

Jean-Sébastien Guay-Leroux
jean-sebastien@guay-leroux.com

LA SÉCURITÉ DES FILTRES DE CONTENU SMTP

<http://www.guay-leroux.com/>
Avril 2006

1. TABLE DES MATIÈRES

1. TABLE DES MATIÈRES.....	2
2. INTRODUCTION.....	3
3. LES FILTRES DE CONTENU	4
3.1. QU'EST-CE QU'UN FILTRE DE CONTENU ?.....	4
3.2. UN FILTRE DE CONTENU COMPLEXE	5
3.3. LE PROBLÈME	5
3.4. SCHÉMA D'INTÉGRATION.....	6
3.5. LES COMPOSANTES EXTERNES VULNÉRABLES.....	7
4. PIRANA : UN OUTIL POUR TESTER LA SÉCURITÉ DE VOTRE FILTRE DE CONTENU..	9
4.1. DESCRIPTION.....	9
4.2. TECHNIQUE UTILISÉE POUR RENDRE L'EXPLOITATION PLUS FIABLE	10
4.3. DIFFÉRENTES TECHNIQUES UTILISÉES POUR MASQUER L'ATTAQUE	11
5. CONCLUSION	18

2. INTRODUCTION

Le courrier électronique est devenu, avec les années, un service essentiel presque à tout le monde. Qui ne possède pas une adresse de courriel aujourd'hui? Avec le temps, il semblait évident que de nombreuses menaces verraient le jour et qu'elles se propageraient à travers ce médium de communication.

Certaines personnes, toujours prêtes à faire de l'argent, ont vu, dans le courriel, une excellente façon de rejoindre des clients potentiels. La sollicitation par courrier électronique (SPAM) était née. De plus, les auteurs de virus ont profité de ce vecteur d'attaque en l'utilisant comme tremplin pour une meilleure propagation virale. Les fraudeurs ont aussi gagné leur part du lot, surtout depuis les récentes menaces d'hammeçonage.

Dans le but de se prémunir contre de telles attaques, les administrateurs de systèmes implantèrent diverses technologies afin de protéger leurs utilisateurs contre ce type de menaces. Mais est-ce que ces programmes sont aussi sécuritaires que les administrateurs le souhaiteraient? Ces bouts de codes sont-ils prêts à affronter tout le contenu malsain retrouvé aujourd'hui sur l'autoroute électronique?

Dans ce papier, il vous sera présenté le problème lié à l'implantation de technologies de filtrage au niveau courriel. Un outil vous sera aussi présenté afin d'aider les experts en sécurité à tester la sécurité des filtres de contenu.

3. LES FILTRES DE CONTENU

3.1. QU'EST-CE QU'UN FILTRE DE CONTENU ?

Un filtre de contenu est un système qui agit après réception du courriel par le serveur SMTP et qui applique différentes politiques de filtrage définies par un administrateur réseau. Une fois le balayage terminé, le filtre de contenu décide si le message doit ou non être rejeté.

Voici les tâches qu'un filtre de contenu effectue sur un courriel reçu :

- Balaie les pièces jointes à la recherche de contenu virulent
- Balaie le courriel pour vérifier que ce n'est pas une publicité non sollicitée
- Bloque le contenu dangereux pour l'utilisateur (exploits MUA, zip bombs, ...)
- Bloque certains types de pièces jointes (.EXE, .COM, .PIF, etc)
- Applique un système de listes blanches et noires

La figure 1 présente un schéma simplifié du parcours d'un message dans un filtre de contenu :

