Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 août 2007
N° CERTA-2007-ACT-034

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-34

Gestion du document

Référence	CERTA-2007-ACT-034
Titre	Bulletin d'actualité 2007-34
Date de la première version	24 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-034.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-034/

1 Des incidents traités cette semaine

1.1 Développement de scripts PHP et incidents

Le CERTA a traité cette semaine un incident de compromission de site Web faisant suite à l'exploitation d'une vulnérabilité de type *PHP Include*. Ces attaques sont assez courantes et affectent généralement des applications Web très populaires et très répandues. La compromission traitée se démarque des autres car le script attaqué ne correspondait à aucune application Web connue. Il s'agissait d'un développement « maison ».

Des administrateurs considèrent -à tort- que les scripts développés pour un besoin propre ne présentent pas de risque de sécurité puisque personne n'a accès à leurs sources. C'est une forme de « sécurité par l'obscurité ». Cette approche est mauvaise car il n'est pas nécessaire d'avoir accès aux sources de ces programmes pour découvrir des vulnérabilités. C'est notamment le cas pour les attaques de type *cross site scripting* et *SQL injection* qui sont toujours de la même forme et peuvent être testées sur tout script PHP. Quant aux cibles d'attaques de type *PHP Include*, elles peuvent être repérées à l'aide d'un simple moteur de recherche, comme c'était le cas pour notre incident traité.

Il est recommandé de soumettre les scripts PHP à des tests de sécurité avant de les mettre en ligne.

1.2 Un bon reflexe concernant la messagerie

Cette semaine le CERTA, après avoir découvert une compromission d'un site web, a prévenu la victime par courrier électronique. Celle-ci, ne connaissant pas le CERTA, s'est rendue sur le site Web et a appelé le numéro de téléphone y figurant afin de confirmer l'authenticité du courriel qu'elle venait de recevoir.

Ceci est un exemple parmi d'autres du principe de précaution qu'il convient d'appliquer à la messagerie electronique : n'accorder qu'une relative confiance à l'émetteur affiché dans un courrier. Cela est d'autant plus vrai quand le message demande explicitement de retourner des informations ou d'exécuter une action.

Il est bon de rappeler à cette occasion qu'il faut éviter de cliquer sur des liens présents dans les courriers (préférer recopier l'adresse à la main dans le navigateur) ; en aucun cas, même si le courriel le demande, transférer érer un mail reçu à tous ses contacts. L'information est souvent fausse (canulars, *hoax*), risque de saturer les systèmes de messagerie, et peut servir de vecteur de propagation.

1.3 Jamais plus jamais

1.3.1 Les faits

Au début du mois de juillet le CERTA avait informé une administration française que son serveur web avait été compromis. L'analyse des journaux des connexions avait révélée de multiples compromissions, le serveur hébergeant aussi des outils d'attaque. La préconisation du CERTA était alors de ne plus accorder aucune confiance au serveur ainsi qu'aux données présentes dessus. Malgré ce conseil, le serveur a fait l'objet d'un nettoyage superficiel des pages vulnérables et d'une simple suppression des outils malveillants détectés par le CERTA.

1.3.2 Nouvelle compromission ?

Cette semaine, en analysant les propres fichiers journaux de son serveur web, le CERTA a constaté des tentatives d'attaques de type *PHP Include*. Elles sont visiblement émises de la machine précédemment citée.

Après avoir repris contact avec le responsable du serveur, le CERTA a pu vérifier que ce serveur n'avait été que sommairement nettoyé. Plusieurs portes dérobées étaient de nouveau actives. Les connexions sortantes de cette machine ne sont pas filtrées, ce qui laisse à tout code malveillant tous moyens de communication et d'échange avec l'extérieur.

Le CERTA insiste donc sur le fait que, lors d'un compromission, il ne faut plus accorder la moindre confiance au système compromis et aux données présentes sur celui-ci ou accessible depuis celui-ci. Dans le cas ou l'intégrité du système est mise en doute, il convient de repartir sur des bases saines :

- installer un système d'exploitation sain à partir de sources de confiance, sans le connecter au réseau ;
- désactiver les services non-nécessaires ;
- mettre à jour le système d'exploitation tout en restant déconnecté du réseau ;
- installer les applications devant être présentes sur le serveur, et seulement celles-ci ;
- mettre à jour ces applications ;
- identifier une sauvegarde de confiance (antérieure à toutes compromissions) ;
- restaurer les données à partir de cette sauvegarde ;
- connecter sur le réseau le serveur.

Cette compromission a été découverte par l'analyse de journaux. Le CERTA rappelle donc à cette occasion que l'analyse des journaux doit être effectuée régulièrement afin de pouvoir mettre en évidence une éventuelle compromission ou des tentatives d'attaques.

