

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-43

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-2010-ACT-043>

Gestion du document

Référence	CERTA-2010-ACT-043
Titre	Bulletin d'actualité 2010-43
Date de la première version	29 octobre 2010
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-2010-ACT-043.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-2010-ACT-043/>

1 Incident de la semaine

Cette semaine le CERTA a eu à traiter une injection d'*iframe* sur un serveur Web. Après analyse, il est apparu que l'attaquant a utilisé une vulnérabilité dans un module du système de gestion de contenu TYPO3. Ce module avait été développé en interne et n'était pas diffusé.

Le CERTA tient à souligner que même sur des outils développé en interne et non diffusé, des attaquants réussissent à découvrir et exploiter des vulnérabilités, il est donc essentiel de bien veiller à la sécurité de ces outils au cours de leur développement.

Documentation

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

2 Les alertes de la semaine

Cette semaine, le CERTA a publié deux alertes CERTA-2010-ALE-017 et CERTA-2010-ALE-018 concernant respectivement des vulnérabilités dans Mozilla Firefox et dans les produits Adobe. De plus, la vulnérabilité détaillée dans l'alerte CERTA-2010-ALE-016 a été corrigée.

2.1 Vulnérabilité dans Mozilla Firefox

Une vulnérabilité non communiquée affecte le navigateur Mozilla Firefox. Elle permet à une personne malintentionnée d'exécuter du code arbitraire à distance au moyen d'une page Web spécifiquement réalisée. Mozilla a depuis publié un correctif, le CERTA recommande donc de mettre à jour cette application afin de ne plus être exposé à cette vulnérabilité.

Documentation

- Bulletin de sécurité Mozilla MFSA2010-73 du 27 octobre 2010 :
<http://www.mozilla.org/security/announce/2010/mfsa2010-73.html>
- Alerte CERTA-2010-ALE-017 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-017/>
- AVIS CERTA-2010-AVI-521 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-521/>

2.2 Vulnérabilité dans les produits Adobe

Une vulnérabilité non corrigée affecte des produits Adobe et permet à une personne malintentionnée d'exécuter du code arbitraire à distance. Cette vulnérabilité est actuellement exploitée sur l'Internet dans des attaques ciblant les logiciels Adobe Acrobat et Reader au moyen de documents PDF ayant du contenu Flash. Dans l'attente d'un correctif de l'éditeur, le CERTA recommande les actions suivantes :

- supprimer ou interdire l'accès au composant authplay.dll (cette action bloque l'exécution de contenu Flash et provoque une erreur à l'ouverture d'un document contenant du Flash) ;
- utiliser un logiciel alternatif.

Le CERTA a, de plus, constaté qu'une campagne de pourriels profitait de cette actualité afin de récupérer des coordonnées bancaires sous couvert de l'obtention d'une mise à jour des produits Adobe. Le CERTA rappelle qu'il ne faut jamais répondre à ce type de sollicitations qui restent pour la plupart des escroqueries.

Documentation

- Bulletin de sécurité Adobe APSA10-05 du 28 octobre 2010 :
<http://www.adobe.com/support/security/advisories/apsa10-05.html>
- Alerte CERTA-2010-ALE-018 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-018/>

2.3 Vulnérabilité dans Adobe Shockwave Player

Une vulnérabilité permet à une personne malveillante distante de provoquer un déni de service ou d'exécuter du code arbitraire via des fichiers au format DIR. Une mise à jour a été publiée par Adobe et permet de corriger cette vulnérabilité. Le CERTA recommande d'appliquer ce correctif dans les plus brefs délais.

Documentation

- Bulletin de sécurité Adobe APSA10-04 du 21 octobre 2010 :
<http://www.adobe.com/support/security/advisories/apsa10-04.html>
- Alerte CERTA-2010-ALE-016 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-016/>
- AVIS CERTA-2010-AVI-523 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-523/>

3 Tromper les outils d'analyse protocolaire réseau

3.1 Faits récents

Une société produisant des boîtiers de sécurité a récemment annoncé avoir découvert de nouvelles techniques d'attaques avancées (appelées AET pour *Advanced Evasion Techniques*) permettant de tromper les analyses d'outils réseau, tels les pare-feux applicatifs ou les sondes dites de détection ou de prévention (IDS/IPS).

Les détails techniques ne sont pas connus à la date de rédaction de cet article. L'objet n'est pas ici de faire des présomptions ou des critiques liées à cette annonce, mais profiter de celle-ci pour rappeler le contexte de ce genre d'attaques.

