Dans le cadre de

SECURIDAY 2010

Et sous le thème de

Computer Forensics Investigation

VOUS PRÉSENTE L'ATELIER :

Analyse des e-mails

Chef Atelier : Trabelsi Ramzi (RT5)

- Amairi Mohamed (IIA5)
- Mehdi Ahmed (RT5)
- Gharbi Ghofrane (RT4)

1. Présentation de l'atelier et de l'outil

Définition d'un e-mail :

Un e-mail ou courrier électronique ou courriel appelé aussi messagerie électronique est l'un des services (avec le Web) les plus utilisé d'Internet. Un e-mail possède de nombreux avantages dont les principaux sont rapidité, asynchronisme, gestion de listes de messagerie (diffusion - mailing lists), gestion de boîtes aux lettres (mailbox) etc.

En-tête d'un e-mail :

L'en-tête d'un courrier électronique n'est autre qu'une succession de lignes, fournissant des informations de nature variée sur le message. L'en-tête d'un mail permet de connaître certaines données concernant l'expéditeur ainsi que le parcours du message sur Internet ; c'est un peu l'équivalent des cachets, timbres et adresses figurant sur une enveloppe postale. Cela est notamment très pratique pour un investigateur afin d'identifier le véritable expéditeur de spam ou mails indésirables.

Voici une liste des champs les plus courants figurant dans un en-tête et leur signification :

From: Adresse électronique de l'expéditeur, en général suivie de son nom.

To: Adresse du destinataire. Plusieurs adresses peuvent être spécifiées, séparées par une virgule.

Cc: Adresses des personnes recevant une copie du message pour information (''Carbon Copy'', copie carbone, du temps où une copie sur papier carbone servait de copie d'un document). Plusieurs adresses peuvent être spécifiées, séparées par une virgule.

Bcc: Adresses des personnes recevant une copie du message sans que ces adresses n'apparaissent dans l'en-tête du message et non transmise aux destinataires spécifiés par les champs *To:* et *Bcc:* (''Blind Carbon Copy'', copie carbone cachée). De cette façon, ni les destinataires des

champs *To:* ou *Cc:*, ni les destinataires des champs *Bcc:* n'ont connaissance des adresses contenues dans le champ *Bcc:*

Subject: Contenu du courrier, en quelques mots.

Date: Date à laquelle le courrier a été expédié.

Reply-To: Adresse à laquelle l'expéditeur veut que les réponses éventuelles lui soient envoyées. Ceci est utile si on veut que les réponses arrivent à une adresse différente de l'adresse d'expédition.

Organization: Nom de l'organisme, de la société, de l'université propriétaire de la machine d'où provient le courrier.

Message-ID: Chaîne générée par l'agent de transport de courrier du système où le message a été généré. Cet identificateur est propre au message, unique dans le monde entier. C'est par exemple le nom de la machine et une date ainsi qu'un identificateur de processus

Received: Chaque site relayant le courrier insère un champ indiquant son nom, un identificateur, la date et l'heure de réception, de quel site le message est arrivé, et quel logiciel de transport a été utilisé.

Return-Path : Lors du dépot dans la boîte aux lettres, l'agent de transport y indique l'adresse de l'expéditeur dans l'enveloppe.

X-nom-quelconque: Informations supplémentaires concernant toute possibilité nouvelle qui n'est pas encore définie dans un document RFC, ou ne le sera jamais.

La plupart des gestionnaires des Emails permettent d'afficher la totalité des en-têtes , pami ces gestionnaire on site Windows live mail , Outlook express, Thunderbide, Opera mail, Gmail, Orange, Yahoo mail…

On a choisit **Outlook Express** comme outil pour la récupération des Emails et par la suite afficher les différents champs contenus dans l'entête.

Spam et anti-spam :

Le spam peut se définir comme étant un e-mail anonyme, indésirable et envoyé en masse. Comme on parle de courriel pour indiquer un Email, on utilise de plus en plus le terme Pourriel pour le SPAM car ce dernier est tiré de l'expression "courriel pourri".

