Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 septembre 2007
N° CERTA-2007-ACT-037

**Affaire suivie par :**
CERTA

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité 2007-37**



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2007-ACT-037 |
| Titre | Bulletin d'actualité 2007-37 |
| Date de la première version | 14 septembre 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-037.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-037/

## 1 Les listes blanches

### 1.1 Le problème

Une approche fréquemment choisie par les administrateurs de réseau pour limiter les risques et les abus liés à la connexion à l'Internet consiste à restreindre les sites sur lesquels la navigationest autorisée. Ce principe de « liste blanche » filtre les adresses demandées au niveau d'une passerelle, et ne laisse sortir *in fine* que celles explicitement mentionnées dans la liste.

Les motivations pour développer de telles listes sont nombreuses. Parmi les plus mentionnées :

– ces « listes blanches » permettent de limiter l'utilisation de la bande passante vers des sites « trop distrayants » (radio, bourse, sport, etc.) ;
– ces « listes blanches » évitent que des utilisateurs naviguent, sciemment ou pas, sur des sites dont le contenu peut être dangereux ;
– ces «listes blanches » limitent les flux sortants vers des sites bien définis. Certains administrateurs système estiment donc qu'il est difficile de voler des informations ou d'en exporter depuis le réseau, si jamais une compromission survient.

C'est le dernier point qui nous intéresse dans cet article.

Par principe, la liste blanche regroupe des sites dits de confiance. Cela peut inclure des sites administrés par les mêmes services, des sites de bonne réputation, ou des sites pratiques.

C'est à ce niveau qu'il faut avoir une extrême vigilance. Avoir une certaine confiance dans les sites autorisés ne garantit aucunement que des informations ne peuvent pas être échangés avec des sites interdits par le biais de sites de confiance. Avoir confiance et empêcher l'échange d'information sont deux considérations différentes.

A valeur d'illustration, un code a été rendu public cette semaine. En voici les détails :

Plusieurs méthodes permettent à une machine au sein d'un réseau de communiquer (envoi/réception) avec une machine arbitraire à distance, malgré une liste blanche. L'hypothèse de départ suppose que la liste blanche contient, dans le document publié, le domaine `google.com`. Les personnes dans le réseau ne peuvent donc accéder qu'à toute adresse réticulaire (URL) associée à ce domaine.

Pour contourner le principe de la liste blanche, une première solution consiste à appliquer l'outil de traduction *Google Translate*. La requête sera bien adressée au site de Google, mais ce dernier va accéder au site distant (interdit) pour demander la page à traduire. En d'autres termes, l'outil de traduction sert alors de relais pour accéder à d'autres sites.

Cela peut laisser des traces dans les journaux de la passerelle web, comme la chaîne particulière : `via translate.google.com`.

Cette technique n'est pas récente, mais suffit à contourner la politique de la liste blanche. Les auteurs ne s'arrêtent pas à cette méthode, et en proposent plusieurs autres :

