TRACK UP

Le 14 Juin 2011

OSSIR

Seed List Management pour la Surveillance des bases de données email

Contacts Market Espace

- **Yannick Denis**
  - ydenis@marketespace.fr
  - 03.20.699.111

- **Lionel OBIN**
  - lobin@marketespace.fr
  - 03.20.699.123

http://track-up.com

@track_up

Préambule

- **La base des clients représente l'un des actifs les plus important de l'entreprise.**
  - → Des données potentiellement convoitées par autrui, et facilement monnayables.
  - → En particulier les emails qui peuvent être surexploités à l'insu du propriétaire

- **Et donc les conséquences sont importantes en cas de vol**

  - **Pour l'entreprise / l'annonceur**
    - Dégradation de l'efficacité de ses campagnes : visibilité, délivrabilité
    - Risque en terme d'image de marque : buzz négatif (monétisation des données clients)
    - Usurpation d'identité de la marque (phishing)

  - **Pour les internautes / les consommateurs**
    - Spamming : réception d'énormément de messages publicitaires non ciblés, sans leur consentement préalable (optin)
    - Tentatives d'escroquerie (phishing…)

Préambule

- Pour parer aux tentatives d'intrusion et de vol de données, des **mesures de sécurité informatique** sont sans doute en place (firewall, DMZ…)

- Néanmoins **le risque zéro n'existe pas,** tant en externe qu'en interne
  - **48% des vols de données sont liés à des utilisateurs « internes »** (+26% v/s 2009)
    Source : *Data Breach Investigations Report 2010* - Verizon Business Risk Team

La solution TrackUP est un **dispositif supplémentaire de contrôle** qui s'intègre en **complément des différents outils et logiciels** déjà en place, et qui permet de disposer de **preuves certifiées** en cas de vol avéré.

