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 mai 2007
N° CERTA-2007-ACT-020

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-20

Gestion du document

Référence	CERTA-2007-ACT-020
Titre	Bulletin d'actualité 2007-20
Date de la première version	18 mai 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-020.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-020/

1 Les incidents traités cette semaine

1.1 Evolution d'un site Web hébergeant des pages de filoutage (*phishing*)

Le CERTA a pu, au travers d'un incident, observer l'évolution d'un site Web hébergeant un site de *phishing*. Pour diverses raisons, notamment un manque de coopération de l'hébergeur, ce site Web compromis n'a pas pu faire l'objet d'un traitement d'incident correct. En particulier, il n'a pas été possible d'accéder aux journaux du serveur, ce qui aurait pu permettre de mettre en évidence la faille exploitée, ainsi qu'une éventuelle utilisation d'une porte dérobée déposée précédemment (cette méthode étant fréquemment employée par les intrus). En revanche, nous avons pu suivre l'évolution des sites de *phishing* installés au gré des messages de notification que nous avons reçus. Nous pouvons établir la chronologie suivante pour le serveur infecté :

- 13 avril 2007 : découverte de la compromission du site, présence d'un site de *phishing* ciblant les utilisateurs d'une banque ;
- 17 avril 2007 : site de *phishing* ciblant la même banque mais situé dans un répertoire différent ;
- 27 avril 2007 : site de *phishing* toujours présent, ciblant toujours la même banque, et qui n'a *a priori* pas évolué depuis le 17 avril 2007 ;

– 09 mai 2007 : présence d'un site de *phishing* ciblant les utilisateurs d'un site d'enchères en ligne, le site concernant la banque n'est plus accessible ;
– 16 mai 2007 : suppression d'une vulnérabilité sur le site ;
– 18 mai 2007 : le site de *phishing* présent le 9 mai 2007 est toujours accessible.

Les sites de *phishing* envoient généralement des messages électroniques chez des fournisseurs de messagerie gratuite. Il est possible que ces adresses de messagerie aient évolué dans le temps. Il est important de préciser que tant qu'au moins une vulnérabilité est présente, le fait de couper l'accès à certaines pages du site est inefficace. En effet, l'intrus peut exploiter une faille ou une porte dérobée (installée lors d'une précédente intrusion) pour réactiver les accès au site frauduleux.

Les incidents de ce type ne peuvent souvent être résolus que par une analyse complète du disque dur, ce qui implique la coopération de l'hébergeur et une interruption de service pour tous les sites co-hébergés.

2 Des problèmes de codage / décodage pour les outils de sécurité

Les caractères Unicode peuvent être représentés de différentes manières. Ainsi, pour des symboles chinois, japonais ou coréens, il est possible de distinguer les caractères codés sur un seul octet (*halfwidth*) ou sur deux (*fullwidth*). Cette distinction est aussi possible pour d'autres caractères, comme ceux de l'alphabet latin. S'il est probable qu'un caractère existe sous les deux formes de codage, cela n'est pas systématique.

En d'autres termes, certaines chaînes de caractères n'auront pas la même signification si elles sont codées par l'une ou l'autre des deux méthodes. Un tableau présentant certaines différences est disponible à l'adresse ci-dessous :

http://www.unicode.org/charts/PDF/

Une vulnérabilité liée à cette propriété a été identifiée dans plusieurs outils de sécurité qui manipulent des chaînes de caractères HTTP, comme les adresses réticulaires (`URL`).

L'exploitation de cette vulnérabilité permettrait de contourner des politiques de filtrage ou d'analyses de contenu. Une liste de systèmes vulnérables est disponible aux adresses suivantes :

– Note de vulnérabilité 739224 de l'US-CERT du 14 mai 2007 :
http://www.kb.cert.org/vuls/id/739224
http://www.gamasec.net/english/gs07-01.html

Peu de constructeurs ont, à la date de publication de ce bulletin, proposé des mises à jour. Des bulletins de sécurité ont néanmoins été émis par certains d'entre eux :

– Avis de sécurité Cisco 91767 du 14 mai 2007 :
http://www.cisco.com/warp/public/707/cisco-sr-20070514-unicode.shtml
– Avis de sécurité Tipping Point 3com 3COM-07-001 du 14 mai 2007 :
http://www.3com.com/securityalert/alerts/3COM-07-001.html

Le CERTA tiendra ses correspondants informés par le biais d'avis quand les mises à jour seront disponibles.