- Google offre le moyen de personnaliser sa page d'accueil, sous forme de composants. Ces derniers peuvent être hébergés sur un serveur distant (interdit), et récupérés par la machine interne. Cette dernière peut donc télécharger des données indirectement sur le site distant. Inversement, quand elle demande le composant sur le serveur distant, elle peut également insérer des données dans sa requête. L'administrateur qui met en œuvre la liste blanche peut trouver des indices d'une telle utilisation en cherchant dans les journaux de la passerelle de connexion à l'Internet la chaîne de caractères `FeedFetcher-Google` ou l'adresse `http://www.google.com/feedfetcher.html`.
- la phase d'authentification avec l'API ClientLogin repose sur le fait qu'au cours de l'authentification, des « jetons » sont créés. A la fin des échanges, ces derniers sont (ou devraient être) détruits (*cookies*). Ceci n'est pas vrai côté serveur, qui les garde pendant une certaine durée. Cette durée est variable selon le type du « jeton » : plusieurs mois pour l'identifiant SID, deux semaines pour l'identifiant Auth ou quelques heures pour l'identifiant GX (messagerie Google Mail). Le code publié démontre qu'il est possible, en exploitant cette propriété, d'échanger des données via un compte Google Mail partagé, entre deux machines distantes. La passerelle Web ne voit, elle, que des connexions vers Google Mail. Ceci fonctionne si le sous-domaine `mail.google.com` n'est pas bloqué, donc si la liste blanche tolère tout sous-domaine de `google.com` (ou `google.fr`).
- La méthode est identique pour des données partagées du tableur Google, avec le sous-domaine http://spreadsheets.google.com .
- Le code élargit la méthode à tout autre service pouvant être partagé par plusieurs machines, comme Google Calendar, Google Base, Google Notebook, ou Google Search History, si les adresses contenant les URLs contenant les chaînes `google.com/calendar`, `google.com/base`, `google.com/notebook` et `google.com/searchhistory` ne sont pas filtrées au niveau de la passerelle.

Il y a bien entendu plusieurs autres scénarios possibles, qui peuvent utiliser d'autres sites que ceux précédemment listés. Cette méthode n'est évidemment pas propre aux sites de Google. Il s'agit de la démonstration de faisabilité du code publié cette semaine.

La liste blanche posée en hypothèse semble restrictive, car limitée au seul domaine `google.com`. Toutefois, elle n'empêche pas, comme le code le démontre, les communications entre une machine interne et tout autre machine distante.

Affiner la liste blanche par des sous-domaines ne résoud pas nécessairement le problème, puisque certains services sont accessibles par des sous-répertoires (exemple : www.google.com/calendar).

## 1.2 Les recommandations du CERTA

Cet article a pour objectif principal de sensibiliser les utilisateurs de listes blanches. Il est important de comprendre ce qu'elles permettent de bloquer, et les moyens possibles de la contourner.

Une liste blanche ne suffit pas pour garantir que des informations ne sont pas échangées entre une machine interne et un site arbitraire distant.

L'élément clé reste l'analyse en profondeur des journaux des serveurs et des passerelles, en quête de ces contournements possibles.

Pour éviter les fuites de données vers l'Internet, la meilleure solution reste de ne pas se connecter à l'Internet. C'est la recommandation lorsqu'on manipule des données sensibles.

# 2 Vulnérabilité QuickTime / Firefox

## 2.1 Présentation

Cette semaine, le CERTA a émis l'alerte CERTA-2007-ALE-014 qui détaille une vulnérabilité non corrigée concernant `Apple QuickTime` et `Mozilla Firefox`.

La vulnérabilité exploite une option appelée `QTNEXT` du format multimédia `QuickTime`, qui permet de spécifier un fichier ou URL à lire après la fin du média en cours de lecture. Si l'option est spécifiée, l'application QuickTime appelle directement le navigateur par défaut de l'utilisateur. Dans le cas où le navigateur par défaut est `Mozilla Firefox`, celui-ci permet l'exécution de code `Javascript` sur le poste de l'utilisateur. Il est à noter que l'ouverture d'un fichier `QuickTime` via un navigateur alternatif n'empêche pas l'exploitation car cette application appellera tout de même le navigateur par défaut.

La désactivation du `Javascript` dans `Mozilla Firefox` (recommandation du CERTA) n'empêche pas l'exécution de ce type de code `QuickTime`, puisque Firefox n'est pas lancé avec les options de l'utilisateur. Les tests du CERTA ont montré que la dernière version du navigateur `Netscape` (9.0.b3) est également affectée ; en revanche les tests d'exploitation sur Seamonkey 1.1.4 n'ont pas fonctionné, mais il convient de rester prudent.