3.2 Rapide historique

Des chercheurs ont expliqué, voilà plus de douze ans, que l'information analysée uniquement au niveau du réseau était insuffisante pour conclure sur les conséquences exactes de l'interprétation des trames par une machine cible. Les outils d'analyse réseau sont intrinsèquement différents des machines qu'ils cherchent à protéger. Les piles protocolaires sont différentes, les réactions à des comportements anormaux également.

Cela est d'autant plus vrai avec certains outils de sécurité actuels qui s'appuient sur des heuristiques et des tests simples pour identifier des protocoles, sans mettre en œuvre de pile protocolaire complète. C'est le cas de plusieurs solutions s'appuyant sur le « DPI » (Deep Packet Inspection).

Peut-on les blâmer ? Non. Les outils de sécurité doivent souvent effectuer à grande échelle le travail d'analyse protocolaire qu'une seule machine fait en principe. Plus le nombre de couches protocolaires à analyser augmente, plus la tâche s'avère complexe. L'une des approches consiste alors naturellement à simplifier l'analyse protocolaire intermédiaire et gagner de précieuses ressources pour les tâches complexes (recherches de chaînes de caractères, etc.).

L'attaquant a ainsi à sa disposition deux grandes méthodes pour agir :

- ajouter des éléments aux trames effectives de l'attaque pour que ceux-ci soient interprétés par l'équipement de sécurité mais négligés par la machine cible (insertion) ;
- omettre des éléments aux trames effectives de l'attaque pour que l'équipement de sécurité ne détecte rien, mais qui seront induites par la machine cible (évasion).

Dans les deux cas, l'équipement échoue dans son analyse. Sa fonction de sécurité est contournée.

Il s'agit d'un sujet très vaste. Parmi les méthodes historiques les plus connues (mais pas nécessairement désuètes) :

- la fragmentation de trames IP ;
- l'absence de vérification des *checksum* ;
- un en-tête incorrect ;
- la gestion des options IP ou TCP ;
- des tunnels ;
- etc.

La liste est relativement longue...

Les cas de contournement font régulièrement l'objet d'articles et/ou de corrections de sécurité. Il s'agit systématiquement de cas issus des zones d'incohérence entre :

1. l'interprétation telle que précisée, parfois de manière imprécise, dans les standards (RFC) ;
2. l'interprétation telle qu'effectuée par les machines à protéger ;
3. l'interprétation telle qu'effectuée par les outils de sécurité.

Un cas assez illustratif est l'interprétation des négociations TCP et les tests publiés sur l'Internet fin 2009 concernant le "*4-way handshake*".

Les attaquants ont différents moyens pour s'attaquer aux boîtiers de sécurité. On peut distinguer, pour trouver des situations de contournement :

- les outils combinant différentes techniques connues, comme celles citées précédemment ;
- les outils testant des contenus aléatoires de trames ou de séquences de paquets (*fuzzing*) ;
- les outils spécifiques visant certains algorithmes propres à un type de boîtier (gestion des états par exemple).

3.3 Que comprendre ?

Chaque outil de sécurité a des limites intrinsèques. En ce qui concerne les outils d'analyse réseau, il faut connaître, demander ou chercher à comprendre les méthodes d'interprétation protocolaire pour :

1. bien identifier les limites intrinsèques du produit ;
2. ne pas appuyer toute son architecture d'analyse sur des briques souffrant de limites similaires.

Des travaux et des outils proposent également de normaliser le trafic en entrée de réseau. Cette méthode n'est pas parfaite. Elle peut avoir d'importants impacts opérationnels mais reste envisageable suivant les cas.

3.4 Références associées

- Annonce publique de la société Stonesoft, 18 octobre 2010 :
http://www.stonesoft.com/en/press_and_media/releases/en/2010/18102010-2.html
- Présentation technique de Stonesoft, octobre 2010 :
<http://www.antievation.com/wp-content/uploads/2010/10/AET-Technical-Presentation.ppt>
- Bloc-notes de Cédric Blancher, 18 et 20 octobre 2010 :
<http://sid.rstack.org/blog/index.php/439-les-aet-le-nouveau-fleau-de-l-internet>
[http://sid.rstack.org/blog/index.php/440-aet-contenu-partiel-et-\(heuristiques,etc.\)reflexions](http://sid.rstack.org/blog/index.php/440-aet-contenu-partiel-et-(heuristiques,etc.)reflexions)
- T. H. Ptacek, T. N. Newsham, « Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection », rapport technique, janvier 1998 :
<http://www.icir.org/vern/Ptacek-Newsham-Evasion-98.ps>
- R. Bidou, « Contourner les ID(P)S sans rien y connaître », SSTIC 2006 :
http://actes.sstic.org/SSTIC06/...IDS/SSTIC06-article-Bidou-Contournement_des_IDS.pdf
- BreakingPoint, « TCP Portals: The Handshake's a Lie! », novembre 2009 :
<http://www.breakingpointsystems.com/community/blog/tcp-portals-the-handshakes-a-lie/>