3 Des nouvelles de Microsoft

3.1 Problème de mise à jour ?

Microsoft a publié mercredi 16 mai 2007 un correctif pour une mise à jour apparue en début du mois : il s'agit du bulletin MS07-027 (KB931768), décrit dans l'avis CERTA-2007-AVI-207.

Cette mise à jour, de référence KB937409, corrige un problème de permissions attribuées aux fichiers temporaires d'Internet Explorer. Les utilisateurs n'utilisant pas le répertoire par défaut, voient apparaître après l'application du correctif une boîte dialogue les avertissant d'un problème de sécurité lié au téléchargement de fichiers (*"File Download - Security Warning"*).

Le récent document de Microsoft explique comment ré-attribuer correctement les droits pour le répertoire choisi, ou revenir à la configuration initiale.

Le CERTA recommande, en cas d'apparition d'un tel message, de vérifier que l'application de la mise à jour est bien la source du problème, et que les fichiers temporaires ne sont pas stockés par défaut :

– sous Windows XP, dans :

```
C:\\Documents and Settings\<USER>\Local Settings\Temporary Internet Files\
```

– sous Windows Vista, dans :
`C:\Users\<USER>\AppData\Local\Microsoft\Windows\Temporary Internet Files\`

Dans ce genre de situation, il est toujours important de vérifier que le message d'erreur correspond à la raison publiée, ou n'est pas l'artefact d'un autre problème, éventuellement de sécurité, sur le système.

Documentation

– Base de connaissances Microsoft KB937409 du 16 mai 2007 :
http://support.microsoft.com/kb/937409
– Base de connaissances Microsoft KB931768 mise à jour le 16 mai 2007 :
http://support.microsoft.com/kb/931768
– Avis CERTA-2007-AVI-207 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-207

3.2 Les annonces préliminaires de Microsoft

Microsoft a annoncé mercredi 16 mai 2007 vouloir changer sa méthode d'annonce avancée sur les vulnérabilités, aussi nommée `ANS` (*Advanced Notification Security*).

Les bulletins sont publiés les deuxièmes mardis de chaque mois, et le jeudi qui précède, un cours résumé est rendu public par Microsoft afin de faire patienter ses clients. L'information fournie indique : le nombre de vulnérabilités, regroupées par « bloc logiciel » (Windows / Office / etc.), ainsi que l'indice de sévérité maximum attribué par Microsoft les concernant.

A partir de juin, cette annonce préliminaire sera plus complète et sera directement accessible sur le lien générique :
`http://www.microsoft.com/technet/security/bulletin/ms07-MOIS.mspx`

Les informations fournies concerneront chaque bulletin qui sera publié la semaine suivante, avec les données ci-dessous :

– l'indice de sévérité maximal du bulletin de sécurité ;
– les conséquences des vulnérabilités qui seront publiées (exploitation à distance, déni de service, etc.) ;
– les logiciels affectés ;
– des informations de détection (*Microsoft Baseline Security Analyzer* par exemple).

4 Fuite d'informations sous Mozilla Firefox

Plusieurs vulnérabilités ont été identifiées dans le navigateur Mozilla Firefox. elles permettraient à une personne malveillante de récupérer des informations intéressantes concernant la configuration du navigateur, afin de mieux cibler une tentative d'attaque.

1. l'accès par Javascript à certains fichiers de configuration de Firefox, grâce à la commande `resource://` placée en tête d'une *URL* ;
2. un accès à plusieurs fichiers du système en utilisant le caractère "`%5C`" qui représente en hexadécimal "\". Ce caractère n'est pas correctement interprété au cours de la manipulation de certaines chaînes. Cette vulnérabilité serait également valable sous Internet explorer.

