PICTET
1805

IT Days 2014

Hery ANDRIANJAFY

20 novembre 2014
Luxembourg

Agenda

1. Introduction
2. Vol d’identité et fraude
3. Q & A

Bio

Hery ANDRIANJAFY

RSSI / CISO

Pictet & Cie (Europe) SA

- 20 ans d'expérience dans l'industrie bancaire (Suisse et Luxembourg)
- Plus de 17 ans d'expérience dans le domaine de la Sécurité de l'Information
- Auparavant auditeur de systèmes d'information
- Titulaire de Master en Administration des Affaires (MBA) et de Mastère en Informatique et Organisation
- Certifié ISACA (CISA - CISM – CRISC)
- Membre du Clusil, ISACA, CPSI
- Administrateur de l'APDL

PICTET
1805

Le groupe Pictet

Hery ANDRIANJAFY

20 novembre 2014
Luxembourg

Les principaux métiers du groupe

GROUPE PICTET

WEALTH MANAGEMENT

Wealth management solutions for private clients

- Pictet Wealth Management

ASSET SERVICING

Fund services, custody and trading services for asset managers, pension fund, banks and wealthy individuals

- Pictet Asset Services
- Trading
- Services for independent asset managers

ASSET MANAGEMENT

Solutions for institutional investors, distribution of investment funds

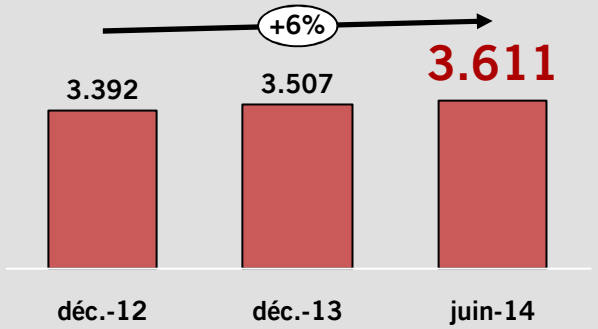
- Pictet Asset Management
- Pictet Alternative Investments

Chiffres clés du groupe Pictet

A fin Juin 2014

26 bureaux dans
17 pays

Collaborateurs du groupe (ETP)