Quelques contournements provisoires sont possibles en attendant des correctifs :

- l'utilisation d'un navigateur par défaut alternatif, qui ne s'appuie pas sur le moteur de rendu `Gecko` ;
- l'affichage d'une alerte lorsque `QuickTime` appelle l'interpréteur `Javascript` de `Mozilla Firefox` (cf. l'alerte CERTA-2007-ALE-014) ;
- l'utilisation d'une extension telle que `NoScript` bloque le `Javascript`, si l'option *Forbid scripts globablly* est activée. L'usage des extensions n'est cependant pas recommandé par le CERTA.

Quelques options des modules (*plugins*) installés avec Firefox sont visibles par la commande `about:plugins` dans la barre d'adressage. Ces modules se trouvent sous forme de fichiers .dll dans `C:\Program Files\Mozilla\Firefox\plugins`. Le simple fait de supprimer ceux associés à QuickTime n'empêche pas Firefox d'interpréter des documents multimédia par QuickTime.

Enfin, la désinstallation de l'application `QuickTime` reste le meilleur contournement jusqu'à la publication d'un correctif.

L'éditeur Mozilla a confirmé la vulnérabilité le jour-même de la publication de celle-ci, et annoncé qu'elle semble ne toucher que les postes sous `Microsoft Windows`. Un rapport de bogue a été créé pour tenter de résoudre le problème du côté de `Firefox`. L'éditeur a également annoncé qu'il travaille avec Apple, et il est donc probable que ce dernier publie également une mise à jour prochainement.

## 2.2 Documentation

- Alerte CERTA-2007-ALE-014 du 13 septembre 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-014/index.html
- Annonce du 12 septembre 2007 sur le bloc-notes de sécurité de Mozilla :
  http://blog.mozilla.com/security/2007/09/12/quicktime-to-firefox-issue/
- Rapport de bogue #395942 de Mozilla :
  https://bugzilla.mozilla.org/show_bug.cgi?id=395942

# 3 Gestion des caches dans Mozilla Firefox

Il est possible avec `Mozilla Firefox` de ne pas utiliser les caches relatifs aux pages visitées ainsi que l'historique de navigation. Cependant, une rapide expérience avec la version 2 de `Firefox` montre que, même en mettant la taille de cache à *0 Mo* et en désactivant l'historique, et après un arrêt de `Firefox`, celui-ci est tout de même capable de restaurer la session précédant l'arrêt. Les options proposées dans l'interface classique de configuration ne sont donc pas suffisantes pour garantir que Firefox ne stocke pas des informations sur la

navigation. Il est cependant tout à fait possible de configurer `Firefox` de façon sûre : Il convient alors d'utiliser l'interface `about:config` et de régler des options comme :

- désactivation de la restauration de session : fixer les valeurs `browser.sessionstore.enabled` et `browser.sessionstore.resume_from_crash` à *false* ;
- désactivation des caches de `Firefox` : fixer les valeurs `browser.cache.disk.enable` et `browser.cache.memory.enable` à *false*

# 4 Les interfaces d'administration Web

La technologie Web est souvent utilisée pour administrer des services à distance. Par exemple :

- un routeur ;
- un site Web ;
- un compte chez un fournisseur d'accès ;
- un dossier chez un prestataire commercial ;
- etc.

Une personne malintentionnée qui accéderait par le biais d'une interface Web au compte d'un utilisateur chez un fournisseur d'accès, ou à la configuration d'un serveur Web, aurait accès à des informations sensibles, comme les différents mots de passes (mail, espace web, voix sur IP, accès au serveur, ...).

Il convient donc de faire très attention lors de l'utilisation de ce genre d'interface :

- utiliser si possible un canal de communication chiffré (HTTPS par exemple) ;
- utiliser une machine de confiance pour se connecter ;
- s'assurer d'un mot de passe d'accès robuste (cf. CERTA-2005-INF-001) ;
- définir des mots de passe distincts pour chaque service.

L'interface Web peut être une sur-couche destinée à apporter du confort à l'utilisateur, comme la présentation graphique d'un fichier de configuration ou d'options de commandes.