Un anti-spam est un logiciel qui permet de filtrer le courriel afin de lutter contre les spams. L'anti-spam consiste souvent en une série de filtres qui visent à détecter des mots qui sont souvent contenus dans les spams, tel sexe, money, argent, etc. Pour détecter si un e-mail est oui ou non un spam, les filtres anti-spam utilisent différentes techniques pour deviner la nature de l'e-mail mais nécessitent tout de même une aide la part de l'utilisateur.

Très souvent, on peut télécharger gratuitement des anti-spams. Le choix d'un anti-spam se fait en se basant sur les points importants du logiciel, les techniques, les solutions, les recommandations et la sélection de logiciel. Parmi les logiciels anti-spam gratuits les plus connus on site pour Windows : MailWasher, SpamPal, Spamihilator, SpamFighter, SpamCombat, et pour Linux : SpamAssassin, SpamBayes, MailScanner…

Pour notre atelier nous avons choisi **SpamPal** pour sa facilité d'installation et de configuration ainsi que la disponibilité d'une documentation claire.

D'autre part, dans l'investigation et l'analyse des e-mails, il est possible d'extraire des informations sur l'historique de navigation web à travers les cookies, l'historique, les URL utilisées… Ces informations peuvent guider l'investigateur pour savoir quels sont les sites visités et plus précisément les sites de messagerie électronique. Pour ce faire nous utiliserons **STG Cache Audit**, un outil gratuit pour d'extraction et la visualisation d'information depuis le cache Internet.

2. Environnement logiciel

Pour la version Windows nous utiliserons **Windows XP SP3**.

Comme nous avons déjà précisé, nous utiliseront **Outlook Express** version 6 pour la récupération des en-têtes des e-mails. Outlook Express est un outil de messagerie électronique gratuit, inclus avec Internet Explorer. C'est l'un des clients de messagerie les plus populaires. Il est très semblable à Microsoft Office Outlook qui lui, payant et disponible avec la suite Office, présente plus de fonctionnalités d'organisation et sert d'assistant personnel. Le successeur Microsoft de Outlook express est Windows Live Mail, ils sont tous les deux disponibles en téléchargement gratuit sur *http://support.microsoft.com*.

En ce qui concerne les logiciels anti-spam utilisés, **SpamPal** version 1.594 est gratuit est disponible en téléchargement sur son site officiel *http://www.spampal.org*.

Pour **STG Cache Audit**, la seule version disponible est la version 1.0.0.0, l'outil est disponible en téléchargement gratuit sur le site du développeur *http://www.stgsys.com*.

3. Installation et configuration

Outlook Express :

Outlook Express est intégré avec Internet Explorer contenu par défaut dans la version Windows que nous utiliserons, XP SP3.

La configuration d'Outlook Express n'est pas compliquée. Pour récupérer les e-mails à partir du compte *securinets@yahoo.fr* nous avons configuré notre client de messagerie avec les paramètres suivants :

