Microsoft a émis une mise à jour (KB976749) qui corrige des problèmes pouvant se produire après l'application de la mise à jour MS09-054. Pour rappel, cette mise à jour corrigeait plusieurs vulnérabilités dans `Internet Explorer` permettant l'exécution de code arbitraire à distance et avait fait l'objet de l'avis CERTA-2009-AVI-434. Selon l'éditeur, les problèmes rencontrés suite à l'application de la mise à jour de sécurité sont limités à des « scénarios de navigation spécifiques », mais le nouveau correctif est tout de même proposé en mise à jour automatique.

L'éditeur indique qu'il faut installer la mise à jour de sécurité KB974455 (MS09-054) avant la mise à jour KB976749, sans quoi `Internet Explorer` pourrait ne plus fonctionner correctement.

6.1 Documentation

- Article #976749 de la base de connaissances :
  http://support.microsoft.com/kb/976749
- Avis CERTA-2009-AVI-434 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-434/index.html

7 Vulnérabilité du noyau Linux

Cette semaine, le CERTA a publié l'avis CERTA-2009-AVI-475 relatif à une vulnérabilité du noyau Linux. Celle-ci concerne un problème dans la gestion des tubes (*pipes*). Encore une fois, l'erreur est de type « pointeur nul » (*null pointer*) et permet à un utilisateur local d'exécuter du code arbitraire dans le contexte du noyau, s'il arrive à « mapper » ce code à l'adresse 0. Ceci lui permet potentiellement d'élever ses privilèges ou de provoquer un arrêt inopiné du système.

Il ne faut, en aucun cas, négliger ce type de vulnérabilités, car bien qu'exploitables « seulement » localement, elles sont souvent utilisées pour prendre le contrôle total de la machine à la suite d'une intrusion frauduleuse via un compte non privilégié. Ainsi, la première phase de l'attaque peut consister à s'introduire sur la machine en profitant d'une faiblesse dans un gestionnaire de contenu sur un serveur Web ou suite à une attaque par dictionnaire sur un

serveur `ssh` ayant des comptes à mot de passe faible par exemple. Une fois le compte standard obtenu, l'attaquant utilisera ce code d'élévation de privilèges pour devenir `root`.

Le CERTA rappelle donc l'impérieuse nécessité de mettre à jour le noyau sans délai, que ce soit par le biais de la version générique (`http://www.kernel.org`) ou bien avec les mises à jour fournies par les distributions.

8 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/

9 Rappel des avis émis

Dans la période du 30 octobre au 06 novembre 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-464 : Multiples vulnérabilités des produits VMware
- CERTA-2009-AVI-465 : Vulnérabilité dans les produits F-Secure
- CERTA-2009-AVI-466 : Multiples vulnérabilités dans CADIC Intégrale
- CERTA-2009-AVI-467 : Vulnérabilité dans Symantec Altiris
- CERTA-2009-AVI-468 : Multiples vulnérabilités dans SquidGuard
- CERTA-2009-AVI-469 : Vulnérabilité dans les cartes mères Intel Desktop
- CERTA-2009-AVI-470 : Multiples vulnérabilités dans KDE
- CERTA-2009-AVI-471 : Multiples vulnérabilités dans IBM WebSphere pour z/OS
- CERTA-2009-AVI-472 : Multiples vulnérabilités dans Adobe Shockwave Player
- CERTA-2009-AVI-473 : Vulnérabilités dans IBM Tivoli Storage Manager
- CERTA-2009-AVI-474 : Multiples vulnérabilités dans Sun Java JDK/JRE
- CERTA-2009-AVI-475 : Vulnérabilité du noyau Linux
- CERTA-2009-AVI-476 : Vulnérabilité dans Solaris Sockets Direct Protocol Driver
- CERTA-2009-AVI-477 : Vulnérabilité de Novell eDirectory
- CERTA-2009-AVI-479 : Vulnérabilité dans Asterisk

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

- CERTA-2009-AVI-459-001 : Multiples vulnérabilités dans Mozilla Firefox (ajout des références aux bulletins de sécurité Debian, RedHat et Ubuntu)
- CERTA-2009-AVI-478-001 : Vulnérabilité dans Snort (correction d'une erreur dans les systèmes affectés)

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.ssi.gouv.fr/fr/formation/

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.

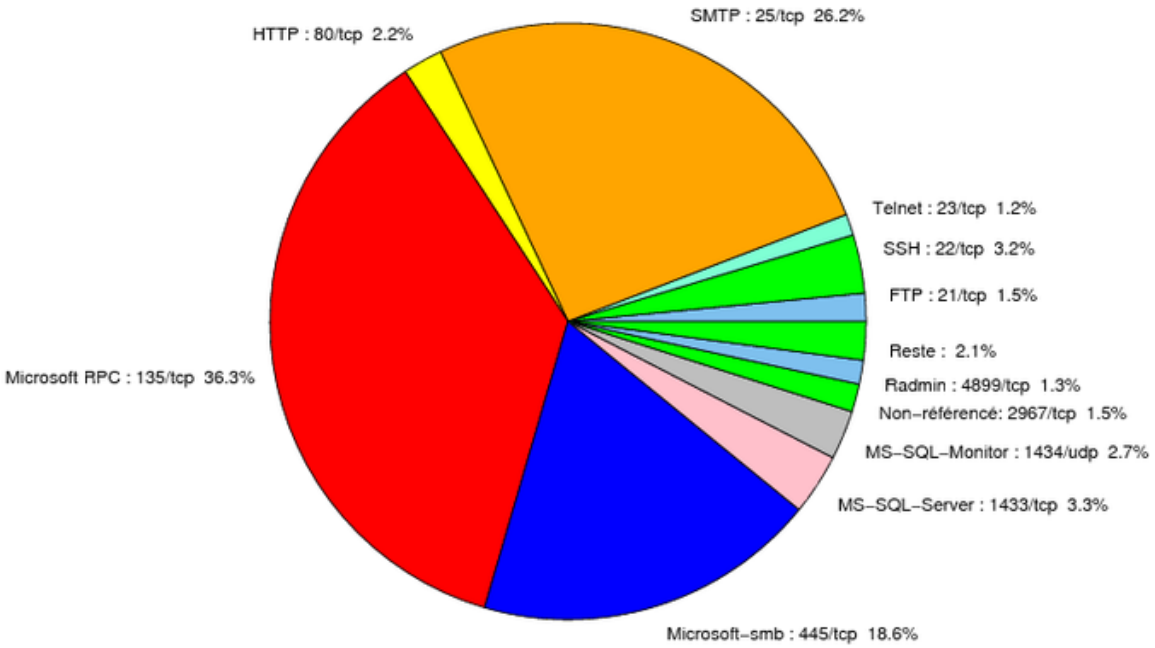

FIG. 1: Répartition relative des ports pour la semaine du 29 octobre au 05 novembre 2009

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	36.28
25/tcp	26.2
445/tcp	18.64
1433/tcp	3.31
22/tcp	3.16
80/tcp	2.73
1434/udp	2.66
21/tcp	1.58
2967/tcp	1.51
4899/tcp	1.29
23/tcp	1.22
3389/tcp	0.71
3128/tcp	0.5
1080/tcp	0.43
2100/tcp	0.14
3306/tcp	0.07

TAB. 3: Paquets rejetés

Liste des tableaux

1 Gestion du document 1
2 Correctifs correspondant aux ports destination des paquets rejetés 9
3 Paquets rejetés 10

Gestion détaillée du document

06 novembre 2009 version initiale.