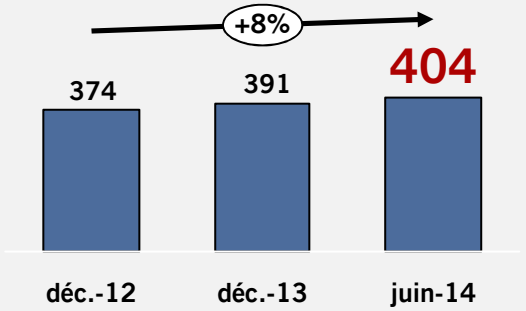


Moody's

Notation à long terme
Aa3

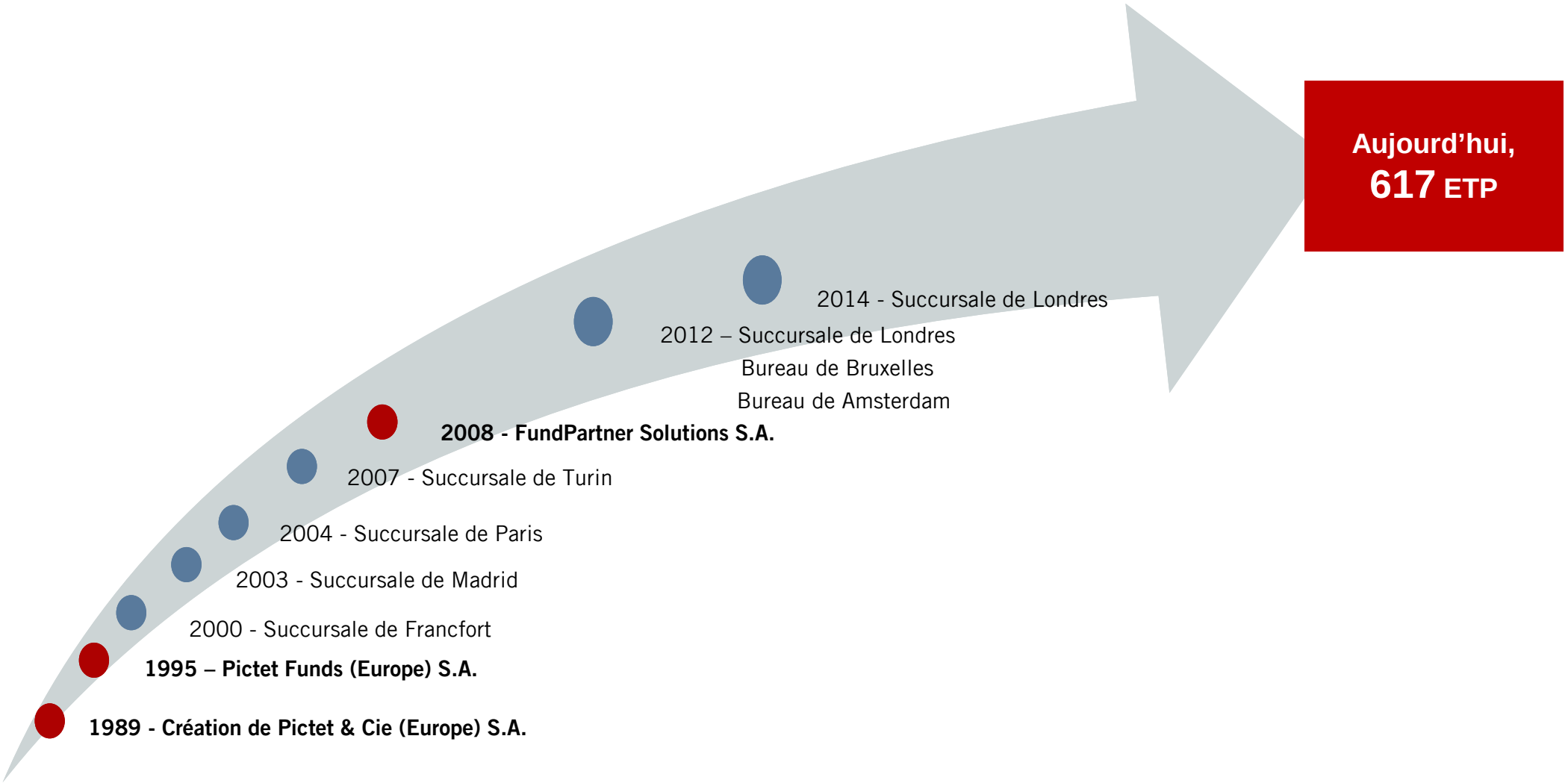
Notation à court terme
Prime-1

Actifs sous gestion ou en dépôt (CHF mia)