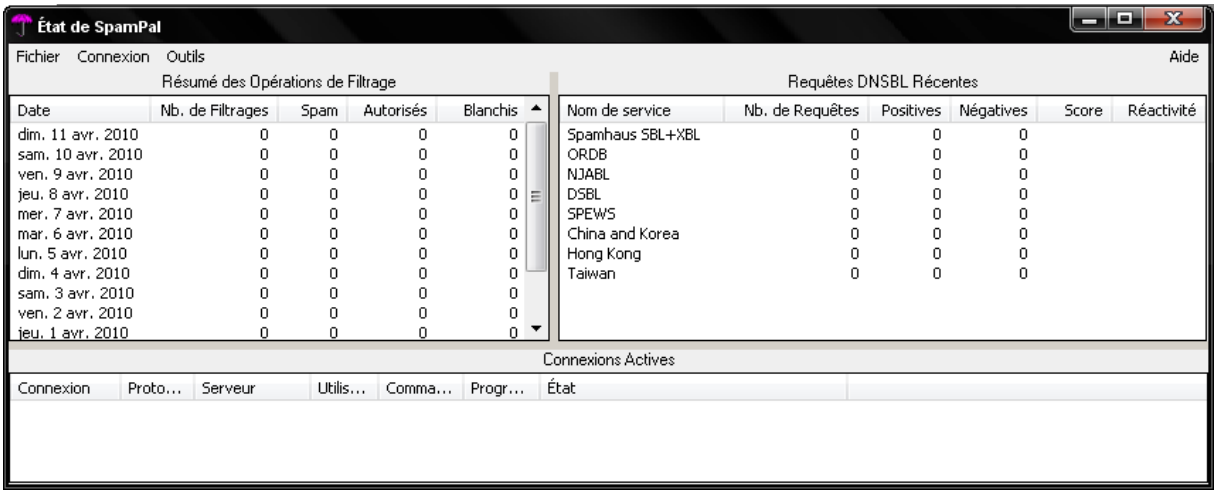
- Nom de compte : **securinets@yahoo.fr**
- Mot de passe : xxxxxxxxxx
- Courrier entrant (POP3) : pop.mail.yahoo.fr /port : 465
- Courrier sortant (SMTP) : smtp.mail.yahoo.fr /port : 995

SpamPal :

L'installation de SpamPal est simple à partir de l'exécutable Windows. Pour la configuration de cet outil anti-spam, il faut définir le client e-mail qui est dans notre cas Outlook Express. SpamPal récupère la configuration

de ce dernier et affiche les comptes disponibles pour en choisir celui pour lequel on veut appliquer le filtrage.

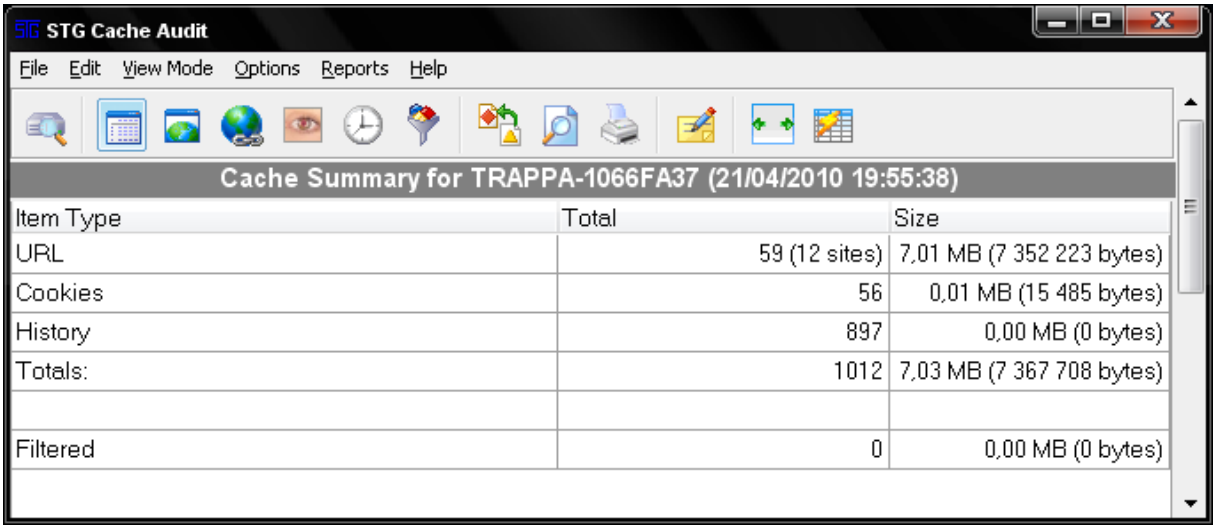
L'interface graphique de SpamPal contient une frnêtre principale divisée en trois panels : Résumé des opérations de filtrage, Requêtes DNSBL Récentes et enfin Connexions Actives comme on peut le voir dans la capture suivante :



Le paramétrage de SpamPal se fait par la définition de la liste blanche et la liste noire. L'utilisateur peut définir des adresses de confiance dans la liste blanche, comme il peut définir des adresses à considérer comme spam dans la liste noir. L'ajout dans la liste blanche ou la liste noire de SpamPal se fait à partir de la fenêtre principale -> Outils -> Ajout à la Liste Blanche ou Ajout à la Liste Noire.

