

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-07

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-2007-ACT-007>

Gestion du document

| | |
|-----------------------------|------------------------------|
| Référence | CERTA-2007-ACT-007 |
| Titre | Bulletin d'actualité 2007-07 |
| Date de la première version | 16 février 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-007.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-007/>

1 Activités en cours

1.1 Nécessité des mesures de contournement

Le traitement d'un incident récent a mis en lumière la nécessité de mettre en œuvre des mesures de contournement permettant de limiter l'impact possible de l'exploitation des vulnérabilités.

A valeur d'exemple, la vulnérabilité dite « PHP include » est exploitée à travers sa présence dans de nombreux logiciels écrits en PHP, dont le codage manque parfois de rigueur. Le temps de publication des correctifs peut être long (de l'ordre de quelques mois) et donnent tout leur sens aux mesures de contournement.

Dans le cas de l'incident traité cette semaine, il s'agissait du module `ExtCalendar`. Ce dernier a fait l'objet d'une alerte CERTA-2006-ALE-008 le 11 juillet 2006.

Cependant, à la date de rédaction de ce bulletin d'actualité, aucun correctif n'a été officiellement publié, et la vulnérabilité est activement exploitée. Cela ne laisse que peu de choix à l'administrateur du site utilisant `ExtCalendar` : ou bien il prend la décision d'appliquer quelques contournements provisoires, comme par exemple retirer le module, dans l'attente d'une mise à jour, ou bien il accepte le risque que son serveur soit compromis (si ce n'est déjà le cas) à son insu et puisse servir à la cyber-délinquance.

Le mois de mars 2007 devrait aussi voir la publication de nombreuses vulnérabilités de PHP (langage ou applications). La vigilance doit donc être renforcée.

Recommandations

Le CERTA recommande de :

- vérifier la version des logiciels PHP en exploitation et de les mettre à jour quand les correctifs existent ;
- mettre en œuvre des mesures de contournement pour les logiciels dont les vulnérabilités connues ne sont pas toutes corrigées ;
- inclure les paramètres des URL dans les journaux.

1.2 Ingénierie sociale et tromperie

1.2.1 Présentation

Le CERTA a été informé cette semaine de la diffusion de courriers électroniques particuliers. Semblant provenir d'organisations gouvernementales (services de police ou de renseignement), le message demande au destinataire s'il a été victime d'une escroquerie financière de type `scam` et propose de l'aider. L'arnaque `scam` se manifeste le plus souvent par une demande d'aide pour un transfert d'argent, en échange de quoi un pourcentage sur la somme serait reversé ; la version la plus connue étant la fraude 4-1-9, ou arnaque nigériane.

Le courriel explique de manière pédagogique ce qu'est une telle fraude, puis invite les personnes victimes à les contacter. Elles doivent envoyer pour cela toutes les informations pouvant aider à l'enquête, et le message garantit que l'argent qui a été perdu pendant la fraude sera rapidement récupéré (sous 24 heures dans le courriel analysé). Les informations demandées sont :

- les prénoms et noms complets ;
- le pays de résidence ;
- les moyens de contact (téléphone mobile ou fixe, fax) ;
- les personnes impliquées dans la transaction, avec tous les détails les concernant ;
- une copie du courriel de la fraude ;
- le montant total qui a été perdu au cours de la fraude ;
- une garantie que ce montant a été effectivement versé.

Il s'agit bien entendu d'un piège. Le procédé utilisé par ce courriel est lui-même une arnaque. Il y a de fortes chances que, une fois ces informations communiquées, elles soient exploitées par des personnes malveillantes, et que la seconde étape consiste à envoyer des coordonnées bancaires, pour permettre (ou faire miroiter) le remboursement de l'argent perdu par la première fraude.

Ce courriel est donc un message purement malveillant. Il a pour particularité de cibler avant tout un ensemble de personnes, qui ont déjà fait preuve d'une certaine candeur (victime de l'arnaque de type `scam`). Celui analysé était rédigé en anglais, mais il est probable que la méthode soit également reprise en langue française.

