

Ecole informatique - SUPINFO International University

Quelle importance doit-on donner à la sécurité de vos données dans le Cloud ?

Travail de fin d'étude présenté en vue de l'obtention du master « International Master of Science »

Quentin CLARENNE

Maitre de stage : **Saber Bariz**

Société : PlanetHoster

Année : 2012-2013

Tables des matières

1. Présentation de la société 6
   1.1. Identification du service 7
   1.2. Zone géographique 7
   1.3. Statut de l'entreprise 8
   1.4. Historique 8
   1.5. Présentation générale et objective 9
   1.6. Fonctionnement du service 9
   1.7. Personnel 10
   1.8. Concurrence 11
   1.1. Quelle est la force de PlanetHoster ? 12
   1.2. Réseau de partenaires 16
   1.3. La clientèle visée par la société 17
   1.4. La marque PlanetHoster 18
2. Introduction au titre du TFE 19
   Introduction 20
   2.1. Taux d'attaque sur internet 20
   2.2. Quelles sont les attaques les plus utilisées et comment s'en prémunir ? 25
      2.2.1. Les attaques bruteforce SSH 25
      2.2.2. Les attaques sur les mails : POP3, IMAP, Exchange 25
      2.2.3. Les attaques FTP(s). 26
      2.2.4. Les attaques IRC 26
      2.2.5. Les attaques DOS et DDOS (SYN Flood) 26
      2.2.6. Les attaques VOIP, SIP/Asterisk 27
      2.2.7. Les brutesForces CMS/Panel admin 27
      2.2.8. Les scans de ports TCP/UDP 27
      2.2.9. Les failles présentes dans les CMS/modules 28
      2.2.10. Le spambot dans les formulaires/forums 28
      2.2.11. Les bruteforces sur les moteurs SQL 28
      2.2.12. Les injections SQL 29
      2.2.13. Le social enginering 29
   2.3. Quelles sont les pertes pour les datacenter/hébergeurs ? 30
   2.4. Un phénomène de mode ? 30
   2.5. Pourquoi tant de violence ? 31
   2.6. Quelles sont les différentes solutions pour se protéger de cela ? 32
      2.6.1. Les protections au niveau des applications 32
      2.6.2. Les protections au niveau de l'environnement 32
      2.6.3. Les protections réseau 32
   2.7. Quelles sont les dernières fuites de données connues ? 33
   2.8. L'augmentation des centres de traitement de calculs 34
   2.9. Quels peuvent être les avantages pour les hackers ? 34
   2.10. Quelles sont les bonnes pratiques à mettre en place ? 35
   2.11. Quelles sont les règlementations/lois en vigueur ? 35
   2.12. Quelle importance donner aux DNSBL ? 37
3. Présentation du projet 38

3.1. Introduction 39
3.2. Analyse fonctionnelle 39
3.2.1. Les attaquants 40
3.2.2. Les évènements 41
3.2.3. Les serveurs 41
3.2.4. Les autres blockings liste ou RBLs 41
3.2.5. Les statistiques publiques totalement transparentes 42
3.2.6. Les vérifications par les utilisateurs 43
3.2.7. La suppression rapide 43
3.2.7.1. La mise à jour automatique par les serveurs 44
3.2.7.2. La page d'aide 44
3.2.7.3. La page de contact 44
3.2.7.4. Un site totalement responsif 45
3.2.7.5. Workflow sur les blacklistage 45
3.2.7.6. Notification en cas de blacklistage 45
3.2.7.7. Classification par type d'attaques 46
3.2.7.8. Dashboard et tableaux d'administration 47
4. Analyse du stage 49
4.1. Administration du serveur de production 50
4.2. Profilingue de Fail2Ban/iptable/netfilter 50
4.2.1. Installation du service dans le parc informatique 51
4.2.2. Résultat obtenu suite à la mise en place de GreeSnow 55
4.2.3. Éducation 56
4.3. Relations humaines 56
5. Conclusion 58
6. Agenda 60
6.1. Planning 61
6.2. Activités durant le stage 62
7. Bibliographie 63

Remerciements

Je tiens à remercier l'ensemble des personnes qui ont pris part à mon projet de fin d'études et ainsi, m'ont permis de réaliser celui-ci au mieux.

J'adresse un merci tout particulier à mes maîtres de stage Saber BARIZ et Mina SHENOUDA qui, durant ces six mois, m'ont guidé dans mes choix, m'ont permis d'utiliser chacune de mes connaissances acquises lors de la formation et d'agrandir mon cercle de savoir, savoir-faire, savoir-être.

Je tiens à exprimer toute ma reconnaissance à Jay, Vincent, Christophe, ainsi que Pierre pour leur aide précieuse dans l'élaboration de mon travail. Ils ont su me guider et m'ont aidé à pousser ma réflexion au plus loin.

C'est avec plaisir que j'ai étudié à SUPINFO Montréal. Je remercie les membres de celle-ci pour leur soutien, leurs encouragements, leur bonne humeur...

Je terminerai en remerciant également toutes les personnes qui m'ont aidé et soutenu lors de la rédaction de mon TFE.

MERCI

Introduction

Lors de la cinquième année du master informatique de SUPINFO, les étudiants sont amenés à réaliser un stage en entreprise en vue de l'obtention de leur diplôme.

Mon stage s'est donc déroulé dans une entreprise canadienne qui s'appelle PlanetHoster. La finalité du stage était la création d'un connecteur entre PlanetHoster (bureau d'enregistrement) et l'AFNIC. De plus, d'autres projets ont été lancés comme le lancement d'une blocklist pour lutter contre les différentes attaques sur les serveurs (sécurité Linux), la vérification de nos IP sur les RBLs comme SpamHaus, SpamCop,… De la R&D sur les systèmes de virtualisation pour les nouvelles offres Cloud et VPS. L'aspect riche et varié des différents projets a été un élément déterminant dans le choix de mon stage. De plus, la programmation web m'attire tout particulièrement. Le stage m'a en outre permis de toucher à la virtualisation sur OpenVZ/OpenStack et à la préparation de serveurs (sécurité, optimisation, mise à jour…)

Au cours de la lecture de ce mémoire, vous trouverez tout d'abord la présentation de la société qui permettra une meilleure compréhension de l'environnement dans lequel j'ai effectué mon stage.

Dans un deuxième temps, j'effectue une analyse globale des différentes problématiques liées aux attaques possibles.

Ensuite, le projet réalisé sera décrit ainsi que les différents objectifs visés sous une analyse fonctionnelle.

Après la description du projet, suivra un descriptif des outils, méthodes et technologies utilisés pour la réalisation de la blocklist. Une bonne compréhension de ceux-ci permettra au portail d'interagir au mieux avec l'utilisateur.

Enfin, une conclusion reprendra le bilan technique du stage et le bilan personnel.

1. Présentation de la société

1.1. Identification du service

« PlanetHoster »

4416 Louis B Mayer

H7P 0G1 Laval (Grand Montréal)

Téléphone : +32 (0)2 743.49.00

Fax : +1 514 802 1644

E-mail : commercial@support.planethoster.info

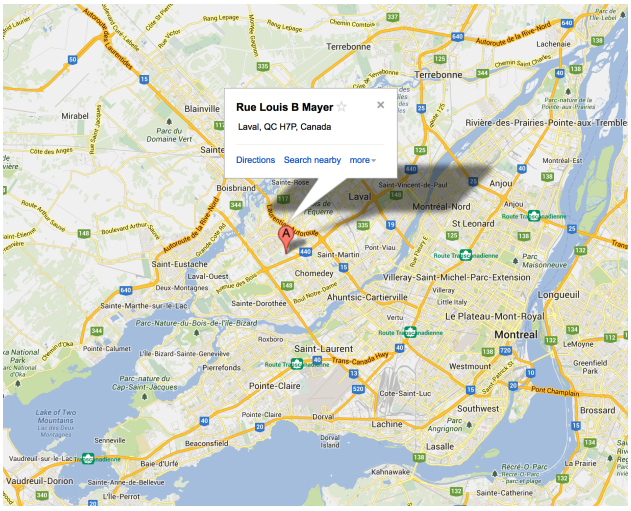


Figure 1 : Localisation de PlanetHoster

Les personnes de référence sont :

— Monsieur Saber BARIZ : Directeur général
— Monsieur Mina Shenouda : Administrateur

1.2. Zone géographique

L'entreprise se situe à 20 kms du centre de Montréal et est facile d'accès en voiture. L'accès au centre de données (qui se trouve au centre de Montréal) se fait en 20 minutes. Toutefois, les employés et clients ne s'y rendent que rarement, car, bien souvent, les employés travaillent à domicile. De plus, il faut savoir que le support doit être en permanence actif ; il y a donc des techniciens qui sont en fonction sur des fuseaux horaires différents afin de garantir un service disponible 24/7.

1.3. Statut de l'entreprise

A l'origine, PlanetHoster est une entreprise familiale qui, au fil du temps, s'est développée en une compagnie incorporée au groupe Barzico (administration et comptabilité).

1.4. Historique

La société PlanetHoster a vu le jour en 2007 à Montréal ; elle a commencé dans l'hébergement mutualisé au Canada. L'entreprise s'est diversifiée au cours des années et offre désormais différents plans d'hébergements. De plus, depuis maintenant un an, des serveurs sont implantés en France et plus précisément à Paris.

Actuellement, l'entreprise compte près de 25.000 clients. Il faut savoir que chaque client a près de 8 noms de domaines en moyenne ; cela fait près de 200.000 domaines enregistrés chez PlanetHoster

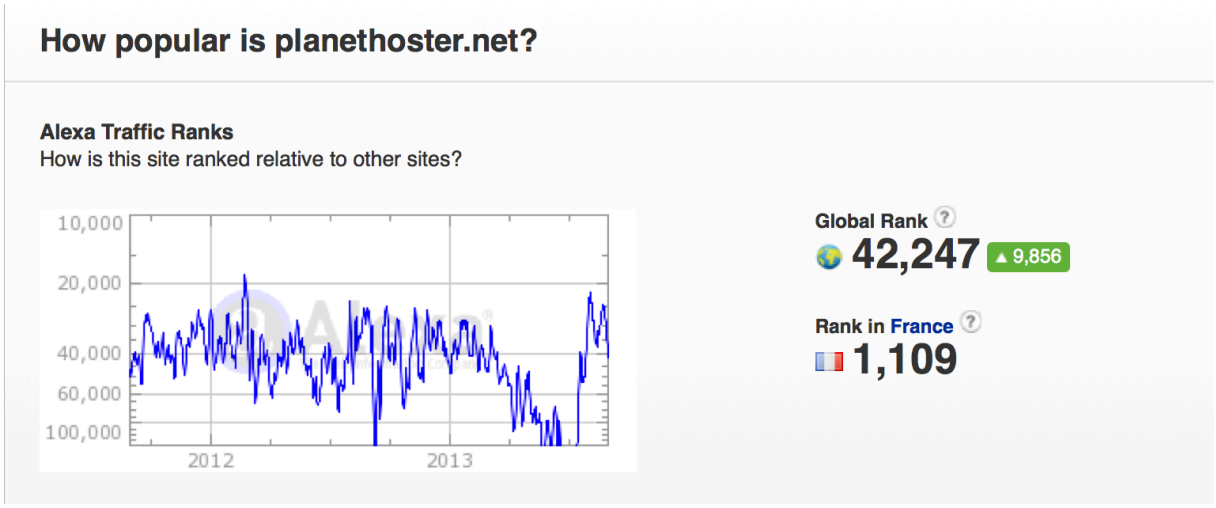


Figure 2 : *Affichage de l'AlexaRank de PlanetHoster.net*

C'est, selon moi, ce qui fait la force. En fait, le point de vue de chaque client est important puisque cela nous permet de comprendre ses besoins particuliers et d'y répondre. De plus ayant conscience que notre clientèle est variée, nous avons développé deux portails, l'un en français, l'autre en anglais.

1.5. Présentation générale et objective

Le slogan est « Héberger votre monde », ce qui signifie que PlanetHoster accompagne les compagnies en pleine expansion à héberger leurs contenus. Vous pouvez donc héberger sur des plans mutualisés des sites en PHP ou RoR avec des bases de données en MySQL ou PostgreSQL. Vous avez la possibilité aussi de prendre un plan d'hébergement E-commerce qui comprend une IP dédiée et un certificat SSL. Ces serveurs sont plus performants que les serveurs mutualisés, car ceux-ci comprennent moins de clients. Et donc, le chargement de pages sur ceux-ci est d'autant meilleur. Après, il existe deux autres sortes de serveurs, les virtualisés (VPS) et les dédiés.

1.6. Fonctionnement du service

L'équipe de travail est composée de 7 personnes qui sont gérées directement par le directeur. Selon ma perception, l'entreprise fonctionne différemment de ce que j'ai pu observer en Europe. En effet, la hiérarchie des employés ne s'effectue pas sous une forme pyramidale. Un technicien de Level 1 est aussi important qu'un technicien de Level 3 et pourrait partager ses avis et opinions avec le directeur avec autant de crédit. La communication y est privilégiée et favorisée afin d'offrir un environnement de travail plus stimulant et motivant. L'objectif de cette organisation est de créer auprès des employés un sentiment d'appartenance à l'entreprise. L'équipe s'en retrouve plus soudée avec une mission commune, celle de faire progresser la société pour l'intérêt de tous puisque chacun contribue à son amélioration. La mission de PlanetHoster est d'offrir à la clientèle le meilleur support possible. Cela implique la création de designs accrocheurs, un support à la clientèle infaillible et des outils de développement efficace pour faire face à la demande du marché.

1.7. Personnel

L'entreprise compte actuellement 7 employés répartis entre l'Europe et le Canada. Le bureau principal qui se trouve à Laval comporte 4 employés, dont le directeur. Les trois autres employés travaillent pour PlanetHoster depuis la France pour assurer un support 24 h/24 h.