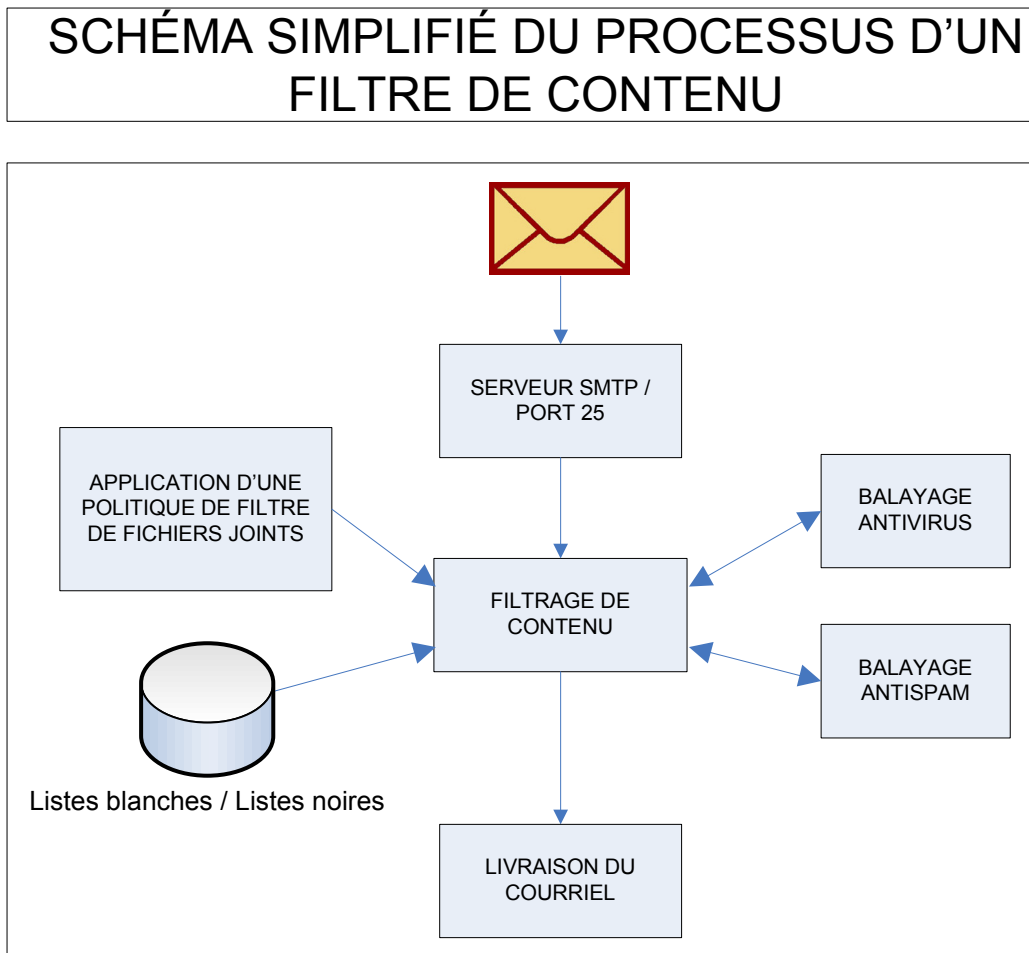


Figure 1 : Schéma simplifié du processus de filtrage d'un courriel

3.2. UN FILTRE DE CONTENU COMPLEXE

Filtrer le courriel, que ce soit pour éliminer les virus, bloquer le pourriel, prévenir les fraudes ou bien seulement pour établir une politique de transmission de courriels, nécessite une technologie complexe.

Quelque soit la solution logicielle envisagée, elle devra intégrer des fonctions de décompression et de décodage du contenu compte tenu des multiples formats de messages en circulation. Ces fonctions sont généralement assumées par des modules ou bibliothèques qui sont optimisées et traitent tous les cas possibles. L'utilisation de bibliothèques facilite et accélère le développement de solutions commerciales.

Alors souvent, les développeurs devront composer avec ce qui existe déjà. Ils intégreront différentes composantes dans un système afin de leur faire réaliser une tâche bien particulière. Ils se procureront des programmes et bibliothèques qui les aideront à désarchiver, classifier, décoder et balayer le courriel et son contenu.

Le filtre de contenu, qui au départ semblait être un outil bien simple, devient un agencement de plusieurs éléments logiciels dont la qualité du code, la maintenance et la sécurité peuvent parfois être très différentes.

3.3. LE PROBLÈME

La présence de nombreuses composantes autour du noyau d'un logiciel de filtrage de contenu aide le programmeur à concentrer son énergie à développer le code de son filtre. Par contre, la qualité du code générique gravitant autour du filtre est incertaine, et ce pour toutes sortes de raisons.

En effet, ces outils n'ont pas nécessairement été créés pour être intégrés dans des infrastructures destinées à améliorer la sécurité d'un réseau. Ils ont été programmés dans le but d'offrir une seule et même fonctionnalité de base, la plupart du temps sans intégrer de saines pratiques de développement sécuritaire. Aujourd'hui, avec les pirates, experts et chercheurs en sécurité, leur robustesse est rapidement mise à l'épreuve.

De plus, les menaces et les besoins pour un engin de filtrage de contenu du courrier électronique changent et évoluent rapidement. Alors les développeurs doivent intégrer rapidement diverses technologies qui ne sont pas nécessairement matures au niveau sécurité. Les différents outils et bibliothèques utilisés dans un filtre de contenu ne subissent, la plupart du temps, plus aucune mise à jour de fonctionnalité ou de sécurité. Ce qui ne veut certainement pas dire qu'ils sont libres de failles ou infaillibles!

En résumé, l'administrateur du filtre de contenu doit faire confiance aux bibliothèques et modules génériques intégrés dans le système, dont la provenance est parfois douteuse. La sécurité de la solution sera tributaire de la robustesse des différentes composantes du système de filtrage. En d'autres termes, il y a beaucoup de chances qu'un des maillons les plus faibles de la chaîne se retrouve dans une de ces composantes.

3.4. SCHÉMA D'INTÉGRATION

Voici un diagramme qui représente à quel endroit, dans le processus de balayage, chacune des composantes potentiellement vulnérable est intégrée. La figure 2 illustre la grande variété de composantes logicielles génériques généralement présentes dans un filtre de contenu. L'existence de toute faille de sécurité dans une de ces composantes peut être fatale à l'intégrité du système.

