



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 juillet 2007
N° CERTA-2007-ACT-027

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-27

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-027>

Gestion du document

Référence	CERTA-2007-ACT-027
Titre	Bulletin d'actualité 2007-27
Date de la première version	06 juillet 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-027.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-027/>

1 Vague de fausses cartes postales

Depuis quelques années, les internautes ont la possibilité d'envoyer des cartes de vœux, des cartes postales ou encore des cartes d'anniversaire via l'Internet. Le principe consiste à se rendre sur un site Web spécialisé, y choisir une carte et personnaliser un message. Cette carte et ce message sont accessibles par l'intermédiaire d'une adresse réticulaire (url) précise. Le destinataire du message doit ensuite se rendre sur le site Web pour consulter la carte.

Depuis quelques jours, de faux messages de cartes postales circulent sur l'Internet. Ces cartes contiennent un lien vers un site malveillant. Une visite sur ce site avec javascript activé dans le navigateur provoque le téléchargement et l'exécution d'un code malveillant. Si le javascript est désactivé dans le navigateur, alors un message apparaît, incitant l'internaute à suivre de lui-même un lien (vers un exécutable). Les codes malveillants ainsi téléchargés ne sont pas reconnus par tous les antivirus.

Pour le moment, ces messages sont rédigés en anglais, mais des versions en français pourraient apparaître prochainement. Ils se reconnaissent facilement par leur titre, qui est de la forme :

```
You've received [a|an] [greeting] [postcard|ecard] from a [admirer|  
class-mate|colleague|family|member|friend|mate|neighbor|neighbour|  
partner|school friend|school mate|worshipper]!
```

Le filtrage de ces messages sur le titre fonctionnera mais ne sera pas efficace contre d'éventuelles évolutions de ces courriels. Le CERTA recommande par ailleurs la lecture du document CERTA-2000-REC-002 daté de 2000 (et toujours d'actualité) intitulé : « Mise en garde au sujet des messages de vœux ».

Documentation :

- Recommandation CERTA-2000-REC-002 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2000-REC-002/>
- Avis CERTA-2003-AVI-084 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-084/>

2 Courriers non sollicités et documents PDF

Le CERTA a reçu cette semaine plusieurs notifications concernant des courriers reçus par messagerie électronique, avec les caractéristiques suivantes :

- le courriel ne contient pas de texte ;
- un document au format PDF (*Portable Document Format*) en pièce jointe, dont le nom suit la syntaxe suivante : *mot_XXXXXXX.pdf*, le mot pouvant être *invitation*, *paid*, *document*, *article*, *cancelled*, etc. et XXXXXXXX étant une séquence visiblement aléatoire de chiffres ou de lettres ;
- l'expéditeur est inconnu mais provient d'un domaine existant (résolution inverse DNS possible à partir de l'adresse IP).

Le document PDF présente à l'ouverture quelques lignes de texte, qui s'avèrent être sous forme d'une image. Concernant les documents analysés, il s'agit de lignes rédigées en anglais, et pouvant servir à des techniques de fraudes financières appelées *pump-and-dump*. Cette activité consiste à gonfler de manière artificielle le prix d'une action par le biais d'une promotion abusive. Cette opération engendre alors une demande artificielle, et permet aux personnes malveillantes de revendre les actions préalablement achetées à un prix inférieur. Dans la situation actuelle, la promotion se fait par l'envoi massif de courriers électroniques.

Il est bien sûr possible que de nouveaux messages apparaissent sous une forme légèrement différente.

Ces messages n'ont cependant rien de bien différent que les autres pouvant être par ailleurs reçus comme pourriels.

Mais plusieurs difficultés sont apparues pour le filtrage de ces messages :

- certains filtres ne contrôlent pas le contenu des documents PDF ;
- dans le cas présent, les chaînes de caractères sont visibles dans des images, mais pas directement dans la source du fichier PDF, à la manière des *captchas* (*Completely Automated Turing Test To Tell Computers and Humans Apart*) ;
- les images insérées dans le PDF sont de taille variable, et le texte qui apparaît peut être de couleur et de taille différentes ;

Pour toutes ces raisons, des filtres qui se basent sur les empreintes des pièces jointes (MD5 par exemple) ont peu d'efficacité. Etant données leurs caractéristiques, il est même possible que le filtrage de tels courriers ne soit pas si simplement résolu, du simple fait des motivations pour les développements de techniques de *captchas* (motivations servant également à renforcer la sécurité d'un service) : il s'agit de tests cherchant à distinguer une machine d'un humain.