STG Cache Audit :

On peut facilement installer STG Cache Audit sur Windows XP. L'outil dispose d'une interface conviviale et facile d'utilisation. Au lancement il affiche des statistiques URL, cookies et historique :



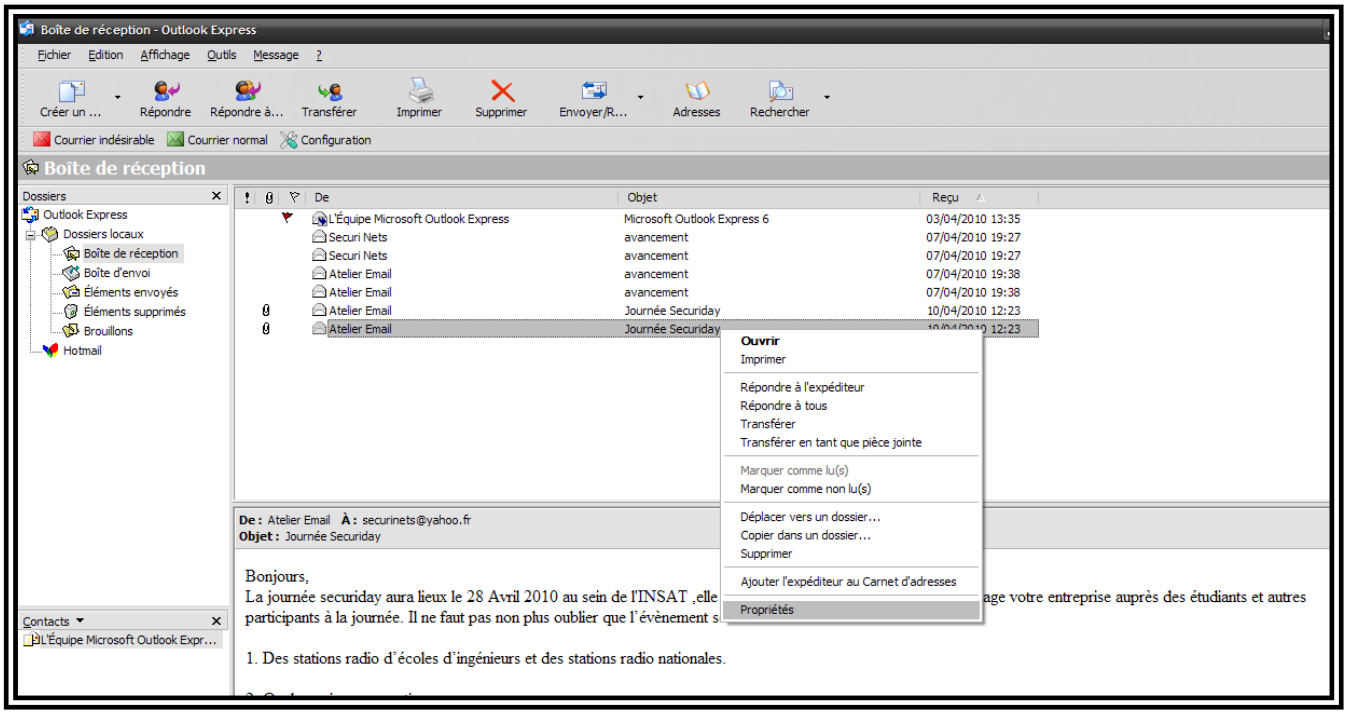
STG Cache Audit permet de voir de façon plus détaillées les informations résumées dans l'interface de lancement. L'investigateur peut utiliser les liens sauvegardés dans l'historique ou les cookies pour se rendre sur des sites visités par l'utilisateur en quête de preuves d'attaque.