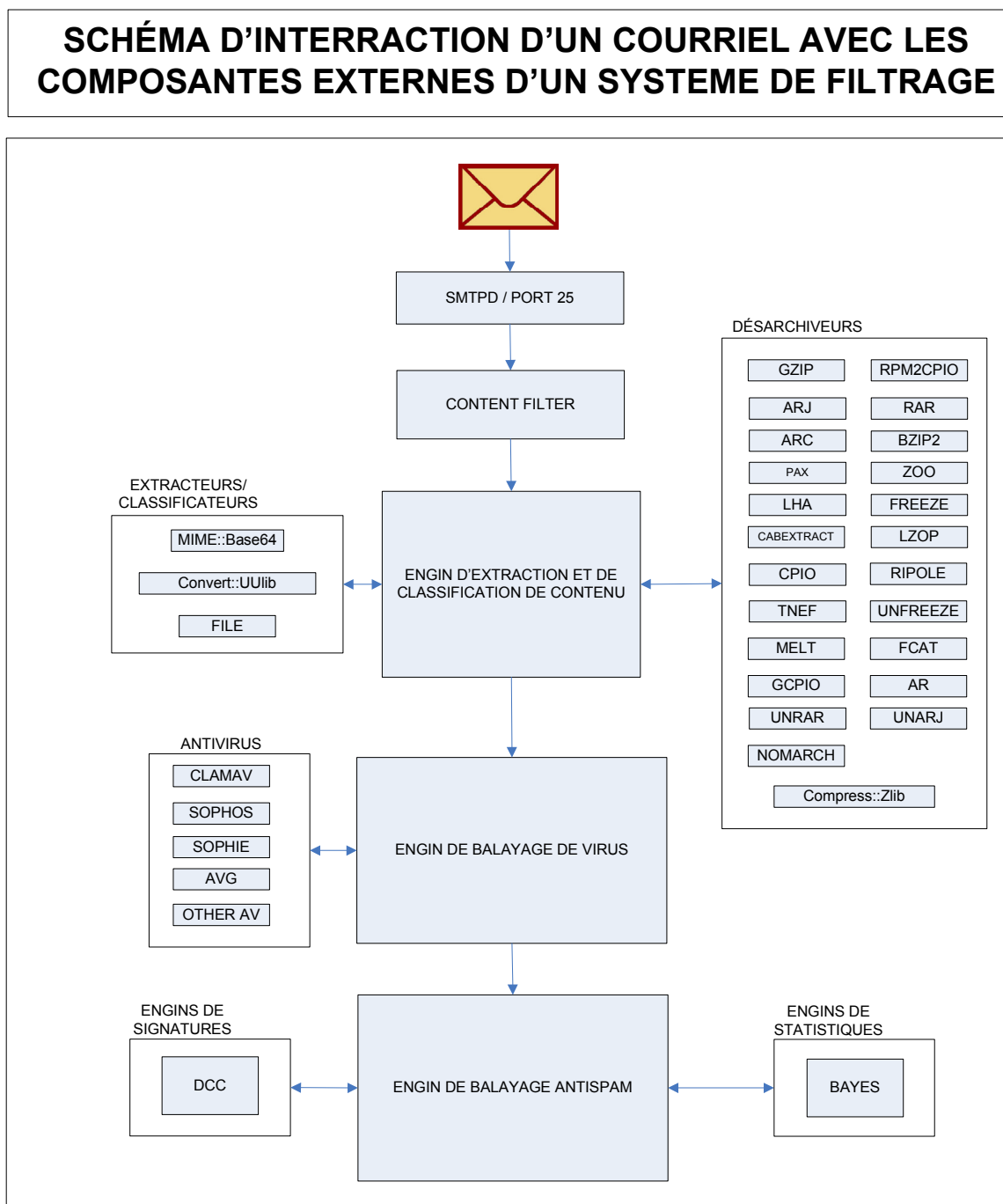


Figure 2

3.5. LES COMPOSANTES EXTERNES VULNÉRABLES

Voici les cinq catégories de composantes externes qu'un filtre de contenu pourrait intégrer, et qui seraient susceptibles de présenter des failles de sécurité.

3.5.1 Les archiveurs

Les auteurs de virus ont rapidement compris qu'ils pouvaient éviter le balayage antivirus en encapsulant leur virus dans une archive. En utilisant un soupçon d'ingénierie sociale pour inciter l'utilisateur à ouvrir l'archive, ils obtiennent une charge virale invisible aux antivirus, mais très dangereux pour l'utilisateur. Il a donc fallut intégrer diverses composantes de décompression dans les filtres de contenu.

Pour ce faire, le filtre de contenu classe chaque pièce jointe en lui attribuant un type. Cette tâche est effectuée par l'outil « file » disponible dans de nombreuses versions UNIX. Une fois la classification faite, le filtre regarde si le fichier est un type d'archive connu, telle que ZIP, ARJ, LHA, etc. et tente d'y associer un décompresseur pour le type de fichier identifié. Si ces conditions sont toutes vérifiées, il appelle le programme avec la pièce jointe en argument et continue son balayage sur le contenu de l'archive, de manière récursive.

3.5.2 Les décodeurs

Afin de bien exécuter ses tâches, le filtre de contenu doit être capable d'extraire les différentes pièces jointes du courriel. Parfois, ces fichiers peuvent être incorporés au courriel directement au format « uuencode », ou bien en pièce MIME. Il existe de nombreuses manières de joindre ces pièces, et la plupart des clients ne le font pas de la même façon. Le filtre de contenu doit pouvoir reconnaître et accepter toutes les formes de contenu encodé, comme le ferait un logiciel client.

Les filtres se doivent donc d'être capable d'émuler le plus fidèlement possible le comportement que pourrait emprunter chacun des logiciels de courriel, afin de bien pouvoir les protéger.

3.5.3 Programme de classification

Un programme de classification sert à déterminer le type d'un fichier. Il exécute cette tâche en examinant les premiers octets d'un fichier et en les comparant à une base de données contenant plusieurs définitions de types. Il est donc capable de déterminer si une pièce jointe est un exécutable, une image, un document PDF, etc.

Ainsi, un filtre de contenu qui veut bannir un certain type de fichier n'a pas à se fier aux extensions de la pièce jointe pour effectuer un jugement, technique beaucoup moins fiable. Il appelle le programme de classification et donne le fichier en argument, et le logiciel retourne une interprétation exacte sur sa nature réelle.

Ce type d'application est aussi utile dans la décompression d'archives. Il permet de confirmer le type du fichier avant de lancer le décompresseur, et ainsi de sauver de précieuses ressources.