Ces fichiers PDF, lisibles par des humains (nous), ont ainsi de fortes chances de ne pas être si simplement filtrés par des moyen mécaniques.

Cette vue reste une perspective, et il apparaît cependant, dans le contexte actuel, quelques caractéristiques dans les messages qui peuvent aider le filtrage. Ces derniers sont cependant des caractéristiques, et peuvent également provoquer des « faux positifs », c'est-à-dire de mauvaises catégorisations :

- le *User-Agent* dans l'en-tête du message semble toujours identique : *Thunderbird 1.5.0.12 (Windows/20070509)* ;
- le format du champ « *Objet* » est dans un format spécifique (voir plus haut) ;
- le paramètre *boundary* contient une succession de 12 tirets (caractère décimal 45) et 24 chiffres. Ce format, mentionné dans le RFC 1341, permet une compatibilité avec des méthodes d'encapsulation décrites dans un précédent standard (RFC 934), mais n'est pas toujours utilisé ;

- certains documents PDF ne seraient pas complètement valides, et provoqueraient une erreur à l'ouverture par certains lecteurs PDF, comme xpdf.

```
labo@certa:/tmp$ xpdf Paid-yugqgr.pdf
Error (0): PDF file is damaged - attempting to reconstruct xref table...
```

2.1 Les recommandations du CERTA

Le CERTA recommande aux administrateurs de bien vérifier les règles de filtrage mises en place, en prenant également garde à l'effet pervers des faux-positifs, et de sensibiliser les utilisateurs à cette méthode qu'ils peuvent apercevoir dans leur messagerie.

Le CERTA tient également à rappeler, à cette occasion, que les fichiers PDF peuvent également contenir du code Javascript, et que toute précaution doit être prise avant l'ouverture d'un document ne provenant pas d'une source de confiance. Il faut par exemple vérifier que, sous Acrobat Reader, l'interprétation du Javascript est désactivée par défaut (décocher : Edition -> Préférences -> JavaScript -> "Activer Acrobat JavaScript"), ou utiliser une application alternative, ne prenant pas en compte les différents codes dynamiques pouvant être insérés (xpdf, foxit PDF Reader sans module additionnel, ghostview, etc.).

3 Les activités de l'Internet et les interprétations de données

3.1 Présentation des faits

Certaines revues ont signalé en début de semaine de bien étranges événements. En voici les détails :

Certains sites Web proposent de visualiser quelques données statistiques, basées sur des remontées de journaux ou sur des données collectées par des sondes. L'un d'eux s'intéresse en particulier à quelques indicateurs comme :

- le nombre total de paquets ayant été observés ;
- le temps de réponse pour une requête type et vers/depuis différents points ;
- le pourcentage de paquets estimés perdus.

L'objet de cet article n'est pas de mettre en doute la validité de ces données, mais de l'interprétation parfois hâtive qui peut être faite de celles-ci. Des personnes ayant aperçu ce site pour la première fois ont constaté une apparente évolution des courbes, notamment du pourcentage de paquets perdus.

Ils ont alors établi une première conclusion : il y aurait eu une augmentation de 5% du trafic global Internet, accompagnée de nombreuses pertes de paquets.

Cherchant une cause à ce phénomène, ils se sont alors rendus sur un autre site, montrant des statistiques différentes, notamment le trafic observé par port de destination. A cette date, le site affichait une activité anormale sur le port 5901/TCP.

Des articles sont donc apparus, expliquant qu'une attaque visant l'application VNC (souvent associée au port 5901) et exploitant une vulnérabilité récente serait la source de ce comportement étrange de tout l'Internet.

3.2 Les risques des interprétations hâtives

Cette information a ensuite été démentie par d'autres spécialistes. Les arguments évoqués sont les suivants :

- le premier site Web est très intéressant, mais les fluctuations observées le jour J ne sont pas inhabituelles, si l'on regarde l'ensemble des valeurs sur plusieurs mois ;
- il y a effectivement un pic d'activité sur le port 5901, mais celui-ci s'est déjà produit à plusieurs reprises cette année, et n'a pas une amplitude très large, comparée à d'autres activités sur d'autres ports. L'amplitude observée ne peut pas expliquer, à elle seule, une variation du trafic Internet global.