4. Un petit scénario de test

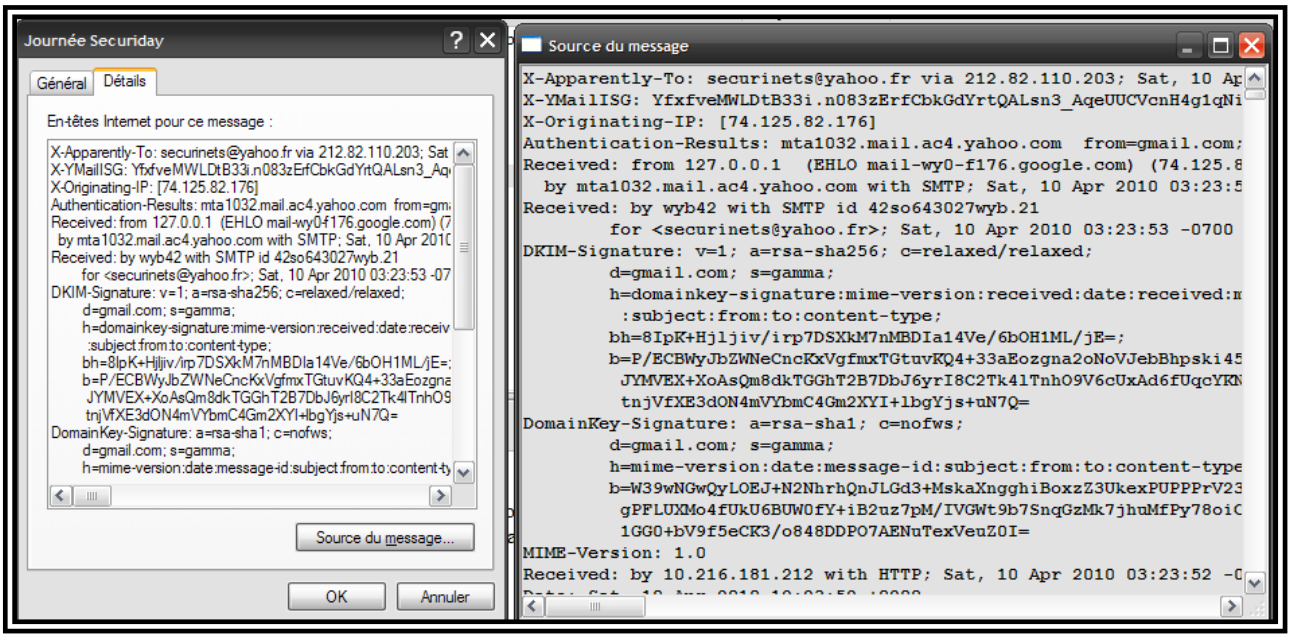
Dans cette partie, nous commencé par envoyer un e-mail de test que nous avons récupéré avec Outlook Express, puis nous avons récupéré l'en-tête de cet e-mail pour voir de plus près les différents champs de l'entête et comment ceci peut nous servir pour savoir s'il s'agit d'e-mail suspect.

L'e-mail de test a été envoyé de l'adresse atelier-securinets@gmail.com vers l'adresse securinets@yahoo.fr.

