Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 janvier 2009
N° CERTA-2009-ACT-002

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-02

Gestion du document

Référence	CERTA-2009-ACT-002
Titre	Bulletin d'actualité 2009-02
Date de la première version	09 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-002.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-002/

1 Incidents de la semaine

1.1 Installation de publicités

Le CERTA a traité cette semaine de nombreuses compromissions de serveurs, ayant pour but -*a priori*- d'installer des pages publicitaires pour des produits pharmaceutiques. Ces pages semblent faire partie d'un kit d'installation et sont rédigées en plusieurs langues.

La particularité de ces attaques réside dans le fait que leur auteur exploite des vulnérabilités différentes. En effet, il profitait soit d'un problème de configuration (possibilité d'écrire dans des répertoires), soit d'une faille connue dans un gestionnaire de contenus. Les logiciels attaqués que le CERTA a rencontrés sont :

- Moodle ;
- SPIP ;
- Joomla! ;
- WordPress.

Cette liste n'est probablement pas exhaustive.

L'analyse de ces incidents montre qu'il y a eu au moins deux vagues d'attaques : une en juillet 2008 et une en décembre 2008.

Pour les cas que nous avons pu examiner, la compromission se manifestait par la présence dans les journaux du serveur Web d'appels à des fichiers nommés `script10.js`, `win.php` et `z.php`. Le CERTA recommande donc aux administrateurs de rechercher explicitement ces trois noms de fichier dans les journaux, au moins pour la période allant de juillet 2008 à aujourd'hui.

1.2 De l'importance des journaux

1.2.1 Présentation

Le CERTA a été informé de la compromission d'un site Web par ajout d'un *iframe* en bas de toutes les pages `index` d'un site Web. L'administrateur du serveur a découvert cet incident seulement quelques heures après la modification des pages, en lisant ses journaux. Si certains éléments militent pour une injection `SQL`, il n'a pas été possible de le démontrer, car les problèmes suivants ont été rencontrés :

- la configuration de datation des journaux n'est pas cohérente avec la configuration générale du serveur. En effet, les dates du serveur sont en GMT+1 (fuseau horaire de Paris) et les dates des journaux en GMT. De plus, le serveur n'étant pas synchronisé en `NTP`, il est plus difficile de faire la corrélation avec les journaux des différents dispositifs du réseau ;
- la granularité des journaux ne permet pas d'afficher les paramètres passés aux fichiers appelés. Il n'est ainsi pas possible de voir s'il s'agit bien d'une injection `SQL` et à quel moment elle a eu lieu.

Un simple nettoyage des pages n'a pas suffi : quelques heures après la découverte de l'incident, un nouvel *iframe* avait été ajouté.

Le CERTA recommande aux administrateurs la lecture de la note d'information CERTA-2008-INF-005 (*Gestions des journaux d'événements*).

1.2.2 Documentation

- Note d'information CERTA-2008-INF-005 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-005/

1.3 Une compromission discrète

L'analyse d'une compromission relativement discrète d'un serveur Web est l'occasion pour le CERTA de revenir sur quelques bonnes pratiques importantes.

Dans les faits, un site utilisant un gestionnaire de contenu (`Joomla!`) se fait compromettre (exploitation de vulnérabilité, recherche exhaustive des comptes...) et l'attaquant dépose un *phpshell* lui permettant de contrôler la machine avec les droits du serveur web. Ce qui est interessant dans cette compromission, c'est la méthode qu'il a utilisé pour rester discret dans l'arborescence des fichiers. En effet, il était courant de trouver des fichiers nommé "C99" ou "R57" par exemple. Ensuite, les noms des fichiers sont devenus plus discrets, mais les fichiers contenaient les mêmes chaines explicites ("C99", "R57"...). Puis sont arrivés les fichiers au code obscurci, par exemple via un encodage en *base64*. Dans notre cas, le *phpshell* était obscurci et, ce qui est nouveau, respectait le nommage du CMS utilisé localement pour les modules, soit « com_article », ressemblant ainsi à un module légitime. Le parcours de l'arborescence ne fait pas apparaître d'incongruité et la recherche de chaînes de caractères habituelles pour ces scripts ne donne rien. Si l'administrateur du site Web avait eu une bonne connaissance de la liste des modules présents, la détection aurait été immédiate.