Les données ont une valeur comparative et illustrative. L'interprétation est une deuxième action qu'il faut prendre garde à manipuler, car elle peut conduire vers des erreurs.

3.3 Les activités sur le port 5901/TCP

VNC (pour *Virtual Network Computing*) est un protocole pour contrôler à distance une machine. Cependant, plusieurs logiciels intègrent tout ou partie de ce protocole (interface de contrôle, client, etc.). Certaines vulnérabilités ont été identifiées ces derniers mois, pouvant être exploitées à distance (cf. par exemple les avis CERTA-2006-AVI-198 et CERTA-2006-AVI-299). L'exploitation de certaines d'entre elles se manifeste actuellement par un trafic destiné aux ports associés au protocole (par défaut TCP 5900, 5901, ainsi que les suivants).

Selon les traces observées par le CERTA et représentées par la figure 1, plusieurs pics d'activité apparaissent, confirmant ce qui a été écrit précédemment. En revanche, il est également possible d'observer que ceux-ci sont apparus dès le mois de mars 2007. Cette courbe a une évolution similaire à celle publiée sur d'autres sites Internet.

On remarque également que le port 5901 n'apparaît pas dans la figure 2 représentant la répartition relative des ports ciblés observée pour cette semaine. Il n'apparaît pas plus dans les figures similaires des deux bulletins d'actualité précédents.

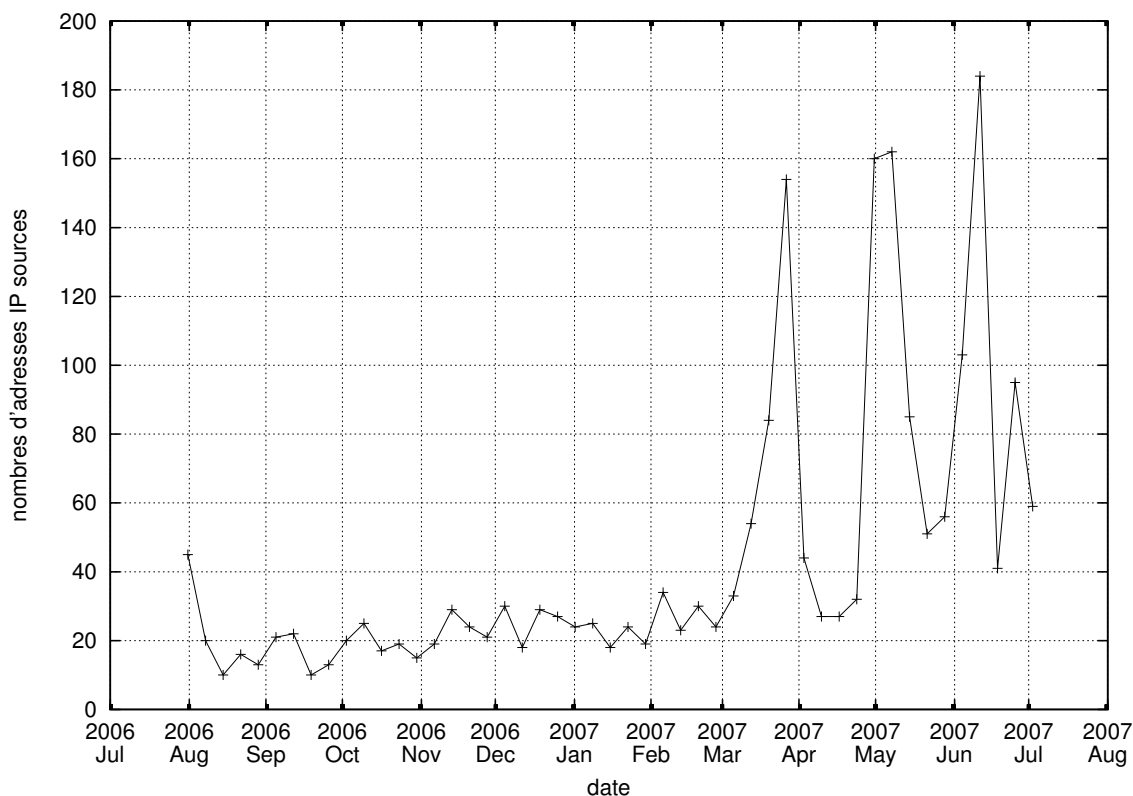


FIG. 1: Nombre de sources distinctes observées ayant sollicité le port 5901

En conclusion, mais sans en exagérer l'impact, il semble néanmoins évident que des activités existent sur ce port. Le CERTA rappelle donc à ses correspondants de bien vérifier les mises à jour de leurs applications VNC, ainsi que la politique de contrôle d'accès et le filtrage concernant VNC.

