

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-35

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-035>

Gestion du document

Référence	CERTA-2007-ACT-035
Titre	Bulletin d'actualité 2007-35
Date de la première version	31 août 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-035.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-035/>

1 Les installations de système *clés-en-main*

1.1 Les cédéroms d'installation *clés-en-main*

Le CERTA a traité cette semaine la compromission d'un serveur Web. Ce dernier a été utilisé pour installer plusieurs sites factices (de filoutage). L'analyse a permis d'identifier des causes à ces intrusions et notamment la mise en œuvre d'applications Web dont les versions ne sont plus du tout d'actualité. On peut citer par exemple des composants Joomla! comme `com_repository`, ou `extcalendar`. Cependant, le problème ne se limite pas à ces quelques composants. En effet, le serveur a été installé à partir d'une distribution *clés-en-main*, proposant à toute personne -y compris des néophytes- d'installer des serveurs sous Linux. Cette distribution se présente sous la forme d'une image à graver sur un cédérom. Le démarrage d'une machine, à partir du cédérom va installer ladite distribution en posant quelques questions élémentaires à l'utilisateur, l'objectif étant de lui offrir une installation simple et rapide.

Les services inclus peuvent être :

- hébergement d'un serveur FTP ;
- hébergement d'un annuaire d'utilisateurs ;

- hébergement d'un site Web avec des contenus dynamiques (forums, projets, systèmes de publication, etc.) utilisables en quelques clics ;
- hébergement d'un serveur de messagerie ;
- gestionnaire de partage de connexions, d'imprimantes et autres ressources.

Le CERTA constate que l'installation par défaut d'une telle distribution présente les faiblesses suivantes :

- seul un compte administrateur `root` est demandé / exigé ;
- aucune exigence de solidité n'est faite sur le mot de passe de ce compte ;
- la distribution repose sur un noyau Linux 2.2.26 datant de 2004 ;
- plusieurs services sont lancés pour une installation par défaut, incluant un serveur de résolution de noms (`named`), un serveur MySQL (`mysqld`), un serveur Apache particulier (`httpd`), un serveur d'impression (`lpd`), `smbd`, etc.
- les applications Web fournies regroupent des logiciels dont les vulnérabilités sont nombreuses et qui doivent être mises à jour fréquemment : `claroline`, `phpbb`, `Phorum`, `dotclear`, `typo3`, `webcalendar`, `agora`, etc. De plus, on constate que les versions fournies ne sont pas récentes, même pour un téléchargement récent de la distribution. Plus précisément, la dernière version de la distribution en question date de l'été 2006. Les versions de toutes les applications associées sont donc antérieures à cette date, parfois de plusieurs années (2003/2004).

Que faut-il donc retenir d'un tel incident ? L'objectif n'est évidemment pas de dénigrer de telles distributions, obtenues par un effort collectif afin de soutenir les personnes ayant peu d'expérience avec Linux. Malgré tout, de telles distributions :

- sont rarement mises à jour ;
- intègrent des composants non mis à jour ;
- ont une configuration de sécurité qui n'est clairement pas adaptée.

Il est donc très dangereux d'exposer de telles machines au monde Internet. Leur utilisation doit se borner aux environnements contrôlés ou confinés.

Le CERTA recommande ainsi d'éviter, pour ceux qui seraient tentés, d'utiliser dans un environnement de production de telles solutions, et, pour ceux qui le déploient déjà, de réfléchir à une solution plus sûre. Les responsables de sécurité doivent également s'assurer que de telles distributions n'apparaissent pas dans leur réseau, car il s'agirait de points faibles potentiels.

1.2 Les cédéroms de démarrage

L'incident précédent soulève un problème plus important : celui des cédéroms de démarrage. Il existe un large choix de cédéroms téléchargeables sur l'Internet, en fonction des besoins : il peut s'agir d'une distribution destinée à fournir un environnement de bureau Linux complet, à faire des tests d'audit ou à installer un routeur ou un pare-feu.

Les arguments intéressants qui conduisent à utiliser de telles solutions sont les suivants :

- éviter la longue procédure d'installation initiale ;
- effectuer un minimum de configuration ;
- obtenir rapidement un système fonctionnel ;
- répondre à un besoin ponctuel sans laisser de traces importantes sur le disque dur d'une machine ;
- assurer que les codes du système ne sont pas modifiés sur le support (cédérom), et donc un certain niveau d'intégrité.

Il faut néanmoins garder à l'esprit que ces solutions posent le même problème que le cas précédemment cité : *quid* des mises à jour ? Ces distributions sont renouvelées peu fréquemment (de l'ordre de plusieurs mois) et peuvent souffrir de quelques vulnérabilités. Les configurations par défaut ne sont également pas toujours parfaites.