1.2.2 Recommandations

Le CERTA rappelle à cette occasion que tout courrier électronique exigeant l'envoi d'informations est par nature suspect, dans la mesure où il n'y a par défaut aucune garantie sur la source du message (identité de l'expéditeur).

Plus précisément, pour ne pas tomber dans le piège, il était possible d'y voir certains détails :

- les images insérées dans le courrier au format HTML pointent vers un vrai site gouvernemental, tandis que les adresses électroniques pour contacter les pseudo forces de l'ordre sont bien plus étranges. Elles ont pour format : `nom_force_d_ordre-pays.org`. Le nom de domaine `nom_force_d_ordre-pays.org` n'est pas commun.
- les forces de l'ordre n'ont pas pour habitude d'envoyer massivement des courriers électroniques pour s'adresser aux citoyens ;
- un effort certain est fait dans la rédaction pour être persuasif : il contient des extraits en lettres capitales, et une argumentation très hiérarchisée ;
- le message insiste auprès du lecteur pour prendre contact rapidement, par l'emploi abusif d'adjectifs et d'adverbes de temps.

Une note rédigée par le CERTA mentionne ces arnaques : CERTA-2005-INF-004. Si de tels messages sont reçus, il est recommandé de le signaler à son responsable de sécurité, ou au CERTA.

2 Vulnérabilités de Sun Solaris

2.1 Vulnérabilité concernant telnetd

L'alerte CERTA-2007-ALE-005 décrit une vulnérabilité concernant l'utilisation conjointe du service `telnetd` et de la commande `/usr/cmd/login` de Solaris 10 et Solaris Express (ou Solaris 11). Cette faille permet à une personne malintentionnée de se connecter à une machine vulnérable sous le nom d'un utilisateur légitime, s'il est connu.

Un correctif a été publié sur le site de l'éditeur pour corriger cette vulnérabilité sur Solaris 10. Aucune mise à jour n'est cependant disponible pour Solaris Express. D'autres services de connexion à distance pouvant être vulnérables (notamment `rlogind`, `klogin`, et `eklogin`), il est également conseillé de les désactiver. Une autre précaution de sécurité est d'interdire l'accès au compte `root` à distance, par exemple en s'assurant que la ligne `CONSOLE=/dev/console` est bien présente et non commentée dans le fichier `/etc/default/login`. Ceci ne corrige en rien la vulnérabilité, mais limite les droits qu'une personne pourrait avoir en exploitant la vulnérabilité à ceux d'un utilisateur autre que `root`.

2.2 Autres vulnérabilités de Sun Solaris

D'autres vulnérabilités ont été annoncées cette semaine concernant Sun Solaris :

- plusieurs vulnérabilités concernant les serveurs Xorg et Xsun sur Solaris 8, 9, et 10, détaillées dans l'avis CERTA-2007-AVI-025. Un correctif est seulement disponible pour Solaris 8.
- deux vulnérabilités non corrigées touchant Solaris 8, 9, et 10, et qui concernent le navigateur Mozilla 1.7, détaillées dans les avis CERTA-2006-AVI-227 et CERTA-200-AVI-568 (CVE-2006-2776 et CVE-2006-6505) ;
- une vulnérabilité dans la mise en oeuvre du protocole TCP sur Sun Solaris 10, détaillée dans l'avis CERTA-2007-AVI-087. Un correctif est disponible sur le site de l'éditeur.

Documentation

- Alerte CERTA CERTA-2007-ALE-005 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005/index.html>
- Bulletin de sécurité de Sun et correctif pour Solaris 10 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102802-1>
- Bulletin de sécurité de Sun pour les vulnérabilités sur Xorg et Xsun (correctif pour Solaris 8) :
<http://sunsolve.sun.com/search/document/do?assetkey=1-26-102803-1>
- Bulletin de sécurité de Sun pour les vulnérabilités sur Mozilla 1.7 :
<http://sunsolve.sun.com/search/document/do?assetkey=1-26-102800-1>
- Avis CERTA CERTA-2007-AVI-087 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-087/index.html>

3 Vulnérabilité de Word

Microsoft a publié cette semaine un ensemble de correctifs, qui ont été documentés dans les avis du CERTA cités dans la section 9. Ils concernent une vingtaine de vulnérabilités de Microsoft Windows, Microsoft Office, Internet Explorer, ainsi que certaines solutions de sécurité Microsoft (Live One Care, Windows Defender, etc.).