Le CERTA recommande d'avoir une politique de gestion des journaux d'événements rigoureuse et de maitriser les éléments installés sur un serveur en les limitant à ceux nécessaires. En effet, quel que soit le gestionnaire de contenus, de nombreux modules facultatifs sont installés par défaut, ce qui ne facilite pas la maîtrise du système, et il peut être interessant de les supprimer. Attention, lors des mises à jour, à ce que ces modules inutiles ne soient pas réinstallés.

1.4 Documentation

- Note d'information du CERTA sur la gestion des journaux d'événements :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-005/

2 Windows 7 et versions Bêta

Ces jours-ci, plusieurs versions bêta de logiciels Microsoft sont en train de faire leur apparition. On peut citer, notamment :

- Windows Vista Service Pack 2 ;
- Windows Server 2008 Service Pack 2 ;
- Windows Server 2008 R2 (*Release 2*) ;
- Windows 7.

Windows 7, qui est sans doute le plus attendu, est disponible publiquement à partir du 09 janvier 2008. Cet article s'attarde sur les nouveautés qui seraient apportées par le système d'exploitation.

Si cette nouvelle version de Windows ne sera pas une révolution par rapport à Windows Vista, elle devrait toutefois apporter quelques nouveautés intéressantes, et selon l'éditeur, de nettes améliorations de performance (ordonnancement, *boot*, gestion de l'énergie).

Parmi les nouveautés qui sont attendues, on peut citer (cette liste n'est bien sûre pas exhaustive) :

- l'utilisation de *BitLocker* sur support amovible ;
- la fonctionnalité *PC Safeguard* permettant d'effacer toute action entreprise et trace de l'utilisateur à la fermeture de session ;
- des améliorations significatives de PowerShell ;
- le support de `DNSSec` ;
- des simplifications dans la gestion des applications autorisées sur un domaine (*AppLocker*) ;
- le support natif et la possibilité de booter sur des disques virtuels `VHD` ;
- une nouvelle barre des tâches ;
- le support de 256 processeurs (probablement dans la version serveur).

Au niveau de la fiabilité, l'éditeur a annoncé ne pas avoir fait de changement majeur pour garder une compatibilité totale des applications et pilotes de Vista.

Pour résumer, Windows 7 va apporter de nombreuses améliorations tout en restant dans la lignée de *Windows Vista*.

Le CERTA tient à rappeler qu'une version de test, que ce soit une `beta` ou même une `release candidate`, ne doit jamais être utilisée comme produit final. Leur seule raison d'être est la recherche de failles et de *bugs* pour l'éditeur. Pour illustation, il est apparu avec la dernière version de Windows 7 qu'elle corrompait les fichiers de type `mp3` en écrivant dans les métadonnées.

Une version de test peut tout au plus servir à préparer une migration ou une conduite de changement.

3 Deux mois et demi après publication, le correctif n'est toujours pas appliqué

3.1 Historique

Il y a maintenant plus d'un mois, Microsoft a publié une mise à jour de sécurité permettant de corriger une faille dans le service *Server* (MS08-067). Le CERTA, à l'occasion de diverses publications (cf. Documentation) a rappelé l'impérieuse nécessité d'appliquer ce correctif. Quelques semaines après, un ver nommé par les éditeurs d'anti-virus *Conficker* ou *Downadup* s'est propagé sur l'Internet via cette faille.

3.2 Les faits

Plusieurs variations de ce ver voient le jour actuellement. Son code permettant d'exploiter la vulnérabilité décrite dans le bulletin MS08-067 a même été intégré comme moyen de propagation supplémentaire dans des variantes de code déjà très connus, tel que *Sdbot*. Les systèmes français sont touchés sans distinction, et les différents codes ont déjà fait plusieurs victimes. Une fois un poste infecté, la propagation est la plupart du temps très rapide.