3.5.4 Antivirus

Une des tâches principales d'un filtre de contenu est bien sûr de s'assurer qu'aucun contenu virulent ne puisse circuler sans autorisation. Une multitude de produits antivirus, commerciaux et à licence ouverte, sont disponibles pour intégration dans le filtre de contenu.

3.5.5 Autres composantes logicielles

D'autres types de composantes logicielles intégrées aux filtres existent. Les classificateurs statistiques Bayesian, des outils de vérification de signatures tels que PYZOR, DCC, etc. Ces logiciels peuvent être écrits dans une multitude de langage, certains plus sécuritaires que d'autres par nature. Il importe de bien comprendre le mode d'opération de toutes les composantes impliquées, de jauger leur exposition ainsi que le risque associé à leur utilisation.

4. PIRANA : UN OUTIL POUR TESTER LA SÉCURITÉ DE VOTRE FILTRE DE CONTENU

4.1. DESCRIPTION

PIRANA est un engin applicatif qui permet de tester la sécurité d'un filtre de contenu. À l'aide d'une base de données de failles, le filtre à l'essai sera bombardé par différents courriels ayant du contenu malsain et destiné à compromettre la plateforme d'exploitation. Pratiquement, PIRANA sert à démontrer si une faille de vulnérabilité existe et si celle-ci peut être exploitée pour donner accès au serveur qui roule le filtre de contenu.

Cet outil est, en résumé, un programme PERL qui bâtit un courriel et qui joint du contenu malsain généré par différents codes d'exploitation et qui l'envoie à une cible. Plusieurs techniques ont été développées qui permettent de rendre l'attaque plus fiable et plus discrète. L'outil est modulaire et il est possible d'ajouter du support pour de nouvelles vulnérabilités qui émergeraient dans le futur.

La figure 3 présente de nombreuses vulnérabilités retrouvées dans les composantes logicielles génériques d'un filtre de contenu. Cette liste ne se veut pas exhaustive, elle affiche seulement certaines vulnérabilités. La disponibilité d'un code d'exploitation pour chacune de ces failles vous est aussi affichée.

TABLEAU DE VULNÉRABILITÉS DES LOGICIELS UTILISÉS LORS DU FILTRAGE DE CONTENU				
Composante vulnérable	OSVDB #	Versions vulnérables	Version actuelle (01/02/2006)	Exploit disponible dans PIRANA ?
LHA	5753	<= 1.17	1.17*	OUI
	5754	<= 1.17		OUI
Zlib	17827	<= 1.2.2	1.2.3*	NON
Unarj	11695	<= 2.65	2.65*	OUI
File	6456	<= 3.38	4.16	OUI
	12255	<= 4.11		NON
Convert ::UUlib	15867	<= 1.05	1.06	NON
Zoo	Xxx	2.10	2.10*	OUI
Clamav	20482	<= 0.87	0.88	NON

Figure 3 : Tableau de failles de filtres de contenu
* Correctif fourni par le vendeur

4.2. TECHNIQUE UTILISÉE POUR RENDRE L'EXPLOITATION PLUS FIABLE

4.2.1 Attaque par force brute possible

Règle générale, lors d'une attaque par débordement de tampon ou par erreur de formatage, beaucoup de variables nécessaires à l'exploitation sont inconnues. Elles sont malheureusement essentielles pour la réussite de l'exploitation.

Beaucoup de techniques ont été développées dans le passé pour faciliter l'exploitation, et diminuer la plage d'adresses des variables inconnues. Une de ces méthodes consiste à précéder le « shellcode » d'une série de « NOP » qui facilitera l'exploitation.

Une technique bien connue pour maximiser les chances d'exploiter un programme est une attaque par force brute. Si le contexte nous le permet, il est possible d'essayer séquentiellement des valeurs qui pourraient être valables et rendre l'exploitation possible. Par exemple, lors d'une attaque par débordement de tampon, l'endroit où faire pointer le pointeur d'instruction une fois celui-ci maîtrisé est inconnu. Avec des essais séquentiels, la bonne valeur sera éventuellement atteinte et le programme sera détourné de sa fonction primaire.

Ce qui détermine si la technique peut être applicable à un contexte particulier, il faut que l'environnement puisse se réinitialiser à son état initial si l'attaque échoue. Dans le cas d'un filtre de contenu, ce n'est pas un problème car le filtre ne meurt jamais lorsque les composantes avortent. Le cas du serveur DNS « Bind » est différent car si celui-ci avorte, le service ne redémarre pas.

La technique d'essais séquentiels est implantée dans PIRANA en joignant plusieurs pièces jointes avec différents « offsets » dans un seul courriel. Ainsi, le filtre de contenu analysera chacune des pièces jointes dans le courriel. Cette technique est beaucoup plus difficile à détecter car au lieu d'envoyer 50 courriels avec 50 fichiers malsains différents, un seul courriel avec les 50 fichiers malsains joints sera transmis.

4.3. DIFFÉRENTES TECHNIQUES UTILISÉES POUR MASQUER L'ATTAQUE

Ce qui bonifie un type d'attaque est bien sûr sa capacité à passer inaperçue. Dans ce cas-ci, deux intervenants peuvent remarquer l'attaque, soit l'administrateur du filtre de contenu, et l'utilisateur qui peut recevoir une copie du courriel.

Des méthodes permettant de camoufler l'attaque et de masquer l'identité de l'attaquant sont discutées dans cette section.