Au sein de l'équipe, il y a des conseillers à la clientèle, des développeurs, des administrateurs systèmes et des techniciens. Ceux-ci sont classés par niveaux de compétence : niveau 1, 2 ou 3.

Les compétences requises sont très vastes et variées. Cela passe du support avec le client à l'administration de serveur, à la sécurisation du réseau, à la recherche et au développement, mais aussi à l'installation des nouveaux serveurs, l'équipement réseau, recherche de SPAM/Phissing,… Le travail est très vaste et il faut se montrer très réactif et professionnel.

1.8. Concurrence

Le secteur de l'hébergement est très concurrentiel. Il faut connaître les différents acteurs qui sont en jeu (OVH, Infomaniak, 1and1, O2Switch, NUXIT, Be2host, Iweb,…).

Passons en revue les différentes compagnies qui offrent des services d'hébergement :

OVH est une compagnie française créée en 1999, elle a commencé à revendre de l'hébergement à Roubaix et maintenant, elle s'est très fort diversifiée (VDSL, Cloud,…). Elle a même récemment ouvert un DataCenter à Montréal. Cette compagnie est cependant tellement grande que vous y serez traité comme un numéro et non une personne humaine.

Infomaniak est une entreprise basée à Genève qui a vu le jour en 1996. Celle-ci fait de l'hébergement mutualisé et vidéo à la demande de bonne qualité ; cependant, le support est relativement lent. Elle se targue aussi de faire de l'hébergement vert conformément à sa charte environnementale.

1& 1 est une société allemande qui a débuté en 1988 avec des offres des télécommunications et ensuite de l'hébergement. Celle-ci offre des serveurs très bas de gamme avec des contrats qui vous obligent à renouveler sur un long terme. Je vous conseille de fuir cet hébergeur très rapidement.

MavenHosting est une société canadienne qui existe depuis 2003. Elle loue des serveurs chez OVH en France. Le support est assez disponible et efficace (Canada). Cependant, pouvons-nous faire confiance à une société qui n'administre pas elle-même ses propres serveurs ?

Dans le domaine où la concurrence est rude, il est important de connaître les entreprises rivales. Cela permet d'évaluer l'offre du marché disponible et de faire en sorte d'offrir une meilleure qualité de service. PlanetHoster a pris en considération chacune de ces entreprises, en a analysé les points forts et faibles afin de ne pas reproduire les mêmes erreurs et de se démarquer.

1.1. Quelle est la force de PlanetHoster ?

Parlons maintenant un peu de PlanetHoster. Nos plans sont très performants, car nous utilisons des serveurs de dernière génération utilisant des disques SSD. Ici sur la photo, ce sont des serveurs avec 196 Go de RAM et 16 SSD 512 Go en RAID10





Les modèles de serveurs sont étudiés avant d'être commandés. Nous travaillons majoritairement avec les marques DELL, les CPU et SSD qui sont choisis, car réputés plus performants, stables et moins énergivores. Pour les serveurs Mutualisés Hyrbride, nous travaillons avec des disques durs 10Ktour/min en RAID 10 pour stocker les fichiers et 2 disques SSD en RAID 0 pour y ajouter la base de données. Au vu de ces différents éléments, PlanetHoster peut certifier une excellente performance.

Figure 3 : *Photos des serveurs VPS et Mutualisés de PlanetHoster*

Côté réseautique, PlanetHoster travaille en partenariat avec Noction. Grâce à leur produit, nous sommes en mesure de « router » le trafic en tenant compte de la latence, des paquets perdus et bien plus. La partie réseau est très bonne, car les serveurs sont reliés à 6 Peering par sites (BGP:Tata, Tella, Tinet, Jaguar, Level3, Cogent, Netilligent) afin de garantir la meilleure route. La majorité des hébergeurs se basent encore sur le protocole BGP4 pour déterminer quelle route prendre pour toute destination. Puisque BGP4 n'est pas conscient de la qualité entre deux réseaux, la performance peut être affectée négativement. Noction IRP examine de manière proactive chaque réseau pour trouver la meilleure route à prendre et dirige le trafic en fonction de la latence et des paquets perdus.

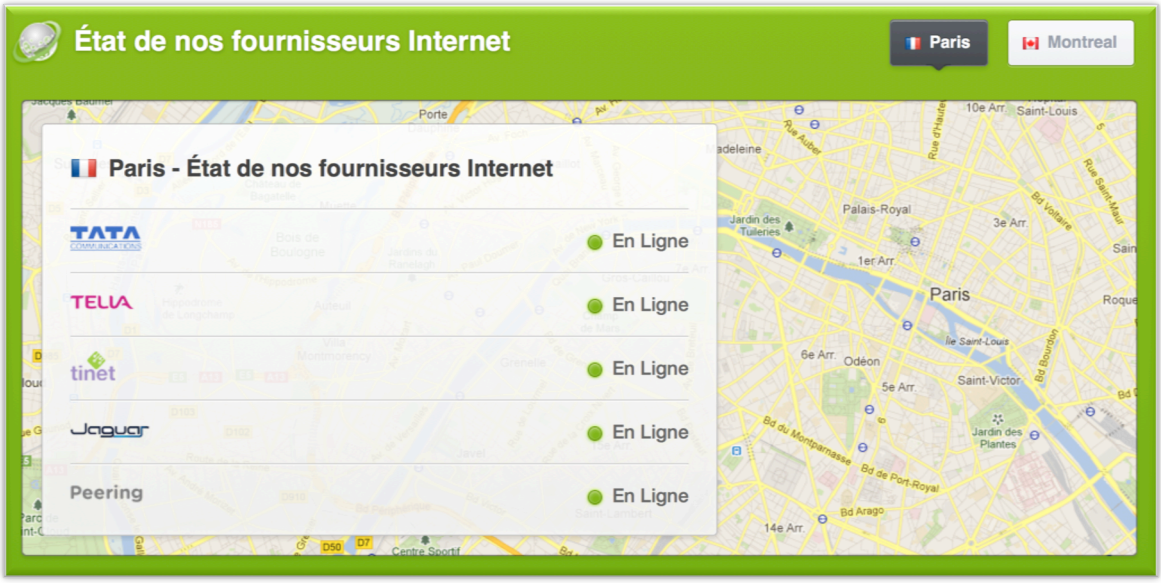


Figure 4 : *Le système de monitoring de PlanetHoster (info.planethoster.net)*

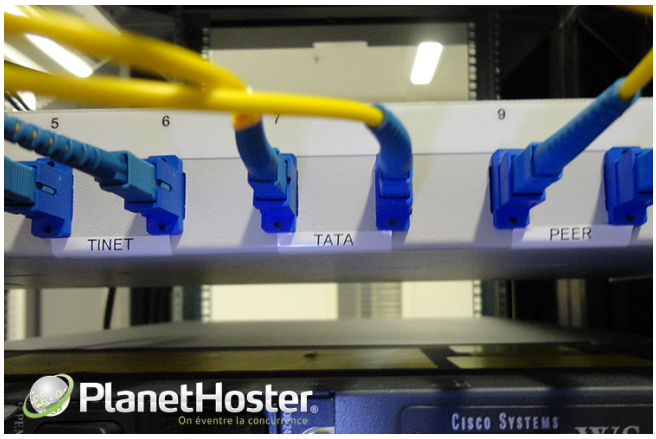
Le support est également très réactif (moins de 10 minutes d'attente pour les tickets et support téléphonique).

ARBOR NETWORKS
DDoS Protection | DDoS Attack Mitigation

Les serveurs sont très bien sécurisés et dernièrement, nous avons mis en place un système de protection non plus sur le serveur, mais directement sur le réseau. Depuis le 12 septembre 2013, nous avons configuré une protection Anti-DDoS continuelle et permanente sur nos services d'hébergement mutualisé, revendeur, VPS et e-commerce, et ce gratuitement. La protection est active 24/7 sur nos installations françaises. Elle sera bientôt active dans nos installations canadiennes. PlanetHoster est l'un des rares hébergeurs à disposer de ce système de sécurité qui se nomme Arbor. Nous en parlerons plus en détail dans la dissertation.

Enfin, les serveurs dédiés à la concurrence sont souvent livrés sans infogérance et sans panneaux d'administration. Le résultat est que le client se retrouve devant un système en ligne de commande et celui-ci n'optimise souvent pas au mieux le serveur (configuration par défaut). De plus, les serveurs sont très fréquemment scannés, bruteforcés et sans aucune protection. La conséquence est que le serveur est régulièrement surchargé à vide et que la sécurité de celui-ci est compromise après quelques mois. Des serveurs de nouvelle génération, des CPUs plus performants, plus de mémoire vive, et surtout une architecture de stockage en SSD, le tout en RAID 10. Sans oublier que la majorité des VPS comprennent l'infogérance et le cPanel et sont sauvegardés quotidiennement par nos serveurs R1SOFT. La nouvelle infrastructure est l'idéal pour les boutiques e-commerce (Prestashop, Magento...), les CMS (WordPress, Drupal, Joomla…) le forum (Vbulletin, Xenforo…) et bien plus ! Votre site se chargera TRÈS RAPIDEMENT !





Il faut savoir que tous les serveurs, équipement réseau (AS53589) appartient à PlanetHoster. Ce qui lui permet d'en avoir le contrôle total sans être tributaire d'autres personnes. Un très grand nombre « d'hébergeurs » achète ou loue à d'autres compagnies des serveurs. Cela entraîne que les hébergeurs n'ont pas la main complète sur les serveurs et qu'en cas de problème, ils sont tributaires d'autres personnes.

Figure 5 : *Les fibres réseau des différents Peerings*

1.2. Réseau de partenaires

Actuellement, le réseau de partenariat de PlanetHoster est très large. Nous avons des accords avec de très grands sites informatiques comme le Site du Zéro qui parle de nous dans les livres suivants : « Concevez votre site web avec PHP et MySQL » et « Apprenez à créer votre site web avec HTML5 et CSS3 »



Figure 6 : *Le logo du Site Du Zéro*

De plus, le site Developpez.com a publié quelques articles sur nous afin de faire connaître au mieux l'hébergeur aux personnes sachant développer.



Figure 7 : *Logo de Developper.com*

Nous avons aussi des sites comme vBulletin-Ressources.com ou immo-sudannonces.fr qui sont hébergés chez nous et qui le revendique sur leur site.



Auparavant, PlanetHoster passait par des bureaux d'enregistrement tiers afin d'enregistrer les noms de domaines. Depuis peu, cela a été changé en collaborant directement avec les entités comme l'Afnic pour l'enregistrement des. fr, DNS.be pour l'enregistrement des. be et EURid pour les. eu cela apporte donc maintenant une meilleure visibilité dans le WHOIS des noms de domaines directement enregistrés chez nous. PlanetHoster est registrar officiel pour les extensions. fr,. re,. pm,. yt,. wf,. tf,. be,. eu. (J'ai, lors de mon stage, eu l'occasion de développer les connecteurs EPP entre nous « bureau d'enregistrement » et ces « organisations de nommages » ; cela fonctionne très bien)



Figure 8 : *Logo des différentes organisations de nommages dont nous sommes accrédités*

1.3. La clientèle visée par la société

Lors de la création de PlanetHoster en 2007, celle-ci s'adressait aux petits clients ayant des offres à bas prix avec des systèmes de paiement comme AlloPass, Paypal. Cela a permis à PlanetHoster de se faire connaître et d'attirer un certain nombre de clients. Cependant, ceux-ci sont majoritairement des privés et réclament pour des petits prix, des serveurs énormes (mauvais codage). Ils demandent un support permanent, car ils n'utilisent pas à bon escient le serveur. Depuis le début de l'année 2012, de nouvelles offres hybrides ont été lancées. Celles-ci sont près de 9 fois plus rapides (SSD, LiteSpeed, nouveau peering, système de sauvegarde…) et le prix a donc dû être augmenté afin de pouvoir offrir cela. Depuis l'augmentation des prix, la clientèle s'est quelque peu modifiée et ce sont désormais majoritairement des personnes qui ont de meilleures connaissances en informatique (Professionnelle, entreprise, autoentrepreneur…). Cela nous permet donc d'offrir un support plus réactif.

1.4. La marque PlanetHoster



Il faut savoir que PlanetHoster est une compagnie écologique utilisant des serveurs basés au Canada qui s'alimentent non pas d'électricité nucléaire, mais bien de l'électricité provenant de barrages hydrauliques. Le fournisseur d'électricité majoritaire au Canada est en effet HydroQuébec.

Ce fournisseur commence aussi à développer un parc d'éoliennes afin de se diversifier et les 3 centrales nucléaires présentes au Canada seront fermées en 2015 afin d'être remplacées uniquement par des énergies vertes. PlanetHoster ne se contente pas d'utiliser de l'énergie verte, ses serveurs sont très puissants et les gammes de CPU sont minutieusement analysées afin de prendre des processeurs ne chauffant pas trop afin d'économiser de l'énergie. Il faut savoir qu'aux bureaux situés à Laval, nous disposons d'une imprimante pour 5 personnes. Cependant, cette dernière est rarement utilisée, car nous privilégions l'utilisation des blocs-notes virtuels. Nous travaillons à la protection de l'environnement (utilisation de l'énergie hydraulique, réduction des déchets…) et nous nous mettons au vert et pas seulement de manière métaphorique. En effet, les bureaux de PlanetHoster sont verts et nous le revendiquons sur nos murs, cartes de visite, poubelles…

Au niveau serveur, nous utilisons des processeurs à faible consommation électrique, mais qui assure d'excellente performance. Notre infrastructure utilise des climatiseurs à énergie verte grâce au climat canadien. Le bâtiment est écologique et utilise les dernières technologies vertes. Un article sera bientôt déposé sur notre site web pour décrire plus en détail nos actions pour l'environnement.