Pour récupérer l'e-mail dans Outlook Expresse, il suffit d'utiliser le bouton « Récupérer tout ». Il suffit maintenant de faire un clic droit sur le message dans la boite de réception puis de sélectionner "Propriétés" :

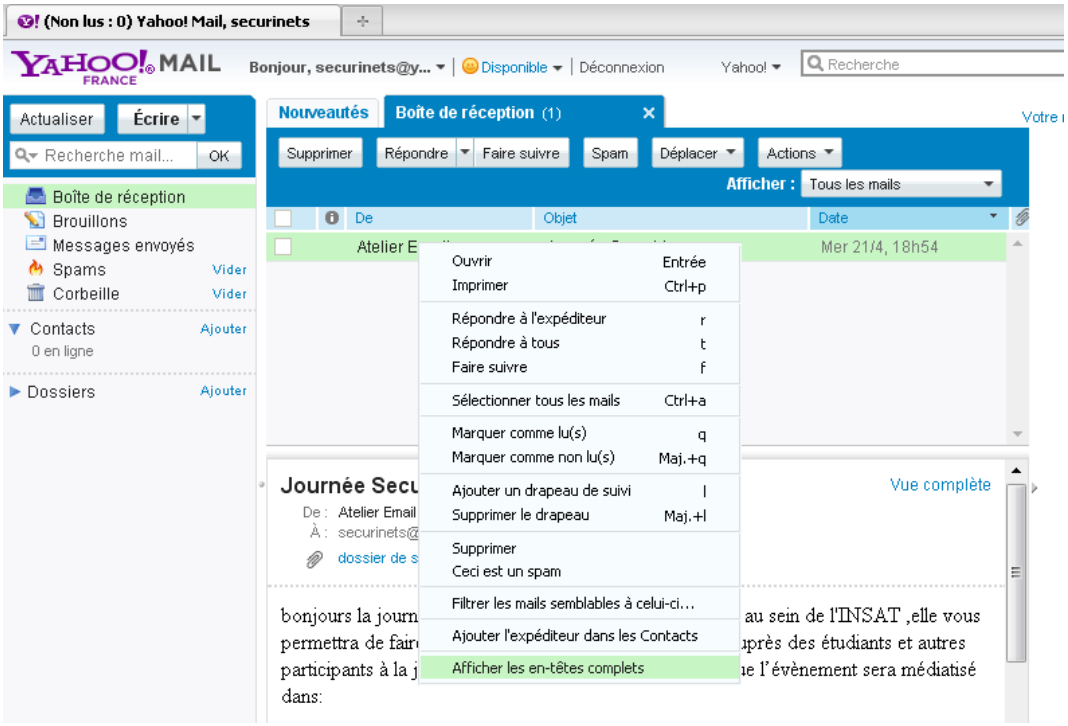


Une nouvelle fenêtre s'ouvre. A ce niveau il ne reste que de cliquer sur l'onglet "Détails" puis sur "Source du message" et le message ainsi que son en-tête apparaissent en détail dans la fenêtre a droite en cliquant sur "Source de message" comme nous pouvons voir ci-dessous :



Nous pouvant aussi récupérer l'entête en utilisant un Web Based Email ou Webmail comme Yahoo. En ouvrant la boite de réception, il suffit de

pointer sur le courriel, un clic droit puis "Afficher les entêtes complets". Nous pouvons voir cette opération ci-dessous :



En analysant l'en-tête du message de plus près, nous pouvons extraire une bonne quantité d'information relative aux éléments impliqués dans la transmission de l'e-mail de l'expéditeur vers le destinataire.

Pour pousser l'analyse, il existe des sites Internet qui offrent gratuitement des moyens d'analyse pour les entêtes des e-mails. Nous citons par exemple le site **http://headertool.apelord.com** qui peut rechercher des informations sur les champs correspondant au transmetteur et au récepteur de l'e-mail.

5. Conclusion

A travers cet atelier, nous avons vu les différents champs de l'en-tête d'un email et comment ces champs peuvent indiquer qu'il s'agit d'un courrier suspect, ce qui peut être pour l'investigateur d'une grande utilité. Nous avons vu aussi un exemple d'anti-spams capable d'analyser un e-mail pour savoir s'il s'agit d'un spam et ainsi déceler des tentatives d'attaque éventuelles prenant la forme de courrier inoffensif. Pour finir nous avons vu comment, par un moyen très simple, extraire des informations sur l'historique de navigation de la victime pour chercher des liens suspects.