4 Une extension controversée pour Firefox

Cette semaine, la presse a beaucoup parlé de l'extension Firesheep pour Firefox. Cet article est l'occasion de revenir sur ce qu'elle fait, les risques associés et les problèmes légaux associés.

4.1 Qu'est ce que Firesheep

Il s'agit d'un module complémentaire, non disponible dans les dépôts officiels, qui s'installe manuellement. Il écoute le trafic réseau visible par la machine (filaire ou WiFi) pour reconstituer les cookies de sessions transitant, et cela pour une vingtaine de sites dont Facebook et Yahoo. Il s'utilise en tant que panneau latéral dans lequel s'affichent les sessions usurpées, et sur lesquelles il suffit de cliquer pour accéder au compte correspondant.

Sa simplicité d'installation et d'utilisation, ainsi que le battage médiatique fait autour, en fait un outil très tentant à utiliser... Cependant, il convient de s'interroger avant.

Tout d'abord, il s'agit d'un outil non testé et au mode de développement inconnu. On ne reviendra pas ici sur les risques qu'il y a à installer de tels logiciels.

Par ailleurs, lors de son lancement, le module va capturer tout les *cookies* possibles et va automatiquement se connecter au site correspondant (cf. ci-dessous « *Accès illégitime automatique* »).

4.2 Des accès illégitimes automatiques

On voit ci-dessous que la machine 172.16.127.128 (*la victime*) échange un *cookie* de session avec l'adresse 66.220.153.23 (Facebook). Automatiquement, moins d'une demi-seconde plus tard, l'adresse 172.16.127.130 (*l'attaquant*) se connecte à l'adresse 69.63.190.10 (un autre serveur Facebook) avec le même *cookie*.

```
11:46:45.465553 172.16.127.128 66.220.153.23 HTTP GET /home.php?
Cookie: datr=8vTHTLeCs109isMbbW7-XXXX; x-referer=https%3A%2F%2F
login.facebook.com%2Floginnotify%2Fsetup_machine.php%23%2F
loginnotify%2Fsetup_machine.php; c_user=126781XXXX;
cur_max_lag=20; lu=QAIsNHycU1vJDpq-fS12XXXX;
```

```
11:46:46.161863 172.16.127.130 69.63.190.10 HTTP GET /home.php
Cookie: datr=8vTHTLeCsl09isMbBW7-XXXX; x-referer=https%3A%2F%2F
login.facebook.com%2Floginnotify%2Fsetup_machine.php%23%2F
loginnotify%2Fsetup_machine.php; c_user=126781XXXX;
cur_max_lag=20; lu=QAIsNHycU1vJDpq-fSl2KXXXX
```

Il n'est donc pas possible, avec cet outil, de simplement écouter le réseau sans commettre d'accès illégitime.

4.3 Extraits du code pénal

Article 323-1 : Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende.

On peut considérer que le premier accès à une session d'un tiers par l'outil n'est pas du fait de l'utilisateur de l'outil. En revanche, le maintien de la session tierce est constitutif de l'infraction à l'article susvisé. La répétition de cette commande fait tenir l'accès et le maintien frauduleux.

Article 323-3-1 : Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

4.4 Remarque

Certains sites proposent une fonctionnalité de sécurité permettant d'identifier les machines qui sont utilisées pour se connecter. Cette identification étant faite avant l'établissement de la session, le fait d'utiliser un *cookie* contourne cette protection.

4.5 Conclusion

Le CERTA recommande bien sûr de ne pas utiliser, installer ou partager un tel outil (sauf très bon motif légitime et avec un encadrement légal approprié). Le CERTA recommande aussi aux utilisateurs des sites de ne pas utiliser de connexion en clair partagée (wifi chiffré, réseau commuté ou maintien des connexions en https).