En effet, aucune action des utilisateurs n'est nécessaire à la contamination. Il suffit que le poste vulnérable soit en marche et connecté au réseau. De plus, il devient alors impossible d'appliquer le correctif.

3.3 Recommandations

Tout d'abord, nous rappelons la nécessité d'appliquer ce correctif si cela n'est pas déjà fait.

En cas d'infection, il est difficile de se contenter d'un outil de décontamination. En effet, certains codes embarquent des caractéristiques mutagènes qui empêchent de déterminer avec précision l'ensemble des éléments de l'infection à supprimer. La seule solution, radicale il est vrai, reste d'isoler du reste du réseau les machines infectées, et de procéder à leur réinstallation complète, mise à jour incluse, avant de pouvoir les reconnecter.

Enfin, dans le cas où l'installation des postes repose sur une image (ou un *master*), il conviendra de mettre à jour cette image.

3.4 Documentation

- Avis du CERTA numéro CERTA-2008-AVI-523 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-523/
- Bulletins d'actualité CERTA-2008-ACT-43, CERTA-2008-ACT-45 et CERTA-2008-ACT-48 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-043/
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-045/
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-048/
- Mémento du CERTA sur les infections virales :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
- Bulletin de sécurité Microsoft numéro MS08-067 du 23 octobre 2008 :
  http://www.microsoft.com/france/technet/security/bulletin/MS08-067.mspx

4 Politique de gestions de bogues et sécurité

Il n'est parfois pas trivial de qualifier une vulnérabilité relative à un logiciel donné. En effet, certaines équipes, bien que travaillant sur un projet *Open Source* ou un logiciel libre ne fournissent pas sciemment les impacts associés à un bogue.

Ainsi, on aura bien une liste de changements apportés au logiciel dans laquelle sera précisée de façon laconique les composants qui ont été modifiés mais sans plus de détail. Il convient, alors, dans ce cas de consulter l'outil de gestion de version qui fournira de manière complète les modifications apportées au code source.

Cependant, et même à la lecture du code source, il est difficile d'apréhender l'impact de la faille corrigée. On pourra prendre comme exemple l'analyse faite par *Sogeti* sur un correctif d'un composant du noyau `Linux` : `http://esec.fr.sogeti.com/blog/index.php?2009/01/08/`.

A la lecture de cet article, on découvre que ce n'est qu'aprés une analyse précise du code source que l'on peut s'apercevoir qu'une modification qualifiée de mineure cachait en fait une faille de sécurité. En effet, cette vulnérabilité corrigée de façon silencieuse dans la dernière version du noyau `Linux` et relative à la mise en œuvre du protocole `SCTP` était de nature à permettre une exécution de code arbitraire en espace `noyau`.

Dans ce cas, le problème est que seule une personne avertie connaissant relativement bien le logiciel peut, dans un délais raisonnable, caractériser le problème. Ceci montre qu'un projet, même libre ou *Open Source*, doit s'accompager d'une documentation claire et d'une communication la plus explicite possible sur sa gestion de versions comme des listes de changements détaillées accompagnées de bulletins de sécurité le cas échéant.

Ceci facilitera grandement le travail des équipes chargées de la mise en production du produit et l'évaluation des risques lorsqu'une vulnérabilité est découverte.

5 Copier-coller trompeur

Dans le cas du filoutage, afin d'éviter de cliquer sur un lien hypertexte méconnu et ne correspondant pas à l'affichage, il est possible de copier-coller l'adresse apparente. Par exemple, dans le code HTML suivant :

```
<a href="http://www.certa.ssi.gouv.fr">http://www.secinfo.gouv.fr</a>
```

Le copier-coller permettra de récupérer l'adresse vue, i.e. "http://www.secinfo.gouv.fr".

