Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 mai 2011
N° CERTA-2011-ACT-019

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-19

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-2011-ACT-019

Gestion du document

Référence	CERTA-2011-ACT-019
Titre	Bulletin d'actualité 2011-19
Date de la première version	13 mai 2011
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-2011-ACT-019.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-2011-ACT-019/

1 Incidents de la semaine

1.1 Défigurations, préliminaires d'intrusions plus graves

Cette semaine le CERTA est intervenu dans le traitement de défigurations dont certaines illustraient clairement l'importance de ces incidents trop souvent considérés comme mineurs.

Quel que soit le contenu de la page de défiguration, la présence de celle-ci est le symptôme d'une vulnérabilité du site web. C'est ce point qu'il faut considérer, plus que la formulation revendicative.

Dans deux affaires, la page modifiée ou insérée pour réaliser la défiguration n'est restée que très peu de temps sur le site. Parce que les sites étaient parfaitement et continuellement supervisés, même en fin de semaine, et que les mesures correctives ont été prises sans délai ? Hélas non !

Dans le premier cas, un intrus bien plus agressif que l'auteur de l'insertion d'une page, a profité de la faiblesse du site pour remplacer toutes les pages par un code de redirection de l'internaute. Cette redirection renvoyait les visiteurs vers une adresse réticulaire (URL) sur un autre site, lui-même compromis. À cette adresse se trouvait

un fichier exécutable Windows dont le nom suggérait qu'il s'agissait d'une mise à jour du navigateur Firefox. En réalité, ce programme infectait le poste de l'internaute assez imprudent pour le télécharger et l'exécuter.

L'analyse des journaux de connexion HTTP montre que le site défiguré puis modifié était sensible aux injections de code PHP (RFI).

Le deuxième cas est similaire dans la brièveté de la page de défiguration initiale. Celle-ci a été remplacée par un script permettant aux agresseurs de naviguer sur le site et d'y déposer des fichiers. Cela suffit à l'attaquant pour créer un entrepôt de contenus illicites, voire illégaux (site *warez*) : contenus contrefaits, enfreignant le respect des droits d'auteurs, outils d'attaque informatique, pornographie infantile, incitation à la haine raciale...

Dans cette intrusion, la non-mise à jour du CMS (*Content Management System*) utilisé pour le site est en cause.

Ces défigurations suivies par des modifications de ces sites, conduisent le CERTA à réitérer ses recommandations :

- une défiguration n'est jamais un incident mineur, mais le révélateur de vulnérabilités graves. Ôter la page indésirable n'est jamais la solution. Il faut analyser en profondeur le serveur et l'activité qui lui est attachée, remédier aux vulnérabilités et remonter un serveur à partir de logiciels de confiance et à jour, et de données scrupuleusement vérifiées ;
- la mise à jour des systèmes et des logiciels, extensions comprises, est primordiale ;
- la vérification de l'intégrité du serveur doit être la plus continuelle possible ;
- la journalisation avec exploitation régulière, idéalement au fil de l'eau, des journaux permet de débusquer les attaques les plus classiques (RFI, injection SQL, recherche exhaustive de mots de passe...) ;
- la supervision, si possible en temps réel, permet de repérer les anomalies et de réagir rapidement à la moindre intrusion.

1.2 Injection malveillante de liens dans des balises HTML d'image

Le précédent bulletin d'actualité du CERTA mentionne l'utilisation de techniques de manipulation du score calculé par les moteurs d'indexation pour présenter des faux antivirus pour PC et Mac.

Le calcul repose en partie sur le nombre de liens qui pointent vers une l'URL. Pour augmenter le score et faire figurer l'URL malveillante dans les premiers résultats proposés par le moteur de recherche, l'agresseur doit augmenter le nombre de liens vers cette adresse réticulaire.

Une vague d'injections de tels liens est en cours. Sur les sites web vulnérables, un lien est ajouté, non pas dans un cadre `IFRAME`, mais dans une balise pour les images :

```
<img heigth="1" width="1" border="0"
src="http://nom-d-hote-malveillant.net/t.php?id=suite-de-chiffres">
```

Le CERTA a rencontré de tels liens dans sa communauté d'usagers. Le lien est alors écrit sur une seule ligne et en fin de page, après la balise de fin de document, `</HTML>`.

La présence d'un cheval de Troie (Fareit.A) sur le poste d'une personne pouvant modifier le site, et le vol des identifiants et mots de passe FTP sont suspectés pour la réalisation de ces injections malveillantes.

Face à cette menace, le CERTA recommande :

- de vérifier l'état des sites web à la recherche des ces liens malveillants, et de procéder au traitement en conséquence ;
- de vérifier l'état de *tous* les ordinateurs à partir desquels les accès FTP sont réalisés ;
- d'établir une politique de mots de passe, robustes et périodiquement renouvelés, pour ces accès.