Les données personnelles ajoutées peuvent donc courir un risque. Si le système est compromis, il peut donner accès à d'autres périphériques (disques durs, supports USB, etc.).

Le CERTA ne dénigre pas de telles solutions, qui présentent des avantages certains, mais insiste sur le fait qu'elles introduisent également quelques problèmes de sécurité à considérer.

2 La défiguration, effet visible pouvant révéler des incidents plus graves

Le CERTA a traité cette semaine un autre cas de défiguration d'un serveur Web. L'analyse des journaux de celui-ci a mis en évidence l'exploitation d'une vulnérabilité affectant le module `xfsection` de `Xoops`. Les

journaux ont également montré que ce module faisait régulièrement l'objet d'attaques depuis mars 2007. La conséquence de ces autres attaques n'a pas été une défiguration visible, mais l'installation de nombreux outils malveillants.

Parmi les outils installés, on retrouve :

- deux *bot irc* écrits en PHP. Ces robots vont se connecter sur des canaux *irc* de serveurs généralement « privés » et ont la capacité de lancer des attaques en déni de service. Ils ont également une fonctionnalité leur permettant d'attaquer d'autres serveurs Web en tentant d'exploiter des vulnérabilités de type *php include* ;
- un programme effectuant des connexions sur une base de données externe afin d'y récupérer une liste d'adresses de messagerie, ainsi que des messages électroniques. Cet outil permet notamment de transformer le serveur Web en plate-forme de *spam* ;
- un interpréteur de commandes PHP encodé en *base64* afin d'échapper à une détection par recherche de chaînes de caractères.

Pour fonctionner, ces outils ont besoin de pouvoir effectuer une connexion vers l'Internet. Il est donc recommandé d'interdire aux serveurs Web d'effectuer des connexions sortantes. Cette mesure aura pour effet de rendre inopérante la plupart des attaques de type *php include*.

3 Des modifications de contenus de pages Web

3.1 Introduction

Les défigurations sont les manifestations les plus visibles de modifications de contenus de pages Web. Cependant, les mois précédents ont montré que d'autres modifications étaient possibles, et non visibles directement. Parmi celles-ci, nous avons mentionné dans nos précédentes publications :

- les cadres incorporés *IFRAME* (CERTA-2007-ACT-025) ;
- les scripts ajoutés (*SCRIPT*) ;
- les images trompeuses intégrant des scripts (CERTA-2007-ACT-026) ;
- l'optimisation de la popularité d'un site, en dissimulant des liens dans une balise *DIV* (CERTA-2007-ACT-033).

Dans cet article, il s'agit d'un autre élément : les données de style, ou CSS (pour *Cascading Style Sheets*). Elles servent à définir la présentation des documents HTML, et couvrent notamment les polices, les couleurs, les marges, les lignes, les images en arrière-plan, les différents positionnements, etc.

Différentes utilisations sont possibles. Les données peuvent être insérées dans une balise :

```
<_body style="background-color: #FF0000;">
```

Ou insérées entre des balises particulières :

```
<_style type="text/css">
  body {background-color: #FF0000;}
</_style>
```

Voir directement insérées dans un fichier dédié reprenant les lignes précédentes :

```
<_link rel="stylesheet" type="text/css" href="style.css" />
```

Les trois méthodes permettent d'obtenir un fond rouge pour les éléments corps de la page.

3.2 La vulnérabilité

Des preuves de faisabilité ont été récemment publiées, et montrent qu'il est possible de balayer certaines plages d'adresses IP locales, lorsque le navigateur interprète une page Web ayant des données de style particulières. Le fonctionnement global est le suivant : un ensemble de styles est défini (*style1*, *style2*, *style3*, etc.), et chacun est associé à une adresse IP à scanner. Ensuite, les styles sont appelés successivement par la page HTML pour déterminer les adresses réactives.

Cette technique peut être utilisée pour différents motifs, comme déterminer l'espace d'adressage utilisé, l'existence de passerelles, ou celles d' interfaces de modems / routeurs par exemple.

Cette modification de style peut être visible soit directement dans le code de la page, soit dans le fichier *.css* associé. Dans le cas du code publié récemment, une succession de lignes est visible, avec des contenus de type :

```
a[href="http://W.X.Y.Z"], où W.X.Y.Z est une adresse IP
```

Une simple page PHP avec une variable de valeur W.X.Y.Z permet ensuite à la personne distante de récupérer l'information.

Cette technique ne nécessite pas forcément de Javascript, mais comme dans les insertions malveillantes précédentes, il peut être employé pour dissimuler le code. La personne malveillante peut utiliser son propre serveur Web hébergeant un tel site, mais elle a tout intérêt à l'ajouter sur un site plus « populaire » et « de confiance », afin de collecter indirectement les informations des postes des personnes navigantes.