L'alerte CERTA-2006-ALE-014 mentionnait plusieurs vulnérabilités de l'application bureautique `Word`. Elle a été créée le 06 décembre 2006, puis mise à jour régulièrement suivant les nouvelles vulnérabilités et les précisions trouvées. Le bulletin MS07-014 corrige ces dernières, et l'alerte pointe donc, suivant la terminologie du CERTA, vers l'avis associé : CERTA-2007-AVI-083.

Cependant, mercredi 14 février 2007, la société d'antivirus McAfee signale sur son site qu'une nouvelle vulnérabilité, référencée CVE-2007-0870, a été identifiée. Elle affecterait les versions 2000 et XP de Word, et serait différente de celles corrigées ce mois-ci par Microsoft. Cette information a été confirmée par Microsoft le même jour, dans son avis de sécurité 933052. Les détails de cette vulnérabilité ne sont cependant pas connus.

Du code d'exploitation est actuellement disponible, et il permettrait l'exécution de code arbitraire sur la machine ayant une application vulnérable.

Documentation

- Avis de sécurité Microsoft 933052 du 14 février 2007 :
<http://www.microsoft.com/technet/security/advisory/933052.msp>
- Alerte du CERTA CERTA-ALE-006 du 16 février 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-006/>
- Référence CVE CVE-2007-0870 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0870>

4 Vulnérabilités dans les téléphones multi-fonctions (*smartphones*)

4.1 Présentation

Une vulnérabilité découverte dans les *smartphones* Palm OS Treo permet à un utilisateur malintentionné de porter atteinte à la confidentialité des données contenues dans l'appareil, malgré la fonction permettant de verrouiller son dispositif.

Une personne malveillante peut porter atteinte à la confidentialité des informations présentes sur le système (messages SMS, mémos, agenda, tâches, etc) en utilisant le moteur de recherche de documents : celui-ci reste accessible, bien que l'appareil soit verrouillé, par le biais d'une combinaison de touches. Dans le bulletin de sécurité publié par l'éditeur (cf. section Documentation) aucune publication de correctif n'est prévue prochainement. Le bulletin d'actualité CERTA-2007-ACT-005 du 02 février 2007 fait mention des difficultés rencontrées pour mettre à jour ces équipements mobiles.

D'une manière générale, il est recommandé pour tout équipement mobile de bien considérer les informations qu'il peut contenir, étant donné les risques existants actuellement pour ces matériels.

Documentation

- Annonce de sécurité dans la liste de discussion Bugtraq :
<http://www.securityfocus.com/archive/1/460059>
- Bulletin d'actualité CERTA-2007-ACT-005 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-005.pdf>

5 Les dangers de l'*autorun*

5.1 Pour désactiver l'*autorun*

Le CERTA rappelle le danger de l'exécution automatique de programmes sur des clés USB de type U3 ou sur des CD-ROM/DVDROM. Cette fonctionnalité, aussi appelée *autorun*, permet l'exécution automatique de programmes contenus sur ces supports amovibles, lors de leur insertion. Normalement réservée aux CDROM/DVDROM, l'*autorun* est également possible sur des clés USB U3 car celles-ci sont reconnues en tant que CDROM USB. Un programme malveillant sur une clé de ce type pourrait donc s'exécuter dès son insertion (CERTA-2006-INF-006).