Documentation

- Note d'information du CERTA « Que faire en cas d'intrusion ? » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/
- Note d'information du CERTA « Gestion des journaux d'évènements » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-005/
- Note d'information du CERTA « Du bon usage du PHP » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/

– Note d'information du CERTA Sécurité des applications Web et vulnérabilités de type injection de données » :
http://www.certa.ssi.gouv.fr/site/CERTA-2004-INF-001/

2 Rumeurs de vulnérabilité dans *Google Chrome*

En début de semaine, une société de sécurité indiquait avoir réussi à exploiter une vulnérabilité dans le navigateur Web *Google Chrome*. Cette vulnérabilité affecterait la version la plus récente du navigateur à la date de rédaction de ce document (soit la 11.0.696.68), et permettrait d'exécuter du code arbitraire à distance, sur des systèmes Windows 32 et 64 bits. Les développeurs à l'origine de la preuve de faisabilité prétendent être capables de contourner les protections contre l'exécution de code arbitraire, comme le bac à sable (*sandbox*) inclus dans *Google Chrome*, ou les protections fournies par Windows comme DEP (*Data Execution Prevention*) et ASLR (*Address Space Layout Randomization*). Malheureusement, aucun détail technique concernant la vulnérabilité exploitée n'a été communiqué : la société a indiqué que les informations techniques ne seront pas divulguées au public, ni aux équipes de sécurité de *Google*. Il n'est donc pas possible de valider la présence de cette vulnérabilité dans le navigateur de *Google*.

Dans tous les cas, plusieurs vulnérabilités affectant *Google Chrome* ont été découvertes et corrigées le 12 mai, et les bonnes pratiques de navigation sur l'Internet doivent être suivies scrupuleusement quel que soit le navigateur utilisé.

Documentation

– Bonnes pratiques de navigation sur l'Internet :
http://www.securite-informatique.gouv.fr/gp_article74.html
– Avis de sécurité du CERTA CERTA-2011-AVI-292 du 13 mai 2011 :
http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-292/

3 Mises à jour *Microsoft*

Cette semaine, Microsoft a publié deux mises à jour de sécurité pour le service WINS et *Microsoft PowerPoint*. La première vulnérabilité permet à une personne malveillante d'exécuter du code arbitraire à distance sur les systèmes *Windows Server* 2003, 2008 et 2008 R2.

Deux vulnérabilités dans *Microsoft PowerPoint* permettent à un utilisateur malintentionné d'exécuter du code arbitraire à distance au moyen d'une présentation *PowerPoint* spécialement formée.

Documentation

– Avis de sécurité du CERTA :
http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-281/index.html
http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-282/index.html
– Bulletins de sécurité Microsoft :
http://www.microsoft.com/france/technet/security/Bulletin/MS11-035.mspx
http://www.microsoft.com/france/technet/security/Bulletin/MS11-036.mspx

4 WebGL

4.1 Présentation

WebGL est une bibliotèque graphique qui permet à un navigateur compatible de restituer des graphismes 3D sans l'intervention de module tiers (ou *plugin*). Cette bibliothèque, basée sur *OpenGL ES 2.0*, étend le langage javascript en fournissant une interface de programmation pour le rendu 3D.

D'un point de vu HTML, *WebGL* est un contexte de l'élément *canvas* du langage HTML5, accessible par l'interface DOM.

Il est par ailleurs supporté par différents navigateurs tels que *Google Chrome*, *Mozilla Firefox 4* ainsi que dans les versions de développement de *Safari* et *Opera*.

Le groupe de travail *WebGL Working Group* à l'origine du projet inclut les sociétés *Apple*, *Google*, *Mozilla* et *Opera*. Tout comme son proche parent *OpenGL*, c'est le consortium *Khronos Group* qui est en charge de le maintenir.

4.2 Dangers potentiels

Dès le début du déploiement de *WebGL*, les différents éditeurs se sont aperçus de problèmes liés à certains pilotes graphiques anciens. Ces pilotes souffrent de problèmes d'implémentation et ne gèrent pas correctement certains appels de fonctions, ce qui conduit le plus souvent à un arrêt brutal pur et simple de la machine. En effet, le pilote graphique s'exécutant en mode noyau, toute erreur lors de son fonctionnement a des conséquences radicales et peut provoquer un dysfonctionnement critique du système (notamment, le fameux *Blue Screen Of Death* (*Bug Check*) sur les systèmes *Windows*).

