Attaques informationnelles : Méthodologie d'analyse

étude de cas réels

Danielle Kaminsky

Chercheur en Cybercriminalité
dkam2@wanadoo.fr

sstic Juin 2004

Attaques informationnelles

- **Sur Internet, réseaux, systèmes d'info :**

  - faciles, peuvent être violentes
  - menaces pour la sécurité économique
  - but : affaiblir, entraver, miner, détruire

- **Critères de choix des cas réels étudiés:**

  - attaques >> systèmes d'information
  - à visage masqué >> investigation
  - données rendues publiques au préalable

Attaques informationnelles

- Méthodologie d'analyse pour aider à :

  - détecter la menace
  - caractériser les attaquants
  - déterminer l'origine
  - comprendre la nature
  - appréhender l'ampleur

>> améliorer la connaissance et la protection contre ces risques

sstic04

Quoi ? Contre qui ? Qui ? Pourquoi ?

Quoi ?

- **Acte délibéré qui utilise l'information pour générer une mauvaise perception, déstabiliser, discréditer, démoraliser, nuire.**
- **Défaire le lien de confiance**

Contre qui ? Cibles ?

- **entreprises, organismes, personnes, produits, projets**

Qui ?

- **Particuliers ou agents**

Pourquoi ?

- **Colère, vengeance, frustration, envie,**
- **Intérêts concurrents ou adverses (éco, financiers, politiques, sociaux, culturels etc)**

Etude des cas :

- **Cas N°1 : attaque informationnelle contre un article scientifique**
- **Cas N°2 : attaque informationnelle contre un groupe pharmaceutique**

Etude des cas :

- **Cas N°1 : attaque informationnelle contre un article scientifique**

SSTIC – Juin 2004

Décrédibilisation d'un article scientifique

Les faits :

- **Novembre 2001 : NATURE publie un article de deux cherheurs de l'Université de Berkeley en Californie**
- **Ignacio Chapela et David Quist**
- **Leur étude montre que du maïs mexicain a été contaminé par du pollen de plante génétiquement modifiée, à très longue distance.**
- **En Mars 2002 : NATURE indique que l'article n'aurait pas dû être publié**

Que s'est-il passé ??

Les faits

- **Le jour de la publication de l'article**
- **Sur le site web de Agbioworld**
- **Dans son espace de discussion , environ 3000 scientifiques du monde entier**
- **Message de Mary Murphy, à propos de I.Chapela :**
- *« not exactly what you call an unbiased writer »*
- **Message de Andura Smetacek :**
- *Le papier de Chapela n'a pas été relu par des tiers*
- **Son auteur est** *« first and foremost an activist »*
- **La recherche a été publiée « en collusion avec des environnementalistes ».**

Les faits

- **Le jour suivant**
- **Message de Andura Smetacek**
- **Pose une question dans la liste de discussion :**
- ***« How much money does Chapela take in speaking fees, travel reimbursements and other donations…for his help in misleading fear-based marketing campaigns ? »***
- **Effet boule de neige dans la liste : répétion, amplification, aggravation**
- **Demandes que Chapela soit évincé de l' Université**
- **Lancement d'une pétition**
- **>>>> Réaction de NATURE : la recherche n'aurait jamais du être publiée**

- Investigations

-- **Article dans The Guardian, 14 mars 2002, Georges Monbiot**

« The Fake Persuaders »

- **Qui sont Mary Murphy et Andura Smetacek ?**
- **Compte email Hotmail**
- **Déclarent être des personnes ordinaires**
- **N'avoir aucun intérêt commercial**

- Investigations

-- Ancien message de Mary Murphy (2 ans avant)

- **sur autre serveur de news**
- **Traces entêtes du message : bw6.bivwood.com**
- **Bivwood.com > Bivings Woodell > The Bivings Group**
- **Monbiot lui écrit pour savoir si Mary Murphy est son vrai nom et si elle travaille chez Bivings**
- **Elle lui répond qu'elle n'a aucun lien avec l'industrie**
- **Refuse de répondre à ses autres questions : motif :**
- **« I can see by your articles that you made your mind up long ago about biotech »**
- **Or, il ne lui avait pas parlé de biotechnologies.**
- **il lui avait dit qu'il faisait une recherche sur le lobbying sur Internet**

- Investigations

Andura Smetacek :