1.3.3 Documentation

- Note d'information du CERTA sur les bons réflexes en cas d'intrusion :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002
- 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

2 MS07-044, et la conversion des fichiers Microsoft Office

2.1 *Microsoft Office Isolated Conversion Environment*

Le CERTA a publié l'avis CERTA-2007-AVI-354 correspondant au bulletin Microsoft MS07-044 du mois d'août 2007. Il concerne une vulnérabilité dans Excel et Excel Viewer.

Cette vulnérabilité est donc officiellement corrigée par l'éditeur, qui présente aussi quelques solutions de contournement afin de limiter les possibilités d'exploitation de cette dernière.

Le CERTA avait mentionné dans le précédent bulletin CERTA-2007-ACT-021 un outil proposé par Microsoft pour convertir des documents Office 2003 et 2007 : `MOICE` (pour *Microsoft Office Isolated Conversion Environment*). L'idée sous-jacente consiste à utiliser une conversion des documents binaires 2003 ou 2007 vers le format Office OpenXML. Cette étape, faite dans un environnement propre, doit en principe produire un document dans un nouveau format et détruire les codes malveillants abusant d'une vulnérabilité concernant uniquement le format initial.

Il est donc légitime de penser que cet outil est également un contournement pour atténuer les risques liés à la vulnérabilité MS07-044. C'est par exemple le cas pour les trois vulnérabilités corrigées dans le bulletin de juillet MS07-036 (CERTA-2007-AVI-291).

Cependant, ce contournement n'est pas valable avec la vulnérabilité décrite dans le bulletin MS07-044. Le bloc-notes de Microsoft en fournit la raison : la vulnérabilité associée au MS07-044 concerne les fichiers d'espace de travail au format `XLW`. Or l'outil `MOICE` ne sait manipuler, en l'état actuel, que les formats suivants : `XLS`, `XLT` et `XLA` (pour *eXcel Additive* et utilisé par les fonctions VBA par exemple).

`MOICE` se limite également à Microsoft Office 2003 et 2007 dans sa version actuelle.

De tels outils de conversion sont importants pour améliorer la sécurité globale. Ils agissent de manière à prévenir d'éventuels risques (ici associés à certains formats). Ils ne peuvent cependant pas se substituer à la vigilance de l'utilisateur, aux bonnes pratiques comportementales (mise à jour des applications, sessions aux droits limités, etc.) et aux solutions antivirales.

2.2 Autre contournement envisageable : *FileBlock*

FileBlock de Microsoft Office 2003 et 2007 permet aux administrateurs de restreindre les manipulations des types de fichiers Excel, Word ou PowerPoint à certains types. Chaque type est associé à une « politique de groupe » dans la base de registres.

Cette fonctionnalité permet un contournement provisoire face à la vulnérabilité définie dans le bulletin MS07-044. Cette solution a plusieurs limitations :

- elle implique intrinséquement que la politique d'accès est précise, avec des utilisateurs et des droits dédiés. Ce n'est malheureusement pas toujours le cas.
- elle permet uniquement à certains utilisateurs de ne pas ouvrir des types de fichiers, mais ne prévient pas du danger ni de l'ouverture par d'autres utilisateurs aux privilèges plus élevés ;
- elle repose sur une nouvelle fonction (*FileBlock*) pour identifier le format de tous les fichiers Office avant leur ouverture complète. Dès qu'il sera possible de leurrer cette fonction, le contournement ne sera plus utilisable.

Une bonne pratique consiste néanmoins à n'autoriser que le nécessaire. Si des formats ne sont jamais utilisés, il est préférable de les filtrer. Cela peut se faire à différents niveaux, sur la machine hôte, par une solution comme *FileBlock*, mais aussi au niveau des différentes passerelles (messagerie, web, etc.) ou par des sondes de détection, etc.

2.3 Documentation associée

- Avis de sécurité Microsoft 937696 du 21 mai 2007, présentant `MOICE` et *FileBlock* :
  http://www.microsoft.com/technet/security/advisory/937696.mspx
- Bulletin d'actualité CERTA-2007-ACT-021 du 25 mai 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-021/
- Communiqué du *Microsoft Security Response Center* le 23 août 2007 à ce sujet :
  http://blogs.technet.com/msrc/archive/2007/08/23/technical-tips-and-insights-on-ms07-049-and-ms07-044.aspx

3 Ver *Storm* : le bon sens reste la meilleure défense

Le ver *Storm* (« tempête » en anglais) ou *Zhelatin* tente de se répandre à large échelle. Plusieurs journaux ont largement repris l'information cette semaine.

L'offensive comprend plusieurs étapes et les bonnes pratiques peuvent le contrer.