2. Introduction au titre du TFE

Introduction/Analyse du contexte

Ayant travaillé dans le milieu de l'hébergement web et plus particulièrement dans l'administration système et réseau et ayant vu toutes les attaques que nous avons reçues et bloquées, j'ai donc voulu débattre de l'importance des outils de sécurisation des données dans le Cloud.

Tout d'abord, qu'est-ce qu'un Cloud exactement ? Un Cloud est une ressource/service disponible à travers le monde via internet. Cela permet de délocaliser les serveurs non plus dans les entreprises, mais bien directement en les mettant sur Internet. C'est donc un avantage pour les entreprises d'utiliser des services Cloud comme Google App Entreprise, Office 365, Dropbox,… Ces outils sont très faciles à mettre en place et permettent d'avoir un système collaboratif simple. Cependant, en cas de problème (infiltration, corruption, vols de données…) à qui incombe la faute ?

2.1. Taux d'attaque sur internet

L'iFop a réalisé en décembre 2011 une étude de près d'un an de recherche sur la hausse d'attaques sur internet en plaçant des serveurs en ligne et en écoutant le trafic demandé sur ceux-ci. Sur un échantillon de plus de 3000 serveurs placés à travers le monde, les résultats sont plutôt intéressants à examiner.

Les premières attaques/scan ont vite été détectées, les services SSH, mails (POP3, IMAPS), FTP ont été demandés par un très grand nombre d'adresses IP à travers le monde (48 % venant de la Chine +26 % venant des USA et 22 % de la France).

Cette étude montre également la croissance des botnets (+ 5 % d'augmentation en un an) et de près de 10 % d'augmentation d'attaques par année. Il est intéressant de mettre en avant quelques chiffres sur ces attaques dont on entend parler quotidiennement sur le web.

À en croire la dernière statistique de « BlockList.de » les PCs/serveurs zombies servent à ceci :

- Pour l'envoi de SPAM
- Pour l'hébergement de phissing, virus, trojan,..
- Pour eux-mêmes, scanner d'autres serveurs
- …

La société américaine Symantec qui est spécialisée dans les logiciels informatiques de sécurité nous a fourni une infographie très intéressante sur ses dernières études. Cette infographie nous montre que les États-Unis, la Chine et l'Inde sont les pays les plus touchés par ces machines zombies.

Pour l'Inde, nous pouvons supposer que les lois concernant les cyberattaques ne sont pas encore écrites dans ce pays. La Chine est quant à elle très peuplée et très développée. De plus, elle connaît un régime dictatorial et cela n'est donc pas une surprise que ce pays soit touché par ces infections à grande échelle. Cependant, pour les USA, le phénomène est relativement étrange, car ce pays semble tout contrôler. Les Américains ont en effet des lois (comme la DMCA) qui arrivent à bloquer des sites très rapidement si ceux-ci enfreignent leurs règles.

Il est donc très possible que certains pays tentent d'avoir un très gros botnet afin de provoquer des cyberattaques de très grande taille afin de bloquer les communications de leurs ennemis. Une preuve en est que Belgacom suspecte la NSA de l'espionner depuis 2011 suite à une infection à très grande échelle (espionnage d'alliés). Ne pensez-vous pas Edward Snowden est recherché par les USA/Interpol parce qu'il en sait beaucoup trop ? Je laisse votre imagination et ces différentes images vous parler.

Symantec. | Website Security Solutions

Norton SECURED powered by VeriSign

MENACES EN LIGNE : GARDEZ UN COUP D'AVANCE

QU'EST-CE QU'UN MALWARE ?

ABRÉVIATION DE « MALICIOUS SOFTWARE » (LOGICIEL MALVEILLANT EN FRANÇAIS), LE « MALWARE » DÉSIGNE UN LOGICIEL CRÉÉ POUR ENDOMMAGER OU DÉRÉGLER LES ORDINATEURS ET SYSTÈMES INFORMATIQUES, VOIRE LES METTRE HORS D'USAGE. PARMI LES MALWARES, ON TROUVE NOTAMMENT LES VIRUS, LES CHEVAUX DE TROIE, LES VERS ET LES LOGICIELS ESPIONS.

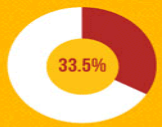


OÙ SONT BASÉES LES PRINCIPALES SOURCES D'ACTIVITÉ MALVEILLANTE ?

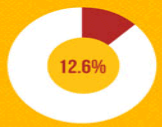
ÉTATS-UNIS, CHINE ET INDE



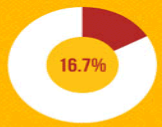
LES ÉTATS-UNIS CONSTITUENT LE PREMIER PAYS D'ORIGINE DE CERTAINES MENACES :



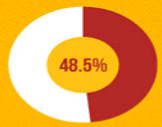
ACTIVITÉ DES BOTS



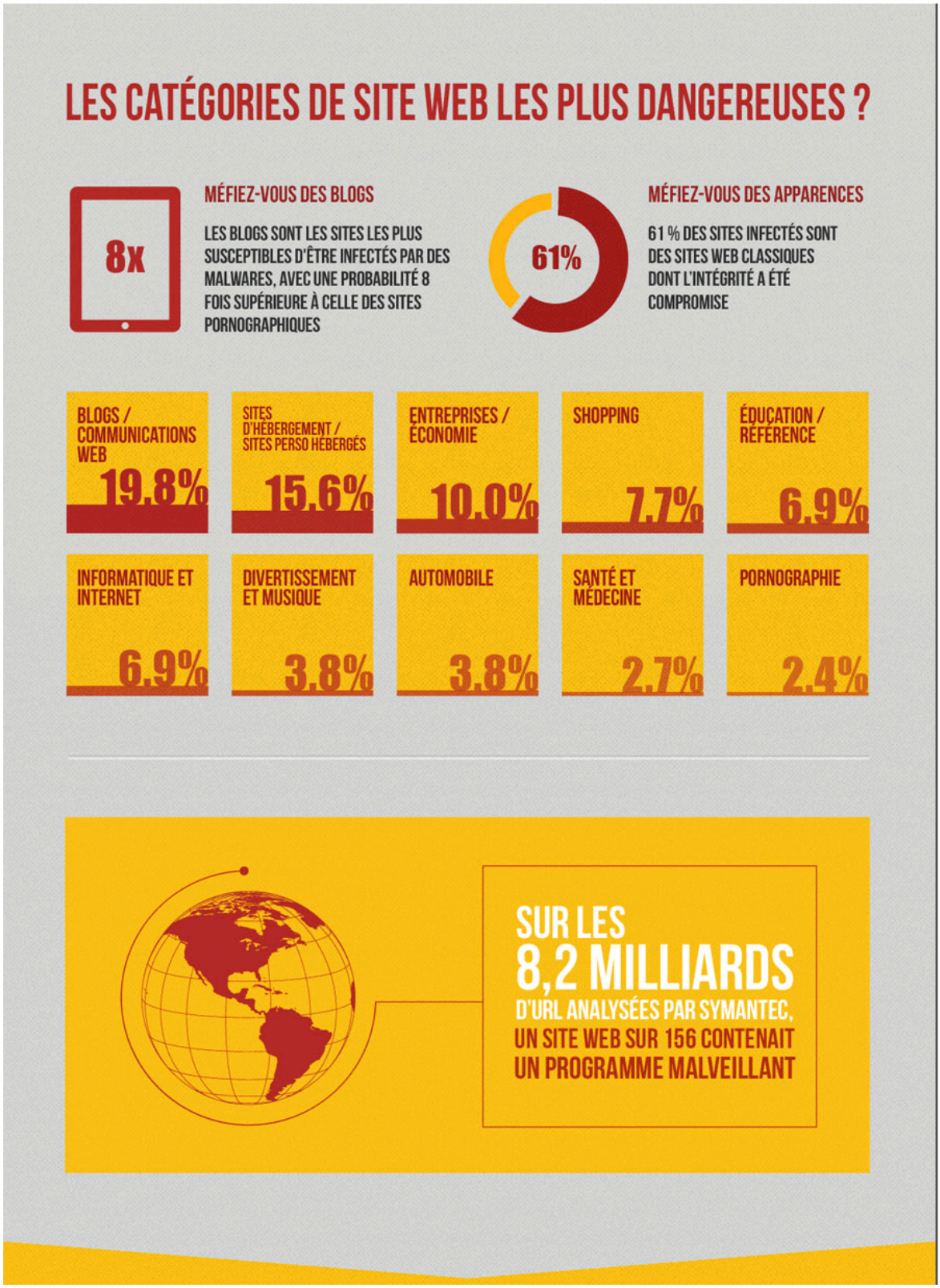
ATTAQUES WEB



ATTAQUES RÉSEAUX



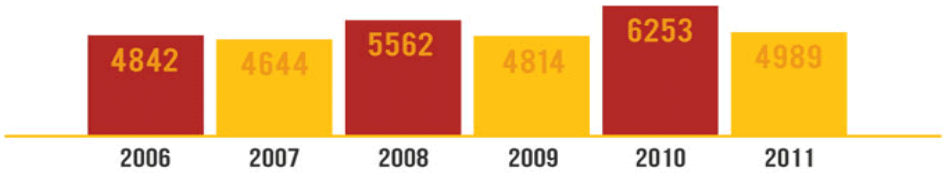
PHISHING


LES CATÉGORIES DE SITE WEB LES PLUS DANGEREUSES ?
8x
MÉFIEZ-VOUS DES BLOGS
LES BLOGS SONT LES SITES LES PLUS SUSCEPTIBLES D'ÊTRE INFECTÉS PAR DES MALWARES, AVEC UNE PROBABILITÉ 8 FOIS SUPÉRIEURE À CELLE DES SITES PORNOGRAPHIQUES
61%
MÉFIEZ-VOUS DES APPARENCES
61 % DES SITES INFECTÉS SONT DES SITES WEB CLASSIQUES DONT L'INTÉGRITÉ A ÉTÉ COMPROMISE
BLOGS / COMMUNICATIONS WEB 19,8%
SITES D'HÉBERGEMENT / SITES PERSO HEBERGÉS 15,6%
ENTREPRISES / ÉCONOMIE 10,0%
SHOPPING 7,7%
ÉDUCATION / RÉFÉRENCE 6,9%
INFORMATIQUE ET INTERNET 6,9%
DIVERTISSEMENT ET MUSIQUE 3,8%
AUTOMOBILE 3,8%
SANTÉ ET MÉDECINE 2,7%
PORNOGRAPHIE 2,4%
SUR LES 8,2 MILLIARDS D'URL ANALYSÉES PAR SYMANTEC, UN SITE WEB SUR 156 CONTENAIT UN PROGRAMME MALVEILLANT

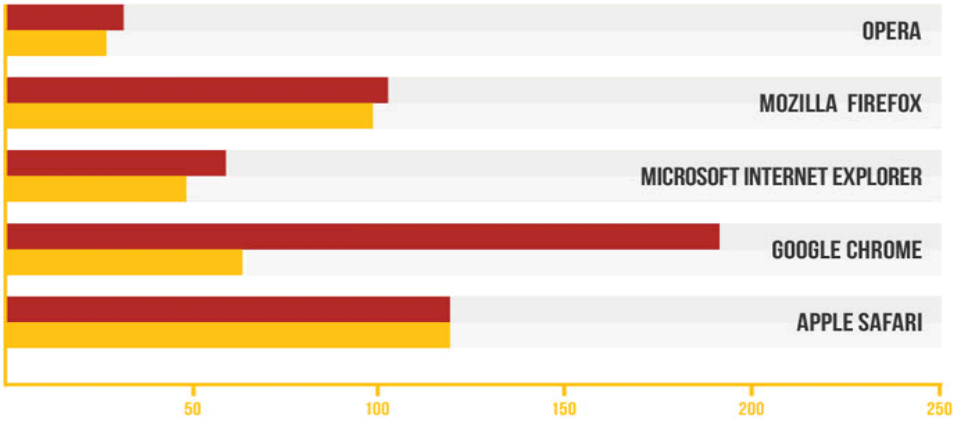
QU'EST-CE QU'UNE VULNÉRABILITÉ ?

UNE VULNÉRABILITÉ EST UNE ERREUR DE CODE OU UN DÉFAUT DE CONCEPTION QUI PERMET À UN HACKER DE COMPROMETTRE LA DISPONIBILITÉ, LA CONFIDENTIALITÉ OU L'INTÉGRITÉ D'UN SYSTÈME INFORMATIQUE.

NOMBRE TOTAL DE VULNÉRABILITÉS DÉTECTÉES ENTRE 2006 ET 2011



VULNÉRABILITÉS DES NAVIGATEURS EN 2010 ET 2011





36 % DES SITES WEB ANALYSÉS PAR SYMANTEC ÉTAIENT VULNÉRABLES AUX ATTAQUES DE MALWARE



INTERNET HÉBERGE 644 MILLIONS DE SITES WEB*



PLUS DE 230 MILLIONS DE SITES POURRAIENT DONC ÊTRE COMPROMIS

Figure 9 : Infographie de Symantec (https://www.symantec-wss.com/fr/malware-infographic)

2.2. Quelles sont les attaques les plus utilisées et comment s'en prémunir ?

La liste ci-dessous est non-exhaustive, car cela dépend des services installés sur le serveur. Cependant, celle-ci permet de se rendre compte du nombre de possibilités impressionnantes de tentatives de corruption de services.

2.2.1. Les attaques bruteforce SSH

On ne présente plus le service SSH tellement utilisé pour l'administration des serveurs Linux ! Celui-ci est souvent placé sur le port 22 par défaut. Les robots passent donc dessus et tentent de se connecter avec un très grand nombre d'identifiants très souvent utilisés : « root », « admin », « test », « user », « administrator »,… Ils essayent d'accéder au service SSH avec des mots de passe très simples comme « azerty », « qwerty », « god »… ou utilisent des générateurs de mot de passe. Il est donc préférable de changer le port par défaut afin de bloquer toutes les IPs qui tentent de se connecter sur le port 22. Après, il est souhaitable d'avoir un Fail2Ban lié à un iptable afin de bloquer ces IP à toutes autres tentatives.