4 Des vulnérabilités dans les processeurs

Cette semaine le responsable du projet OpenBSD, ainsi que le responsable du projet DragonflyBSD se sont exprimés sur le dernier *errata* de Intel relatif à ses processeurs de dernière génération, les Core 2 Duo. En effet, selon le fabricant, les Core 2 Duo seraient victimes, comme leur ancêtres les Pentium 1, d'erreurs de conception. Selon les deux responsables, les erreurs pourraient être exploitées pour provoquer des dénis de service ou exécuter du code arbitraire. Ces vulnérabilités seraient d'autant plus critiques, qu'elles ne nécessiteraient pas de privilèges élevés pour être exploitées. Dans la mesure où les vulnérabilités sont inhérentes au processeur, il est impossible pour Intel de fournir un correctif. Une piste envisagée est de contourner ou de limiter le problème en apportant des modifications au BIOS (Basic Input Output System) des cartes-mères ou bien encore au système d'exploitation lui-même. Mais certaines de ces erreurs ne pourront être totalement contournées.

4.1 Références :

Errata de Intel :
<http://download.intel.com/design/processor/specupdt/31327914.pdf>

5 Une forme d'attaque ciblée

Généralement, les attaquants, pour avoir un retour sur investissement correct en ciblant des personnes représentant un butin relativement bas devaient en atteindre un grand nombre. Le butin pouvant être direct (détournement de fonds, ventes virtuelles ...) ou indirect (informations revendables ou utilisable dans des opération boursières...). La problématique de ces grandes campagnes d'infection est qu'elles sont bien souvent repérées, contrées et obsolètes après une certaine durée.

Or de nombreux sites de réseaux sociaux permettant maintenant d'accéder directement aux profils des utilisateurs, triés par catégorie professionnelle. Il est donc possible d'en extraire des coordonnées et des informations permettant de personnaliser les attaques. Ainsi, récemment, des chefs d'entreprises et des responsables ont reçu des mails nominatifs et bien formulés contenant des programmes malveillants.

Ces attaques étant limitées à un certain nombre de personnes, il y a de fortes chances qu'elles atteignent l'utilisateur. En effet, les filtres risquent de ne pas connaître les signatures adéquates.

Ce qu'il faut retenir de ces nouvelles activités :

1. les sites de réseaux sociaux sont une source intéressante d'informations, qui intéressent les codes malveillants. Il est ainsi important de maîtriser et limiter les données fournies sur ces sites ;
2. que les courriers de ces attaques soient plus ciblés vers un groupe d'utilisateurs ou pas, il faut rester vigilant à la réception de toute pièce jointe à un courrier électronique ;
3. il ne faut pas hésiter à signaler à son responsable de sécurité, RSSI, ou au CERTA tout courrier étrange, afin d'en effectuer une analyse approfondie.

6 MOSEB : bilan du mois de juin

Dans le bulletin d'actualité du 22 juin, le CERTA présentait l'initiative *MOSEB : Mont Of Search Engine Bugs* dont le but était de divulguer des vulnérabilités liées aux moteurs de recherche. Cette initiative a pris fin cette semaine. L'auteur indique que bon nombre de vulnérabilités n'ont pas ou mal été corrigées par les éditeurs. Il indique notamment comment exploiter des vulnérabilités par redirection, non corrigées par les éditeurs. Par ce biais des personnes malintentionnées peuvent tromper leurs victimes en leur présentant un lien vers un moteur de recherche connu pour en réalité les conduire directement vers un site malveillant.

Le CERTA recommande d'accorder la plus grande d'attention aux liens utilisant l'adresse d'un moteur de recherche. Plutôt que d'utiliser ces liens, il est préférable de reproduire soit même la recherche dans le moteur. De plus le CERTA recommande une nouvelle fois de ne pas cliquer sur lien présent dans un courrier électronique.