C'est justement cet accès direct à l'espace noyau qui soulève de nombreuses questions quant à la sécurité de *WebGL*. En effet, habituellement les différentes fonctionnalités du navigateur ainsi que les greffons s'exécutent en mode utilisateur et contiennent différents mécanismes de vérification afin de s'assurer de la conformité des données avant de faire appel aux fontionnalités du système d'exploitation. Or, dans le cas de *WebGL*, c'est directement une interface de programmation en lien avec le pilote graphique, et donc l'espace noyau, qui est mise à disposition. Les contenus en provenance de l'Internet ont alors un accès direct au matériel graphique (GPU) au travers de cette interface. Il devient ainsi possible d'exécuter du code directement sur le GPU. Cette possibilité ouvre donc de nouvelles voies d'attaque.

Il est par exemple possible de déclencher un déni de service en demandant à la carte graphique d'afficher des éléments géométriques 3D extrêment complexes ou bien encore de faire exécuter par le GPU une boucle infinie. Ce type de déni de service affecte l'ensemble de la machine et pas simplement le processus du navigateur.
Par ailleurs, l'exécution de code sur le processeur graphique permet de sortir du contexte du navigateur et donc de contourner les politiques de sécurité inter-domaine. Bien que le processeur graphique ne dispose pas de capacités permettant d'accéder directement au contenu des pages Internet, il est cependant possible d'avoir accès aux pixels les composant, et ainsi de voler une image. Des preuves de concept sont d'ailleurs d'ores et déjà disponibles sur l'Internet.

Une deuxième catégorie d'attaque bien plus préoccupante est aussi à prendre en compte. Afin d'exposer le matériel graphique à l'Internet, *WebGL* repose sur les pilotes graphiques présents sur le système. Ces pilotes, sont des codes complexes et souvent de taille importante qui permettent d'interfacer le matériel et le système d'exploitation. Or, un code complexe est d'autant plus affecté par des vulnérabilités que sa taille est importante. Il est donc envisageable que des attaques ciblant les vulnérabilités d'un pilote voient le jour. Les conséquences d'une telle attaque s'échelonnent depuis un simple déni de service jusqu'à la possibilité d'exécuter du code arbitraire en espace noyau.

4.3 Quelles solutions ?

Plusieurs solutions sont envisageables afin de résoudre ces différents problèmes. Certaines sont d'ailleurs déjà déployées.

Par exemple, les différents navigateurs supportant *WebGL* définissent des niveaux de version minimaux pour les drivers graphiques, en dessous desquels *WebGL* ne sera pas activé, résolvant ainsi les problèmes de stabilité rencontrés lors du déploiement.
D'autre part, les systèmes *Windows 7* et *Windows Vista* mettent en œuvre un mécanisme permettant de réinitialiser le GPU en cas de blocage de ce dernier, prévenant ainsi les tentatives de déni de service. Il reste cependant un problème majeur : après un certain nombre de remise à zéro sur une période de temps limitée, le système considère être en présence d'un problème majeur et déclenche un *Bug Check*, ce qui conduit à l'arrêt brutal de la machine.

D'autres projets visant à améliorer la sécurtié de *WebGL* en lui-même ont aussi vu le jour. Parmis ceux-ci, *ARB_robustness* semble être prometteur. Il s'agit d'une extension de la librairie *OpenGL* qui met en place différents mécanismes de sécurité. Ses objectifs sont les suivants :

- fournir des fonctions sécurisées pour chaque requête *OpenGL*, notamment en limitant la taille des données écrites dans un tampon par la spécification explicite de cette dernière (similaire à la fonction `snprintf()` pour `sprintf`) ;
- définir un mécanisme de communication permettant à une application *OpenGL* de connaître l'évolution d'un contexte graphique ;

– mettre en place un mécanisme de protection mémoire permettant de mieux contrôler les accès à la mémoire de la carte graphique.

Cette extension est d'ailleurs déjà déployée par certains fabricants de cartes graphiques. Le *Khronos Group* précisant que les navigateurs devraient tester la présence de cette extension avant d'activer *WebGL*.

4.4 Conclusion

Comme beaucoup de technologies Web, lors de leur introduction, *WebGL* souffre de nombreuses faiblesses.

Cependant, dans ce cas, il ne s'agit pas simplement d'un module fonctionnant dans le contexte du navigateur mais d'une interface directe vers le matériel graphique et son pilote en mode noyau. Ainsi, une vulnérabilité pourrait permettre à un utilisateur malintentionné d'exécuter du code noyau arbitraire à distance.

L'utilisation de *WebGL* semble donc induire une augmentation non négligeable de la surface d'attaque du système et l'aggravation de l'impact. Aussi, il est recommandé de ne pas utiliser cette option dans l'immédiat.