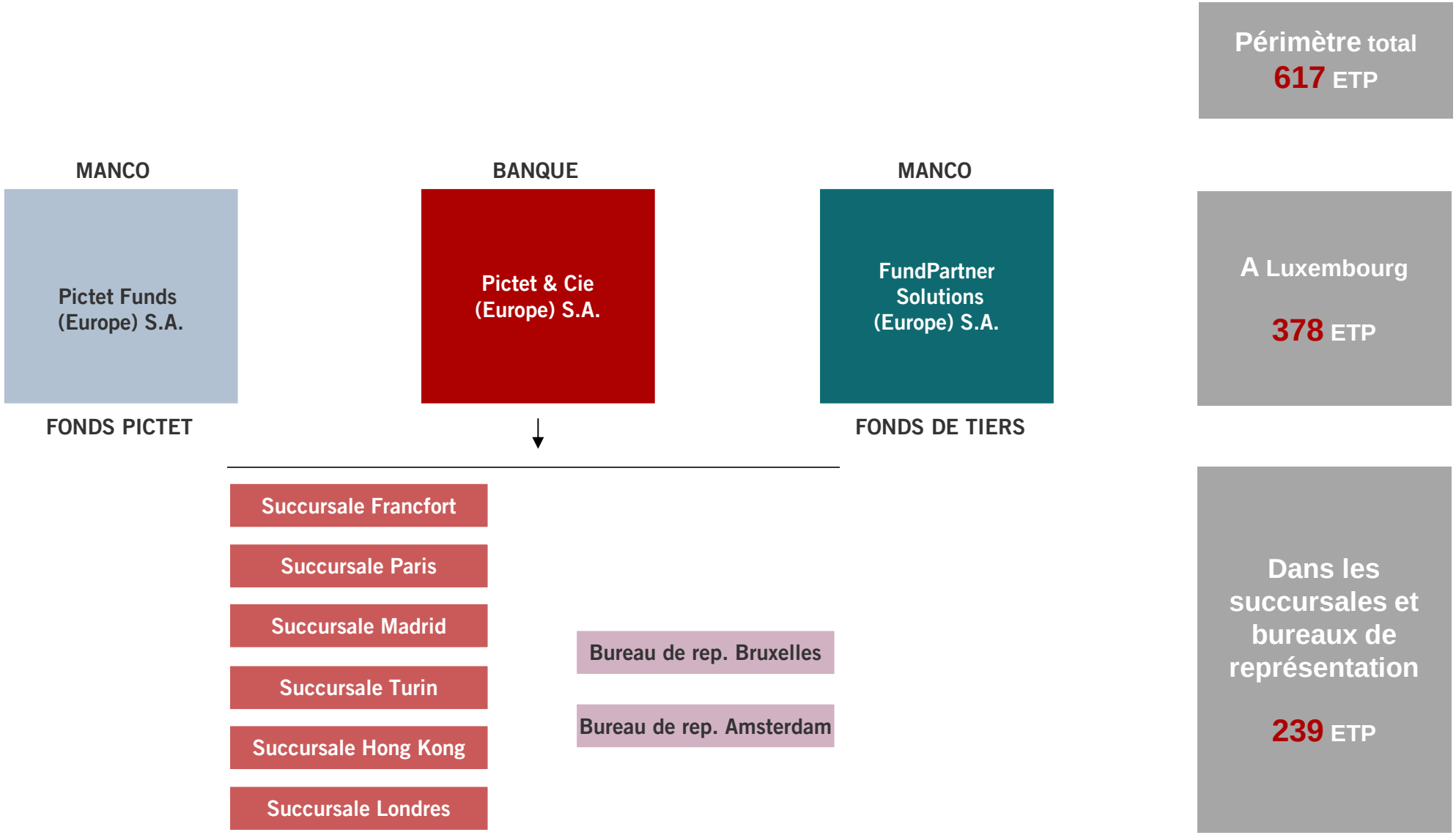
Produits d'exploitation	CHF **975** mio
Bénéfice consolidé	CHF **203** mio
Ratio de fonds propres totaux	**21.7%**
Ratio de fonds propres de 1ère catégorie	**21.7%**
Ratio de liquidité à court terme	**166%**

Pictet à et à partir de Luxembourg: une croissance continue



Les différentes entités Pictet à et à partir de Luxembourg

(groupe Pictet: 3.611 ETP)



PICTET
1805

Vol d'identité et fraude

Hery ANDRIANJAFY

20 novembre 2014
Luxembourg

Top 10 des menaces !