Il est donc très important, compte-tenu de ces méthodes, de contrôler préventivement l'intégrité de l'ensemble des fichiers et données du site Web. C'est l'une des seules méthodes pour s'apercevoir qu'un tel code malveillant est présent sur l'une des pages du site administré.

4 Les paramètres d'installation par défaut oubliés

4.1 Le problème

Cette semaine le CERTA a rencontré un site Internet compromis dont tous les composants semblaient à jour. Ce site, dynamique, respectait des préconisations simples :

- les produits et composants utilisés étaient à jour ;
- les composants non-utiles étaient désactivés ;
- le code PHP contrôlait les variables utilisées ;
- l'archivage et la journalisation des connexions était en place.

L'analyse de la compromission a montré que ce serveur dédié utilisait une application accessible depuis l'Internet dont l'installation proposait un mot de passe par défaut. Ce mot de passe n'ayant jamais été changé, certains individus malintentionnés ont pu se connecter sur la machine et réaliser des attaques par rebond. Au-delà des actions réalisées par les attaquants, il est dommageable de constater que des précautions basiques n'ont pas été respectées sur ce serveur (alors qu'elles l'ont été sur le site Internet qu'il contenait) :

- tous les accès par mot de passe doivent être surveillés dans la mesure du possible ;
- les mots de passe initiaux doivent être immédiatement remplacés par des mots de passe forts qu'il convient de changer régulièrement ;
- les services et applications non utilisés doivent être arrêtés

4.2 Documentation associée

- Note d'information du CERTA sur les mots de passe :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001>
- Note d'information du CERTA sur le filtrage et les pare-feux :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-001>
- Note d'information du CERTA sur la sécurisation des applications Web :
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-INF-001>

5 Nouveaux correctifs pour Windows Vista

5.1 Les correctifs

Le 28 août 2007, soit en dehors des dates usuelles de publications de mises à jour (deuxième mardi de chaque mois), Microsoft a rendu disponible via des mises à jour automatiques deux correctifs pour Windows Vista qui avaient été publiés le 7 août 2007 ainsi que deux supplémentaires :

- une mise à jour concerne l'arrêt inopiné du *Background Intelligent Transfer Service* (service de transfert intelligent) qui peut se produire lors du téléchargement de mises à jour (KB939159) ;
- un correctif traite divers problèmes de performance et de fiabilité : suppression de la passerelle par défaut après hibernation, fuites mémoire, lenteur de transferts de fichiers, corruptions de fichiers, etc. (KB938979) ;
- une autre mise à jour corrige davantage de problèmes de stabilité (arrêt inopiné de Windows Calendar, du partage Internet, du service d'impression) mais aussi de compatibilité matérielle, notamment pour les cartes graphiques (KB938194) ;
- le dernier correctif traite une erreur dans le libellé de langue traditionnelle chinoise (KB938952).

La liste complète des correctifs est fournie à la fin de cet article. D'autres mises à jour ont également été publiées sur le site de Microsoft (en téléchargement manuel). Elles concernent Windows XP et Vista en versions 32 et 64 bits et corrigent des problèmes plus marginaux.

5.2 Problèmes concernant la validation WGA

La validation WGA (*Windows Genuine Advantage*) permet à Microsoft de s'assurer que la copie de l'utilisateur est bien originale. Dans la nuit du vendredi 24 août au samedi 25 août 2007, de nombreux utilisateurs n'ont toutefois pu valider l'authenticité de leur Windows Vista. Par conséquent, certaines fonctionnalités de Windows n'ont pu être disponibles pour ces personnes, notamment : *Windows Aero*, *Readyboost*, fonctionnement de *Windows Defender* en mode dégradé, téléchargement limité aux mises à jour de sécurité critiques et affichage d'un message persistant.

Le problème a été résolu par Microsoft. Il était dû à une mauvaise manipulation lors de la mise à jour des serveurs de validation qui ont ainsi, selon Microsoft, décliné les demandes de validation. Les utilisateurs ayant rencontré ce problème peuvent maintenant valider leur exemplaire correctement.