La seconde vulnérabilité est actuellement corrigée dans la version de test de Firefox, et sera prochainement intégrée dans une mise à jour publique du navigateur.
https://bugzilla.mozilla.org/show_bug.cgi?id=367428

Ces deux vulnérabilités permettent, si elles sont exploitées, de récupérer des informations contextuelles importantes pour une personne malveillante. Cela inclut :

– des informations sur la configuration du navigateur :
  – l'activation ou non de Java et de Javascript ;
  – la langue utilisée ;
  – la politique associée aux fichiers de session (*cookies*) ;
  – la liste des extensions installées (QuickJava, NoScript, etc.) ;
  – une liste de sites visités, si l'historique est activé ;

– des informations sur le systèmes d'exploitation :
  – le système utilisé, avec le type de plate-forme ;
  – l'adresse publique, et privée, si la machine se trouve dans un réseau « NATé »;
– des informations sur les modules activés :
  – le langage Java et ses versions ;
  – liste des outils Windows Media, et les extensions qui leur sont associées ;
  – liste des formats ouverts par QuickTime ;
  – liste des formats ouverts avec Shockwave Flash ;
– etc.

Au bout du compte, cela représente une quantité importante d'informations, qui permettent ensuite de mieux cibler une tentative d'attaque, soit en choisissant sciemment une application suivant la liste retournée, soit par une approche de type « ingénierie sociale ».

Dans l'attente de correctifs, le CERTA rappelle qu'il est vivement recommandé de désactiver Javascript par défaut, et de ne l'employer que sur certains sites de confiance, quand cela s'avère nécessaire.

Si des passerelles filtrant le contenu sont utilisées, il faut également vérifier que des adresses de type `resource://` soient correctement filtrées.

5 Le mois des vulnérabilités...

Certains groupes ou particuliers proposent depuis maintenant un an, de dédier un mois à la recherche de vulnérabilités dans un domaine particulier. Les résultats sont mitigés, certaines de ces initiatives correspondant davantage à une annonce tonitruante et publicitaire, d'autres offrant par contre à certains l'occasion de publier des vulnérabilités méconnues.

Le CERTA a suivi et commenté dans ses précédentes publications plusieurs de ces initiatives, comme :

– `MoBB`, le *Month of Browser Bugs*, en juillet 2006 ;
– `MoKB`, le *Month of Kernel Bugs*, en novembre 2006 ;
– `MoAB`, le *Month of Apple Bugs*, en janvier 2007 ;
– `MoPB`, le *Month of PHP Bugs*, en mars 2007 ;
– `MoAxB`, le *Month of ActiveX Bugs* en mai 2007.

Le mois de juin réserve une nouvelle initiative, `MoSeB`, qui devrait être dédiée aux vulnérabilités dans les moteurs de recherche.

Le CERTA informera ses correspondants à la parution des premières vulnérabilités, si cette initiative se confirme.

6 Quelles relations entre des réseaux sociaux et des activités malveillantes ?

Plusieurs vers récents, ainsi que des courriers de filoutage, ont été développés dans l'objectif de dérober des identifiants de connexion pour des sites offrant des « réseaux sociaux », comme *MySpace*, *LinkedIn*, etc. Ces sites offrent à leurs clients des espaces personnels, dans lesquels ils peuvent spécifier leurs loisirs, leurs activités et leurs contacts professionnels, etc. On peut donc se demander pourquoi il existe un tel attrait pour ces identifiants, dont le vol est, selon plusieurs rapports, en croissance. Voici quelques explications :

– les pages personnelles contiennent souvent des listes de contacts ; quand une personne travaille dans la société X, elle a de fortes chances d'avoir dans ses contacts plusieurs noms de ses collègues. Cette information peut servir pour lancer des attaques d'ingénierie sociale, ou des courriers de filoutage plus réalistes ;
– les données personnelles permettent de cibler les courriers électroniques commerciaux et publicitaires. Les données collectées peuvent être à valeur d'exemple des dates d'anniversaire, des lieux de résidence, des loisirs, etc. Certaines campagnes de publicité sont par ailleurs rémunérées à l'ouverture des courriers ou à la visite d'une page (*Cost Per Action*) ;
– ces « réseaux sociaux » peuvent participer à un faux sentiment de confiance, facilitant les attaques par filoutage. Ils sont souvent utilisés pour des attentes bien précises, comme une recherche d'emploi, ou une recherche de personnes partageant les mêmes loisirs ;

– les personnes ont malheureusement l'habitude de réutiliser les même identifiants et mots de passe sur plusieurs sites ; l'obtention de ces derniers peut donc ouvrir l'accès à d'autres sites ;
– etc.