2.2.2. Les attaques sur les mails : POP3, IMAP, Exchange

Les courriels sont aussi très sensibles, car ils contiennent un très grand nombre d'informations. Souvent, les mots de passe sont envoyés sur ceux-ci ou les réinitialisations. Il est donc primordial de protéger au maximum ces tentatives d'accès. Les accès se font souvent par webmail ou directement sur POP3, IMAP ou Exchange. Il faut donc analyser avec Fail2Ban les tentatives d'accès infructueux, vérifier le nombre d'envois dans la queue d'envoi.

2.2.3. Les attaques FTP(s).

Le protocole FTP est très souvent utilisé sur les serveurs pour déposer des fichiers. Une fois le fichier déposé sur un espace, celui-ci est bien souvent accessible en sur Apache et celui-ci peut être interprété par PHP/CGI/PERL… Il est donc conseillé d'utiliser des mots de passe forts en utilisant et mélangeant des caractères spéciaux, numériques et majuscules et d'avoir également un IP2Ban sur ce service afin de bloquer les attaques par bruteforce qui pourraient compromettre le serveur.

2.2.4. Les attaques IRC

Un serveur IRC sert à la création de salons sur lesquels des clients, « les chatteurs », peuvent discuter en temps réel. Le protocole IRC est assez simple (je vous renvoie à developpez.com qui explique très bien son fonctionnement). Ce protocole étant ouvert et très souvent mis en place sur les serveurs de jeux est très facilement attaquable. Les attaques passent souvent par un très grand nombre de proxy et tente de bruteforcer le mot de passe du modérateur ou administrateur du salon.

2.2.5. Les attaques DOS et DDOS (SYN Flood)

Les attaques par déni de services sont très souvent utilisées pour surcharger le serveur et rendre le service indisponible. Il existe deux sortes d'attaques : les DOS et les DDOS. Les attaques DOS sont occasionnées par un seul ordinateur qui tente de rendre inaccessible un service ; cela est très facilement bloquable, car il ne s'agit que d'une adresse IP. Les attaques DDOS utilisent quant à elles des Botnets (PCs zombie) afin de faire un très grand nombre de demandes, il est donc difficile de voir si le serveur est attaqué ou si le site « BUZZ » il faut donc utiliser un système de localisation d'IP afin de voir la provenance. Ces attaques sont les plus difficiles à bloquer, car il faut distinguer les vraies demandes des fausses.

2.2.6. Les attaques VOIP, SIP/Asterisk

Les serveurs de voix sont aussi mis à l'épreuve. Ils peuvent être utilisés pour téléphoner gratuitement ou se faire passer pour quelqu'un d'autre. Les panneaux d'administration comme FreePBX ou Asterisk arrivent sans aucune protection par bruteforce et avec des identifiants par défaut. Ils doivent être configurés par le client afin de ne pas avoir de mauvaises surprises.

2.2.7. Les brutesForces CMS/Panel admin

Les pages d'identification sont très vulnérables au bruteforce. Par exemple, le CMS WordPress subit actuellement de très grosses attaques sur les pages d'identification, car celui-ci par défaut n'a pas de module qui détecte le bruteforce. Il est donc conseillé de mettre un captcha et/ou un système de détection de bruteforce. Durant la présentation du mémoire, je vous projetterai une petite vidéo qui montre un de nos serveurs se faire bruteforcer la page appelée « wp-login.php ». Cette attaque est de petite importance ; cependant, les fichiers de logs grandissent très vite et cela peut surcharger un serveur assez rapidement.

2.2.8. Les scans de ports TCP/UDP

Les scans de ports sont bien souvent la première analyse faite par les pc zombies. Ces scans permettent de vérifier un range d'adresses IP en vérifiant si les serveurs répondent bien au ping. Cela permet aussi de vérifier les ports ouverts afin de faire une liste des protocoles et souvent des versions utilisées sur ces différents serveurs. Il en résulte donc que l'on peut voir les différentes failles/attaques possibles sur ce range d'IPs. Il est préférable de surveiller ces scans et d'avoir les dernières versions d'outils installés sur le serveur. Les outils afin de surveiller cela sont logwatch et iptable.

2.2.9. Les failles présentes dans les CMS/modules

Les erreurs se situent très souvent ici, il s'agit de CMS non mis à jour, étant donné que ceux-ci sont très souvent Open source (WordPress, Joomla, Drupal, …) quand une faille est corrigée il existe des « . diff » qui permettent de voir la différence entre une ancienne version et une nouvelle, il est donc très facile de voir si le correctif est pour de la sécurisation ou de l'optimisation. Une fois une faille corrigée et publiée, les attaques sont souvent plus importantes, car un grand nombre de personnes ne mettent pas à jour leur CMS. Souvent, les webmasters ne comprennent pas la nécessité de mettre à jour celui-ci s'il fonctionne bien. Cela est souvent vu comme une perte de temps, car les modules ne sont souvent pas compatibles avec les nouvelles versions. Cependant, il est très important de mettre à jour les CMS et module et de sécuriser les parties d'administration via un « . htaccess » afin d'avoir une double authentification.

2.2.10. Le spambot dans les formulaires/forums

Cette attaque est une des seules qui n'a pas pour but de prendre possession du site, mais bien de le polluer afin de générer des liens de retours et d'avoir un meilleur référencement. Pour se protéger de cela, il existe plusieurs moyens. Cependant, ceux-ci sont souvent cassables ; le premier est de mettre un captcha sur les formulaires. Toutefois, certains bots ont la possibilité de lire ces captchas. La deuxième façon est la validation par email ; dans beaucoup de cas, les emails utilisés sont faux et donc pas relevés pour la validation. Sinon, il existe certains modules comme Akismet pour WordPress qui permet de signaler les IPs qui polluent votre site afin de les bloquer automatiquement.

2.2.11. Les bruteforces sur les moteurs SQL

Les bases de données contiennent souvent des tas d'informations critiques comme la liste des clients, des fournisseurs, des factures… Il est donc très important d'avoir une bonne intégrité sur ces données. Les bruteforces sur les moteurs SQL sont assez rares, car il existe très souvent une protection native (MySQL : Flush Host) ; cependant, il nous arrive souvent de voir des petites attaques sur le port 3306. Il est donc important d'avoir de bons utilisateurs

et mot de passe, de ne pas autoriser toutes les IPs à se connecter sur la base, d'utiliser IP2Ban. Si la base de données n'est lue qu'en internet (localhost), il est donc conseillé de couper le port 3306.

2.2.12. Les injections SQL

Les injections SQL sont aussi très souvent exploitées sur les sites ; très souvent, les CMS acceptent des POST ou GET sans trop les vérifier et les utilisent pour faire les requêtes SQL. Il est donc possible de récupérer des informations que l'on pensait non accessibles. Pour se prémunir de cela, il existe certains modules Apache comme « mod_security » ou « sushoin » qui permettent de bloquer des requêtes si celles-ci semblent anormales.

2.2.13. Le social enginering

Celle-ci est la plus compliquée à contrecarrer, le « social enginering » étant le fait qu'une personne mal intentionnée se fasse passer pour une autre afin d'avoir ses mots de passe. Par exemple dans une grosse entreprise, une personne téléphone en se faisant passer pour l'informaticien et demande les mots de passe de la secrétaire afin de vérifier X ou Y. Bien souvent, les personnes donnent leurs mots de passe sans trop réfléchir. Il est donc très conseillé de faire une petite formation aux employés afin de leur expliquer quelques conseils élémentaires de sécurité informatique.

2.3. Quelles sont les pertes pour les datacenter/hébergeurs ?

Aujourd'hui, en Europe, nous parlons de moins en moins du prix de la bande passante. Cependant, au Canada, les offres internet sont bien plus onéreuses et bien plus limitées : par exemple, pour une connexion ADSL 25/15M ayant 75 Go de bande passante, cela coute 80 $/mois. En Belgique, cette offre coûterait 35 EUR et aurait très probablement une bande passante illimitée. Il est donc très important de bloquer cette attaque afin de réduire la bande passante et donc, le prix de la facture.

De plus, les attaques font travailler les serveurs. Cela implique qu'ils chauffent plus, qu'ils consomment plus et qu'ils sont plus lents. Si ces tentatives d'intrusion fonctionnent, cela ralentit le serveur et peut lui donner une mauvaise réputation au niveau de l'adresse IP.

2.4. Un phénomène de mode ?

Effectivement, les attaques augmentent d'année en année. Les botnets deviennent de plus en plus gros et les propriétaires de ces botnets commencent à devenir très influents. Peut-on dire que c'est un phénomène de mode ou une activité en pleine expansion ? Il faut savoir qu'il y a aussi un très gros aspect financier là-dessous. Certains botnets appartiennent à de grosses sociétés ou pays. Nous avons constaté une baisse des attaques durant les grandes vacances ; les employés étaient très certainement en congé durant ce laps de temps. De plus, si vous cherchez un peu sur certains forums, vous trouverez des botnets à louer à l'heure.

2.5. Pourquoi tant de violence ?

Dans un cas très important, les attaques ne sont pas ciblées. Ce sont des attaques de range d'adresses IP prise au hasard avec un premier scan pour vérifier que les serveurs répondent bien, suivis d'un scan de port pour vérifier quels sont les services installés puis les attaques. Cela a pour but d'augmenter le nombre de machines zombies qui peuvent attaquer (Plus le nombre de machines est important et diversifié, plus l'attaque sera lourde).

Le second cas est l'attaque ciblée. L'attaquant connaît le serveur qu'elle attaque pour le rendre indisponible (Deny de service) ou pour le brutforcer et prendre les informations présentes sur le serveur. Ce second type d'attaque est la plus dangereuse, car elle risque d'arriver fréquemment.

L'une des plus grosses attaques que j'ai pu analyser est l'attaque d'un site de téléréalité assez connu, près de 140.000 IP différents dans le monde se sont connectés en moins de 20 minutes sur la même page d'identification afin de bruteforcer le système d'authentification. Cette page n'avait malheureusement pas été protégée par le bruteforce ou par la double authentification par .htaccess qui découragent dans un très grand nombre de cas ce type d'attaque.

2.6. Quelles sont les différentes solutions pour se protéger de cela ?

Actuellement, on peut différencier 3 sortes de protections :

2.6.1. Les protections au niveau des applications

Celles-ci sont utilisées directement au sein de l'application ; par exemple, une page d'authentification vérifie le nombre de fois que le client tente de s'authentifier et bloque si trop d'accès infructueux ont été tentés. Une des autres protections est d'utiliser une double authentification comme une validation par SMS ou génération d'un Token. N'oublions pas aussi le Captcha afin d'éliminer les robots.

2.6.2. Les protections au niveau de l'environnement

Celles-ci sont souvent propres au système d'exploitation. Par exemple, sous Linux, nous allons installer IPtable couplé à Fail2Ban qui va bloquer les différentes attaques comme le Scan de port, tentative d'intrusion sur différents services… Sinon, sur Windows, il existe des solutions anti-virus/Parfeux spécialisées pour les serveurs.

2.6.3. Les protections réseau

Celles-ci sont les plus difficiles à mettre en place, car elles demandent du matériel très spécialisé et très onéreux. Elles ne sont utilisées très souvent que par de très gros hébergeurs. Lors de mon stage chez PlanetHoster, nous avons pu mettre en place une solution de protection nommée Arbor qui permet de filtrer les attaques afin de laisser passer le trafic sain seulement.

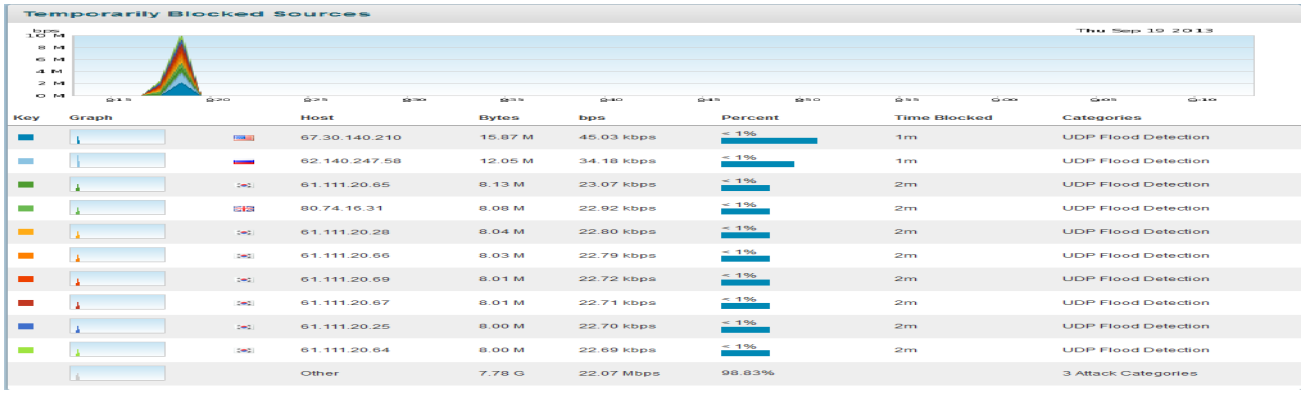


Figure 10 : Petite attaque DDOS de 10 Mbps sur un de nos clients filtrée par Arbor

