Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 juin 2008
N° CERTA-2008-ACT-023

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-23

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-2008-ACT-023`

Gestion du document

Référence	CERTA-2008-ACT-023
Titre	Bulletin d'actualité 2008-23
Date de la première version	06 juin 2008
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-023.pdf
Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-023/

1 Les incidents de la semaine

1.1 Le danger du cohébergement

1.1.1 Les faits

Cette semaine, le CERTA a participé au traitement d'un incident relatif à la compromission d'un site Web. Le CERTA a été informé de la présence de pages frauduleuses sur un site hébergé en France. Suite à ce signalement, le CERTA a pris contact avec le propriétaire du site pour bloquer l'accès aux pages malveillantes. Le responsable du site Web fut étonné de constater cette compromission, son site ne contenant, à l'origine, qu'un fichier statique au format HTML. Le compte légitime, utilisé pour modifier le site, n'a visiblement pas été compromis. Les soupçons se sont donc rapidement tournés vers le mode d'hébergement. En effet, le site était cohébergé sur un serveur avec des sites dont la sécurité a pu être contournée. Une fois l'un de ces sites compromis, l'attaquant pouvait modifier à sa guise l'ensemble des sites et des données du serveur.

Le CERTA recommande de considérer avec la plus grande attention la solution de cohébergement et de ne pas hésiter à questionner l'hébergeur sur l'étanchéité entre les différents espaces des clients. La note d'information du CERTA sur l'hébergement mutualisé aide le lecteur dans son éventuelle analyse de risques et le choix d'exigences (cahier des charges) et de mesures adaptées.

1.1.2 Documentation

– Note d'information sur les bonnes pratiques concernant l'hébergement mutualisé :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/

1.2 Des applications orientées « jeux » attaquées

La veille du CERTA en matière de vulnérabilités ne couvre pas l'ensemble des applications utilisées. Parmi les failles qui nous ne traitons pas, on retrouve notamment toutes celles qui concernent des jeux en réseau (qui sont loin de ne pas être concernés par les vulnérabilités).

Le CERTA n'a pas de visibilité directe ni de remontées à propos d'attaques ciblant les jeux en réseau (que ce soit du côté serveur ou du côté client). En revanche, nous constatons que les sites Web utilisés par les joueurs pour discuter entre eux sont régulièrement compromis. Cela a récemment été le cas, suite à la découverte d'une vulnérabilité affectant l'applicatif *phpRaider* (logiciel facilitant l'organisation d'événements pour les jeux massivement multi-joueurs).

Les applications orientées « jeux » doivent être considérées par leurs administrateurs comme tout autre logiciel. Elles ont des mises à jour de sécurité à appliquer, et leur déploiement sur des sites Web doit être fait avec la même rigueur que pour un site « professionnel ».

1.3 Des redirections trompeuses

Cette semaine, le CERTA a traité plusieurs cas de redirections malveillantes. Il existe sur l'Internet bon nombre de sites offrant la possibilité de réduire considérablement des adresses réticulaires (URL) trop longues ou trop compliquées à retenir ou à échanger. Ces sites permettent de créer un lien court qui redirigera le visiteur vers la page enregistrée sous une autre adresse. Or, bien souvent, aucun contrôle sur la validité de la page destination n'est effectué par les responsables du service. Des individus malintentionnés profitent donc de la fonctionnalité pour rediriger leur victime vers des pages frauduleuses ou falsifiées imitant, parfois à la perfection, des sites légitimes (ce sont typiquement des sites de filoutage ou *phishing*).

Le CERTA recommande de ne pas suivre ce genre de liens pour accéder à des sites sécurisés (comme des sites bancaires). Il est préférable dans ce cas de recopier manuellement l'adresse d'origine dans son navigateur.

De manière générale, le CERTA rappelle qu'il ne faut pas cliquer directement sur des liens contenus dans les corps de messages électroniques pour accéder à la page.