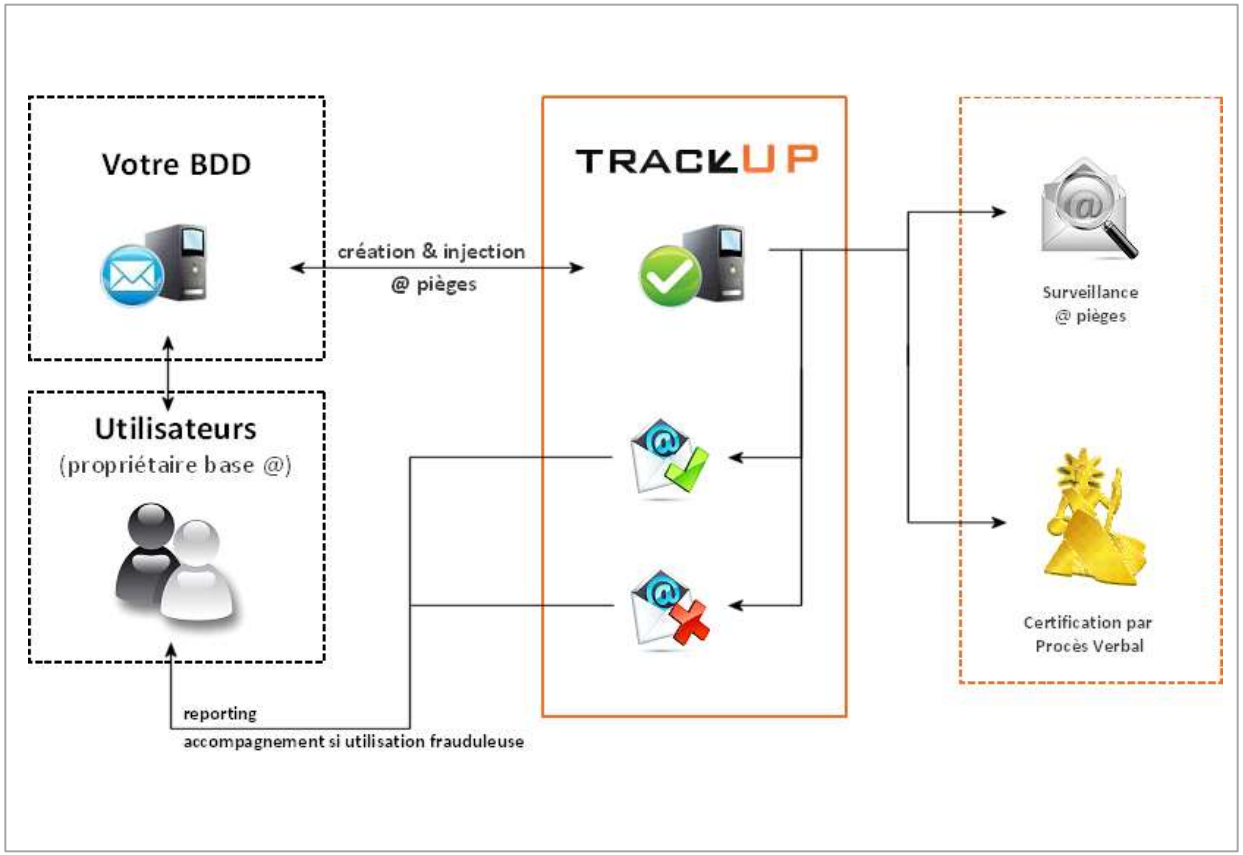
La solution de Seed List management

→ **injection d'emails pièges dans votre BDD**

1. Audit de votre base de données (volume, profil, critères,…)
2. Préconisation du volume et création des pièges (sur mesure)
3. Injection des emails pièges
4. Certification des emails pièges
5. Tracking de tous les flux

→ **Reporting des flux** qui permet de contrôler leur conformité avec vos campagnes,…

→ …et de **détecter immédiatement** toute utilisation anormale.



La solution de seed list management

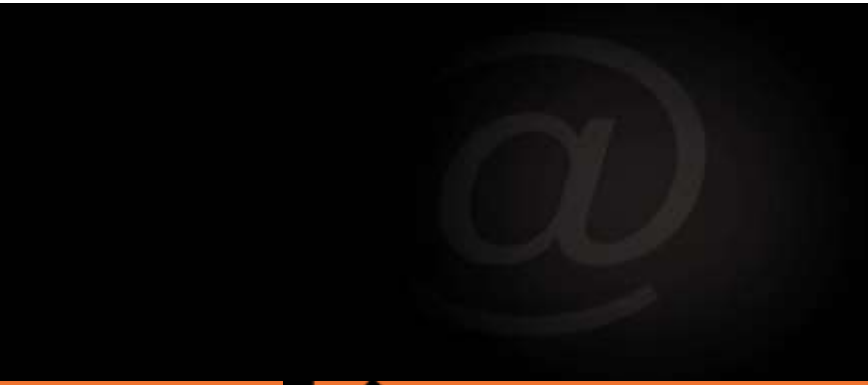
- TrackUP est une solution de **gestion d'emails pièges** qui assure au propriétaire des données une **surveillance automatisée, continue et certifiée** de ses emails :
  - **Surveillance automatisée en temps réel, et illimitée des pièges**
  - **Process de certification des pièges par autorité de justice**
  - **Déploiement de la solution en mode SaaS**

→ **Tracking de tous les flux sortants de la base emails**

- Objectif : valider que les emails ne font pas l'objet d'exploitations illicites ou frauduleuses à l'insu du propriétaire.

En cas de détournement ?

- **TrackUP vous permet :**
  - de **détecter immédiatement** toute utilisation frauduleuse de vos adresses emails,
  - de disposer de **preuves certifiées pour enclencher une procédure** de saisine (contrefaçon de données),
  - et de réagir ainsi rapidement pour **stopper les envois illicites et éviter la propagation** de vos données vers d'autres tiers.



OSSIR - Le 14 Juin 2011

TRACK UP

Exemples de cas client

Cas LDLC

- Le cas a été relevé sur le forum OVH en septembre 2010
- 10-09: Un spammeur est identifié au nom de leo-et-lea.com
  - « J'ai moi aussi reçu ce spam, ainsi que deux personnes de mon entourage. Dans tous les cas, nos nom et prénom étaient bien mentionnés. Dans tous les cas, nous considérons ces mails comme du spam, clairement non solicité »
- 11-09: La collaboration des membres du forum permettent d'identifier LDLC comme l'origine du SPAM
  - « J'ai également reçue ce mail sur une adresse qui n'est utilisée que pour mon comte LDLC. Ça m'a fait tout drôle de recevoir un spam sur cette adresse que j'ai depuis 6 ans sans avoir eu le moindre problème. Soit LDLC à vendue sa base de client soit il s'agit d'un nouveau site lancé par LDLC pour lequel ils ont procédé à une inscription automatique plus que douteuse »
  - Le site www.leo-lea.com est pris pour cible des internautes mécontent, certains écrivent aussi à LDLC
- 12-09: Les membres déduisent par recoupement que le fichier utilisé est un extrait de clients LDLC, inscrits entre fin 2006 et 2008