Cette solution n'est cependant pas toujours valide. L'action de copier-coller ne copie pas toujours rigoureusement les chaînes de caractère ASCII qui sont mises en surbrillance. C'est le cas pour une grande majorité de

navigateurs et quelques clients de messagerie, dont le copier-coller interprète le style du texte, et en particulier les balises SPAN pouvant avoir des options de la forme `style="display:none"`.

L'utilisateur croit alors copier la chaîne de caractères visible bien qu'il copie une tout autre séquence précisée par la balise SPAN.

Le CERTA rappelle donc les mesures principales à appliquer pour éviter de se faire piéger par cette astuce, utilisable pour le filoutage par exemple :

- lire et envoyer les courriels en texte brut ;
- taper directement l'adresse voulue dans la barre de navigation de son navigateur.

6 L'usage des téléphones de technologie DECT

6.1 DECT ? Rapide aperçu

DECT (*Digital Enhanced Cordless Telecommunications*) est une norme de téléphonie sans-fil numérique développée initialement par l'ETSI. Elle utilise en Europe la bande de fréquence des 1800-1900 MHz et permet à des équipements sans fil de se raccorder à un réseau de télécommunication filaire via les ondes radio.

Ces usages sont assez variés mais on le retrouve :

- pour un usage domestique : les téléphones sans-fil permettent de rester racordé au réseau téléphonique filaire tout en permettant une certaine mobilité dans son domicile ;
- pour un usage professionnel : un réseau micro-cellulaire peut être créé à partir du PABX afin de couvrir un bâtiment. Des relais peuvent également être installés pour augmenter la couverture.

La technologie peut également être utilisée dans d'autres contextes.

6.2 Les faits récents

Des chercheurs ont récemment montré au cours d'une conférence la faisabilité et le faible coût d'investissement pour récupérer des échanges entre équipements utilisant la technologie DECT (*Digital Enhanced Cordless Telecommunications*).

Ils ont également rendu publiques différentes informations concernant les algorithmes de chiffrement et d'authentification jusqu'alors diffusés de manière confidentielle aux constructeurs. Ils ont enfin rappelé que certaines mises en œuvre d'équipements ne sont pas satisfaisantes en terme de sécurité, avec des authentifications non mutuelles et/ou une absence totale de chiffrement.

6.3 Les recommandations du CERTA

Les faiblesses de la technologie DECT ne sont pas récentes. Cette présentation a l'occasion de le rappeler.

Dans le cadre d'un déploiement professionnel, il est vivement conseillé d'auditer son réseau avec les mêmes précautions que d'autres technologies sans-fil comme le Wi-Fi :

- répertorier les équipements utilisés ;
- vérifier les solutions de sécurité mises en place par l'équipementier ;
- connaître la puissance d'émission actuelle ;
- utiliser dans la mesure du possible des tunnels chiffrés pour les couches protocolaires supérieures ou des solutions alternatives plus robustes ;
- sensibiliser les responsables en télécommunication et prendre en compte les risques dans la politique de sécurité globale.

7 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 01 et le 08 janvier 2009.

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 02 au 09 janvier 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-001 : Vulnérabilité dans Samba
- CERTA-2009-AVI-002 : Vulnérabilité dans xterm
- CERTA-2009-AVI-003 : Vulnérabilité de Solaris
- CERTA-2009-AVI-004 : Vulnérabilité dans Check Point VPN-1
- CERTA-2009-AVI-005 : Vulnérabilités dans Symantec Mail Security pour SMTP
- CERTA-2009-AVI-006 : Vulnérabilité dans OpenSSL
- CERTA-2009-AVI-007 : Vulnérabilité dans CA Service Metric Analysis et CA Service Level Management
- CERTA-2009-AVI-008 : Vulnérabilité dans Cisco Global Site Selector
- CERTA-2009-AVI-009 : Vulnérabilité de ISC BIND

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

- CERTA-2008-AVI-512-001 : Multiples vulnérabilités dans Adobe Flash Player
  (ajout de la référence au bulletin de sécurité Sun)
- CERTA-2008-AVI-593-001 : Vulnérabilité dans PHP
  (ajout d'une référence CVE associée)
- CERTA-2008-AVI-612-001 : Vulnérabilités dans SPIP
  (ajout des références CVE associées)

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.