2.7. Quelles sont les dernières fuites de données connues ?

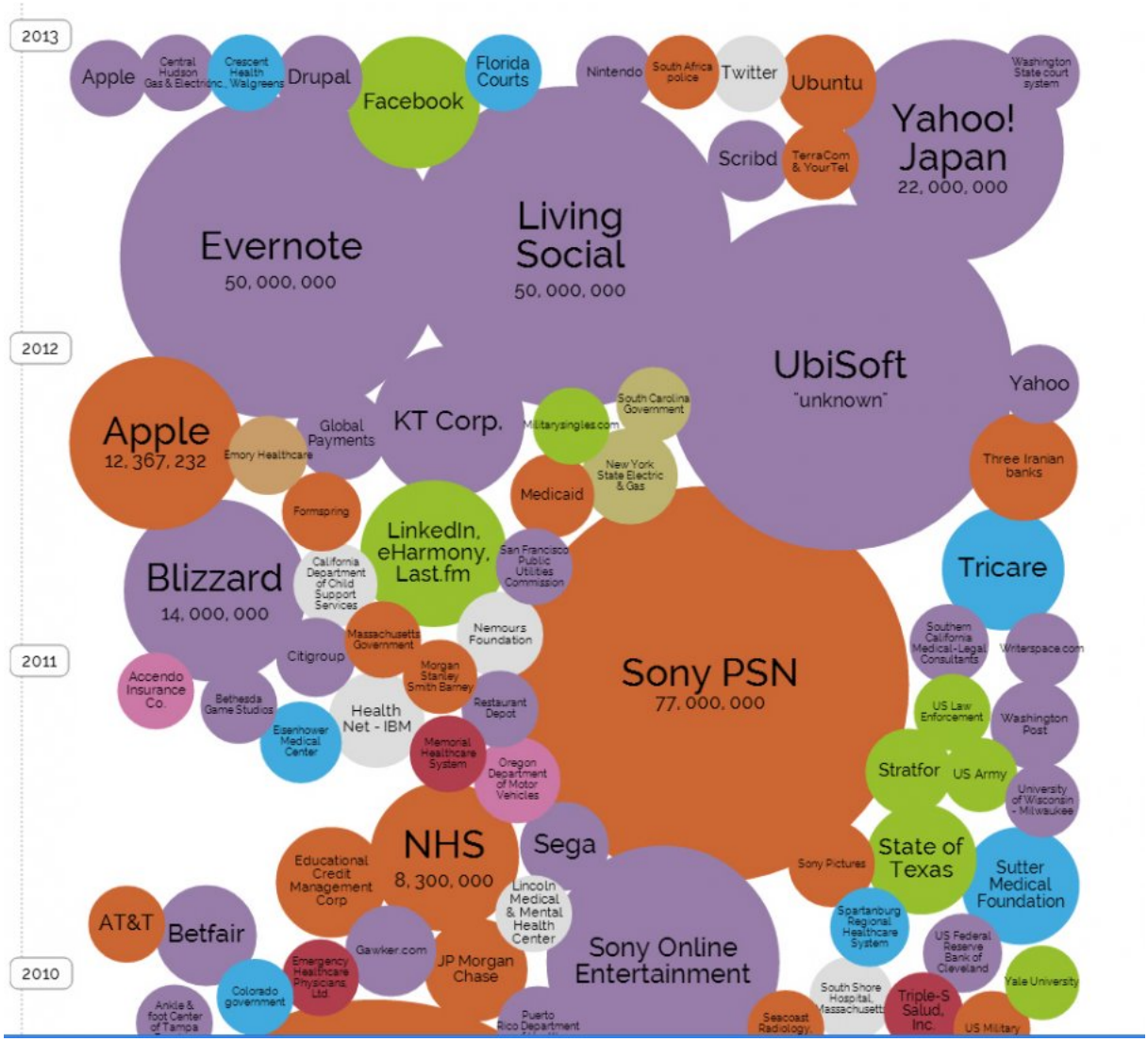


Figure 11 : Les fuites de données (compagnies) connues entre 2010 et 2013

- Toutes les compagnies peuvent être touchées par ce genre d'attaque. L'une des plus importantes est celle de Sony qui s'est vu voler une base de clients de près de 77.000.000 client. Ceux-ci avaient des cartes de crédit associées à leurs comptes afin d'acheter directement les jeux. Cela a eu comme effet une très grosse diminution de la valeur en bourse et des clients mécontents.
- Cela ne concerne pas seulement les compagnies, mais également beaucoup d'organismes gouvernementaux, militaires… qui peuvent être touchés par ce genre

de fuite. Un des sites très connus est WikiLeak qui a publié un grand nombre de documents secrets.

Pensez-vous vraiment que seules de grandes compagnies comme Apple, Ubuntu, Sony, Twitter ou encore LinkedIn se font attaquer ? Celles-ci ont normalement beaucoup de moyens pour se défendre, car c'est leur business. Que pensez-vous de votre banque ? De votre fournisseur Internet ? De votre courtier d'assurances ?

2.8. L'augmentation des centres de traitement de calculs

Parlons un peu de l'augmentation des centres de traitement de calculs. Il n'y a pas encore longtemps, seuls les CPU étaient utilisés pour casser les mots de passe MD5. Après certaines recherches, des hackers ont utilisé et le GPU de la carte graphique, car ceux-ci arrivent à 1000GFLOPS. Maintenant, des services comme Amazon Cloud, BitCoint ou encore des Botnets vous permettent de casser des mots de passe/cartes bancaires assez rapidement même si ceux-ci sont chiffrés.

Donc, même si des données chiffrées en AES, MD5, SHA,… sont volées, il est fort probable que ces informations soient retrouvées ; cela n'est qu'une question de temps et de puissance. La meilleure façon de faire actuellement est de rajouter une « sel » aléatoire en plus du mot de passe afin de complexifier le cassage.

2.9. Quels peuvent être les avantages pour les hackers ?

Les avantages pour une entreprise peuvent être multiples :

- « L'espionnage industriel ou espionnage économique est l'espionnage qui vise le commerce, par opposition à celui, plus habituel, qui vise la sécurité nationale. Il peut être effectué par un gouvernement ou une entreprise privée. C'est le complément de l'intelligence économique dont les moyens sont légaux, mais le terme "espionnage" inclut aussi ces méthodes, dans le langage courant. Ces méthodes particulières ainsi qu'illégales incluent les pots-de-vin, le chantage, la surveillance électronique et parfois même la violence. Il peut être avantageux pour un gouvernement d'espionner

des entreprises privées et aussi à l'inverse, par exemple afin de pouvoir soumissionner pour un montant plus bas » dixit Wikipedia.

- Rendre inactif un concurrent afin de nuire à sa réputation : celui-ci sera privé de tous contacts électroniques comme ses mails, ses sites internet, ses outils en lignes… Cela peut paralyser et fragiliser une entreprise.

2.10. Quelles sont les bonnes pratiques à mettre en place ?

Les serveurs et applications doivent être sécurisés et garantir la protection et la confidentialité des données des entreprises et des professionnels utilisant les services du réseau. La sécurité est basée sur l'authentification et la vérification des membres du réseau. Aucune information ne peut être postée anonymement et le cryptage des communications de bout en bout du réseau (certificats émis par une autorité et transmissions cryptées au moyen du protocole de communication HTTPS) ou entre une entreprise et ses clients.

Il faut de plus garder tous les logs de connexions, de modifications afin de tracer d'où vient le problème afin de le localiser et de le fixer. Sans cela, les administrateurs ne peuvent pas travailler avec une vision claire ; il est donc essentiel d'avoir des logs clairs et précis avec l'heure, l'IP et l'action.

2.11. Quelles sont les règlementations/lois en vigueur ?

Les Botnets ont conduit la justice à se pencher sur la question de la protection des données personnelles en imposant à certains éditeurs de réseaux sociaux de modifier leurs politiques de confidentialité à l'avantage des utilisateurs. Cependant, les systèmes de législation sont différents d'un pays à un autre. Les pays germano-latins ont adopté un système de législation pénale tandis que les pays anglo-saxons ont choisi la voie d'une législation civile, beaucoup plus permissive.

Si la législation protège plus ou moins bien les relations verticales entre utilisateurs et éditeurs de services, elle reste silencieuse sur les relations horizontales entre les différents utilisateurs.

Avec Facebook, la question était posée de savoir qui peut avoir accès aux informations personnelles. L'essor de la géo localisation pose désormais la question de savoir qui peut connaitre les faits et gestes de chacun à l'intérieur de l'outil.

2.12. Quelle importance donner aux DNSBL ?

Les DNSBL sont des blacklist qui ne donnent pas toute leur liste d'adresses IP afin de ne pas se faire copier leur contenu et afin qu'on y effectue des requêtes très souvent. Le DNS Black Listing (DNSBL) est une méthode permettant de consulter une liste noire d'émetteurs de courriers électroniques en utilisant le protocole DNS. Le nom DNS Black Listing vient de l'expression anglaise « black list » qui signifie « liste noire ». Les DNSBL font l'objet de controverses depuis la création du premier système en 1997. Les gestionnaires de serveurs de messagerie qui y ont recours les considèrent comme des outils antispam efficaces, tandis que d'autres y voient une forme de censure et d'arbitraire, les critères d'inclusion et d'exclusion relevant du seul gestionnaire du DNSBL. Certains DNSBL ont fait l'objet de poursuites judiciaires intentées par des spammeurs. Il suffit de prendre l'IP qu'on veut interroger, la retourner (192.0.0.1 devient 1.0.0.192) et de faire un nslookup sur 1.0.0.192.dnsrbl.exmple.net Si cela vous retourne une entrée comme 127.0.0.1, c'est que l'IP est blacklisté sur la DNSBL.

Certains DNSBL comme SpamHaus (organisation connue pour lutter contre les courriels non désirés) ont subi durant une dizaine de jours des attaques DDoS majeures suite à leur mise sur liste noire de CyberBunker. Selon le fournisseur de transit Akamai, interrogé par le New York Times, cela aurait atteint parfois un débit de 300 Gb/s. Des ralentissements du réseau pourraient même avoir été constatés selon un FAI Britannique contacté par The Guardian.

3. Présentation du projet

3.1. Introduction

La décision de créer un outil afin de protéger les serveurs de ces attaques répond à un triple besoin :

- La nécessité de sécuriser les informations de nos clients contre tous vols numériques. Cela en va de notre réputation ; il faut que les serveurs soient robustes et ne donnent pas d'informations trop facilement.

- La volonté d'utiliser moins de bande passante, de CPU, de RAM afin de réduire les coûts d'exploitation des serveurs. Ceux-ci ont souvent une charge élevée, car ils sont très souvent bruteforcés et/ou scannés.

- Le désir d'offrir à tout le monde une liste de sécurité afin d'avoir une meilleure réputation sur internet.

3.2. Analyse fonctionnelle

L'analyse fonctionnelle est une partie cruciale du projet. Elle est destinée à constituer un cahier de charges de l'application. Une fois le cahier de charges approuvé, le propriétaire de l'application doit s'y tenir et ne peut changer les grandes lignes sans quoi les nouvelles modifications feront l'objet d'une requête d'une prochaine version. C'est la méthode que j'avais pu observer en Europe lors de mes stages chez IBM ; cependant, chez PlanetHoster, cela est très différent. La méthodologie appliquée se rapproche très fort de SCRUM avec des SPRINT et une amélioration constante de l'application.

Lors de mon stage, j'ai été convié à participer à toutes les réunions d'analyse du projet, à rencontrer toutes les personnes qui participeront de près ou de loin au projet et à me familiariser avec tous les services mis en place sur les serveurs.

J'ai donc été suivi de très près par la direction avec laquelle nous avons bien étudié les différentes attaques reçues en vue de trouver la façon idéale de les bloquer.

Les clients s'écartent parfois de l'utilité primaire de l'application et il est alors nécessaire de les canaliser afin qu'ils aient une vue précise de l'application et du temps qui nous est imparti.

L'analyse fonctionnelle a été rédigée sans prendre en compte les fonctionnalités de Drupal (le CMS qui m'est imposé), car la technique ne doit pas influencer la partie fonctionnelle.

Les différents types de contenus sur l'intranet seront les suivants.

3.2.1. Les attaquants

Les attaquants sont les principales informations qui constitueront notre blockinglist. Il s'agit essentiellement d'adresses IP ou de range qui attaquent les serveurs de PlanetHoster.

- Informations venant des « attaquants » :
  - IP
  - Reverse DNS
  - ASN Number
  - Pays
  - Dernier type d'attaques
  - Nombre d'attaques
  - Premières attaques enregistrées
  - Dernières attaques enregistrées
  - Dernier serveur attaqué
  - Nombre de serveurs
  - Emails de suppression
  - Date de suppression

Ces informations sont très importantes et ne pourront pas être modifiées autrement que par le système afin de garder une intégrité des données.

Le système devra, au moment d'ajouter les attaquants, définir le type d'évènements le plus approprié à celui-ci.

3.2.2. Les évènements

Un « évènement » est une attaque enregistrée par le système, qui est directement liée à un attaquant. Il annonce et décrit (le jour, l'heure, le type d'attaque et le serveur attaqué). Il permet également, lorsque l'utilisateur consulte sur le site de voir les attaques qui lui sont reprochées afin de corriger cela avant de demander un déblocage de son adresse IP. Il faut donc voir cela comme des logs qui permettront d'avoir plus de détails sur le pourquoi du comment.

3.2.3. Les serveurs

Il est très important de vérifier quels sont les serveurs qui utilisent la liste afin d'avoir une meilleure vision du réseau que nous allons protéger.

Cela va permettre de voir le nombre de rapports d'attaques, du dernier téléchargement de la liste et de vérifier les reverse DNS.

Tout cela devrait concourir à configurer au mieux notre parc de serveurs afin d'avoir une protection homogène et qui s'autogère automatiquement.

3.2.4. Les autres blockings liste ou RBLs

Afin d'éviter d'avoir des faux positifs, il est recommandé de comparer ces résultats avec d'autres RBLs ; cependant, il n'y a aucun intérêt à prendre directement l'information chez eux. La valeur ajoutée est juste de confirmer si une IP est bien mauvaise si nous avons seulement une seule attaque dans notre base de données.