Recommandations du CERTA

Le CERTA rappelle à cette occasion quelques bonnes pratiques :
– les mots de passe doivent être robustes, et différents pour chaque site ;
– il faut être vigilant quant aux informations laissées sur les sites, et restreindre si possible l'accès à son « profil » ;
– il faut adapter la politique de sécurité en tenant compte de cette problématique, et sensibiliser les utilisateurs aux risques ;
– les courriers électroniques n'offrent par défaut aucune garantie de leur origine ; il faut donc rester méfiant quand ceux-ci demandent de se connecter à un site, ou proposent des offres *sur les conseils de...*.

7 Deux retours sur les problèmes de navigation

7.1 Publicités et liens malveillants

Récemment, une expérience intéressante a été réalisée par un chercheur.

Celui-ci a acheté pour une somme négligeable un domaine et plusieurs mots-clés Google (*Google Adwords*) pointant vers celui-ci. Les publicités retournées par le moteur de recherche indiquaient clairement que l'utilisateur serait infecté par un virus (le nom donné au domaine étant lui aussi très explicite et indiquant un code malveillant pouvant être téléchargé automatiquement sans action de l'utilisateur). Le descriptif indiquait en effet "*Is your PC virus-free? Get it infected here!*" (« Est-ce que votre PC est ouvert aux virus ? Venez l'infecter ici ! »). En réalité, les utilisateurs étaient alors simplement dirigés vers une page les remerciant de leur visite.

L'expérience a duré six mois. Sur un total de 259 723 affichages sur des navigateurs d'individus, la publicité a engendré 409 clics, soit environ pour 0.16% des affichages. Ceci n'est pas un nombre très élevé, mais montre que des internautes visitent des liens malgré le descriptif. On remarque également que les moteurs de recherche n'offrent pas nécessairement de garantie sur le type de publicité, ni le contenu des pages qui seront retournées.

Certains cas de véritables publicités malveillantes (pas d'expérience inoffensive ces fois-là) et non explicites ont été signalés.

Le CERTA rappelle donc à cette occasion que :
– les pages retournées par les moteurs de recherche ne sont pas nécessairement toutes de confiance ;
– il faut cliquer avec bon sens sur les liens ;
– le navigateur doit être configuré correctement par défaut, avec l'interprétation de Javascript, Java ou de contrôles ActiveX désactivée par défaut ;
– la navigation doit se faire depuis des comptes utilisateurs aux droits limités.

7.2 L'exécution automatique au cours de la navigation

Certains codes malveillants utilisent le navigateur de la victime pour infecter sa machine. Une des méthodes fréquemment rencontrée consiste à utiliser du code JavaScript dans une page web vulnérable mettant en œuvre la méthode `ShellExecute` de l'API (Advanced Programming Interface) Windows. Cette fonction permet l'exécution ou l'interprétation d'un fichier si son extension (comme ".exe" par exemple) est connue du système.

Une façon simple de limiter l'impact d'une telle infection consiste dans un premier temps à désactiver par défaut la mise en œuvre des JavaScript dans le navigateur. Il est également fortement recommandé de ne pas naviguer avec une session administrateur ou qui en aurait les mêmes droits.

8 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 10 et le 17 mai 2007.