2 Injection de code indirecte non persistante ... réellement ?

Faisons un petit retour sur les vulnérabilités par injection indirecte de code. Ce type d'attaque, aussi appelé *Cross-Site Scripting* ou *XSS*, consiste à injecter du code dynamique (javascript, vbscript, .NET ASP, ...) dans un champ d'un site Internet. En retour, le site restitue le code injecté au moment de répondre au client, et le code dynamique est donc exécuté par son navigateur. Mais, derrière cette définition générale, on peut décliner deux concepts : le *cross-site scripting* persistant et le *cross-site scripting* volatil.

Le *cross-site scripting* dit persistant profite de l'enregistrement des informations transmises au serveur pour rester actif dans le temps. C'est par exemple le cas des forums de discussion vulnérables à l'injection de contenu dynamique. Le message posté et contenant du script hostile est enregistré dans un espace de stockage (une base de données par exemple) et restitué à chaque internaute souhaitant consulter ce message. Le script contenu dans celui-ci est alors interprété avec tout ce que cela implique.

Le *cross-site scripting* dit volatil, quant à lui, profite d'une faille à la création de contenu dynamique dépendant de la requête de l'utilisateur. C'est par exemple le cas des pages d'erreurs affichant dans le message renvoyé à l'internaute le contenu de la requête générant l'erreur. On peut donc imaginer que cette requête est dépendante d'une action volontaire de la personne consultant le site, et que, par conséquent, elle est nettement moins facilement exploitable. C'est en tout cas ce que pensent certains administrateurs de tels sites lorsque le CERTA les appelle pour leur signaler ce genre d'incident.

Et pourtant, quelques techniques voient peu à peu le jour afin d'exploiter ce genre de failles malheureusement très répandues :

– la première consiste à s'inspirer des techniques de *phishing* afin de forcer, via un courriel spécialement construit, un utilisateur à aller consulter le site vulnérable à partir d'une requête contenant de l'injection de code indirecte. Cette technique est efficace mais très peu ergonomique pour un attaquant ;

– la deuxième consiste à créer une page Web ayant un grand nombre d'URL contenant l'exploitation de *cross-site scripting* touchant des sites divers et variés. Cette page peut se trouver référencée par des moteurs de recherche, ce qui implique que les liens malveillants exploitant des failles de sites vulnérables sont proposés à tout internaute faisant une recherche sur l'Internet. On passe alors du mode volatile au mode persistant, tout cela grâce aux moteurs de recherche. Une faille considérée comme anodine peut alors avoir un impact important.

Outre une forte atteinte à l'image, ces attaques impliquent la responsabilité pénale des créateurs et hébergeurs de ces sites, dès lors qu'avisés d'une telle vulnérabilité, ils ne prennent aucune disposition pour empêcher ce détournement de fonctionnalité.

Comment se prémunir de ces failles ? Tout simplement en appliquant le meilleur précepte de la sécurité informatique : interdire tout par défaut, et n'autoriser que ce qui est spécifiquement attendu. Pour un site Internet, cela se concrétise par une gestion et une vérification rigoureuse des valeurs retournées à un site (que ce soient des valeurs saisies par l'utilisateur ou des paramètres dynamiques générés par le navigateur). Il est par exemple inutile d'autoriser les caractères spéciaux lorsqu'on s'attend à recevoir un paramètre numérique. Cette gestion est bien souvent plus facile lorsqu'elle est mise en place au cours du développement initial que lorsque l'on doit réagir suite à la découverte d'une vulnérabilité.

– Note d'information CERTA-2002-INF-001, « Vulnérabilité de type Cross Site Scripting » :
http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001/

3 État des mises à jour pour Flash Player

L'actualité récente a fait état d'une vulnérabilité d'Adobe Flash Player massivement exploitée. Cette vulnérabilité est corrigée depuis la dernière version de Flash Player (9.0.124), et a fait l'objet de l'avis CERTA-2008-AVI-197.

