Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 juillet 2008
N° CERTA-2008-ACT-029

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-29

Gestion du document

Référence	CERTA-2008-ACT-029
Titre	Bulletin d'actualité 2008-29
Date de la première version	18 juillet 2008
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-2008-ACT-029.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-2008-ACT-029/

1 Retour sur les incidents traités cette semaine

Récupération d'identifiants de connexion par ingénierie sociale

Le bulletin d'actualité de la semaine dernière en parlait déjà, le CERTA a été informé de nombreux cas de tentatives de récupération d'identifiants de connexion suite à l'envoi de messages électroniques. Ces derniers sont rédigés en français de qualité variable et usurpent généralement, plus ou moins habilement, la signature des administrateurs du réseau. Les victimes sont invitées à envoyer leurs identifiants de compte *webmail* soit en réponse au message, soit sur un site web externe.

Jusqu'à présent, les personnes ayant reçu ces messages sont des utilisateurs de *webmail* construit à partir du logiciel *Horde3*. Les comptes ainsi obtenus frauduleusement sont ensuite réutilisés pour émettre du *pourriel*.

L'un des cas signalés a attiré notre attention : les victimes étaient dirigées vers un site Web effectuant un *typosquatting* sur leur domaine d'origine (les attaquants utilisaient un nom de domaine identique à celui de leurs victimes, à l'exception de deux lettres interverties).

Il s'agit du premier cas d'attaque de ce type (très proche du filoutage) s'appuyant sur du *typosquatting* et signalé au CERTA.

2 Correctifs Mozilla Firefox

Le CERTA a émis cette semaine l'avis CERTA-2008-AVI-368 mentionnant la publication de correctifs pour le navigateur *Mozilla Firefox*.

La version 3.0.1 corrige trois vulnérabilités importantes :

- MFSA2008-35 : cette vulnérabilité découle de l'interaction de différents produits et des protocoles associés. Ce type de vulnérabilité a déjà fait l'objet d'avis de sécurité et a impacté la grande majorité des navigateurs. Il laisse l'opportunité à une personne malveillante d'insérer un lien spécialement construit dans une page web. Lorsque celui-ci est interprété par le navigateur avec son protocole particulier (comme `mailto:`, `firefoxurl:`, etc.), il conduit à l'exécution de commandes. Cela est possible car le navigateur interprète incorrectement la ligne qui lui est présentée et dont il ne maîtrise pas complètement la syntaxe. Dans la vulnérabilité MFSA2008-35, il s'agirait d'une mauvaise interprétation du caractère « | ». Le protocole impliqué est ici `chrome:`.
- MFSA2008-34 : cette vulnérabilité provient d'une mauvaise manipulation par le navigateur du compteur de référence de la classe `nsCSSValue:Array`. Ce dernier est codé sur 16 bits et peut donc provoquer sous certaines conditions une exécution de code dès que le nombre maximal (65535) de références est atteint.
- MFSA2008-36 : l'interprétation de fichiers au format *GIF* sous *Mac OS* via le navigateur ne serait pas correctement effectuée. Cette vulnérabilité peut conduire au dysfonctionnement du navigateur et, sous certaines conditions, à l'exécution de code arbitraire.

Plusieurs remarques découlent de ces vulnérabilités :

- Les vulnérabilités mentionnées ci-dessus peuvent conduire à l'exécution de code arbitraire à distance. Il n'est pas suffisant de désactiver le *JavaScript*. Les mesures de prudence classiques restent applicables et montrent encore ici leur intérêt :
  - naviguer sur des sites de confiance uniquement ;
  - naviguer depuis un compte utilisateur aux droits restreints ;
  - mettre à jour ses applications et les configurer de manière restrictive.
- *Thunderbird* utilise le moteur de navigation de *Firefox* et peut également être affecté. Il est important de vérifier par exemple que son client de messagerie n'interprète pas les codes dynamiques comme le *JavaScript* (Options -> Avancé -> Général -> Editeur de configuration -> Javascript.enabled), comme le précise le bulletin *Mozilla*. De manière générale, il est plus prudent d'afficher les courriels au format texte brut (Affichage -> Corps du message en -> Texte seul). La version *Thunderbird* 2.0.0.16 existe mais n'est pas encore disponible en téléchargement à la date de publication de cet article. Aucune précision sur la date de publication n'est à ce jour donnée par *Mozilla*.
- *Mozilla* a publié les mises à jour pour la version 2.0.0.16 du navigateur mardi et a attendu mercredi pour la version 3.0.0.1. Les raisons ne sont pas connues.
  La mise à jour peut perturber le fonctionnement de certains modules additionnels. *Mozilla* explique dans un article que ces derniers sont développés par des tiers qui ont déclaré comme `MaxVersion` « 3.0 » au lieu de « 3.0.* » .
  L'utilisation de ces modules est à éviter car leur code n'est pas audité et ils peuvent augmenter la surface d'attaque via la navigation.
  - Bloc-notes Mozilla, « AMO adds Firefox 3-compatible versions » , 12 mai 2008 : http://blog.mozilla.com/basil/2008/05/12/amo-adds-firefox-3-compatible-versions/
  - Bloc-notes Mozilla, « Firefox 3.0.1 and add-on compatibility » , 17 juillet 2008 : http://blog.mozilla.com/basil/2008/07/17/firefox-301-and-add-on-compatibility/
- *Mozilla* a par ailleurs annoncé que la branche 2.0.0.x de *Firefox* sera maintenue jusqu'à la mi-décembre 2008.
  http://developper.mozilla.org/devnews/index.php/2008/07/15/firefox-20016-security-and-stability-update-now-available-for-download/