9 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.f r/site/CERTA-2000-INF-006/
- Note d'information du CERTA CERTA-2006-INF-009 sur les outils d'indexation et de recherche :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/
- Note d'information du CERTA CERTA-2007-INF-001 sur la gestion des noms de domaine :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/
- Note d'information sur le bon usage de PHP :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002

10 Rappel des avis émis

Durant la période du 11 au 17 mai 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-217 : Multiples Vulnérabilités des produits CA
- CERTA-2007-AVI-218 : Vulnérabilité dans MySQL
- CERTA-2007-AVI-219 : Multiples vulnérabilités dans Samba
- CERTA-2007-AVI-220 : Vulnérabilité dans HP Systems Insight Manager

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

- CERTA-2007-AVI-214 : Vulnérabilités dans Novell NetMail
  (précision sur la nature de la vulnérabilité)
- CERTA-2007-AVI-219-001 : Multiples vulnérabilités dans Samba
  (ajout des références aux bulletins de sécurité Debian, Ubuntu et Gentoo)

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'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.

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 œuvre (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 COSSI/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.

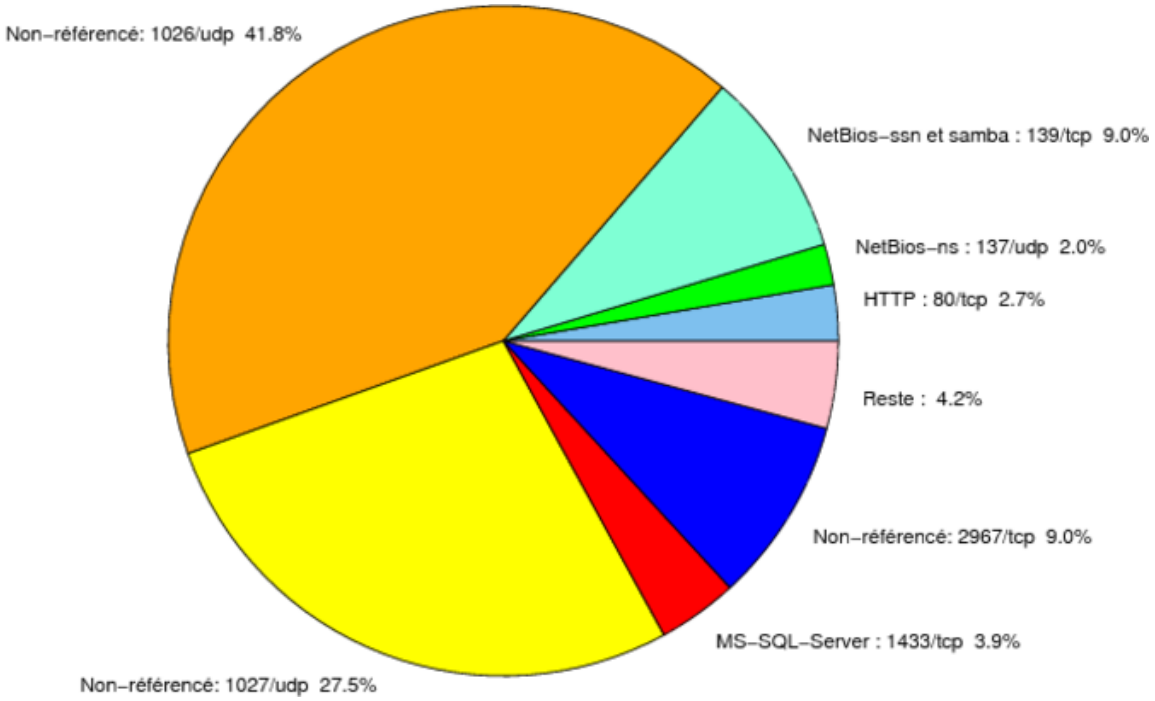

FIG. 1: Répartition relative des ports pour la semaine du 10.05.2007 au 17.05.2007

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	41.8
1027/udp	27.49
139/tcp	9.01
2967/tcp	8.95
1433/tcp	3.86
80/tcp	2.68
137/udp	1.96
1434/udp	0.86
4899/tcp	0.81
22/tcp	0.58
1080/tcp	0.39
3128/tcp	0.28
3306/tcp	0.26
21/tcp	0.21
25/tcp	0.19
15118/tcp	0.11
443/tcp	0.08
2100/tcp	0.07
143/tcp	0.05
3389/tcp	0.04
11768/tcp	0.03
9898/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

18 mai 2007 version initiale.