Des menaces nécessitant pas ou très peu de support technologique

Top Threats	Current Trends	Top 10 Threat Trends in Emerging Areas						
		Critical Infrastr.	Mobile Computing	Social Networking	Cloud Computing	Trust Infrastr.	Big Data	Internet of Things
1. Drive-by Downloads	↑	↑	↑	↑		↑	↑	
2. Worms/ Trojans	↑	↑	↑	↑	↑	↑	↑	↑
3. Code Injection	↑	↑	↑	→	↑	↑	↑	
4. Exploit Kits	↑	→	↑	↑	↑	↑	↑	
5. Botnets	→	↑	↑	↑	↑			
6. Physical Damage/Theft /Loss	↑	↑	↑	↑	↑	↑	↑	↑
7. Identity Theft/Fraud	↑		↑	↑	↑	↑	↑	↑
8. Denial of Service	↑	↑			↑			↑
9. Phishing	↑	↑	↑	↑	↑	↑	↑	↑
10. Spam	→			↑				↑

Table 1: Overview of Threats and Emerging Trends of the ENISA Threat Landscape 2013[1]

De plus en plus de victime …

› **EDOUARD LEDERER** / JOURNALISTE AU SERVICE FINANCE | LE 21/08 À 21:31, MIS À JOUR À 21:43

› http://www.youtube.com/watch?v=vsDCI8IKcVU

Sept Mille Milliards

Le vol d'identité coûte cher…

Constats

- Les moyens de communication électroniques sont très activement utilisés
- Ces canaux ont leurs faiblesses
- Les arnaques commises au travers de ces canaux sont en augmentation

Risques

- Financier
- Réputation

Une fraude en quelques étapes

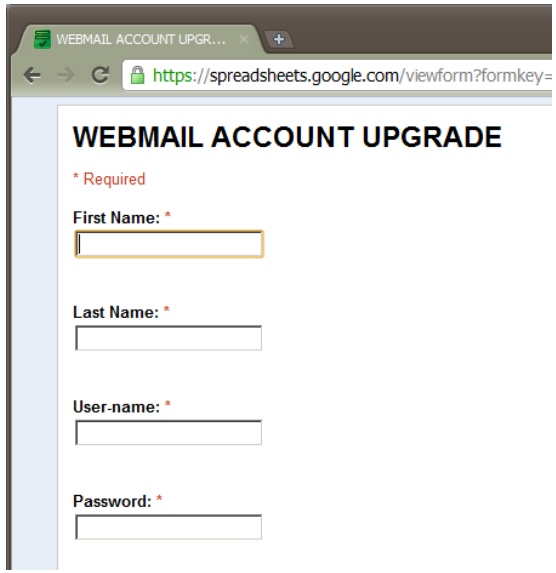
Mode opératoire

- Le mode opératoire suit des schémas précis et utilise des canaux connus (e-mail, fax ou téléphone)

Qui ?

- Ces «attaques» sont réalisées par des groupes bien organisés
  - A chacun sa spécialité
  - Difficiles à démanteler

① Obtenir un mot de passe et une adresse électronique



Date: Wed, 15 Oct 2014 21:51:16 +0100

From: [redacted]@post.lu<mailto:[redacted]@post.lu>

Subject: Nouveau

To: [redacted]

Chers clients :

Votre Mot de passe a été changé avec succès .

Votre sécurité est importante pour nous.

Si vous n'êtes pas au courant de ce changement

Connectez-vous<http://chai4car.com/2557/nordea/luxpost/> à votre compte

Un message piégé est envoyé à une très large population:

- «Problème de sécurité sur votre compte PayPal»
- «Vous avez un paquet à la poste»
- Logiciels malveillants (virus) interceptant les mots de passe sur le clavier
- Tout autre prétexte permettant d'inciter la victime à donner son mot de passe

Ou utiliser une liste de mots de passe «fréquents», bénéficier d'une des multiples fuites survenues (LinkedIn…)

Ils me demandaient mon mot de passe…

② Obtenir l'accès à la messagerie

Les mots de passe sont réutilisés d'un site à l'autre par environ **70% des utilisateurs**

A l'aide du mot de passe et de quelques autres informations

- Essayer d'accéder au compte sur Google Mail, Yahoo! Mail, etc.
- Ou créer une adresse similaire: james.wood@gmail.com et james.vvood@gmail.com sont difficiles à distinguer…

Ce mot de passe peut également avoir été utilisé sur d'autres services (Facebook, Twitter, etc.), mais cela n'est pas intéressant ici.