- **dit habiter Londres et New York**
- **Pas de traces dans ces villes**
- **Son « nom » apparaît seulement sur AgbioWorld**
- **Et quelques autres serveurs de listes**
- **Monbiot lui écrit : pas de réponse**
- **Autres messages de Andura Smetacek**
- **fait la promotion de « The Center For Food and Agricultural Research » (cffar).**
- **Le site web cffar.org enregistré par un homme**
- **Qui se trouve être le Directeur des associations de Bivings Woodell**

- Investigations

-

- Le modérateur du site web où a été lancée la pétition soutient n'avoir aucune connection avec Bivings Group
- Un message d'erreur lors d'une recherche sur ce site :

« can't connect to MSQL server on Appollo.bivings.com »

- Appollo.bivings.com est le serveur principal de Bivings Groups
- BG : firme spécialisée dans le lobbying sur Internet («Viral Marketing : How to Infect the World »)

- Investigations-

- 2ème article du Guardian :
- « Corporate Phantoms »
- Mary Murphy > web designer de Bivings
- Andura Smetacek > chef marketing Internet de la société
- Site Bivings (société spécialisée lobbying sur Internet):

« There are some campaigns where it would be undesirable or even disastrous to let the audience know that your organization is directly involved ».

Méthodologie d'analyse

1) Fait déclencheur :

- **La publication de l'article dans NATURE**
- **Fait connu au moment de l'attaque**
- **Il est mentionné par les attaquants eux-mêmes**

2) Auteur(s)-perpétrant(s) de l'attaque :

- Deux personnes
- **Agissant à visage masqué (pseudos etc)**
- **Ne sont pas des chercheurs scientifiques du domaine**
- **Se révèlent être :**
- **Reliés à une entreprise commerciale**
- **Clients acteurs biotechnologies, OGM**
- **= Intérêts en opposition avec le résultat de l'étude publiée par les chercheurs**

3) Lien attaquants – cible :

- **Pas de liens personnels**
- **Intérêts antagonistes**
- **Intérêts défendus ou servis par les attaquants en opposition avec le résultat de l'étude publiée par les chercheurs**

4) Lieu où s'effectue le lancement de l'attaque

- **Lieu choisi**
- **Site spécialisé biotechnologies**
- **Appartient à une fondation soutenant les biotechnos**
- **Caractéristique du lieu choisi :**
- **Espace public à forte visibilité**
- **Portée mondiale**
- **Fréquenté par des scientifiques concernés**

5)Assistance choisie pour l'attaque:

- **Scientifiques**
- **« Pairs » des auteurs de l'article**
- **Rapport avec le sujet traité par l'article**
- **Public « conquis » d'avance**

6) Contenu de l'attaque, axes thématiques :

- **Doute sur crédibilité de l'étude**
- **Fond sapé par attaque « ad hominem »**
- **Objectivité des auteurs mise en cause**
- **Désignés comme *« activistes »***
- **article *« pas relu par tierce partie »***
- **Renforcement sur doute et manque d'objectivité**
- **Argument argent, alimentation d'intérêts**

« Campagnes de marketing trompeur basé sur la peur »

- **Mots « campagnes »,« marketing »**
- **Évoquent stratégie, plan, plan de communication**
- **> Manipulation**
- **Expression : « basé sur la peur » :**
- **Renforcement de la notion de plan**
- **+ : Provoque méfiance, rejet**

« Marketing trompeur basé sur la peur »

- **Qualificatif : « trompeur »**
- **Pièce maîtresse de l'édifice**
- **Avec « campagnes » et « marketing » Effrite et supprime la valeur de recherche de l'étude**
- **Lui substitue celle**
- **D'opération de manipulation**

- **7) Intensité :**

- **Attaque conduite en crescendo**
- **En quelques paliers seulement**
- **Passage entre notion de manque d'objectivité à opération calculée et trompeuse : rapide**
- **Quelques phrases**

- **8) Amplification :**
- **Effet boule de neige**
- **Amplification par l'assistance**
- **Instrumentalisée à son insu**
- **Chacun en rajoute, contribue, amplifie le doute**
- **Point culminant-étape : la pétition**
- **Impact- réussite : la revue remet en cause l'article qu'elle avait publié**