De récentes statistiques ont été publiées sur un bloc-notes, concernant selon l'auteur plusieurs centaines de millieurs de visiteurs uniques. Ces chiffres ont été obtenus par `Google analytics`. Si l'on ne peut se fier entièrement à ce genre de données, les statistiques publiées nous donnent un ordre d'idée de l'état des mises à jour de Flash Player. Ainsi, seuls 17,5% des visiteurs du site avaient la dernière version du logiciel le 29 mai 2008, alors que la mise à jour est disponible depuis le 08 avril 2008.

La raison de ce chiffre très bas est simplement que l'application ne se met pas à jour automatiquement et qu'il faut le faire manuellement via le site d'Adobe.

Le CERTA rappelle que plusieurs versions d'Adobe Flash Player peuvent être présentes sur la machine en fonction des navigateurs présents. Comme cela a été dit dans le dernier bulletin d'actualité, il est possible de vérifier les versions que l'on a en visitant un `swf` présent sur le site d'Adobe. Il est vivement recommandé de mettre à jour le plus rapidement possible *toutes* les instances d'Adobe Flash Player présentes sur sa machine.

3.1 Documentation

– Entrée sur le bloc-notes zdnet, « Flash attack may as well have been zero-day » :
http://blogs.zdnet.com/security/?p=1236
– Listes des versions à jour :
http://www.adobe.com/products/flash/about/
– Installation d'Adobe Flash Player :
http://www.adobe.com/go/getflashplayer
– Fichier swf montrant la version de Flash Player installée :
http://www.adobe.com/support/flash/ts/documents/test_version/flashplayerversion.swf

4 Compromission indirecte par triche ARP

Le CERTA avait mentionné dans un précédent bulletin d'actualité (CERTA-2007-ACT-038) le scénario d'un incident bien particulier : les utilisateurs qui naviguaient sur un site récupéraient des pages contenant des cadres `iFrames` malveillants, bien que le code source de ces pages sur le serveur Web soit resté intègre.

Cette attaque se réalise en trichant au niveau du protocole ARP (`Address Resolution Protocol`) qui sert à la traduction d'une adresse réseau (IP par exemple) en adresse « locale », et essentiellement ethernet (`MAC`).

Des incidents relatés cette semaine dans la presse permettent d'enrichir ce scénario par d'autres cas de malveillance. Voici un scénario envisageable :

1. l'hébergeur a positionné différentes machines d'hébergement dans une même zone de diffusion (*broadcast*) ARP ;
2. l'une de ces machines a pu être compromise par le biais d'une configuration trop laxiste ;
3. la personne malveillante décide alors de faire un empoisonnement de tables ARP. La machine compromise se fait ainsi passer pour une interface de l'un des routeurs (passerelle) ;
4. les autres machines d'hébergement envoient le trafic destiné à la passerelle de routage vers la machine compromise, ayant leurs tables ARP corrompues ;
5. la machine malveillante réceptionne ce trafic, et décide de modifier toute réponse HTTP par des données différentes ou une redirection ;
6. les utilisateurs allant naviguer sur l'un des sites hébergés par une de ces machines voient un contenu différent : les sites semblent être compromis !

Le fait que les machines victimes de ce détournement de trafic soient configurées de manière propre et sécurisées (mises à jour établies, tests d'intégrité des fichiers effectués, configuration restrictive mais suffisante, etc.) n'intervient pas dans le scénario.

Ces attaques par empoisonnement de tables ARP ne sont pas récentes. Des mesures existent pour les prévenir et/ou les détecter. De manière générale, certaines méthodes consistent à :

- cloisonner les zones de diffusion ARP. Des réseaux virtuels VLANs peuvent réduire ces zones ;
- associer de manière statique des adresses MAC et IP dans les tables ;
- considérer toute trame ARP et signaler toute incohérence de réponses ;
- comparer les trames IP qui transitent afin de détecter des condensats (*hash*) répétés ;
- etc.

La grande difficulté dans cette attaque est l'interprétation faite par l'utilisateur. Ce dernier ne peut pas distinguer si le réseau de l'hébergeur subit des détournements de trafic indésirables ou la machine du site Web est réellement compromise. Il ne peut constater qu'une chose : les données qui lui sont transmises en réponse sont malveillantes (injections de codes, etc.) et/ou ne correspondent pas à ses attentes (défiguration).