③ Analyser le contenu du butin

La messagerie électronique est un centre névralgique de communication

- Y a-t-il des relations avec des organismes financiers?
- Mention de comptes / de dossiers?
- Solde sur ces comptes?
- Personne/s de contact?
- De quelle manière la victime s'adresse-t-elle à ces personnes?
- Y a-t-il des procédures internes de contrôle ?
- D'autres détails qui pourraient permettre de se faire passer pour la victime?
  - Environnement familial, anniversaires, endroits, vacances…
  - Anecdotes dans les échanges avec les personnes de contact
- Eventuellement: autres mots de passe…

④ Rédiger le scénario

- Rédiger le scénario d'attaque
- En s'appuyant sur les informations trouvées précédemment
- En anticipant d'éventuelles procédures de contrôle
- Préparer une chaîne de relations bancaires
  - Utilisation de «mules»

⑤ L'attaque

"Now, Mrs. Stevens, go to work, relax, and leave the social engineering to us."

- Envoyer le message conçu à l'étape précédente
- Mettre en œuvre les techniques de *social engineering*
  - La ou les personnes de contact habituelles sont connues par l'analyse de la boîte aux lettres
- Eventuellement choisir une personne de contact secondaire moins proche du dossier
  - Profiter des périodes de vacances, etc.

Un butin de € 250 millions …

› **EDOUARD LEDERER** / JOURNALISTE AU SERVICE FINANCE | LE 21/08 À 21:31, MIS À JOUR À 21:43

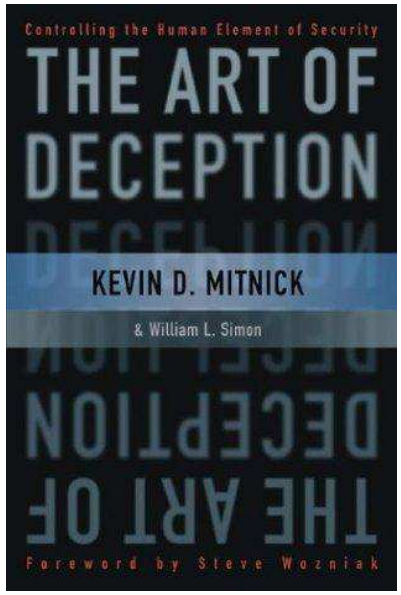
Les entreprises sont de plus en plus souvent ciblées par les escrocs. Les préjudices atteignent à ce jour plus de 250 millions d'euros

La mobilisation est discrète mais constante. Pouvoirs publics et organisations professionnelles tirent le signal d'alarme : les entreprises – notamment les grands groupes – sont de plus en plus souvent la cible d'une fraude aux virements internationaux. Sous différentes formes, l'escroc dupe l'entreprise et parvient à lui faire transférer des fonds vers l'étranger. Dans une récente vidéo mise en ligne sur le site de la Fédération bancaire française (FBF), la direction centrale de la police judiciaire prévient que « *plusieurs centaines de procédures sont en cours au sein de la police judiciaire* ». La FBF mais aussi des représentants de la police et de la justice devraient rencontrer prochainement leurs homologues chinois – pays d'où proviennent de nombreuses fraudes – pour en discuter. Le montant total des préjudices n'est pas négligeable, puisqu'il se porte à ce jour à « *plus de 250 millions d'euros* ».

Le *social engineering*

- Ne nécessite pas ou très peu de support technologique
  - Les garde-fous technologiques sont donc **inopérants**
- Amener le propriétaire légitime d'une messagerie à donner son mot de passe (cf. l'étape ① plus avant)
- Amener la victime à effectuer un virement frauduleux
- etc.

- Techniques d'incitation
  - Sentiment d'urgence, intimidation, inconfort
  - Empathie
  - Donner de l'importance à son interlocuteur
  - Appel aux bons sentiments
  - Référence à des personnes / des processus / des évènements internes
  - etc.



Vos questions?