4.3.1 Évasion des systèmes de détection d'intrusion avec encodage de pièces jointes

Le protocole SMTP, à la base, supporte seulement un ensemble de caractères représentés sous 7 bits ASCII (RFC 821). À priori, cette règle semble poser un problème pour la transmission de contenu binaire ou de jeux de caractères étendus.

Pour pallier à cette limitation, il est possible d'utiliser la spécification MIME. En effet, à l'aide de MIME, il est possible d'encoder du contenu représenté sous 8 bits en 7 bits.

Cette limitation inhérente à SMTP devient intéressante pour PIRANA car en encodant le contenu malsain, l'évasion de systèmes de détection d'intrusion est alors possible. Ces systèmes analysent le trafic réseau à la recherche de signes évident d'attaques, par exemple un « shellcode » ou une série de « NOP ». Si le contenu malsain est encodé, il passera inaperçu auprès de certains IDS.

Il est donc possible de faire d'une pierre deux coups avec la spécification MIME, soit en permettant le transfert de fichiers binaires et en camouflant une attaque vers le filtre de contenu.

4.3.2 Joindre un virus

Aujourd'hui, la majorité des filtres de contenu incluent un ou plusieurs antivirus dans leurs fonctionnalités, ce qui permet d'empêcher une infection tôt dans le processus de livraison, car le virus ne se rend jamais sur la station de l'utilisateur.

Parfois, les filtres de contenu traitent la totalité du courriel avant de prendre une décision sur quoi faire avec celui-ci. Ils balayeront le message avec un antispam et un antivirus, ils décodent le contenu, décompresseront les archives et attribueront un type aux pièces jointes. Ces tâches seront toutes effectuées avant qu'une décision soit prise sur l'avenir du message.

Si le filtre de contenu détecte un virus, il y a de fortes chances que le message ne se rende jamais à destination. Par contre, le filtre de contenu traitera quand même la totalité du message avant de prendre action sur celui-ci. Le code explosif, destiné à prendre contrôle du filtre de contenu, a donc la chance d'être traité par les composantes vulnérables.

Il est donc possible de profiter de ce comportement chez les filtres de contenu pour ajouter une touche de subtilité au test de pénétration.

TABLEAU DES ACTIONS ET CONSÉQUENCES POSSIBLES SUR UN COURRIEL INFECTÉ PAR UN VIRUS	
Action	Visibilité de l'attaque
Destruction du message sans égard à son contenu	Basse
Mise en quarantaine du courriel	Moyenne
Substitution ou destruction de la pièce jointe infectée	Moyenne

Figure 4

4.3.3 Envoi à partir d'un service de messagerie gratuit

Il est aussi possible d'exploiter le caractère anonyme de plusieurs sites qui offrent des adresses de courrier électronique gratuites. En effet, en générant les différents fichiers malsains et en les envoyant à partir de l'interface web d'un service de messagerie gratuit, il est possible de lancer une attaque totalement anonyme.

Les seules traces qui seront laissées sur le serveur cible seront l'adresse IP et l'adresse de courriel utilisées lors de l'attaque, toutes deux anonymes.

4.3.4 Compression des fichiers malsains en un seul fichier

Parfois, il arrive qu'un grand nombre de fichiers doivent être transmis. Par exemple, une attaque de force brute nécessitera l'envoi de plusieurs fichiers, chacun comprenant un « offset » différent.

Cette méthode propose donc de compresser la totalité des fichiers en une seule et unique archive. Beaucoup plus subtile, le filtre de contenu s'occupera de décompresser cette archive, et de faire un traitement sur chacune de ses pièces.