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 22 au 28 octobre 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-512 : Vulnérabilité dans Ruby on Rails
- CERTA-2010-AVI-513 : Multiples vulnérabilités dans Mac OS X Java
- CERTA-2010-AVI-514 : Vulnérabilités dans Pidgin
- CERTA-2010-AVI-515 : Multiples vulnérabilités dans Moodle
- CERTA-2010-AVI-516 : Vulnérabilités dans HP Systems Insight Manager
- CERTA-2010-AVI-517 : Vulnérabilités dans CiscoWorks Common Services
- CERTA-2010-AVI-518 : Vulnérabilité dans HP Virtual Server Environment
- *CERTA-2010-AVI-519 : Vulnérabilité dans HP Virtual Connect Enterprise Manager
- CERTA-2010-AVI-520 : Vulnérabilité dans glibc
- CERTA-2010-AVI-521 : Multiples vulnérabilités dans des produits Mozilla

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

- CERTA-2010-AVI-474-001 : Multiples vulnérabilités dans TYPO3 (ajout des références CVE)
- CERTA-2010-AVI-498-001 : Multiples vulnérabilités dans Opera (ajout des références CVE)
- CERTA-2010-AVI-509-001 : Multiples vulnérabilités dans Google Chrome (mise à jour du lien vers la note de version et ajout des références CVE)

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 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.

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 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.

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_rubrique67.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.

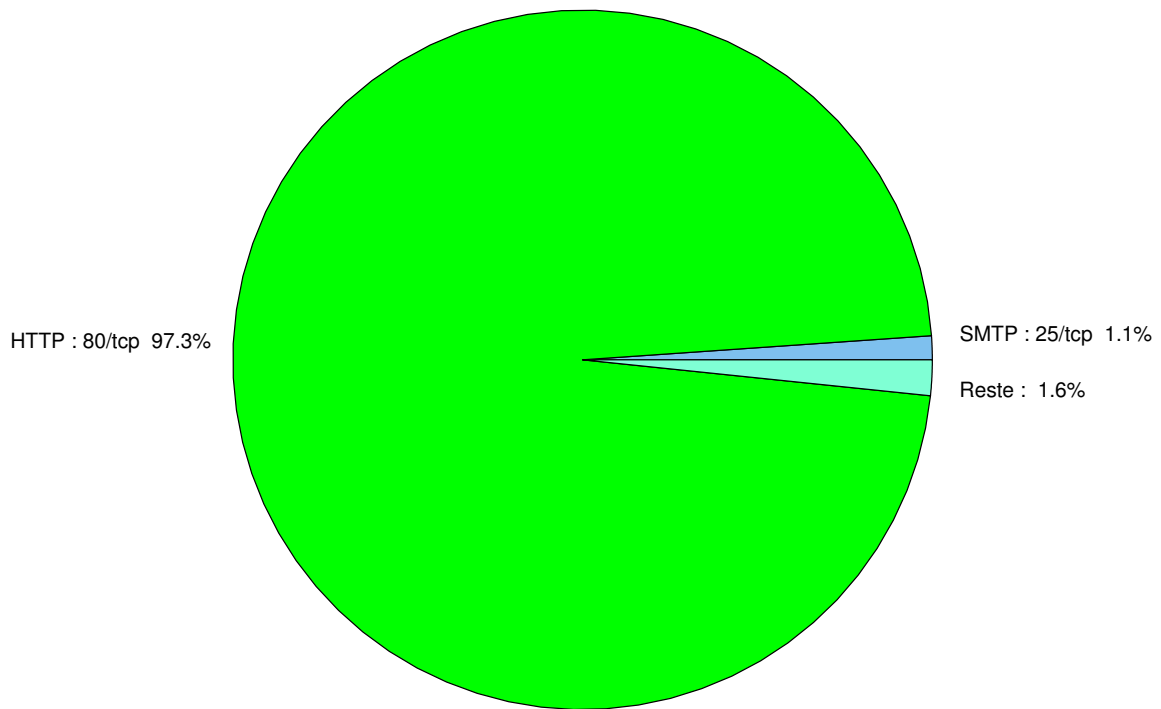


FIG. 1: Répartition relative des ports pour la semaine du 22 au 28 octobre 2010

port	pourcentage
80/tcp	97.31
25/tcp	1.09
1080/tcp	0.52
445/tcp	0.3
22/tcp	0.19
1433/tcp	0.1
3128/tcp	0.08
3389/tcp	0.06
3306/tcp	0.04
1434/udp	0.03
4899/tcp	0.01

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	8

Gestion détaillée du document

29 octobre 2010 version initiale.