Ce confort apporte des risques, car il peut être lui-même source de vulnérabilités. Par exemple, le CERTA observe fréquemment dans ses analyses de journaux de serveurs web compromis des tentatives de connexions sur des URL propres à des versions vulnérables de l'interface Web `phpmyadmin`. Celle-ci gère des bases de données.

Ces interfaces d'administration via l'Internet doivent donc être traitées comme des services critiques en terme de sécurité.

# 5 Déménager un site Web : des précautions à prendre

## 5.1 Les faits

Lors d'une opération de migration globale du serveur Web, un service a changé d'hébergeur et de nom de domaine. La rupture du contrat d'hébergement n'a pas déclenché un nettoyage par l'hébergeur. Il restait sur une de ses machines un site Web, avec des pages HTML, qui répondait aux requêtes HTTP. Il n'était toutefois plus maintenu.

L'abandon du nom de domaine ne s'est pas accompagné d'un nettoyage particulier dans le système DNS. Les tables DNS dirigent donc toujours les requêtes vers le site abandonné.

Deux inconvénients apparaissent alors :

- les internautes qui n'ont pas actualisé leurs favoris (signets ou marque-pages) ou qui ont cliqué sur un lien d'un site ne s'étant pas mis au vent du nouveau nom de domaine se retrouvent sur un site au contenu obsolète ;
- le site abandonné, non maintenu, peut être détourné (mauvaise publicité, filoutage, etc.)

## 5.2 Recommandations

Avant de quitter un hébergeur, le plus salutaire est de nettoyer soi-même son site. Il faut :

- supprimer toutes les pages ;
- remplacer la page d'accueil par de une en HTML statique et sans script qui indique la nouvelle adresse ou qui fait une redirection ;
- indiquer la redirection sur la page d'erreur 404.

Il faut modifier le DNS pour que les requêtes soient dirigées sur la nouvelle adresse (le nouveau site). L'incident prouve l'importance de cette modification, même quand le nom de domaine doit bientôt être abandonné.

Le changement de nom de domaine doit s'accompagner de précautions décrites dans la note d'information du CERTA :

http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/index.html

# 6 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 06 et le 13 septembre 2007.

# 7 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/

# 8 Rappel des avis émis

Dans la période du 07 au 13 septembre 2007, le CERTA a émis l'alerte et les avis suivants :

- CERTA-2007-ALE-014 : Vulnérabilité dans Apple QuickTime

- CERTA-2007-AVI-393 : Vulnérabilité dans CAS
- CERTA-2007-AVI-394 : Vulnérabilité dans l'antivirus Sophos
- CERTA-2007-AVI-395 : Vulnérabilité de WebSphere
- CERTA-2007-AVI-396 : Vulnérabilités des produits Cisco Catalyst
- CERTA-2007-AVI-397 : Vulnérabilité dans Microsoft Agent
- CERTA-2007-AVI-398 : Vulnérabilité dans Visual Studio
- CERTA-2007-AVI-399 : Vulnérabilité dans les services Windows pour UNIX
- CERTA-2007-AVI-400 : Vulnérabilité dans MSN Messenger et Windows live Messenger
- CERTA-2007-AVI-401 : Multiples vulnérabilités de Wordpress
- CERTA-2007-AVI-402 : Multiples vulnérabilités de Apache
- CERTA-2007-AVI-403 : Vulnérabilité de XOrg