En d'autres termes, il est important de considérer la politique de sécurité de son site Web comme un tout. Il n'est pas suffisant de la limiter à la configuration d'une seule machine.

Cette politique doit également prendre en compte l'environnement d'hébergement et les risques sous-jacents.

Documentation

- RFC 826, "An Ethernet Address Resolution Protocol", novembre 1982 :
  http://www.ietf.org/rfc/rfc826.txt
- Bulletin d'actualité CERTA-2007-ACT-038 du 21 septembre 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-038.pdf

5 Un safari qui fait parler de lui

Cette semaine, différents sites ont fait état de la présence d'une vulnérabilité non corrigée présente dans le navigateur Safari. Cette vulnérabilité est couverte par une alerte du CERTA (CERTA-2008-ALE-008). Revenons un peu sur cette vulnérabilité afin de mieux comprendre ses impacts suivant les systèmes d'exploitation.

5.1 Principe de base de la vulnérabilité

Comme décrite dans l'alerte CERTA-2008-ALE-008, cette vulnérabilité permet, via un site spécifiquement construit, de forcer le téléchargement de n'importe quel type de fichier à l'insu de l'utilisateur. Les fichiers ainsi téléchargés se retrouvent alors dans le répertoire défini par défaut :

- **Sous Windows** : le répertoire par défaut est le « bureau » de l'utilisateur.
- **Sous Mac OS X, version 10.4 et versions antérieures** : le répertoire par défaut est le « bureau » de l'utilisateur.
- **Sous Mac OS X, version 10.5** : le répertoire par défaut est le répertoire `Downloads` de l'utilisateur.

5.2 Impact immédiat de la vulnérabilité

Pour la personne ayant découvert la faille, l'impact réside dans le fait de forcer le téléchargement d'un grand nombre de fichiers sur le disque. Cependant, sans contester de la gêne occasionnée par une telle exploitation, certains scénarios pourraient être plus hostiles (téléchargement de binaires par exemple).

5.3 Impact indirect de la vulnérabilité sous Windows

Microsoft a publié un bulletin de sécurité officiel à propos de cette vulnérabilité. Si l'on regarde de plus près ce bulletin, on découvre qu'il existe un impact indirect résultant à la fois du comportement vulnérable de Safari, mais aussi d'un comportement par défaut de Windows et d'Internet Explorer, non précisé, mais qui permettrait, selon Microsoft, d'exécuter du code de manière subtile et cachée à distance.

Dans l'attente de détails sur la vulnérabilité, le CERTA rappelle quelques principes de navigation : il est important de désactiver par défaut l'interprétation de tout code dynamique (ActiveX, JavaScript, Flash, etc.) et de ne pas ouvrir en ligne des fichiers susceptibles de contenir de tels codes (PDF, etc.).

6 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 29 mai et le 05 juin 2008.

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 30 mai au 05 juin 2008, le CERTA a émis l'alerte CERTA-2008-ALE-008 et les avis suivants :

- CERTA-2008-ALE-008 : Vulnérabilité du navigateur Safari
- CERTA-2008-AVI-283 : Multiples vulnérabilités dans les produits VMware

– CERTA-2008-AVI-284 : Vulnérabilité dans Tomcat
– CERTA-2008-AVI-285 : Vulnérabilités dans CA Secure Content Manager
– CERTA-2008-AVI-286 : Vulnérabilité dans Sun Solaris
– CERTA-2008-AVI-287 : Plusieurs vulnérabilités dans Cisco PIX et ASAX
– CERTA-2008-AVI-288 : Vulnérabilités dans Skype
– CERTA-2008-AVI-289 : Vulnérabilité dans IBM WebSphere Application Server
– CERTA-2008-AVI-290 : Vulnérabilité dans des produits Kaspersky
– CERTA-2008-AVI-291 : Multiples vulnérabilités dans les produits VMware

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 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.

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 oeuvre (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 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 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.