6.1 Documentation

- Bulletin d'actualité du CERTA CERTA-2007-ACT-025 du 22 juin 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-025.pdf>

7 Ports observés

Le tableau 3 et la figure 2 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 28 juin et le 05 juillet 2007.

8 Liens utiles

- Mémento sur les virus :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/>
- Note d'information sur l'acquisition de correctifs :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/index.html>

- Note d'information sur les systèmes obsolètes :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html>
- Note d'information sur les bonnes pratiques concernant l'hébergement mutualisé :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/index.html>
- Note d'information sur les mots de passe :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html>
- Note d'information sur la terminologie d'usage au CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/index.html>
- Note d'information sur les enjeux de sécurité liés à une migration vers IPv6 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/index.html>
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
<http://www.auscert.org.au/render.html?it=1935>
- Note d'information du CERTA CERTA-2006-INF-006, Risques associés aux clés USB :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-006/>
- Note d'information du CERTA CERTA-2006-INF-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>

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.

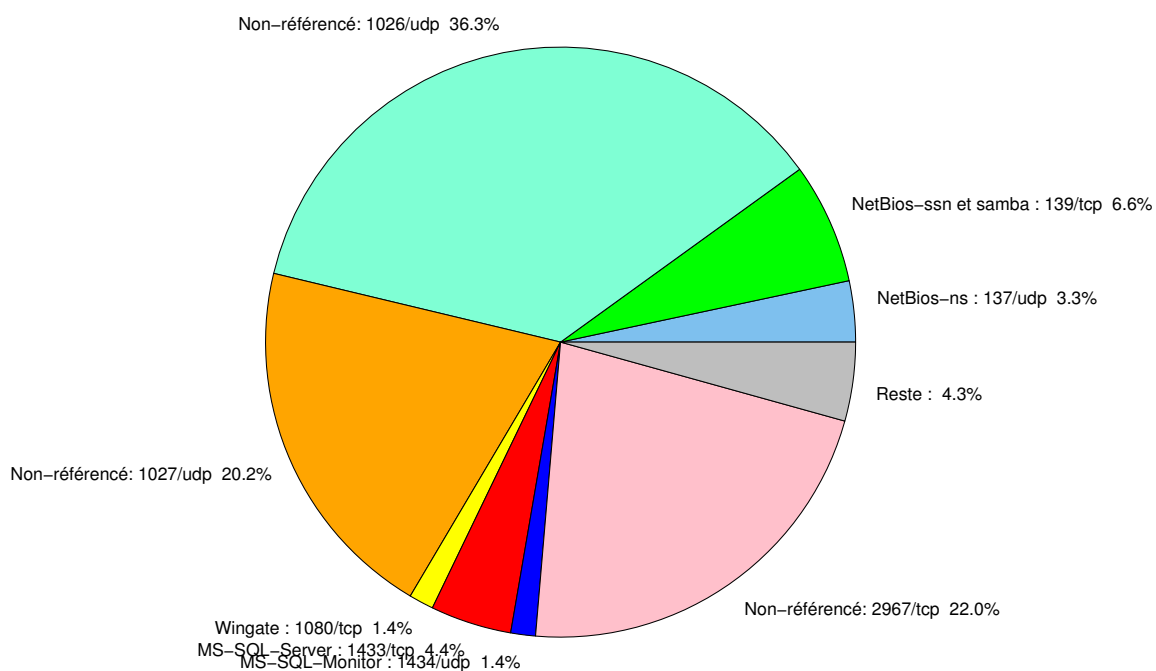


FIG. 2: Répartition relative des ports pour la semaine du 28.06.2007 au 05.07.2007

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	36.29
2967/tcp	22.04
1027/udp	20.23
139/tcp	6.61
1433/tcp	4.44
137/udp	3.34
1434/udp	1.35
4899/tcp	0.93
22/tcp	0.9
443/tcp	0.48
21/tcp	0.33
3128/tcp	0.31
15118/tcp	0.3
23/tcp	0.26
25/tcp	0.21
80/tcp	0.18
3306/tcp	0.11
3389/tcp	0.08
143/tcp	0.06
42/tcp	0.03

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

06 juillet 2007 version initiale.