Pour désactiver la fonctionnalité *autorun* sous Windows, il suffit de modifier la clé suivante dans la base de registres :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CDRom
```

Si la valeur "Autorun" est 0, l'*autorun* est désactivé. Si sa valeur est 1, il est activé.

Cette méthode fonctionne sur les systèmes Windows 95, Windows 98, windows ME, Windows NT, Windows 2000, Windows XP, Windows 2003, et Windows Vista.

Sur Windows Vista, il est également possible de paramétrer l'exécution automatique dans le menu Démarrer/Panneau de Configuration/Lire des CD ou d'autres medias automatiquement. Le paramètre "Installer ou exécuter un programme" ne doit pas être activé pour la liste déroulante logiciels et jeux.

6 Ver Storm Worm

Storm Worm, également connu sous le nom de W32/Small.DAM ou Trojan.Peacomm, est un ver qui se répand par la messagerie. Dès l'infection de la machine, le ver tente de se connecter à une liste de machines compromises en utilisant les techniques des réseaux pair à pair. Le protocole utilisé est identique à celui des logiciels eDonkey et Overnet. Une fois connecté à ce réseau de machines compromises, le ver obtient une adresse réticulaire lui permettant de télécharger plusieurs outils d'attaques.

L'un des Chevaux de Troie installé par le ver lui permet de réaliser des attaques par déni de service en envoyant massivement des requêtes ICMP (ping) ou HTTP (TCP 80). Les adresses des cibles de ces attaques sont susceptibles d'être mises à jour fréquemment.

Les éditeurs de logiciels antivirus constatent que ce type d'attaques est de plus en plus fréquent. Afin d'éviter que votre réseau ne soit utilisé dans ce genre de compromission, vous pouvez surveiller (ou le cas échéant interdire) les connexions sortantes de type ICMP ou utilisant le protocole associé à eDonkey ou Overnet (identifiant 0xE3 dans l'en-tête UDP).

Afin d'éviter l'infection, il convient de suivre les bonnes pratiques de la messagerie décrites dans la note d'information ci-dessous ainsi que les recommandations présentes dans le mémento du CERTA sur les virus informatiques.

- Note d'information CERTA-2005-INF-004, « Limiter l'impact du SPAM » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-004>
- Les mémentos du CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002.pdf>

6.1 Documentation

- Note d'information du CERTA : risques associés aux clés USB
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-006/index.html>

7 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 08 et le 15 février 2007.

8 Liens utiles

- Mémento sur les virus :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/>
- Note d'information sur l'acquisition de correctifs :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/index.html>
- Note d'information sur les systèmes obsolètes :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html>
- Note d'information sur les bonnes pratiques concernant l'hébergement mutualisé :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/index.html>