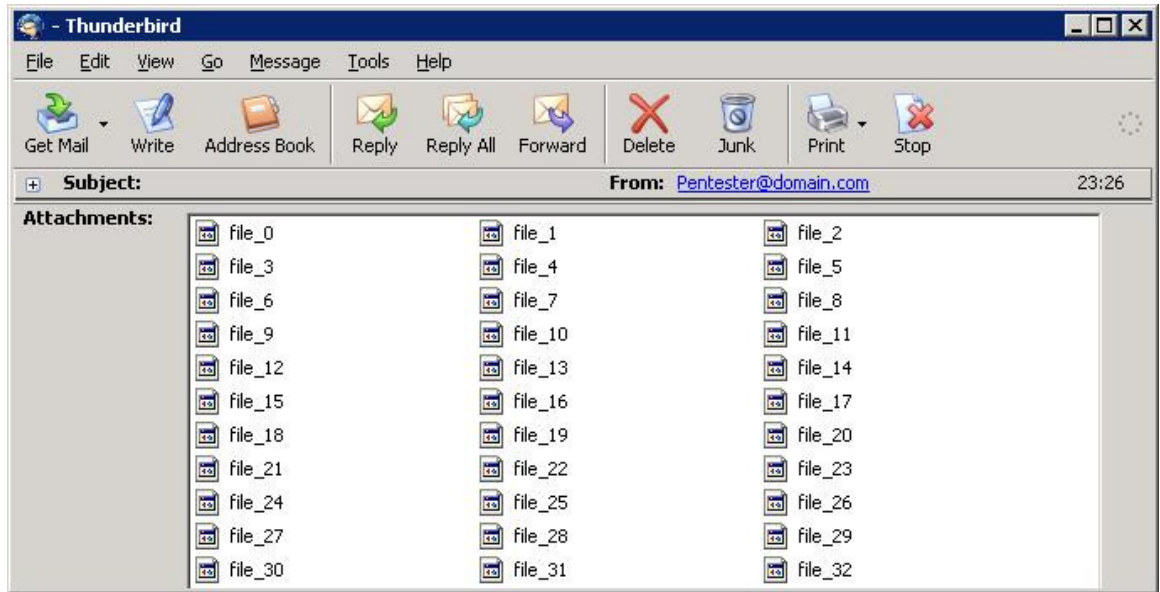


Figure 5 : Un courriel qui n'a pas subi la technique de compression

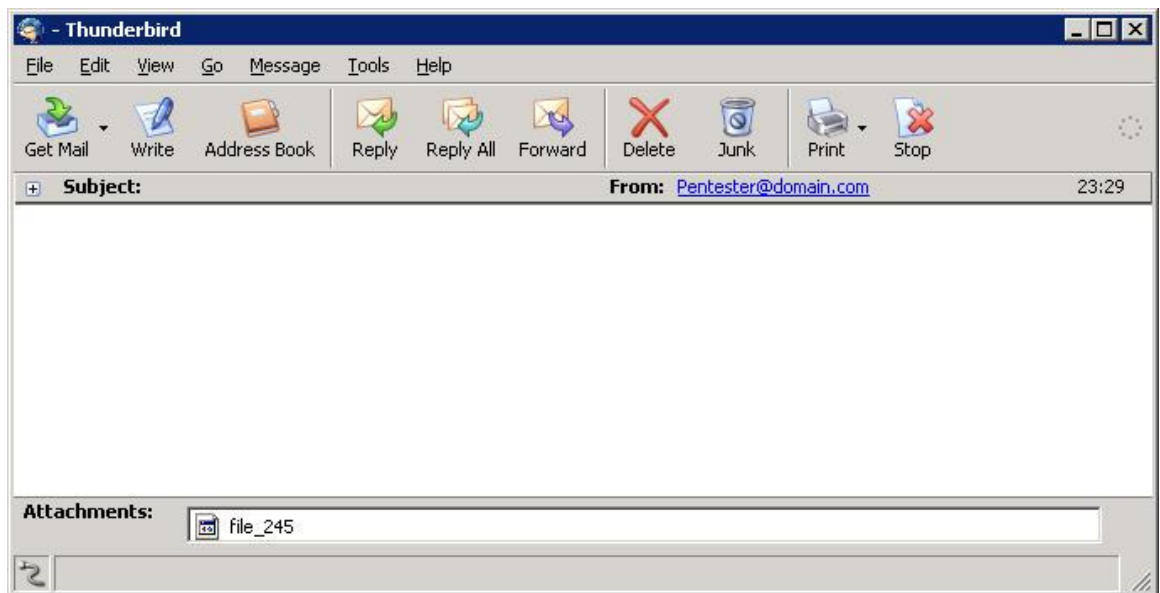


Figure 6 : Un courriel qui a subi la technique de compression.

Un message avec une seule pièce jointe demeure plus discret et génère moins d'entrées de journal.

4.3.5 Suppression du contenu malveillant de la liste de pièces jointes

Bien sûr, avec une seule pièce jointe, le message hostile demeure discret. Pour atteindre un niveau de discrétion supérieur, il est souhaitable de faire disparaître toutes les pièces jointes susceptibles d'éveiller l'attention de l'utilisateur qui reçoit le courriel.

PIRANA implante deux techniques pour éliminer les pièces jointes de la vision du client de courrier électronique.

Technique de l'image invisible

Lorsqu'un message est envoyé en format HTML, les logiciels de courriel affichent la liste de toutes les pièces jointes. Par contre, lorsque le code HTML référence directement une des pièces jointes, celle-ci disparaît de la liste des fichiers attachés. PIRANA utilise cette particularité pour camoufler ses envois.

Pour ce faire, il suffit de joindre en pièce MIME les différents fichiers dont PIRANA se servira pour tester la sécurité du filtre. Afin d'y accéder ultérieurement, un "Content-ID" sera attribué avec lequel il sera possible de référencer le fichier dans le HTML. Une fois cette tâche effectuée, il faudra référencer toutes les pièces précédemment attachées à l'aide d'une directive HTML appropriée.

La directive suivante intègre la pièce jointe file-01 dans le résultat HTML final, à l'aide du mot clef "cid" :

```

```

Technique du multipart/alternative

Par définition, le type MIME "multipart/alternative" définit des versions alternatives de la même information. Lorsque le client de courriel voit la directive, il va choisir la meilleure version des pièces jointes qu'il peut afficher à l'écran.

Par exemple, si un courriel est de type multipart/alternative, il pourrait contenir une version texte et HTML du même document. Le logiciel décidera ensuite, selon ses paramètres, la meilleure version à afficher.

PIRANA utilise cette fonctionnalité. Les pièces jointes sont toutes spécifiées comme une version alternative du courriel final. Étant donné que le logiciel du client ne sera jamais capable d'afficher les fichiers binaires, il affichera la version HTML et le code explosif passera inaperçu.