On y trouvera d'une part, plus d'autres données dans ces blockings liste afin de récolter davantage d'informations afin que nos données soient les plus complètes.

D'autre part, on pourra aussi vérifier rapidement sur le site si votre IP est bloquée au niveau de GreenSnow ou d'une autre RBL. Cela permet d'avoir une meilleure vue sur ce type de blocage. À savoir que les RBLS utilisés seront : Blocklist.de, SpamHaus , SpamCop, TOR, BOGON, DSHIELD, HONEYPOT et RBN.

3.2.5. Les statistiques publiques totalement transparentes

Contrairement aux autres listes de blocage, notre système sera totalement transparent. Il sera possible à tout un chacun de voir les statistiques afin de comprendre le nombre d'attaques rapportées sur les 30 derniers jours, les pays qui attaquent le plus et le type d'attaques le plus utilisé afin de pouvoir s'en prémunir. Les statistiques devront être très simples à visualiser afin que les visiteurs se rendent bien compte que l'internet n'est pas un endroit sécuritaire et qu'il faut bien s'en protéger lorsqu'on met en place une solution sur le Cloud.

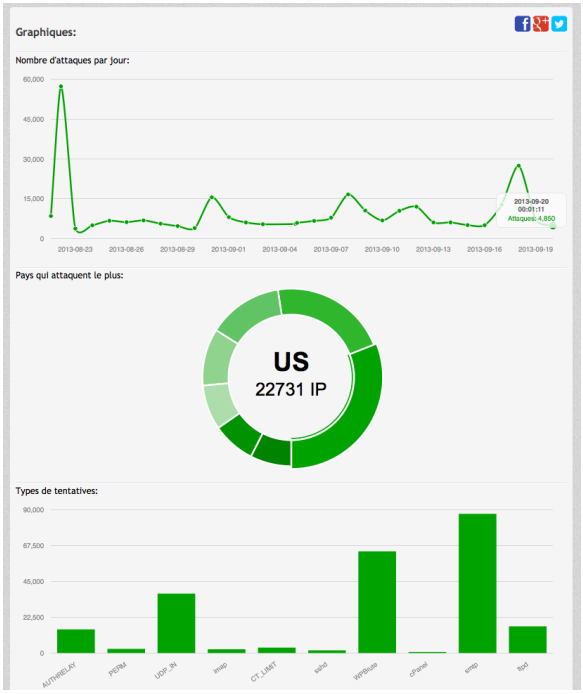
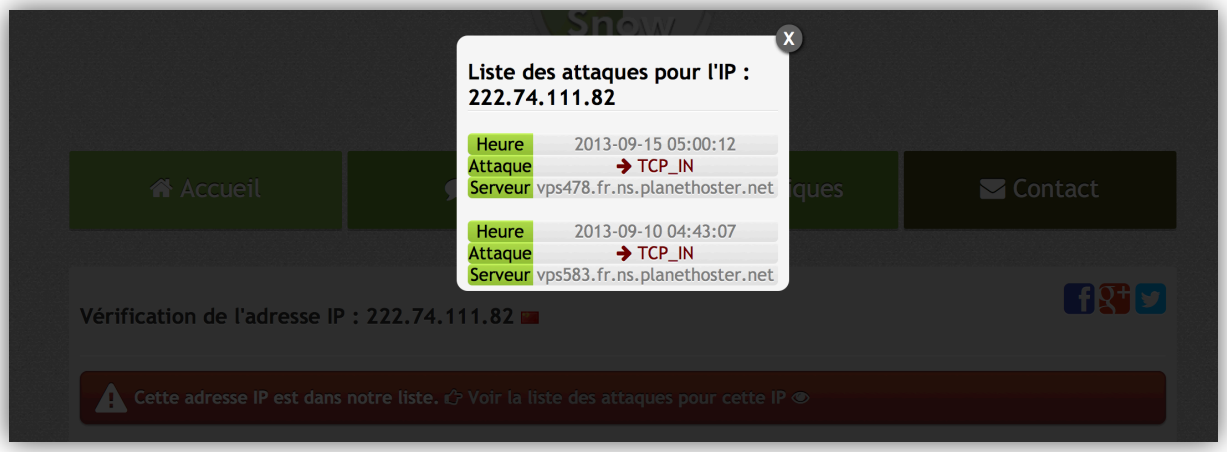


Figure 12 : *Affichage de la page de statistiques*

3.2.6. Les vérifications par les utilisateurs

Cette fonctionnalité permet aux utilisateurs de vérifier eux-mêmes si leur IP est bloqué et si c'est le cas, d'avoir les journaux d'attaques afin de comprendre ce qui leur est reproché.



3.2.7. La suppression rapide

Cette page permet aux utilisateurs de demander un dé-blacklistage de leur IP ; pour cela, un email de validation leur sera envoyé afin de confirmer leur identité.



Figure 13 : *Affichage d'une adresse IP et du formulaire afin de la retirer.*

3.2.7.1. La mise à jour automatique par les serveurs

La seule possibilité de rajouter une adresse IP est qu'un serveur nous alerte d'une attaque. Il faut donc que celui-ci communique avec notre système afin de rapporter les IP apparaissant dans les logs. Nous avons donc conçu un système basé sur la technologie Fail2Ban qui permet de bannir une IP dans iptable et de nous alerter afin de recenser ces IP qui tentent de forcer le système. Cependant, pour des raisons de confidentialité et afin de garder le secret de fabrication, je ne pourrai vous en dire plus dans ce mémoire. Sachez cependant que ce système a été exclusivement conçu pour PlanetHoster et que nous ne comptons pas pour le moment partager ce fonctionnement.

3.2.7.2. La page d'aide

Cette page sera publique et servira à tous afin de donner plus de détails sur les différentes attaques, d'aider le visiteur à supprimer son IP, à lui expliquer rapidement le but du projet.

3.2.7.3. La page de contact

La page de contact permet au visiteur de nous contacter rapidement.

En cas d'erreur sur le système, celui-ci peut ainsi avoir plus d'informations ou prendre contact avec nous en vue d'un partenariat potentiel.



Figure 14 : *Affichage du site via un iPhone et un iPad*

3.2.7.4. Un site totalement responsif

Un très grand nombre de visiteurs sont souvent sur leur téléphone, tablette. Il est donc primordial que les pages soient totalement optimisées pour les Smartphone. Nous avons donc pris « Front Awesome » afin d'avoir un système ergonomique. Je vais donc vous faire une petite capture d'écran sur un iPad ou iPhone afin de voir le rendu.



Figure 15 : *Affichage du site via un iPhone et un iPad*

3.2.7.5. Workflow sur les blacklistage

Certaines IP « sensibles » doivent être soumises à une approbation avant de pouvoir être listées. Le « processowner » doit donc recueillir l'avis d'une ou plusieurs personnes déterminées avant de pouvoir valider l'adresse IP. Concrètement, il devra être en mesure de prouver qu'il a demandé et obtenu cette approbation avant d'avoir publié le contenu révisé.

Nous avons choisi de ne pas implémenter un véritable workflow d'approbation. Néanmoins, nous répondrons à cette obligation en offrant au « processowner » la possibilité, à chaque modification, de garder une trace « logging » de celui-ci, la preuve de l'approbation obtenue.

3.2.7.6. Notification en cas de blacklistage

La notification est un processus qui permet de prévenir les personnes concernées que leur IP/ASN/Serveur ou leurs serveurs subissent une attaque.

Nous préférons ne pas rendre ce processus totalement automatique afin de ne pas surcharger les clients de mails, mais laisser plutôt le choix au « propriétaire du serveur » de l'opportunité ou non d'envoyer un e-mail pour annoncer un blocage sur le serveur. Cela permettra d'éviter d'envoyer des dizaines d'e-mails à la moindre petite attaque.

Dans la pratique, au moment où le « propriétaire » voudra s'inscrire sur GreenSnow, il devra remplir/mettre à jour certaines données :

- Son serveur (IP)
- Son email et/ou contact(s)
- L'adresse IP de ses clients
- corrections éventuelles d'autres méta datas
- + désirez-vous envoyer une notification automatique ?
-

Selon la réponse à cette dernière question, le système enverra ou non un mail automatique à toutes les personnes appartenant aux « contacts » listés dans le champ « Target Audience », afin de les prévenir que « l'IP a été bloquée et qu'elle est maintenant consultable et de voir la cause sur le site de GreenSnow ».

Deux remarques concernant cet e-mail :

— Le système devrait vérifier qu'il n'y a pas doublons dans la liste des destinataires du mail.

Les méta datas concernant la « Target Audience » permettent au « propriétaire » de définir les différents groupes de personnes dont les IP sont directement impactés par ce blocage.

3.2.7.7. Classification par type d'attaques

Le fichier texte de base nous donne toutes les différentes attaques. Cependant, pour certains serveurs par exemple ceux de jeux uniquement, le blocage des attaques comme du service IMAP, ou bruteforce de CMS n'est pas utile.

On sait déjà qu'il s'agira d'une arborescence d'au moins 3 niveaux.

Les différents types de fichiers sont

- Mod_security
- IMAP
- SSHD
- AUTHRELAY
- CT_LIMIT
- FLOOD
- ICMP_IN
- UDP_IN

Cette classification est très importante, et ce au moins à 2 titres.

D'une part, elle doit permettre aux utilisateurs de retrouver très facilement, et de savoir immédiatement, grâce à la classification, à quel type d'attaque de document ils peuvent s'attendre.

D'autre part, le système va utiliser la classification des IP pour réduire le nombre d'adresses IP à bloquer dans le système. En effet, chaque « machine » (cela peut être un équipement réseau ou un serveur) va bloquer la liste. Cela permet donc de bloquer moins d'adresses IP pour des VLAN de jeux ou si cela est un VLAN pour un serveur WEB. La configuration à appliquer sera donc différente selon le type de serveur mis en place.

3.2.7.8. Dashboard et tableaux d'administration

Les personnes exerçant le rôle d'administrateur chez PlanetHoster ont besoin de disposer d'une vue globale sur laquelle elle peut en un coup d'œil détecter les IPs qui sont proches de leur date de péremption (date prévue pour la rédemption).

Elles pourront ainsi déclencher les actions utiles afin qu'une IP devenue obsolète soit immédiatement maintenue.

Il s'agirait ici d'une sorte de tableau de bord représentant l'ensemble des IP (classés en fonction de leur attaque, ou selon d'autres critères à spécifier) associés à un code couleur selon qu'ils sont :

- Parfaitement saine (débloquée) — code vert
- En péremption (plus d'un mois) — code orange
- Bloquée (dans la liste) – code rouge

Il serait également très utile pour les administrateurs de l'application de pouvoir disposer de tableaux donnant une vue d'ensemble sur les serveurs qui utilisent les RBLS. Cela va permettre de voir le nombre de serveurs, leur RDNS, le dernier téléchargement et le dernier report d'attaques.

Une fois les 20 pages d'analyse terminées, le dossier a été envoyé pour approbation.

4. Analyse du stage

4.1. Administration du serveur de production

Durant l'analyse fonctionnelle, j'ai pu installer un serveur de développement sous l'environnement CentOS. C'est une demande de PlanetHoster de travailler avec ces technologies, car l'entreprise est partenaire avec cPanel. Le service IT qui devra reprendre la gestion du serveur doit en effet être compétent en ce qui concerne la technologie utilisée. J'ai donc installé cPanel et sécurisé près de 250 services dans un premier temps.

Toutefois, l'installation de MongoDB couplé à MySQL sur PHP5.4 ne s'est pas déroulée sans mal, car pour ce faire, PHP nécessite l'installation du connecteur approprié. Sans cela, PHP ne pouvait pas communiquer avec MongoDB.

Cependant, par la suite, pour des raisons de performance, nous avons dû changer le Handler PHP de SuPHP à FGCI afin que les pages chargent plus rapidement pour pouvoir répondre à de très nombreuses visites. Il est à noter que toutes ces étapes ont dû être documentées sur un wiki afin qu'une tierce personne puisse reprendre le contrôle du serveur.

4.2. Profilingue de Fail2Ban/iptable/netfilter

Ne connaissant pas encore parfaitement Fail2Ban, j'ai installé la dernière version, à savoir la 8^{e} (0.8.10) en date. Celle-ci est sortie près d'un mois avant le début de mon stage et j'ai pu constater que nombreux modules n'étaient pas encore développés sur la V0.8.10/9 ou existaient encore en version Alpha (Version Beta disponible pour les développeurs).

J'ai donc analysé les fonctionnalités de Fail2Ban qui reposent sur Netfilter afin de comprendre son fonctionnement, ses fonctionnalités de base. Ce service est une conception Open source et est utilisé sur la majorité des serveurs Linux par exemple celui de la maison blanche, de MTV, de Symantec, de Sony, etc.…

Un des grands atouts de ce service est qu'il est très flexible par défaut et permet, une fois quelques modules installés, de réaliser des tâches très complexes. Par exemple, la fonction de regex des logs est totalement ouverte, il est donc très facile de parser les logs du service que nous avons installé afin de trouver l'heure, l'IP, l'attaque…

Le changement entre les versions 7 et 8 est assez net, la version 7 étant plus rapide. Il y a également moins d'appels au fichier de logs et surtout une bibliothèque de modules très riche.

4.2.1. Installation du service dans le parc informatique

Suite au package du Fail2Ban, l'étape de mise en production sur un environnement de test de près de 50 machines a été mise en place. Pour cette implémentation, nous avons fait cela à la main afin de bien vérifier qu'il n'y avait pas de message d'erreur ou avertissement en cas d'incompatibilité. Les installations se sont pour la très grande majorité très bien déroulées. Nous avons repéré sur une machine un problème ; cependant, cela venait d'une repository du gestionnaire de paquet qui était introuvable. Nous en avons donc profité pour corriger cela.