5.3 Références

- Base de connaissances Microsoft n°938194 :
<http://support.microsoft.com/kb/938194>
- Base de connaissances Microsoft n°939159 :
<http://support.microsoft.com/kb/938194>
- Base de connaissances Microsoft n°938979 :
<http://support.microsoft.com/kb/938194>
- Base de connaissances Microsoft n°938952 :
<http://support.microsoft.com/kb/938194>

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 23 et le 30 août 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 24 au 30 août 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-375 : Vulnérabilité dans EMC Legato Networker
- CERTA-2007-AVI-376 : Multiples vulnérabilités dans Trend Micro ServerProtect
- CERTA-2007-AVI-377 : Vulnérabilité dans GNU tar
- CERTA-2007-AVI-378 : Vulnérabilité de Sylpheed
- CERTA-2007-AVI-379 : Multiples vulnérabilités de Bugzilla
- CERTA-2007-AVI-380 : Vulnérabilité dans Qt
- CERTA-2007-AVI-381 : Vulnérabilités dans Sophos Anti-Virus
- CERTA-2007-AVI-382 : Vulnérabilité d’Emacs
- CERTA-2007-AVI-383 : Vulnérabilité dans Subversion (svn)
- CERTA-2007-AVI-384 : Multiples vulnérabilités dans Konqueror
- CERTA-2007-AVI-385 : Multiples vulnérabilités de BEA Weblogic

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

- CERTA-2007-AVI-290-002 : Vulnérabilités dans GIMP
(ajout des références aux bulletins de sécurité Mandriva et Ubuntu)
- CERTA-2007-AVI-318-001 : Multiples vulnérabilités dans Mozilla Firefox
(ajout des références aux bulletins de sécurité Gentoo, Debian, Mandriva, Red Hat, SuSE et Ubuntu)
- CERTA-2007-AVI-363-001 : Vulnérabilités dans Opera
(ajout d’une vulnérabilité, de la référence CVE et des bulletins de sécurité Gentoo et SuSE)
- CERTA-2007-AVI-373-001 : Vulnérabilité dans NuFW
(la vulnérabilité ne touche pas les versions 20.x.)

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’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.

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 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.

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.

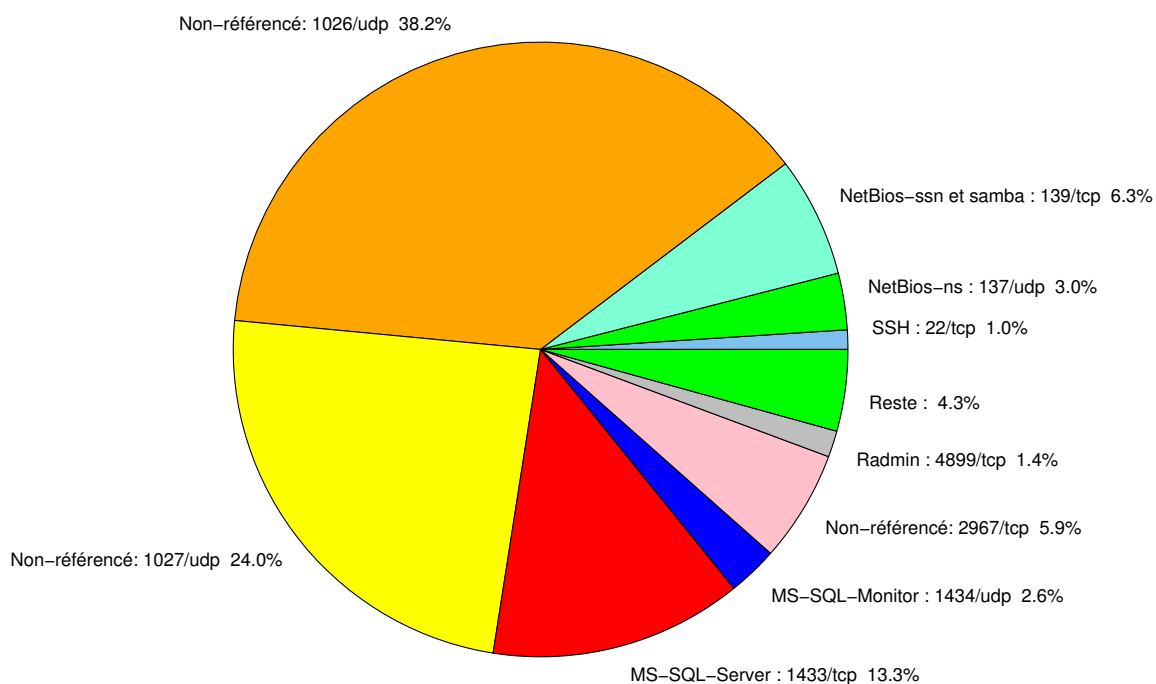


FIG. 1: Répartition relative des ports pour la semaine du 23.08.2007 au 30.08.2007

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	38.17
1027/udp	24.03
1433/tcp	13.3
139/tcp	6.32
2967/tcp	5.86
137/udp	2.97
1434/udp	2.62
4899/tcp	1.38
22/tcp	1.01
25/tcp	0.93
80/tcp	0.76
1080/tcp	0.69
3128/tcp	0.51
3306/tcp	0.39
21/tcp	0.25
443/tcp	0.15
143/tcp	0.11
15118/tcp	0.05
5554/tcp	0.04
6129/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

31 août 2007 version initiale.