Cas client LDLC

- 13-09: Démenti de LDLC envoyé par mail à l'un des membres, puis publié

  « Aucun fichier n'a été donné a qui que ce soit, et il n'a pas pu être piraté.

  Tout au plus dans le pire des cas le responsable des envois de mail aurait pu en faire une copie un jour et la redonner (ou vendre) a quelqu'un.

  Cela dit nous n'avons jamais eu aucun retour dans ce sens avant votre mail ce qui rend la chose tout aussi peu probable. J'opterai donc pour une coïncidence le fait que ce soit un email que vous utilisiez chez nous, mais que la source est ailleurs.

  Quand au mot de passe, ils sont « hachés » ce qui signifie qu'ils ne sont pas lisibles sans connaitre l'original. Aucune chance de se les faire 'voler' »

- 13-09: Ce démenti ne satisfait pas les membres et réclament des explications à LDLC

  « Bon, décidément on ne veut rien nous dire chez LDLC. Ce qu'il faudrait c'est leur donner l'URL de ce forum. »

Cas client LDLC

- 14-09: Communication de LDLC sur le Forum

  « bonjour
  Nous avons passé la journée sur ce problème et enquêtons sur la façon dont ces données ont pues sortir de chez nous. Il n'y a aucun moyen de récupérer de façon "externe" le mail + nom + prénom. Malgré tout l'ensemble des éléments que vous avez transmis indique qu'il y a une très très forte probabilité que les données viennent de nos bases.
  Le mail indiquant que les mots de passes étaient hachés vient bien de chez nous et c'est une erreur, effectivement ils ne le sont plus depuis très longtemps. Pour permettre aux clients de les récupérer à la demande.
  Il est donc presque certain que l'un de nos anciens employés, n'est pas parti les mains vides et a soit donné soit revendu un fichier de ces mails et nom/prénom. Dans tous les cas de notre coté nous allons tout faire pour retrouver et attaquer la personne qui a utilisée ces mails, ainsi que sa source.
  La direction de LDLC »

→ **Quelles conséquences pour LDLC, et quelles actions possibles ?**

Cas client #1

- Société du secteur Internet (éditeur)
  - **Vol des données en interne (collaborateur DSI) : 1,9M d'emails**

- Le collaborateur a quitté la société, puis rejoint une agence de e-marketing qui réalise notamment des campagnes à la performance pour le compte d'annonceurs.

- Le fichier a été injecté dans le programme « bons plans » de l'agence, puis exploité à des fins de monétisation publicitaire.

→ **TrackUP a permis à notre client :**

- De détecter rapidement l'utilisation frauduleuse de ses emails

- D'obtenir des preuves certifiées permettant de déclencher une procédure
  - Saisie des serveurs de l'agence incriminé (où ses emails ont été retrouvés)
  - Citation à comparaître

→ L'utilisation illicite des emails a été stoppée… un arrangement « à l'amiable » a été trouvé entre les parties.

Cas client #2

- Société du secteur E-Commerce
  - **Vol des données en externe (prestataire) : 2,7M d'emails**

- Notre client a confié au prestataire une copie de sa base de données.
  - Un jeu de pièges spécifiques a été injecté dans la base transmise à ce prestataire

- Le fichier est été volé chez ce prestataire, puis exploité à des fins de monétisation publicitaire par une autre société.

→ **TrackUP a permis à notre client :**

- De détecter immédiatement l'utilisation frauduleuse de ses emails, et son origine

- D'obtenir des preuves certifiées permettant de déclencher des procédures
  - A l'encontre de la société qui utilise les emails (saisie des serveurs,…)
  - A l'encontre du prestataire dont la responsabilité est mise en cause (défaut de sécurité)

→ Les procédures sont en cours…