Une fois le service installé et fonctionnant sur cet échantillonnage, j'ai très vite commencé à faire les pages de statistiques afin de voir le nombre de blocages, de téléchargements, de bande passante gagnée… ceci avec les procédures que PlanetHoster m'a apprises.

Les premiers retours des serveurs ont été très rapides, nous avons vu de très nombreux scans de port, et d'attaque sur des ranges, sur 50 machines nous avons reçu près de 800 IP distinctes dans les premières 2 premières heures, de provenance très exotique (USA, Chine, Russie, Taiwan, Thaïlande, Japon…) Après vérification avec d'autres RBLs, nous avions bien de mauvais IP en provenance d'un très grand botnet.

Ce test a duré près d'un mois et nous n'avons constaté qu'un très petit nombre de faux positifs. Cela était dans la grande majorité des cas, du a des clients qui ont plusieurs serveurs et qui utilisaient de mauvais identifiants sur plusieurs serveurs différents. Notre système a donc vu cela comme une attaque généralisée et a bloqué préventivement cette IP sur tout notre réseau à l'exemption de GreenSnow et PlanetHoster.net. Nous avons donc un peu changé l'algorithme afin de le rendre un peu plus permissif pour certains pays (ceux de nos clients : France, Canada, Belgique, Suisse…).

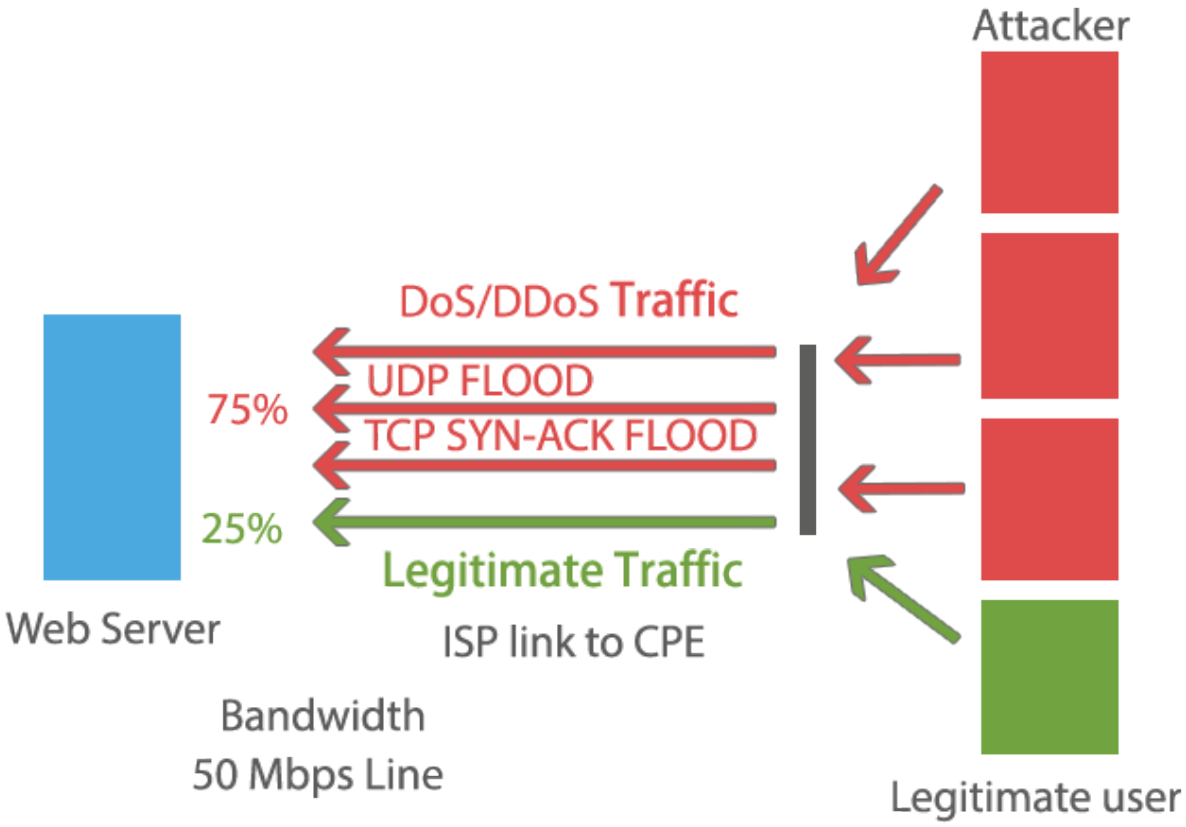


Figure 16 : *Schématisation du trafic légitime contre ceux ces attaquants.*

Après cet échantillonnage, il m'a été demandé d'implémenter la solution sur une autre range de serveurs cependant cette fois avec « Puppet Entreprise ». Ce procédé permet de ne pas rentrer manuellement sur le serveur, mais bien de basher les procédures d'installation et de les envoyer sur les serveurs directement. Cela permet donc d'administrer un nombre de machines très rapidement sans pour autant devoir se connecter.

Une fois cette installation réalisée sur ce nouveau bloc de serveurs, nous avons vu le nombre de rapports augmenter très fortement, car ces serveurs sont des serveurs mutualisés donc très fort utilisé, ceux-ci transmettent donc un très grand nombre d'informations à GreenSnow et téléchargent la nouvelle liste toutes les heures. Dans les premières heures, nous pouvons constater une baisse de trafic de près de 10 %. Cependant, il n'y a eu aucune plainte de clients. Nous devons voir ces retours sur le long terme et non sur les premières impressions. Un problème apparaissait tout de même après quelques mois sur certains serveurs ayant de très nombreuses connexions et de ressources assez limite : le fait de bloquer autant d'IP au niveau de l'iptable n'est pas forcément assez optimisé.

Il a donc fallu trouver une autre solution. Il est donc préférable de bloquer directement cela au niveau du réseau (Arbor) et non au niveau du serveur. Nous allons donc porter la liste directement sur le panneau d'administration de Arbor afin de filtrer directement le trafic selon le type de VLAN.

Nous avons donc trouvé un bon compromis, un blocage sur le réseau pour les IPs étant connu sur le différent RBL afin d'être certain que ces paquets n'arrivent pas sur les différents serveurs et un blocage des autres IP sur le serveur. À savoir que nous avons déterminé une rédemption d'un mois afin de limiter la grandeur de la liste.

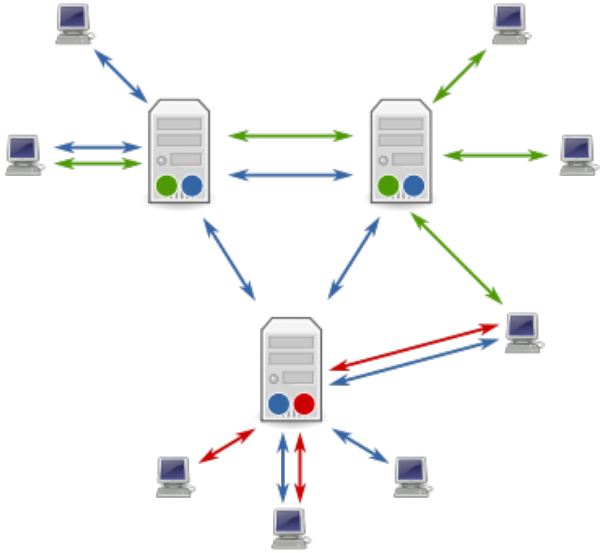


Figure 17 : *Les différentes interconnexions des protections chez PlanetHoster*

La majorité des serveurs sont donc en communication directe avec GreenSnow afin de rapporter les IP, et ces serveurs vont télécharger la liste et l'introduire dans l'Iptable toutes les heures.

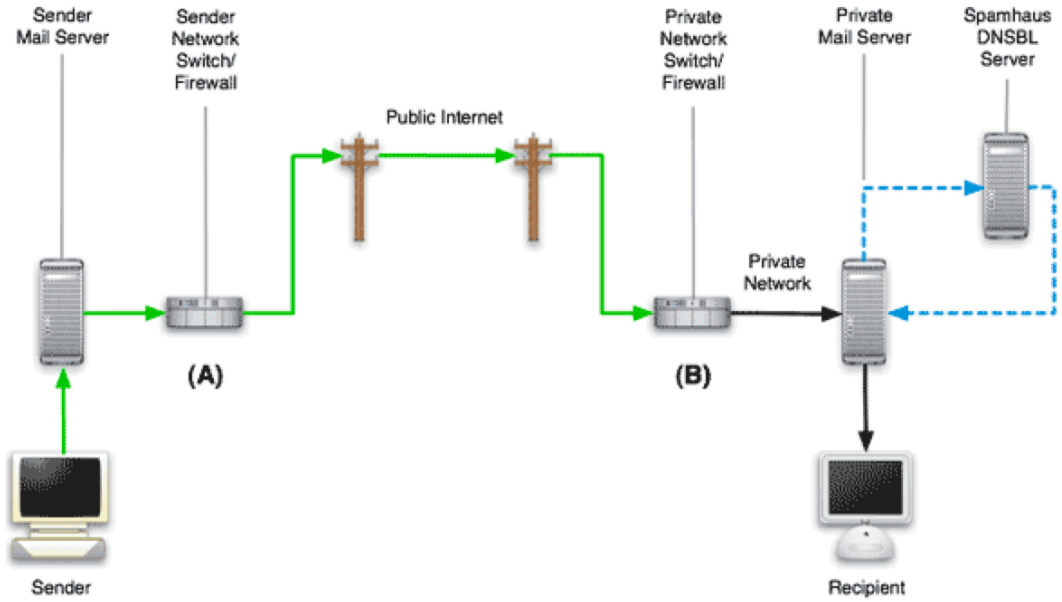


Figure 18 : *schéma de fonctionnement d'une DNSBL comme Spamhaus*

Les DNSBL sont très bien pour les envois d'emails qui peuvent attendre entre 1 à 2 secondes afin qu'on retourne un résultat ; cependant, dans notre cas nous devons avoir un système plus rapide. Il est donc impossible de fonctionner avec une interrogation DNS, car celle-ci prend trop de temps. Il faut donc directement charger la liste dans le serveur afin que l'IP source (sender dans l'exemple) fasse la demande.

4.2.2. Résultat obtenu suite à la mise en place de GreeSnow

Place au résultat que nous avons observé suite à la mise en place de ce système de blacklistage interne. Nous avons constaté une baisse au niveau de la bande passante et du CPU utilisé sur l'ensemble des machines (-10 %). Cependant, les bruteforces de WordPress continuaient à grande échelle. J'ai donc du coder des HoneyPot WordPress afin de récupérer un très large nombre d'adresses IP qui bruteforcent les formulaires d'authentification wp-login.php. L'une des attaques les plus importantes que nous avons pu observer est celle des bruteforce de WordPress (http://www.bbc.co.uk/news/technology-22152296) ; les analystes ont estimé le botnet à près de 90.000 machines zombie à l'heure actuelle. Cela correspond à une des plus grosses attaques observées sur un CMS. De plus, avec le temps celle-ci s'est aussi développée sur le CMS Joomla. À savoir qu'un grand nombre de sites tourne aussi sur la version 1.5.

Nous avons donc codé de fausses pages afin de récupérer ces adresses IP, nous avons mis en place une vingtaine de HoneyPot en place et nous avons récolté près de 1350 IP distinctes dans les moins de 12 heures par site (HoneyPot).

Les charges des serveurs et bandes passantes ont alors très fortement diminué. Il faut savoir que 1& 1 (société allemande) n'a pas pris les devants de l'attaque et qu'un très grand nombre de leurs serveurs sont tombés suite à ce genre d'attaque. De plus, une fois un CMS introduit, c'est celui-ci qui se met à attaquer afin de rentrer dans le BotNet. Donc une fois que le compte a été infiltré, celui-ci se met à attaquer et surcharge le serveur et augmente aussi la bande passante descendante.

Actuellement, ces listes sont gratuites et téléchargeables par toute personne voulant avoir une liste de mauvaises adresses IP. Cependant, vu le résultat obtenu, ces listes pourraient être vendues directement à des organismes comme Arbor afin que ceux-ci augmentent encore leurs performances.

Pour ce qui est du support, nous avons remarqué une nette diminution des tickets liés au hack, defaced, SPAM,… Cela a permis de mettre en place un très bon écosystème au niveau de l'administration. De plus, les clients savent maintenant vérifier si leurs IPs sont blacklistés ou pas sans devoir faire la demande par le service technique.

Le tout est administrable dans le back-office de GreenSnow sous forme très visuelle ; c'est donc très simple d'administration et de configuration.

4.2.3. Éducation

Avant de mettre le nouveau système GreenSnow en production, l'analyste et moi avons présenté officiellement celui-ci au directeur général et au responsable sécurité afin d'avoir leur accord de mise en production.

Une séance a été organisée afin de leur montrer le fonctionnement interne de l'application, mais également dans le but qu'ils en aient une bonne compréhension et sachent l'utiliser à bon escient. Le projet fut donc accepté avec enthousiasme par la direction.

Les techniciens s'occupant du support ont très bien accueilli le projet, car cela leur permet d'avoir un historique sur les IP des clients et d'avoir un outil afin de montrer aux différentes personnes la cause du blocage.

4.3. Relations humaines

Durant mon stage au Québec, j'ai pu observer la manière de fonctionner, comprendre le fonctionnement interne de la boîte et analyser celui-ci. J'ai constaté que les valeurs humaines des employés étaient mises en avant, bien plus que les compétences techniques. Par exemple, une personne ayant un background très complet, mais ayant des problèmes à communiquer avec l'équipe aurait du mal à s'épanouir et donc à s'intégrer dans un environnement de travail agréable.