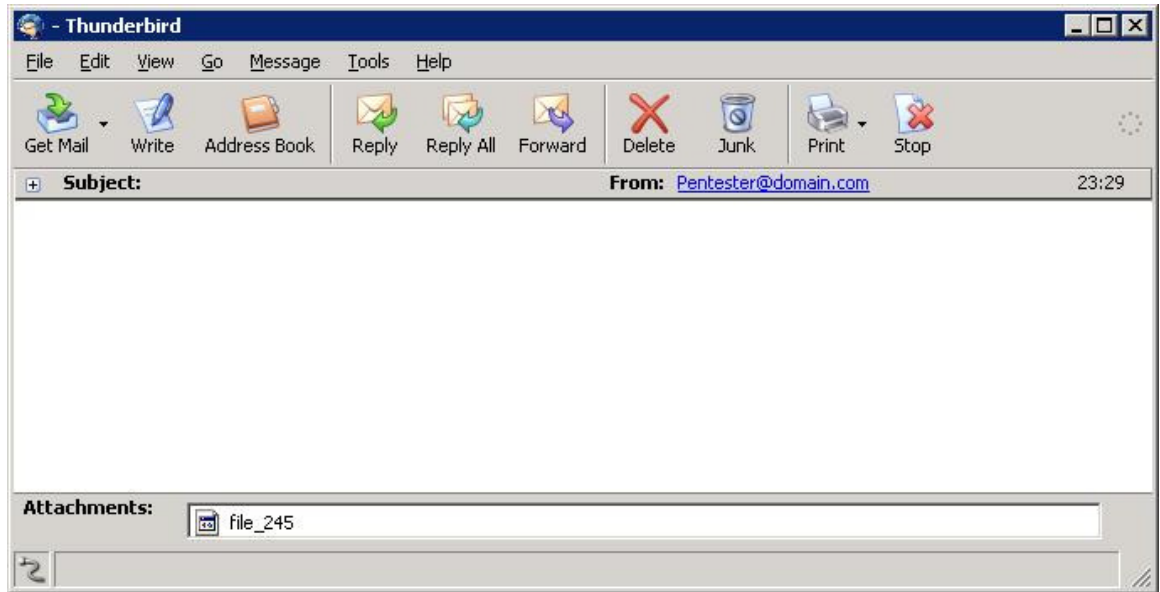


Figure 7 : Courriel envoyé sans technique de suppression

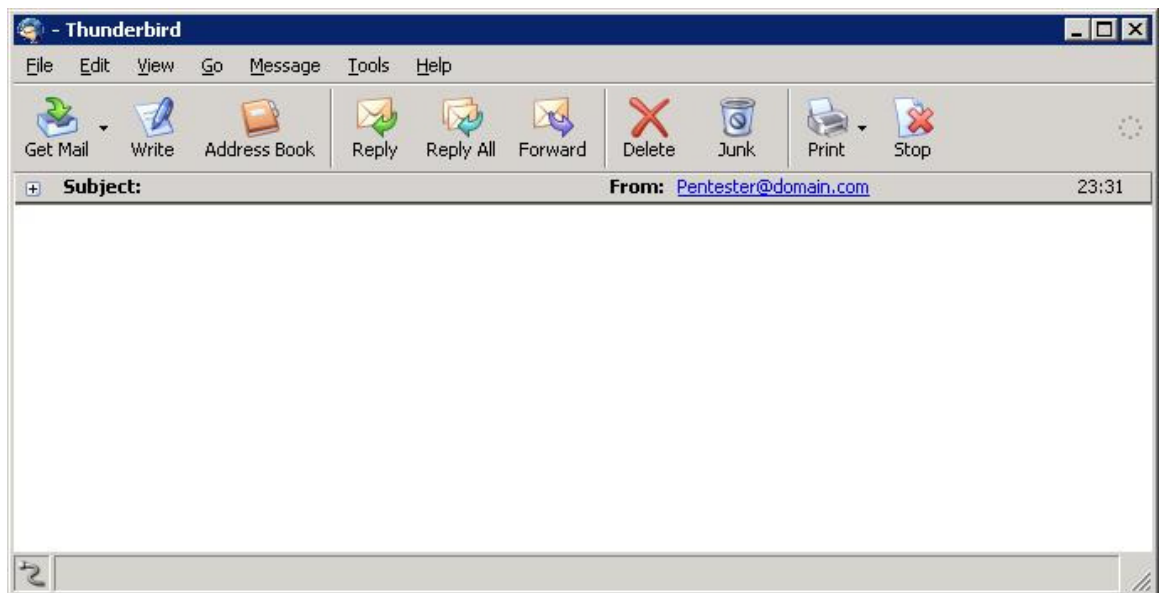


Figure 8 : Courriel envoyé avec une technique de suppression

Les figures 7 et 8 présentent le contenu visible pour la même charge utile. Le courriel sans pièce jointe apparente passe inaperçu.

4.3.6 Déguiser le message pour le rendre moins louche

Il est aussi possible d'utiliser l'ingénierie sociale afin de passer inaperçu. Si un utilisateur reçoit un courriel dont le contenu semble suspect, il pourrait peut-être, par prudence, contacter son administrateur réseau qui serait alors en mesure d'analyser les détails de l'attaque et le subterfuge de l'attaquant serait démasqué.

Par contre, si le courriel hostile est déguisé en envoi d'apparence inoffensive, il ne croira pas utile de contacter son administrateur réseau et il jettera probablement le courriel.

En regardant les deux courriels ci-dessous, il est extrêmement difficile de se douter qu'ils contiennent du contenu destiné à compromettre la sécurité du filtre de contenu.