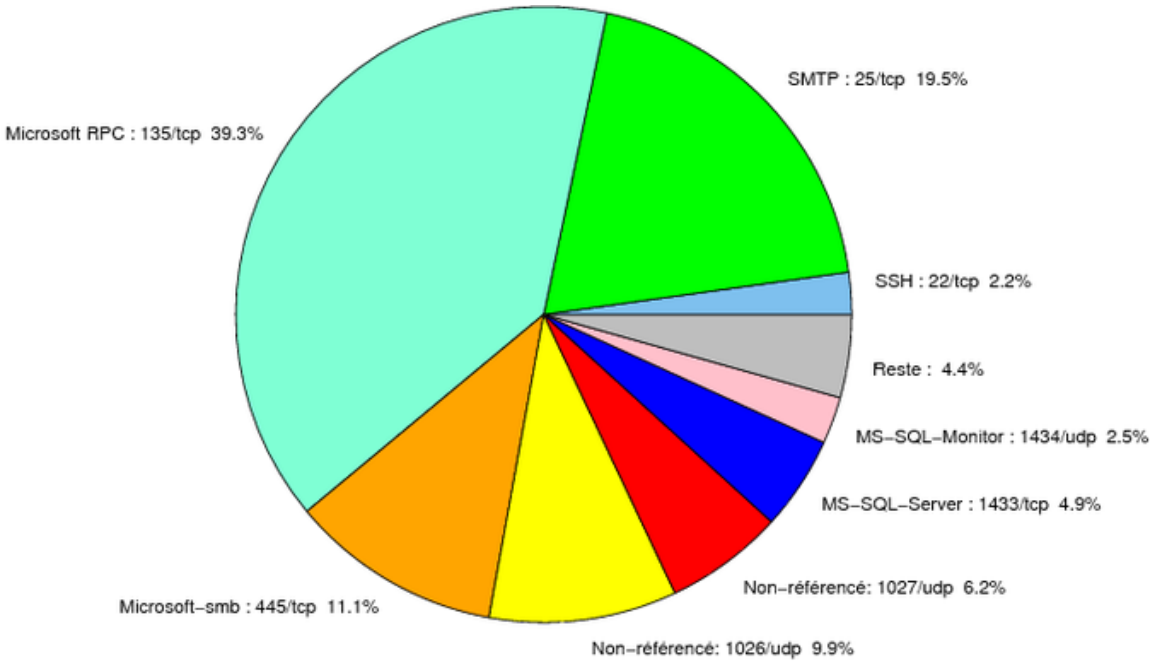

FIG. 1: Répartition relative des ports pour la semaine du 01.01.2009 au 08.01.2009

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/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERT
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CERT
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CERT
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERT
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CERT
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CERT
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CERT
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CERT
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CERT
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CERT
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CERT
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CERT
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CERT
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CERT
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CERT
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERT
6106	TCP	Symantec Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERT
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
6502	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CERT
6503	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CERT
6504	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CERT
8080	TCP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CERT
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CERT
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	http://www.certa.ssi.gouv.fr/site/CERT
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CERT
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CERT
54345	TCP	HP Mercury	–	http://www.certa.ssi.gouv.fr/site/CERT
65535	UDP	LANDesk Management Suite	–	http://www.certa.ssi.gouv.fr/site/CERT

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

port	pourcentage
135/tcp	39.32
25/tcp	19.5
445/tcp	11.11
1026/udp	9.85
1027/udp	6.24
1433/tcp	4.92
1434/udp	2.46
22/tcp	2.2
80/tcp	0.99
2967/tcp	0.68
4899/tcp	0.57
143/tcp	0.15
3128/tcp	0.1

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

09 janvier 2009 version initiale.