3 Exploitation de la vulnérabilité du contrôle ActiveX de Access Snapshot Viewer

Le bulletin de *Microsoft* #955179 concernant une vulnérabilité du contrôle *ActiveX* de *Access Snapshot Viewer*, qui a fait l'objet de l'alerte CERTA-2008-ALE-009, décrivait des cas d'exploitation isolés. Depuis, l'exploitation a

été plus fréquemment observées, notamment par `Symantec`. Il semblerait que cette vulnérabilité soit maintenant exploitée avec le kit d'exploitation `Neosploit`.

L'éditeur décrit que deux attaques ont été observées, la première vise des systèmes en anglais et la deuxième en chinois. L'exploitation se fait sur des versions linguistiques particulières seulement car elle consiste à télécharger un fichier exécutable dans un répertoire spécifique de l'ordinateur. Ainsi, dans le cas d'un système anglais, le téléchargement de l'exécutable se fait dans le répertoire suivant :

```
Documents and Settings\All Users\Start Menu\Programs\Startup
```

Ceci provoque l'exécution automatique du fichier téléchargé au prochain redémarrage de `Windows`.

Le site exploitant la vulnérabilité du contrôle *ActiveX* de *Access Snapshot Viewer* contient également un *iFRAME* vers un autre site utilisant `Neosploit`. Ainsi, `Symantec` signale qu'au moins quatre autres vulnérabilités seraient exploitées, notamment :

- une vulnérabilité dans le contrôle *ActiveX AOL SuperBuddy* ;
- une vulnérabilité de débordement de mémoire dans *Apple Quicktime* ;
- une vulnérabilité dans le contrôle *ActiveX Microsoft MDAC RDS.Dataspace* ;
- une vulnérabilité dans le contrôle *ActiveX ADODB.stream* de *Internet Explorer*.

Ces quatre vulnérabilités sont corrigées. On remarque toutefois la présence forte de vulnérabilités dans les contrôles *ActiveX*. Le CERTA rappelle qu'il est vivement recommandé de désactiver l'utilisation des *ActiveX*, ou au minimum de demander une confirmation avant chaque exécution.

Pour rappel, il existe un contournement permettant de désactiver le contrôle *ActiveX* de *Access Snapshot Viewer*, décrit dans l'alerte CERTA-2008-ALE-009. Les administrateurs peuvent également filtrer certaines chaînes de caractères au niveau des serveurs mandataires inverses (cf. CERTA-2008-ACT-028).

3.1 Documentation

- Alerte CERTA-2008-ALE-009 du 08 juillet 2008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-009/index.html
- Bulletin d'actualité CERTA-2008-ACT-028 du 11 juillet 2008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-028.pdf

4 Nouvelle note d'information du CERTA

Cette semaine a été publiée sur le site Internet du CERTA une nouvelle note d'information. La note d'information CERTA-2008-INF-001 fait le point sur la balise *HTML*, *iFRAME*.

Il y est rappelé le principe de fonctionnement de cette balise ainsi que les risques associés aux détournements de fonctionnalité par des personnes malintentionnées. En effet, la balise *iFRAME* permet l'insertion dans une page d'un cadre contenant une page hébergée sur une autre source. Des personnes malintentionnées exploitent cette fonctionnalité afin de compromettre des ordinateurs d'internautes.

Le schéma de compromission est souvent le même :

- l'individu malveillant compromet un serveur web ;
- une fois une porte d'entrée trouvée, du code *HTML*, en l'occurrence des balises *iFRAME*, est ajouté dans des pages légitimes ;
- ces balises pointent vers des pages malveillantes contenant par exemple des *JavaScript* exploitant des vulnérabilités de navigateur ;
- ces *iFRAME*s sont écrites de façon à ce qu'elles soient invisibles pour l'internaute ;
- ces balises provoquent ainsi des connexions vers le serveur malveillant de façon transparente pour l'utilisateur lors de la visite de la page.

