Gérer vos domaines sur la nouvelle plateforme antispam de RENATER

Webinar du 30 septembre 2013, 14h

Laurent Aublet-Cuvelier et Olivier Salaün
support-antispam@support.renater.fr

RENATER
CONNECTEUR DE SAVOIRS

Organisation du webinar

- La nouvelle plateforme : panorama
- Démonstration du portail d'administration
- Focus sur certains aspects
  - logs, champs d'entête, seuils de filtrage, signalement, phishing, publicité
- Vos questions...
  - ...posées via le "chat"

RENATER
CONNECTEUR DE SAVOIRS

La nouvelle plateforme

- Une nouvelle solution logicielle
  - Vade Retro Cloud
  - hébergée chez RENATER
- Solution plus industrialisée
  - portail d'administration
- Retro-compatibilité
  - même moteur de filtrage
  - même RBL
  - import des configurations de chaque site raccordé

RENATER
CONNECTEUR DE SAVOIRS

Le portail d'administration

- raccordement (LDAP et relais SMTP)
  - ajout de domaines
- politique de filtrage
- listes noires/blanches
- journaux, moteur de recherche
- tableau de bord et statistiques

RENATER
CONNECTEUR DE SAVOIRS

Gestion des droits d'accès au portail d'administration

- authentification SAML (Shibboleth)
  - IdP d'établissement ou Compte CRU
  - identification = eduPersonPrincipalName
- 1-n administrateurs par site
  - redécoupage éventuel des sites
- désignation des administrateurs
  - via guichet antispam
  - gestion autonome des administrateurs

RENATER
CONNECTEUR DE SAVOIRS

Vos différents points d'accès

- portail des services
  - https://services.renater.fr/antispam/index
- guichet antispam
  - https://membres.renater.fr/antispam
- portail d'administration
  - https://antispam.renater.fr/
- serveur FTP
  - ftp://log-paris1.relay.renater.fr

RENATER
CONNECTEUR DE SAVOIRS

Portail d'administration

- Démonstration

RENATER
CONNECTEUR DE SAVOIRS

Accès à vos logs de filtrage

- Anciennement
  - 1 fichier de log par domaine
  - synchronisable via FTP
- Maintenant
  - moteur de recherche dans le portail d'admin
- Très bientôt
  - des fichiers de logs par domaine

RENATER
CONNECTEUR DE SAVOIRS

Champs d'entête SMTP systématiques

- X-Renater-ServerName: mxb2-2.relay.renater.fr
- X-Original-Source-IP: 81.255.196.200
- X-Renater-SpamState: 0
- X-Renater-SpamScore: 0
- X-Renater-SpamCause: gggruggvucftvg...

RENATER
CONNECTEUR DE SAVOIRS

Champs d'entête SMTP conditionnels

- X-Renater-Spam-Status: Yes
- X-UCE-Status: Yes
- X-UCE-Type: DCE|MCE|PCE
- X-Renater-AvState: 1
- X-DSN-Status: Yes

RENATER
CONNECTEUR DE SAVOIRS

Seuils de filtrage

- Selon Spam Score :
  - 0-99 : ham
  - 100-299 : spam low
  - 300 à 499 : spam medium
  - 500 ou plus : spam high

RENATER
CONNECTEUR DE SAVOIRS

Signalements FP, FN, Phishing

- via plugin Report-Spam (Thunderbird)
  - faux-positifs, spams non détectés
    - remontée à Vade Retro
  - phishing
    - signalement au CERT RENATER
- via boîte IMAP
  - faux-positifs, spams non détectés

RENATER
CONNECTEUR DE SAVOIRS

Filtrage de la "publicité"

- intitulé trompeur
  - apparence de message publicitaire
- comportement par défaut
  - marquage Subject : [PUB]
  - ajout champs SMTP
    - X-UCE-Status: Yes
    - X-UCE-Type: PCE|MCE|DCE
- gestion des faux positifs
  - signalement via boîte IMAP
  - ajout règle sur liste blanche
  - modification du marquage
- Plugin Report-Spam
  - ne gère pas les publicités pour l'instant

RENATER
CONNECTEUR DE SAVOIRS

Evolutions

- fonction check SMTP
  - permet de vérifier la validité des destinataires via le protocole SMTP
  - à la place des requêtes LDAP
  - pas encore testé par RENATER
- portail de décryptage des SpamCauses
  - X-Renater-SpamCause: gggruggvucftvghtrhhoucdtuddrfeeiledrtdeigdeggecutefuodetggdotefrucfrrhhofhhilhgvmecutffgpfetvffgtfenucurghilhhouhhtmecufedttdenucdnodfutggrmhihqdfnohhtvghrihgvqdgvnhdqfhhrucdlfedttddm
  - donne des éléments sur la cause du marquage des spams

RENATER
CONNECTEUR DE SAVOIRS

Vos questions...