# 9 Actions suggérées

## 9.1 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.

## 9.2 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.

## 9.3 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.

## 9.4 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.

## 9.5 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.

## 9.6 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.

### 9.7 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

## 10 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.

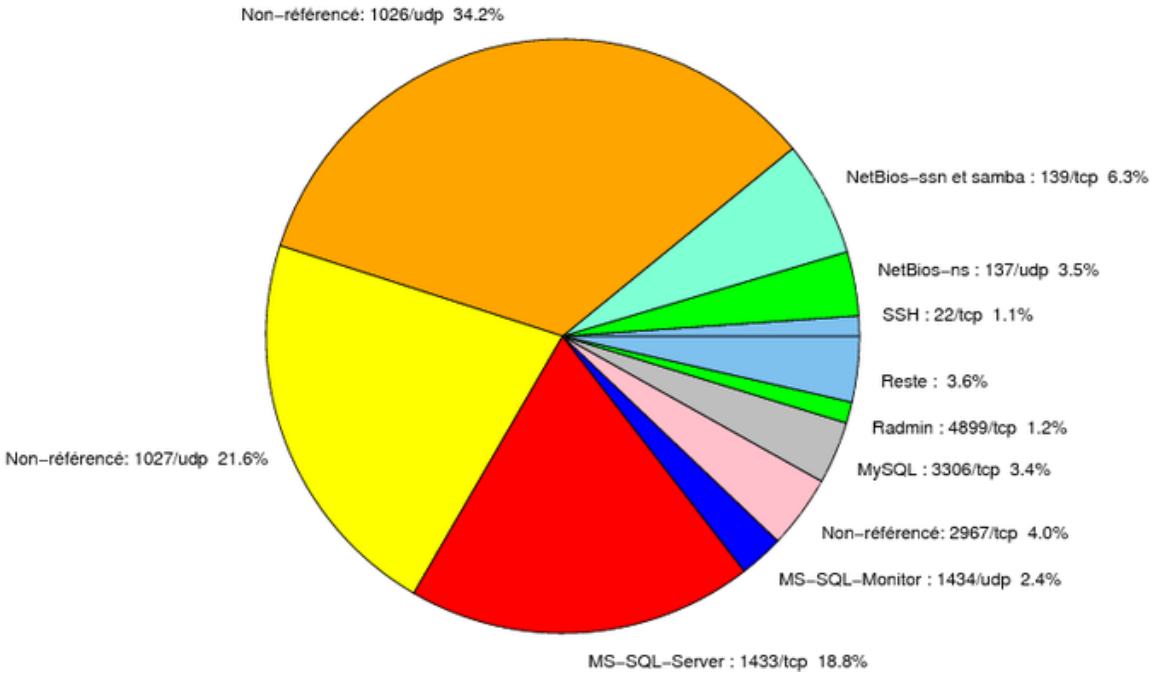


FIG. 1: Répartition relative des ports pour la semaine du 06.09.2007 au 12.09.2007

| Port | Protocole | Service | Porte dérobée | Référence possible CERTA |
|---|---|---|---|---|
| 21 | TCP | FTP | – | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 22 | TCP | SSH | – | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 23 | TCP | Telnet | – | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 25 | TCP | SMTP | – | http://www.certa.ssi.gouv.fr/site/CE<br>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<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>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<br>http://www.certa.ssi.gouv.fr/site/CE<br>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<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>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<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 443 | TCP | HTTPS | – | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 445 | TCP | Microsoft-smb | – | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>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<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>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<br>http://www.certa.ssi.gouv.fr/site/CE<br>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<br>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<br>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<br>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 | 34.18 |
| 1027/udp | 21.57 |
| 1433/tcp | 18.84 |
| 139/tcp | 6.29 |
| 2967/tcp | 3.97 |
| 137/udp | 3.49 |
| 3306/tcp | 3.39 |
| 1434/udp | 2.41 |
| 4899/tcp | 1.15 |
| 22/tcp | 1.09 |
| 3128/tcp | 0.82 |
| 80/tcp | 0.65 |
| 1080/tcp | 0.63 |
| 21/tcp | 0.19 |
| 15118/tcp | 0.17 |
| 143/tcp | 0.15 |
| 2100/tcp | 0.07 |
| 23/tcp | 0.05 |
| 6101/tcp | 0.03 |
| 9898/tcp | 0.01 |

TAB. 3: Paquets rejetés

# Liste des tableaux



# Gestion détaillée du document

**14 septembre 2007** version initiale.