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.

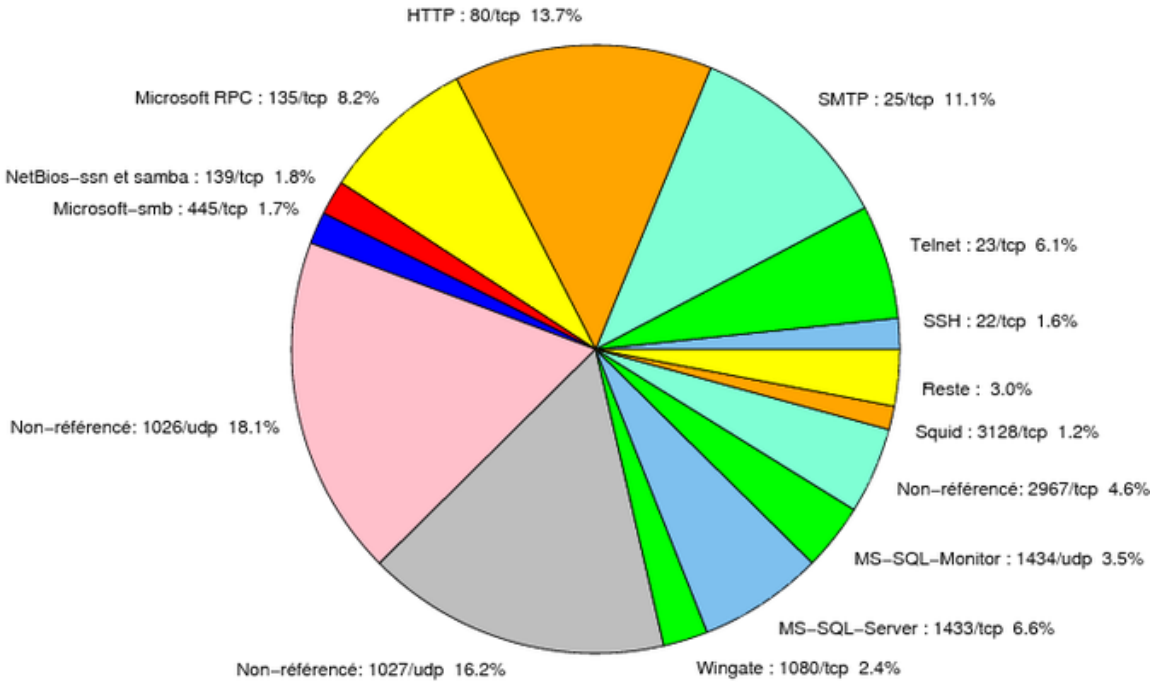

FIG. 1: Répartition relative des ports pour la semaine du 29.05.2008 au 05.06.2008

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER CERTA-2007-ALE-005-001
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CER
69	UDP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
106	TCP	MailSite Email Server	–	– http://www.certa.ssi.gouv.fr/site/CER
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CER
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CER
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CER
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CER
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CER
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER

				http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CER
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CER
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CER
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CER
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CER
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6106	TCP	Symantec Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6502	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6503	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6504	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
8080	TCP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	http://www.certa.ssi.gouv.fr/site/CER
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CER
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CER
54345	TCP	HP Mercury	–	http://www.certa.ssi.gouv.fr/site/CER
65535	UDP	LANDesk Management Suite	–	http://www.certa.ssi.gouv.fr/site/CER

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

port	pourcentage
1026/udp	18.1
80/tcp	16.37
1027/udp	16.18
25/tcp	11.1
135/tcp	8.21
1433/tcp	6.63
23/tcp	6.12
2967/tcp	4.59
1434/udp	3.54
1080/tcp	2.38
139/tcp	1.84
445/tcp	1.7
22/tcp	1.64
3128/tcp	1.24
3306/tcp	0.99
137/udp	0.68
4899/tcp	0.65
143/tcp	0.22
3389/tcp	0.11
9898/tcp	0.05

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

06 juin 2008 version initiale.