La note d'information fournit également un ensemble de recommandations et de bonnes pratiques afin de limiter les risques et impacts de ces balises. Ces recommandations sont faites pour tous les niveaux d'utilisation d'un site web :

- le développement ;
- l'hébergement ;
- l'exploitation de site web :
- la navigation.

Documentation

– Note d'information CERTA-2008-INF-001 du 17 juillet 2008 :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-001/

5 *BlueCoat* et vulnérabilité *DNS*

Le CERTA a publié de multiples avis sur la faille protocolaire touchant les *DNS* : CERTA-2008-AVI-353, CERTA-2008-AVI-358, CERTA-2008-AVI-359, CERTA-2008-AVI-360. Or , cette faille touche également les équipements de la marque `BlueCoat`. Les produits affectés sont :

– Proxy SG ;
– Director ;
– Proxy AV ;
– Proxy RA ;
– PacketShaper ;
– iShaper.

L'éditeur a publié par ailleurs un bulletin de sécurité précisant que la vulnérabilité serait corrigée dans les prochaines versions de ses systèmes d'exploitation embarqués. Cependant, pour l'instant, ces produits restent vulnérables et il n'est proposé à l'utilisateur par `BlueCoat` qu'un contournement provisoire.

Recommandations :

Dans l'attente de la publication des correctifs, il convient d'appliquer les mesures présentées dans le bulletin de sécurité : `http://www.bluecoat.com/support/security-advisories/dns_cache_poisoning`.

En l'espèce, il faudra configurer ces équipements pour qu'ils n'interrogent que des serveurs DNS « fiables » comme, par exemple, un autre serveur `DNS` non-vulnérable du réseau local. Remarque : Si les éditeurs et distributeurs *Linux* ont proposé des correctifs, les systèmes embarqués (appliances) ne sont pas forcément corrigés.

6 Poppler, Xpdf et produits dérivés

`Poppler` est une bibliothèque de fonctions sous licence libre (`GPL v2`) utilisée pour manipuler des fichiers `PDF`. Cette bibliothèque est portable et disponible pour les principales plates-formes : `GNU/Linux`, `*BSD`, `Unix` et `Windows`. Elle est en fait basée sur le code d'une autre application : `Xpdf`.

La vocation de `Poppler` est de proposer une bibliothèque unifiée sur laquelle d'autres projets vont s'appuyer pour manipuler des fichiers au format `PDF`.

Cependant, en l'état, `Poppler` n'est pas le passage obligé pour développer un analyseur de `PDF` et nombre de projets, bien que basés sur `Xpdf` ou `Poppler`, font encore leur propre maintien de versions spécifiques insérées « en dur » dans leur propre code.

Ainsi, généralement, quand une vulnérabilité est identifiée dans `Xpdf`, on la retrouve également dans `Poppler` mais également dans un certain nombre d'autres applications comme le serveur d'impression `CUPS` par exemple. Dès lors, plutôt que d'avoir une seule mise à jour pour une bibliothèque (`Poppler`), on devra donc appliquer des correctifs spécifiques pour chaque application de ce type.

Ici, le problème peut être que la même vulnérabilité qui a été corrigée dans `Xpdf` ou `Poppler`, ne le sera peut-être pas forcement dans d'autres applications.

Le cas de `Poppler` et `Xpdf` est assez classique. Cette pratique de développement qui consiste à insérer une copie d'un code existant dans un autre projet plutôt que d'utiliser une bibliothèque unifiée peut avoir des conséquences désastreuses en termes de politique de maintenance (problème de coût) mais également en termes de sécurité et d'application de correctif.

7 Prolongation du support pour Microsoft XP

Fin juin, *Microsoft* publiait sur son site Internet une lettre de son vice-président, *Bill Veghte*, annonçant la prolongation du support et de la vente de *Windows XP*.

Depuis le 30 juin 2008, il est impossible pour les revendeurs d'acheter des versions seules de *Windows XP* (les revendeurs pouvant néanmoins finir d'écouler leurs stocks). En revanche, afin de faire face à l'émergence du

marché des ordinateurs ultra-portables à bas coûts (comme le `EEE PC` d'*Asus*, les `Wind U100` de *MSI*, l'`Aspire One` d'*Acer*, etc.), *Microsoft* a décidé de fournir des versions OEM jusqu'au 31 janvier 2009.