- Note d'information sur les mots de passe :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html>
- Note d'information sur la terminologie d'usage au CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/index.html>
- Note d'information sur les enjeux de sécurité liés à une migration vers IPv6 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/index.html>
- 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 CERTA-2006-INF-006, Risques associés aux clés USB :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-006/>
- Note d'information du CERTA CERTA-2006-INF-008 sur les outils d'indexation et de recherche :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-008/>

9 Rappel des avis émis

Durant la période du 09 au 15 février 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-075 : Vulnérabilité dans les produits HP Mercury
- CERTA-2007-AVI-076 : Multiples vulnérabilités dans php
- CERTA-2007-AVI-077 : Vulnérabilité dans HP OpenView
- CERTA-2007-AVI-078 : Vulnérabilité dans la commande rm de Sun Solaris
- CERTA-2007-AVI-079 : Vulnérabilité du service Microsoft de détection matériel noyau
- CERTA-2007-AVI-080 : Vulnérabilité de l'Acquisition d'Image Windows (WIA)
- CERTA-2007-AVI-081 : Vulnérabilité du moteur de protection mpingedll de Microsoft Windows
- CERTA-2007-AVI-082 : Vulnérabilités de Microsoft concernant un objet OLE associé à un fichier RTF
- CERTA-2007-AVI-083 : Multiples vulnérabilités de Microsoft Office
- CERTA-2007-AVI-084 : Multiples vulnérabilités du navigateur Internet Explorer de Microsoft
- CERTA-2007-AVI-085 : Vulnérabilités dans des composants ActiveX de Microsoft Windows
- CERTA-2007-AVI-086 : Vulnérabilités dans ColdFusion

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 réglementaire, 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 œuvre (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 COSSI/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 inexplicables 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.formation.ssi.gouv.fr>

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.

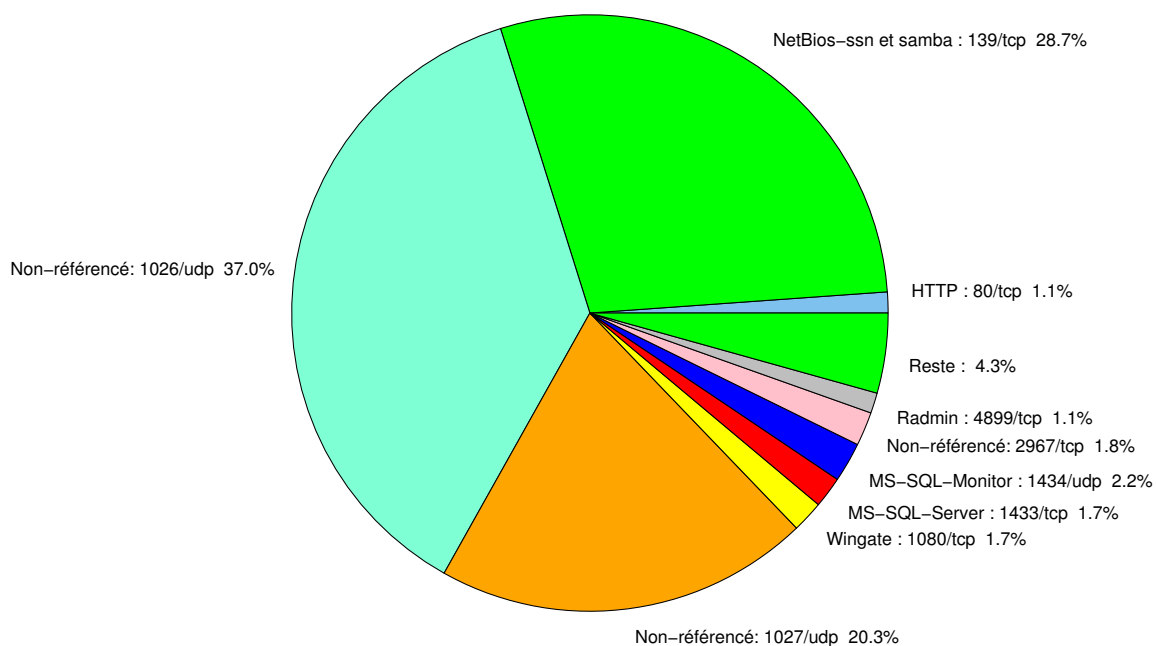


FIG. 1: Répartition relative des ports pour la semaine du 08.02.2007 au 15.02.2007

| Port | Protocole | Service | Porte dérobée | Référence possible CERTA |
|------|-----------|-----------------------|---------------|--|
| 21 | TCP | FTP | – | CERTA-2003-AVI-132 CERTA-2004-AVI-064 CERTA-2004-AVI-066 CERTA-2006-AVI-040 |
| 22 | TCP | SSH | – | CERTA-2003-AVI-152 CERTA-2006-AVI-100 |
| 23 | TCP | Telnet | – | CERTA-2003-AVI-209 CERTA-2003-AVI-131 |
| 25 | TCP | SMTP | – | CERTA-2006-AVI-124 CERTA-2006-AVI-135 |
| 42 | TCP | WINS | – | CERTA-2004-AVI-384 |
| 80 | TCP | HTTP | – | CERTA-2004-AVI-195 CERTA-2004-AVI-239 CERTA-2006-AVI-055 CERTA-2006-AVI-069 CERTA-2006-AVI-156 CERTA-2006-AVI-315 |
| 106 | TCP | MailSite Email Server | – | – |
| 111 | TCP | Sunrpc-portmapper | – | CERTA-2003-AVI-052 |