Les petites choses de tous les jours par exemple : dire Bonjour, remercier, souhaiter un bon anniversaire, demander comment ça va, s'intéresser à l'autre peuvent refléter un bien-être et donc retentir sur le travail effectué. Pour moi, le rôle du manageur est de s'intéresser à ses employés et de prendre la peine de discuter des choses qui vont ou de celles qui ne vont pas. Les 5 à 7 (rendez-vous entre collègues pour boire un verre) sont très importants ; ils permettent d'avoir une équipe soudée.

Par exemple, j'ai rencontré quelques difficultés lors de l'installation de varnish et ne voyant pas de solution et me désespérant un peu, j'en ai référé à mon manageur qui avait plus d'expérience que moi dans le domaine de l'administration de ce service.

Celui-ci m'a donc écouté, m'a montré tout le chemin que j'avais parcouru et affirmé que la partie sur laquelle je butais était minuscule par rapport à tout ce que j'avais appris. Nous

avons donc pris le temps, réfléchi ensemble aux différentes solutions en pesant le pour et le contre et au final, opté pour une solution qui émanait de chacun.

Ce stage m'a donc permis d'acquérir de très grands atouts du côté stratégique en ayant élaboré une solution assez technique. J'ai en outre eu l'occasion de travailler et de gérer une petite équipe de techniciens avec lesquels j'ai fort progressé. Cela permet donc de se sentir très utile au niveau de l'entreprise ; je pense que celle-ci fonctionne très différemment pour ne pas dire mieux maintenant.

5. Conclusion

L'expérience acquise durant la réalisation de ce projet a été très enrichissante à plusieurs niveaux.

Tout d'abord, j'ai été amené à travailler au sein d'une équipe québécoise et à m'adapter à cette atmosphère de travail très différente de celle connue en Europe. Ceci m'a permis de constater l'importance du travail en équipe et de la bonne communication entre les différents membres de cette équipe malgré la distance.

Ensuite, j'ai pu assister à plusieurs réunions internes avec différents responsables de services au sein de PlanetHoster. Durant ces séances, j'ai pu présenter le travail que j'avais effectué et écouter attentivement les critiques et suggestions que l'on m'adressait. Grâce à ces meetings, j'ai notamment pris conscience de l'importance du respect du délai des projets et qu'il y a souvent une différence entre les attentes des utilisateurs et ce qu'il est réellement possible d'effectuer en respectant ce délai.

En outre, le stage m'a confronté au monde du travail et aux exigences professionnelles. En effet, c'était pour moi la première fois que je devais travailler sur un projet d'une telle envergure au sein d'une véritable équipe. Il fallait donc avoir une très bonne ouverture d'esprit avec les autres membres de l'équipe. Il fallait aussi pouvoir accepter de m'être trompé ou que l'idée d'une autre personne pouvait être meilleure que la mienne. Mais d'un autre côté, je devais aussi pouvoir défendre mes idées lorsque celles-ci me semblaient particulièrement judicieuses.

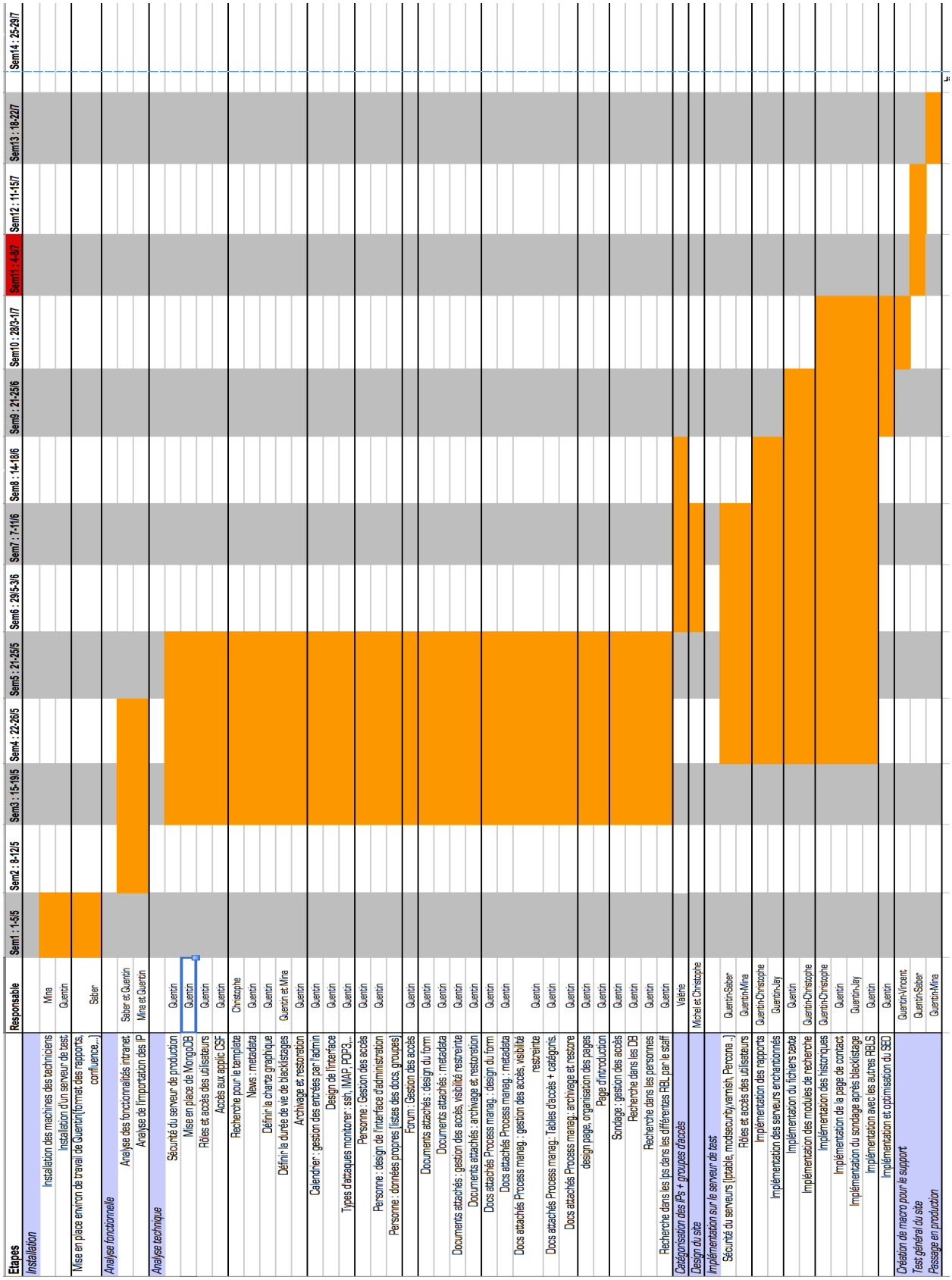
En ce qui concerne les objectifs du stage, je pense qu'ils ont été respectés. Les statistiques sur les trois premiers mois d'utilisation sont très concluantes, j'espère que le projet va grandir et s'étendre à d'autre réseau.

Enfin, ce stage fut une source d'enrichissement, une expérience unique à l'étranger et qui constitue sans nul doute un tremplin idéal pour la future vie professionnelle. J'espère donc rester encore un petit temps chez PlanetHoster au Canada afin d'améliorer mon expérience internationale.

Je tiens aussi à souligner que cela n'aurait pas été rendu possible sans le campus de SUPINFO Canada.

6. Agenda

6.1. Planning


Etapes
Responsable
Sem1 : 1-5/5
Sem2 : 8-12/5
Sem3 : 15-19/5
Sem4 : 22-26/5
Sem5 : 21-25/5
Sem6 : 29/5-3/6
Sem7 : 7-11/6
Sem8 : 14-18/6
Sem9 : 21-25/6
Sem10 : 28/6-1/7
Sem11 : 4-8/7
Sem12 : 11-15/7
Sem13 : 18-22/7
Sem14 : 25-29/7
Installation
Installation des machines des techniciens
Mina
Installation d'un serveur de test
Quentin
Mise en place environ de travail de Quentin(format des rapports, confluence,...)
Saber
Analyse fonctionnelle
Analyse des fonctionnalités intranet
Saber et Quentin
Analyse de l'importation des IP
Mina et Quentin
Analyse technique
Sécurité du serveur de production
Quentin
Mise en place de MongoDB
Quentin
Rôles et accès des utilisateurs
Quentin
Accès aux applic CSF
Quentin
Recherche pour le template
Christophe
News : metadata
Quentin
Définir la charte graphique
Quentin
Définir la durée de vie de blacklistages
Quentin et Mina
Archivage et restoration
Quentin
Calendrier : gestion des entrées par l'admin
Quentin
Design de l'interface
Quentin
Types d'attaques monitorer : ssh, IMAP, POP3,...
Quentin
Personne : Gestion des accès
Quentin
Personne : design de l'interface d'administration
Quentin
Personne : données propres (listes des docs, groupes)
Forum : Gestion des accès
Quentin
Documents attachés : design du form
Quentin
Documents attachés : metadata
Quentin
Documents attachés : gestion des accès, visibilité restreinte
Quentin
Documents attachés : archivage et restoration
Quentin
Docs attachés Process manag. : design du form
Quentin
Docs attachés Process manag. : metadata
Quentin
Docs attachés Process manag. : gestion des accès, visibilité restreinte
Quentin
Docs attachés Process manag. : Tables d'accès + catégories.
Quentin
Docs attachés Process manag. archivage et restore
Quentin
design page, organisation des pages
Quentin
Page d'introduction
Quentin
Sondage : gestion des accès
Quentin
Recherche dans les DB
Quentin
Recherche dans les personnes
Quentin
Recherche dans les ips dans les différentes RBL par le staff
Quentin
Catégorisation des IPs + groupes d'accès
Valère
Design du site
Michel et Christophe
Implémentation sur le serveur de test
Sécurité du serveurs (iptable, modsecurity,varnish, Persona ..)
Quentin-Saber
Rôles et accès des utilisateurs
Quentin-Mina
Implémentation des rapports
Quentin-Christophe
Implémentation des serveurs enchantionnés
Quentin-Jay
Implémentation du fichiers texte
Quentin
Implémentation des modules de recherche
Quentin-Christophe
Implémentation des historiques
Quentin-Christophe
Implémentation de la page de contact
Quentin
Implémentation du sondage après blacklistage
Quentin-Jay
Implémentation avec les autres RBLS
Quentin
Implémentation et optimisation du SEO
Quentin
Création de macro pour le support
Quentin-Vincent
Test général du site
Quentin-Saber
Passage en production
Quentin-Mina

6.2. Activités durant le stage

Les activités lors du stage n'ont pas seulement été le développement de GreenSnow (Blocking list) ; j'ai aussi eu l'occasion de mettre à bien un certain nombre d'autres projets qui ont été très enrichissants. Ces projets ont été très variés au niveau de leurs applications :

- montage de serveurs (montage de SSD, de mise à jour BIOS, configuration RAID,…) diagnostic de problèmes sur des serveurs en production
- support client par ticket ou par téléphone afin de bien les guider dans l'utilisation des services d'hébergement
- recherche dans les systèmes de virtualisation et Cloud comme OpenStack/OpenVZ
- mise en page d'une page d'accueil pour les nouveaux hébergements
- optimisation et sécurisation des serveurs afin de les rendre très performants
- gestion de la qualité des services sur les réseaux sociaux
- mise en place de système de monitoring afin de lutter contre le SPAM,
- mise en place de connecteurs EPP entre PlanetHoster et l'AFNIC, l'EURid et DNSbe.

Ces différentes activités m'ont permis d'avoir une vue d'ensemble de l'entreprise et de faire évoluer celle-ci. Actuellement, les services sont bien mieux organisés et cela permet même d'être proactif. Par exemple, en cas d'intrusion, infiltration, SPAM sur des comptes clients, nous pouvons suspendre ceux-ci très rapidement, localiser la cause et informer le client afin que celui-ci corrige ces problèmes.

7. Bibliographie

Livres

Christophe Wolfhugel, Sécurité informatique : Principes et méthodes à l'usage des DSI, RSSI et administrateurs, Edition Eyrolles

Robet S.Kaplan and David P.Norton, The Balanced scorecard, Harvard Business

Alain Lefebvre, Tout sur la Sécurité informatique, Edition M21

Sites Internet

- http://www.itespresso.fr/etude-arbor-networks-attaques-ddos-menacantes-67188.html
- http://www.blocklist.de/en/index.html
- http://www.slate.fr/life/69993/cyberguerre-internet-apocalypse-danger-mensonge
- http://greensnow.co/
- http://techno.lapresse.ca/nouvelles/internet/201308/27/01-4683474-linternet-chinois-victime-dune-attaque-informatique-massive.php
- http://www.clubic.com/linux-os/debian/ubuntu/actualite-573696-intrusion-forums-ubuntu-comptes-utilisateurs-compromis.html
- http://techcrunch.com/2013/07/23/viber-attacked-by-syrian-electronic-army/
- http://www.itespresso.fr/piratage-drupal-cms-65139.html
- http://pro.clubic.com/it-business/hebergement-site-web/hebergement-dedie-internet/actualite-573944-ovh-intrusion-base-donnees-clients-europe-mot-octave-klaba.h
- http://www.popsci.com/technology/article/2013-07/infographic-biggest-thefts-data-visuali
- http://www.useo.fr/strategies-de-communication-en-ligne-des-collectivites.html
- https://secure.wikimedia.org/wikipedia/fr/wiki/Six_degr%C3%A9s_de_s%C3%A9paratior
- http://www.gizmodo.fr/2013/01/11/anonymous-ddos-protestation-legale.html
- http://www.sans.org/reading-room/whitepapers/firewalls/leveraging-load-balancer-fight-ddos-33408?show=leveraging-load-balancer-fight-ddos-33408&cat=firewalls