Les pourriels

Une vague très importante de pourriels a lieu. Le sujet est rédigé actuellement en anglais. Il change sans cesse, en cohérence avec le corps du message : de la proposition de voir des photos ou de charger des musiques en MP3 à la demande de confirmation d'information utilisateur, en passant par les cartes postales électroniques (*ecard*), le spectre est très large.

Des points communs à ces pourriels doivent éveiller la vigilance :

- le message est en texte brut, pour tromper les filtres antispam qui pénalisent les courriers en HTML ;
- dans certaines variantes, un numéro de compte, un identifiant (login) , un mot de passe temporaire et un avertissement veulent laisser croire que l'expéditeur prend en compte la sécurité ;
- le lien sur lequel le destinataire crédule est invité à cliquer est numérique. Il n'a pas une forme textuelle `http://Domaine-douteux/`, mais contient l'adresse IP d'une machine sous la forme `http://W.X.Y.Z/`

  L'internaute responsable ne clique pas sur ce lien.

L'infection

Le destinataire très imprudent qui, malgré le caractère étrange du pourriel, a cliqué sur le lien est connecté sur un serveur web. La page d'accueil du site l'invite à télécharger une applette, par exemple pour sécuriser la connexion. C'est cette applette qui va infecter le poste de l'utilisateur.

Cette infection ne réussit, dans les versions actuelles du ver, que si les logiciels présents sur le poste de l'utilisateur ne sont pas à jour.

Le comportement, défense non coûteuse

Un comportement raisonnable suffit pour prévenir l'infection par ce ver :

- maintenir son système d'exploitation et ses applications à jour ;
- ne pas ouvrir les courriels inattendus (expéditeurs, langue, sujet...) ;
- ne pas cliquer sur les liens dans les pourriels, en particulier si le lien contient une adresse numérique ou des caractères obscurs ;
- ne pas télécharger de programmes exécutables (.exe, . msi, .scr, etc.) ou d'applettes à partir de sources inconnues ;
- naviguer sur l'Internet en utilisant un compte qui n'a pas les droits d'administration, et auquel le droit d'installer un logiciel sera retiré.

4 Les événements sous Windows Vista, suite

L'article "Les événements sous Microsoft Windows Vista" du bulletin d'actualité CERTA-2007-ACT-017 présentait les événements sur Vista.

On peut y lire l'apport de nombreuses nouveautés :

- le nouveau format XML binaire ;
- l'exportation des événements aux formats XML, evtx et texte ;
- le filtrage et la création de vues personalisées ;
- la nouvelle numérotation et pour la majorité une correspondance des numéros par rapport à Windows XP (`EventIdVista = 4096 + EventIdXP`).

Sur Windows Vista, l'emplacement des fichiers d'événements a également changé : ils se trouvent maintenant dans le répertoire :

```
C:\Windows\system32\Winevt\Logs
```

On y trouve plus de 50 fichiers, correspondant chacun à une catégorie d'événement, par exemple : applications, sécurité, système, mises à jour windows, etc.

Le nouveau service "*Event Collector Service*" également disponible sur Windows 2003 Server, permet à des ordinateurs distants de déporter des événements d'un type prédéfini vers un poste pour centraliser les informations.

Enfin, il est également possible d'attacher une action à un événement. Par exemple, l'on peut décider d'envoyer un courrier électronique, lancer une application, ou afficher un message lorsqu'un utilisateur se connecte sur le poste, lorsque des mises à jour sont disponibles, etc. Ces actions peuvent être ensuite supprimées dans le planificateur de tâches, qui regroupe également les actions par défaut de Windows. On y remarque d'ailleurs, que certaines tâches utilisent déjà le système d'événements (conflit d'adresses IP, par exemple). D'autres tâches basées sur des critères différents peuvent évidemment y être ajoutées ; et on peut notamment y changer des actions par défaut (lancement du défragmenteur de disque tous les mercredis, création automatique de points de restauration tous les jours, par exemple).

4.1 Références

– "Les événements sous Microsoft Windows Vista"
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-017.pdf

5 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 16 et le 23 août 2007.