| 119 | TCP | NNTP | – | CERTA-2004-AVI-340 |
| 135 | TCP | Microsoft RPC | – | CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127 |
| 137 | UDP | NetBios-ns | – | CERTA-2004-AVI-031 |
| 139 | TCP | NetBios-ssn et samba | – | CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-213 CERTA-2005-AVI-302 CERTA-2005-AVI-398 CERTA-2006-AVI-283 |

| | | | | |
|-------|-----|---------------------------------------|-------------------------|--|
| | | | | CERTA-2006-AVI-338 |
| 143 | TCP | IMAP | – | CERTA-2005-AVI-185 |
| 389 | TCP | LDAP | – | CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126 |
| 443 | TCP | HTTPS | – | CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343 |
| 445 | TCP | Microsoft-smb | – | CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-302 CERTA-2006-AVI-283 CERTA-2006-AVI-338 |
| 1023 | TCP | – | Serveur ftp de Sasser.E | – |
| 1080 | TCP | Wingate | MyDoom.F | CERTA-2006-AVI-232 |
| 1433 | TCP | MS-SQL-Server | – | CERTA-2002-ALE-006 |
| 1434 | UDP | MS-SQL-Monitor | – | CERTA-2002-AVI-157 |
| 2100 | TCP | Oracle XDB FTP | – | CERTA-2005-ALE-002 |
| 2381 | TCP | – | HP System Management | CERTA-2006-AVI-248 |
| 2745 | TCP | – | Bagle | – |
| 2967 | TCP | Symantec Antivirus | Yellow Worm | CERTA-2006-AVI-221 |
| 3127 | TCP | – | MyDoom | – |
| 3128 | TCP | Squid | MyDoom | CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348 |
| 3306 | TCP | MySQL | – | – |
| 3389 | TCP | Microsoft RDP | – | CERTA-2002-AVI-213 |
| 4899 | TCP | Radmin | – | – |
| 5000 | TCP | Universal Plug and Play | Bobax, Kibuv | CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297 |
| 5554 | TCP | SGI ESP HTTP | Serveur ftp de Sasser | – |
| 5900 | TCP | VNC | – | CERTA-2006-AVI-198 CERTA-2006-AVI-299 |
| 6070 | TCP | BrightStor ARCserve/Enterprise Backup | – | CERTA-2005-AVI-293 |
| 6101 | TCP | Veritas Backup Exec | – | CERTA-2005-AVI-024 |
| 6112 | TCP | Dtspcd | – | CERTA-2002-ALE-001 |
| 6129 | TCP | Dameware Miniremote | – | CERTA-2003-AVI-214 CERTA-2005-AVI-326 |
| 8866 | TCP | – | Porte dérobée Bagle.B | – |
| 9898 | TCP | – | Porte dérobée Dabber | – |
| 10000 | TCP | Webmin, Veritas Backup Exec | – | CERTA-2005-AVI-229 CERTA-2005-AVI-313 |
| 10080 | TCP | Amanda | MyDoom | – |
| 13701 | TCP | Veritas NetBackup | – | CERTA-2005-AVI-447 |
| 18264 | TCP | CheckPoint interface | – | CERTA-2005-AVI-310 |

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

| port | pourcentage |
|-----------|-------------|
| 1026/udp | 37.02 |
| 139/tcp | 28.71 |
| 1027/udp | 20.31 |
| 1434/udp | 2.15 |
| 2967/tcp | 1.83 |
| 1080/tcp | 1.71 |
| 1433/tcp | 1.68 |
| 80/tcp | 1.13 |
| 4899/tcp | 1.1 |
| 137/udp | 0.95 |
| 22/tcp | 0.78 |
| 3128/tcp | 0.55 |
| 25/tcp | 0.37 |
| 21/tcp | 0.26 |
| 2100/tcp | 0.23 |
| 3306/tcp | 0.2 |
| 15118/tcp | 0.17 |
| 143/tcp | 0.08 |
| 3389/tcp | 0.05 |
| 42/tcp | 0.02 |

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

16 février 2007 version initiale.