Documentation

– US-CERT Current Activity du 11 mai 2011 :
http://www.us-cert.gov/current/index.html#web_users_warned_to_turn
– *WebGL* - A New Dimension For Browser Exploitation :
http://www.contextis.com/resources/blog/webgl/
– *ARB_robustness* :
http://www.opengl.org/registry/specs/ARB/robustness.txt
– Blocklisting/Blocked Graphics Drivers :
https://wiki.mozilla.org/Blocklisting/Blocked_Graphics_Drivers

5 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=1937
– 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/

6 Rappel des avis émis

Dans la période du 6 mai au 12 mai 2011, le CERTA a émis les avis suivants :

- CERTA-2011-AVI-276 : Vulnérabilité dans OpenSSH
- CERTA-2011-AVI-277 : Multiples vulnérabilités dans HP Proliant Support Pack
- CERTA-2011-AVI-278 : Vulnérabilité dans le paquet Ubuntu usb-creator
- CERTA-2011-AVI-279 : Vulnérabilité dans ISC BIND
- CERTA-2011-AVI-280 : Vulnérabilité dans Exim
- CERTA-2011-AVI-281 : Vulnérabilité dans le service WINS de Windows
- CERTA-2011-AVI-282 : Vulnérabilités dans Microsoft PowerPoint
- CERTA-2011-AVI-283 : Vulnérabilité dans Postfix
- CERTA-2011-AVI-284 : Vulnérabilité dans Skype
- CERTA-2011-AVI-285 : Vulnérabilités dans les produits VMware
- CERTA-2011-AVI-286 : Vulnérabilités dans Xen
- CERTA-2011-AVI-287 : Vulnérabilité dans syslog-ng
- CERTA-2011-AVI-288 : Multiples vulnérabilités dans HP Intelligent Management Center

7 Actions suggérées

7.1 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.

7.2 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.

7.3 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.

7.4 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.

7.5 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.

7.6 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.

7.7 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, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique62.html

8 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.

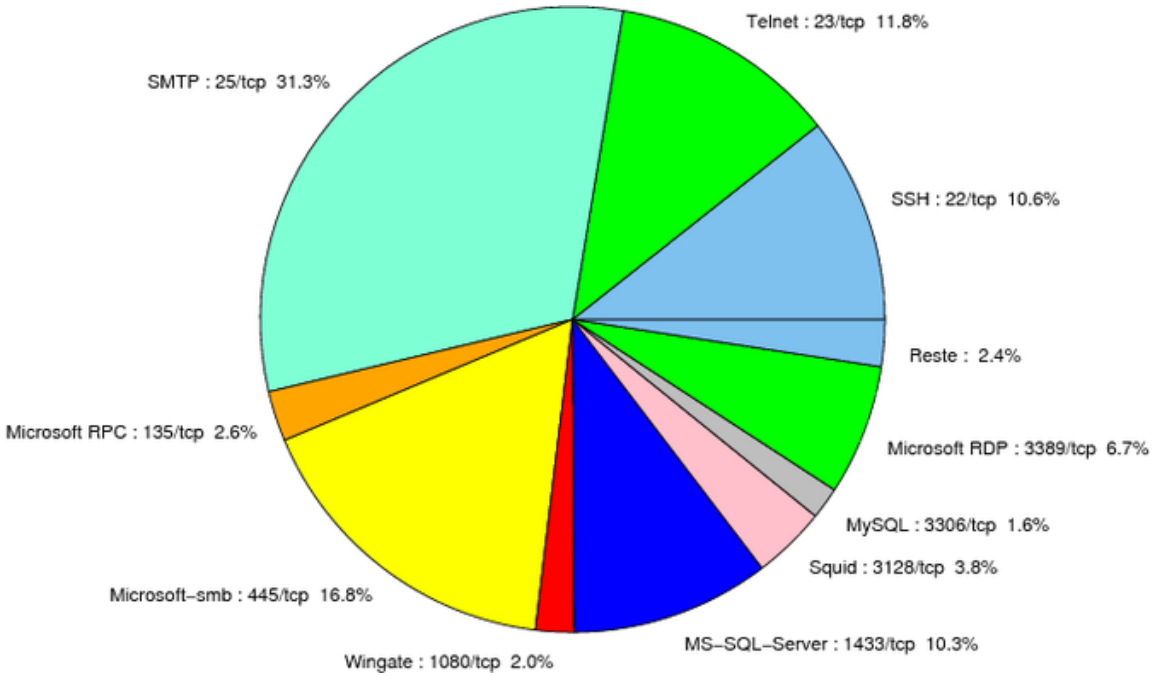

FIG. 1: Répartition relative des ports pour la semaine du 6 au 12 mai 2011

port	pourcentage
25/tcp	31.31
445/tcp	16.78
22/tcp	11.85
23/tcp	11.76
1433/tcp	10.29
80/tcp	9.16
3389/tcp	6.74
3128/tcp	3.8
135/tcp	2.59
1080/tcp	1.98
3306/tcp	1.64
2967/tcp	0.6
3127/tcp	0.43
10080/tcp	0.34
1434/udp	0.17

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

13 mai 2011 version initiale.