- **9) Temps :**
- **Les 2 lanceurs de l'attaque restent peu de temps dans l'espace de discussion**
- **Ils s'éclipsent rapidement, après avoir enclenché la mécanique du doute**
- **Laissent les participants se charger de la dissémination et de l 'amplification**
- **1ère phase de temps : intervention des lanceurs : courte**
- **2ème phase : la machine est lancée, ce sont les autres qui vont l'alimenter = phase + longue**
- **3ème phase : la pétition**
- **4ème phase : obtention du mea culpa de la revue**
- **= couperet**
- **En tout : environ 4 mois !**

10) Anomalies et erreurs commises :

- **Permettent de déceler attaque informationnelle**
- **Intervention à visage masqué**
- **Pas de face à face avec les auteurs de l'article**
- **Traces techniques reliant à firme**
- **Traces Convergentes**
- **Info fausse – affirmation : pas relu par des tiers**
- **Réponse au journaliste : parti pris contre biotech**
- **Thématique en miroir ou attaque symétrique :**
- **(intérêts > attaque sur intérêts)**

11) Contexte de l'attaque :

- La culture de plantes transgéniques n'est pas autorisée au Mexique à l'époque des faits.
- La culture transgénique suscite des oppositions dans plusieurs pays.

12) Forme de l'attaque :

- **Il ne s'agit pas d'une attaque frontale**
- **Attaque indirecte**
- **Attaque ciblée contre auteurs de l'article**
- **Attaquants ne s'adressent pas aux auteurs de l'article, mais à un public tiers**
- **Attaque perpétrée en public**
- **Insinuations, affirmations, questions**
- **Il est dévolu au public d'amplifier l'attaque :**
- **Attaque par infusion**
- **Attaquants à visage masqué**
- **Sans investigation, pas de compréhension de la situation**

13. Impact souhaité :

- **Mise en doute de l'étude auprès d'autres chercheurs du domaine concerné**
- **Auprès de leurs propres « pairs »**
- **Discrédit**
- **Dévalorisation**

14. Impact effectif :

- **Mise en doute de l'étude auprès d'autres chercheurs du domaine concerné**
- **Auprès de leurs propres « pairs »**
- **Discrédit**
- **Dévalorisation**
- **Discrédit auprès de la revue scientifique**

15. Impact potentiel supplémentaire :

- **Discrédit auprès de l'Université où travaillent les deux chercheurs auteurs de l'article**
- **Eventualité de leur renvoi ou mise à l'écart**
- **Difficultés éventuelles de financement de leurs prochaines recherches**
- **Difficultés éventuelles pour publier d'autres recherches**

Etude des cas :

- **Cas N°2 :**

  attaque informationnelle contre un groupe pharmaceutique

Les faits :

- **Le groupe pharmaceutique Smith & Nephew a reçu pendant presque 2 ans des messages électroniques dénigrants.**
- **Les messages sont adressés à des salariés et dirigeants du groupe en France, à l'étranger.**
- **Aussi : à des partenaires, des concurrents, des analystes financiers, des organes de presse.**

Les faits :

- **Les messages affirment que les produits du groupe sont défecteux, les dirigeants corrompus, etc.**
- **Semblent provenir de l'intérieur de la société**
- **En 18 mois : plusieurs centaines de milliers de messages sont envoyés**

SSTIC – Juin 2004

1) Fait déclencheur :

- **Non connu au moment de l'attaque**

2) Public visé par l'attaque :

- **Les messages sont adressés à des destinataires précis**
- **Spécifiés par leur adresse email**
- **Destinataires choisis**

2. Destinataires de l'attaque:

- **L'attaque est portée directement sur plusieurs cercles de l'entreprise visée**
- **Public interne : salariés et dirigeants**
- **Interne élargi : autres filiales du groupe à l'étranger**
- **Public externe : partenaires fonctionnels de l'entreprise, commerciaux, interlocuteurs financiers**
- **Public externe élargi : les concurrents**
- **Public externe encore + élargi : les médias**

3 . Impact souhaité :

- énorme, tous cercles importants visés dans l'attaque
- Attaque a la capacité de briser le lien de confiance qui unit l'entreprise à ses propres salariés, ses interlocuteurs, ses clients
- Volonté de nuire
- Attaque a la capacité d'atteindre à la pérénnité de l'entreprise
- Très haut degré de risque pour l'entreprise attaquée

4) Temps : durée de l'attaque :

- Presque 2 ans
- Presque tous les jours
- Parfois plusieurs heures par jour
- Parfois 6 à 9 heures par jour
- Beaucoup de temps
- Une activité quasiment à temps complet
- Sur une très longue durée

5. Contexte de la cible :

L'entreprise est le N°5 mondial

En pourparlers de rapprochement

Enjeu important : devenir le N°1

Produits santé

- **Attaque en provenance**

de concurrents ?