6 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/

7 Rappel des avis émis

Dans la période du 16 au 23 août 2007, le CERTA a émis les avis suivants :

– CERTA-2007-AVI-367 : Vulnérabilité dans ESRI ArcSDE

– CERTA-2007-AVI-368 : Vulnérabilité dans Symantec Enterprise Firewall
– CERTA-2007-AVI-369 : Vulnérabilité dans Sun Solaris RBAC
– CERTA-2007-AVI-370 : Vulnérabilités dans les produits ZoneLabs
– CERTA-2007-AVI-371 : Vulnérabilités dans rsync
– CERTA-2007-AVI-372 : Vulnérabilités des pilotes WiFi Atheros pour Windows
– CERTA-2007-AVI-373 : Vulnérabilité dans NuFW
– CERTA-2007-AVI-374 : Multiples vulnérabilités de ClamAV
– CERTA-2007-AVI-375 : Vulnérabilité dans EMC Legato Networker
– CERTA-2007-AVI-376 : Multiples vulnérabilités dans Trend Micro ServerProtect

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

– CERTA-2007-AVI-278-001 : Vulnérabilités dans Wireshark
(ajout des références aux bulletins de sécurité Gentoo, Mandriva, SuSE et Debian)
– CERTA-2007-AVI-327-005 : Vulnérabilité dans BIND
(ajout de la référence au bulletin de sécurité Gentoo)
– CERTA-2007-AVI-339-001 : Multiples vulnérabilités dans Apache
(ajout de la référence au bulletin de sécurité Ubuntu)
– CERTA-2007-AVI-341-002 : Vulnérabilité dans gpdf
(ajout de la référence au bulletin de sécurité Debian)

8 Actions suggérées

8.1 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.

8.2 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.

8.3 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.

8.4 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.

8.5 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.

8.6 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.

8.7 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

9 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.

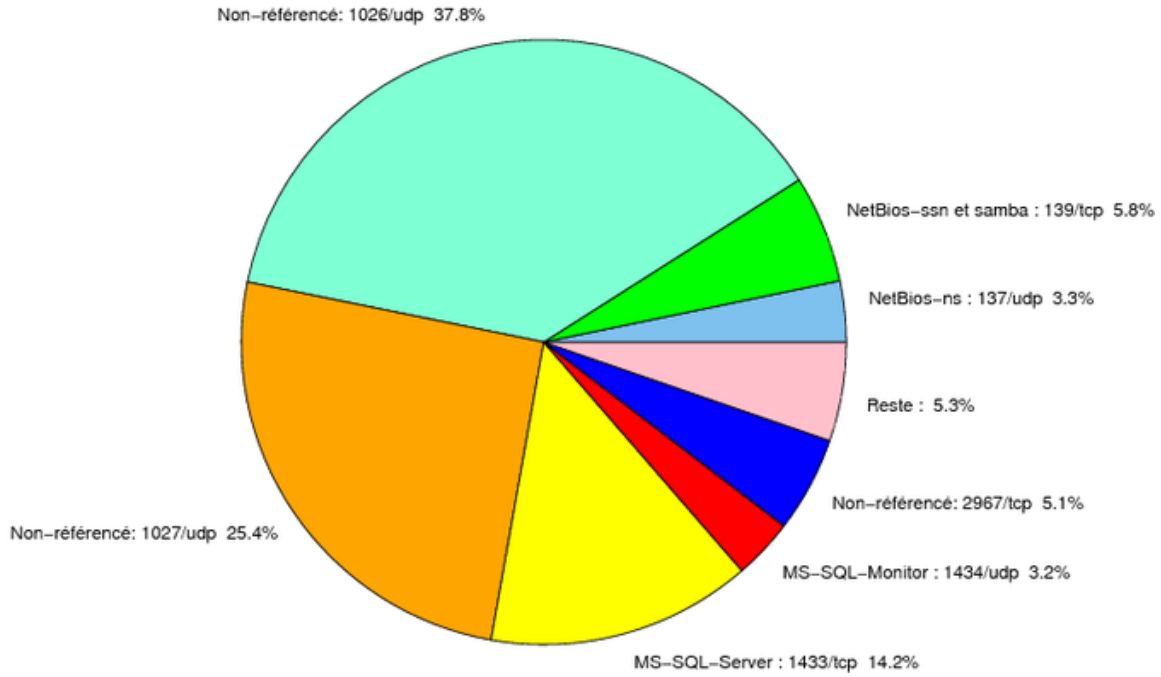

FIG. 1: Répartition relative des ports pour la semaine du 16.08.2007 au 23.08.2007

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CE 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 http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE 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 http://www.certa.ssi.gouv.fr/site/CE 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 http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE

				http://www.certa.ssi.gouv.fr/site/CE 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 http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE 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 http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE 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 http://www.certa.ssi.gouv.fr/site/CE 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 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 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 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	37.8
1027/udp	25.4
1433/tcp	14.15
139/tcp	5.75
2967/tcp	5.11
137/udp	3.25
1434/udp	3.23
4899/tcp	0.85
1080/tcp	0.76
22/tcp	0.74
25/tcp	0.66
3306/tcp	0.56
3128/tcp	0.51
80/tcp	0.4
21/tcp	0.32
443/tcp	0.18
3389/tcp	0.08
143/tcp	0.06
23/tcp	0.05
6129/tcp	0.03
9898/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

24 août 2007 version initiale.