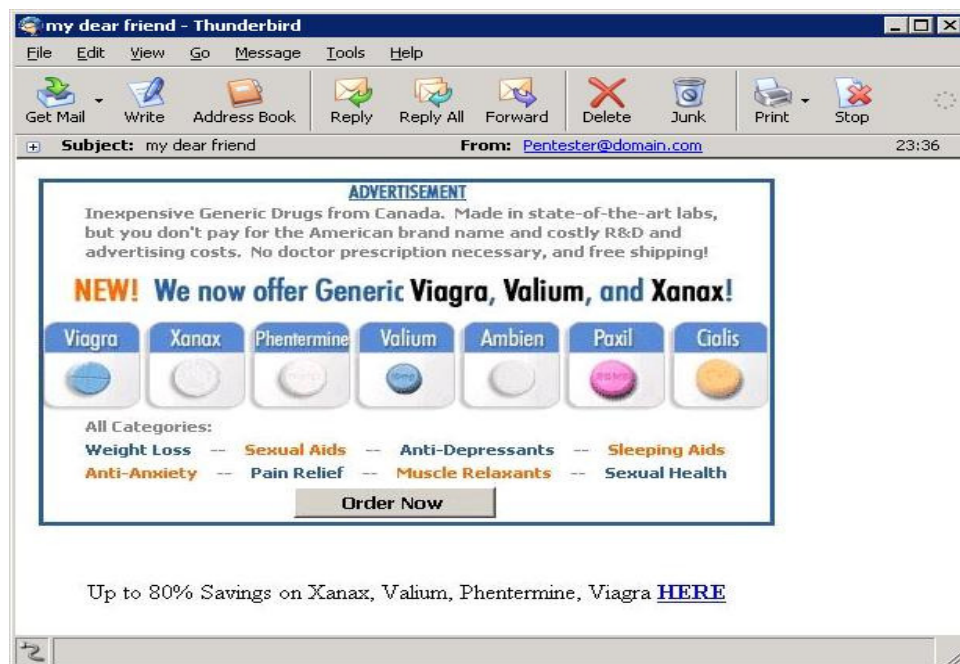


Figure 9 : Courriel empruntant l'identité d'un pourriel pour passer inaperçu

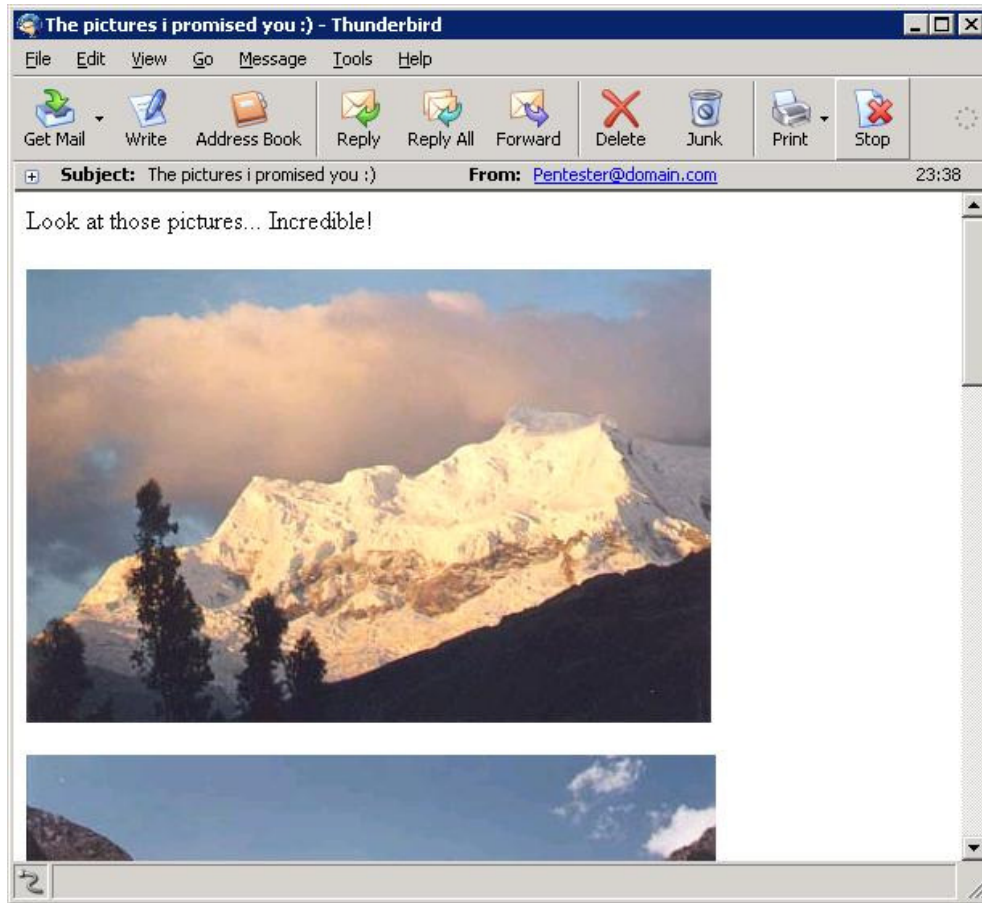


Figure 10 : Courriel empruntant l'identité d'une personne faisant parvenir des photos de voyage

5. CONCLUSION

Ce papier avait comme but premier de présenter les filtres de contenu et les différentes vulnérabilités associées à ceux-ci. Les différentes composantes externes se sont avérées être le lien le plus faible de la chaîne.

La position de choix d'un filtre de contenu dans un réseau, ainsi que la nature des données qui circulent par celui-ci en fait une cible prisée par les pirates. PIRANA a été écrit pour démontrer que le risque n'était pas seulement hypothétique mais bel et bien réel. Différentes techniques ont été présentées qui améliorent l'efficacité et la discrétion des attaques.

Un important point à retenir est que la sécurité n'est pas un produit qui s'achète. Il est impossible de parler de sécurité si la mesure correctrice qui est à implanter est elle-même affligée par des failles de sécurité. Il serait préférable d'y penser la prochaine fois que vous achèterez un produit de sécurité. Est-ce que ce dernier sera le talon d'Achille de votre réseau?