6. Attaquant(s)

Qui attaque ?

Qui envoie ces messages ?

Combien sont-ils?

Signes apparents : plusieurs personnes

Adresses expéditeurs : personnes internes

En provenance de plusieurs pays

9 langues différentes utilisées

Attaquants coordonnés ?

-**Attaquant(s)**

En réalité, non.

Un seul attaquant

7. Mode opératoire technique

Mode opératoire identique

Emails envoyés via sites web

« Envoyez à un ami »

80 sites de lancement utilisés

Tous offrent cette possibilité

Falsification d'adresse expéditeur

Remplacement contenu à transférer

8. Thématique de l'attaque -contenu

- Corruption des dirigeants
- Méthodes de vente malhonnêtes
- Produits affectés de malfaçons
- Procès en cours
- Thématique Justice

8) Contenu de l'attaque :

- **messages composés à partir de bouts de news + inventions**
- **Apparence de news**

9) Analyse comportementale du contenu :

- Thématique Justice très présente
- Récit sur mode croisade
- L'entreprise doit être punie
- Les dirigeants visés ne sont pas nommés directement
- Il est accusateur par la bouche de qqn d'autre (forme news)

10. Relation attaquant-cible:

- **Probabilité de relation personnelle avec l'entreprise visée.**
- **Il la connaît vraisemblablement**
- **Corrélation : Adresses emails spécifiques : il les connaît**
- **Corrélation : temps passé : temps libre et acharnement**
- **Corrélation : nombre de messages : colère, inassouvissement**
- **Corrélation : nombre messages + durée :**
- **harcèlement**

11. Contexte de l'attaquant :

Temps libre et temps consacré à l'attaque : évincé ou licencié

Thématique Justice : a eu vraisemblablement lui-même des problèmes qui lui ont valu action en Justice

(attaque en miroir, symétrique)

S'il a été licencié : vengeance

Entraîner l'autre dans sa propre « perte »

12. Précédents :

L’attaquant : salarié licencié

Motifs

Agissements similaires précédents

(corrélations)

>) Fait déclencheur :

- **Non perçu au moment de l'attaque**
- **Licenciement**

Méthodologie :

Grille d'analyse: paramètres

-

sstic04

- Cible de l'attaque
- Domaine d'activité de la cible
- Contexte de la cible
- Evènement déclencheur
- Evènement prétexte
- Contexte de l'attaque
- Public de l'attaque
- Impact souhaité
- Impact effectif
- Publicité donnée à l'attaque

- **Dissémination**
- **Recherche de caisses de résonnance**
- **Public et impact souhaité**
- **Réinjection**
- **Attitude vis à vis de la réinjection**
- **Temps**
- **Moment du lancement de l'attaque**
- **Attaque éclair ou distillée**
- **Durée dans le temps**
- **Amplitude**
- **Temps passé à l'attaque**
- **Organisation dans le temps**
- **Rythme, pics et pauses**
- **Relances, réactivation, entretien de l'attaque**

- Moyens techniques employés
- Précautions techniques
- Acteur principal
- Unique
- Identifié
- Historique
- Personne sous pseudonyme ou masque
- Comment l'individu se présente
- Mode opératoire
- Comportement
- Idées défendues, valeurs exprimées
- Réactions face à la contradiction

- Thématique de l’attaque
- Précédents sur ce thème ou ces thèmes
- Teneur
- Tonalité
- Evolution de la thématique
- Variations , aggravations, escalade
- Espace
- Lieu de lancement de l’attaque
- Particularité, raison du choix
- Ampleur
- Autres lieux

- Agents, renforts, assistants
- Nombre
- Organisation
- Action simultanée ou en relai
- Rôle
- Qui intervient
- Sur quel sujet
- A quel moment
- En réponse ou réaction à qui
- Réactions face à la contradiction
- Réseau de liens

- Intérêts servis par l'attaque
- Besoins assouvis par l'attaque
- Niveau de risque pris
- Niveau de risque pour la cible
- Niveau de contrôle de l'attaquant
- Niveau de réussite de l'attaque
- Où en est l'attaque au moment où elle est comprise
- Nécessité absolue de comprendre le tableau de la situation