Malgré cette fin de vie commerciale annoncée à court terme, le support de *Microsoft* continuera de proposer des mises à jours (et en particulier des mises à jour de sécurité) jusqu'en avril 2014, soit 13 ans après le lancement du premier *Windows XP*.

Documentation

- Politique de support Microsoft :
  http://support.microsoft.com/lifecycle/
- Lettre ouverte de Bill Veghte :
  http://www.microsoft.com/windows/letter.html
- Note d'information du CERTA numéro CERT-2005-INF-003 sur les logiciels et systèmes obsolètes :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html

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 10 et le 17 juillet 2008.

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 11 au 17 juillet 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-364 : Vulnérabilité du langage Ruby
- CERTA-2008-AVI-365 : Multiples vulnérabilités dans Drupal
- CERTA-2008-AVI-366 : Multiples vulnérabilités dans la machine virtuelle Java de Sun

– CERTA-2008-AVI-367 : Multiples vulnérabilités dans les produits Oracle et Weblogic
– CERTA-2008-AVI-368 : Vulnérabilités dans Mozilla Firefox
– CERTA-2008-AVI-369 : Multiples vulnérabilités dans Claroline

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

– CERTA-2008-AVI-359-002 : Vulnérabilités dans ISC BIND
(ajout de la référence au bulletin de sécurité FreeBSD)

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.formation.ssi.gouv.fr

12 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

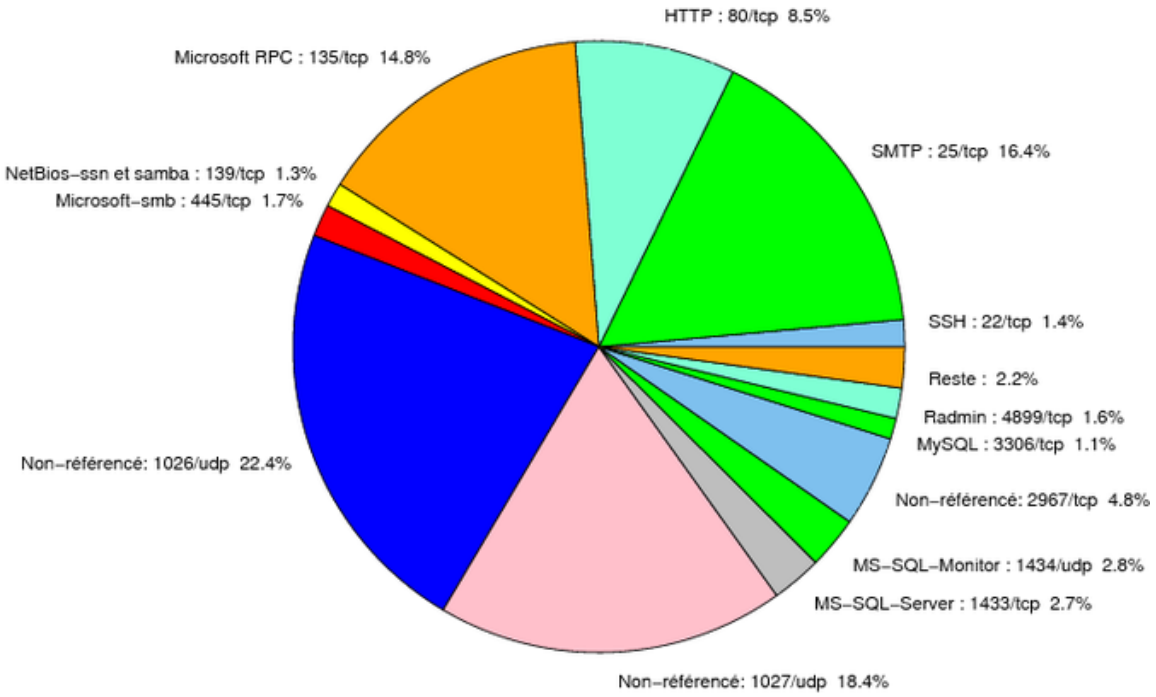

FIG. 1: Répartition relative des ports pour la semaine du 10.07.2008 au 17.07.2008

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
1026/udp	22.42
1027/udp	18.38
25/tcp	16.36
135/tcp	14.84
80/tcp	12.63
2967/tcp	4.82
1434/udp	2.75
1433/tcp	2.66
445/tcp	1.74
4899/tcp	1.6
22/tcp	1.42
139/tcp	1.28
3306/tcp	1.1
23/tcp	1.01
21/tcp	0.5
137/udp	0.36
3389/tcp	0.18
143/tcp	0.09

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

18 juillet 2008 version initiale.