HIGH-TECH BRIDGE®

INFORMATION SECURITY SOLUTIONS

Bienvenue dans le World Wild Web

4ème FORUM DES COURTIERS 2013

6th June 2013

Frédéric BOURLA
Chief Security Specialist

À propos de moi

Frédéric BOURLA

Chief Security Specialist chez High-Tech Bridge SA

Directeur des départements Ethical Hacking & Forensics

~13 ans d'expérience dans les technologies de l'information

GXPN, LPT, CISSP, CCSE, CCSA, ECSA, CEH, eCPPT

GREM, CHFI

RHCE, RHCT, MCP

[frederic.bourla@htbridge.com]

À propos de cette conférence

HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

- ✓ Le but de cette conférence est de **vous familiariser avec le concept de sécurité de l'information**, et de vous permettre **à plus long terme de minimiser les risques** de subir des attaques informatiques dispendieuses.
- ✓ **1 round de 30'**, et 10-15' de questions-réponses.
- ✓ **Inutile de prendre des notes**, la présentation vous est fournie.
- ✓ Si quoique ce soit venait à devenir abstrus ces prochains jours, **n'hésitez pas à m'envoyer un email**.

Sommaire

Quelques faits

- ✓ Dans notre monde contemporain, **l'information est le nerf de la guerre**.
- ✓ L'information n'a de de sens que lorsqu'**elle circule**.
- ✓ Les réseaux d'entreprise se sont donc tournés vers l'extérieur… Et **tout le monde est aujourd'hui plus ou moins interconnecté**.
- ✓ Sur le plan de la communication et du traitement informatisé, **nous profitons d'une ère technologique considérable**.

"***With great power comes great responsibility.***" [Voltaire]

Quelques faits

- ✓ **Ce monde interconnecté est hostile**. Chacun d'entre vous à de très fortes [mal]chances de devenir proie [ciblée ou aléatoire].

Quelques faits

- ✓ D'après l'Internet Security Alliance, **1 milliard de dollars serait annuellement dérobé** à travers le monde grâce au **vol de propriétés intellectuelles** ou à la **subtilisation d'informations sensibles** chez les sociétés victimes.
- ✓ Les attaques cybernétiques ont malheureusement beaucoup évolué ces dernières années. Il y a nettement **moins de « Hacking For Fun »**, et considérablement **plus de « Hacking For Profit »**. La cybercriminalité est ainsi devenue une entreprise complexe disposant d'une **économie souterraine florissante** :
  - ➢ Les cyber-attaques sont devenues **sophistiquées**.
  - ➢ Elles ne sont **pas toujours ciblées**.
  - ➢ Il n'est pas rare aujourd'hui d'observer des attaques **orchestrées par des groupes spécialisés** à la solde de **concurrents déloyaux**.

Quelques faits

- ✓ **Les cybercriminels d'aujourd'hui n'ont plus à développer leurs propres codes**... Ils peuvent louer des botnets et même acheter des logiciels malveillants sous licence, disposant alors eux-mêmes d'un support technique.
- ✓ **De nombreuses informations peuvent être intéressantes pour un attaquant**, notamment celles relatives aux clients, aux parties prenantes, au marketing ou aux données financières.
- ✓ **Tout le monde est concerné**… De la petite PME aux multinationales en passant par les particuliers et les agences gouvernementales.

Sommaire

Sécurité de l'information

HIGH-TECH BRIDGE
INFORMATION SECURITY SOLUTIONS

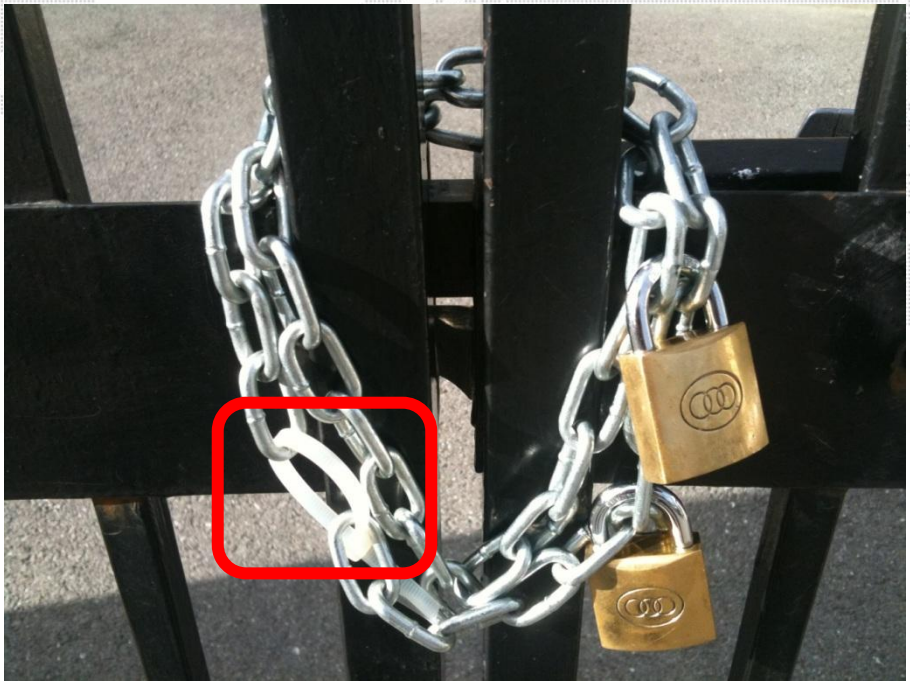
- ✓ Il faut donc **protéger l'information** d'un vaste éventail de menaces **dans le but d'assurer la continuité des activités et de réduire les dommages éventuels** pour l'entreprise **tout en maximisant le retour sur investissement et les opportunités d'affaires**.
- ✓ Vous pouvez globalement comparer la sécurité de l'information à la robustesse d'une porte, qui peut souffrir de **3 faiblesses distinctes** :
  - ➢ L'aspect **architectural**
    Est-elle construite avec des matériaux solides ?
  - ➢ L'aspect lié à l'**implémentation**
    A-t-elle été installée correctement ?
  - ➢ L'aspect **opérationnel**
    Conservez-vous une clé sous le paillasson ?

Sécurité de l'information

- La sécurité de l'information implique la préservation de:
  - La **confidentialité**. Cela consiste à s'assurer que l'information n'est divulguée qu'aux personnes autorisées.
  - L'**intégrité**. Cela consiste à assurer l'exactitude et l'exhaustivité des informations et des processus.
  - La **disponibilité**. Cela consiste à s'assurer que l'information et les actifs afférents sont accessibles aux personnes autorisées quand elles en ont besoin.
- Ce **principe fondamental dit « CIA »** est à la base du concept de sécurité informatique.
- **Le concept de CIA est très simple sur le plan théorique**… Mais en pratique, cela peut être très **difficile à accomplir**.

- ✓ L'une des raisons de ces difficultés rencontrées « sur le terrain » repose notamment sur le fait que **la longue chaîne de la sécurité de l'information est aussi forte que son maillon le plus faible**.

- ✓ Ainsi le concept même de **sécurité informatique est asymétrique**. Les « gentils » ont pléthore de variables complexes à maitriser, mais il suffit qu'une seule tombe sous le joug des « méchants » pour qu'un **effet domino** soit à redouter **sur tout ou partie de la triade CIA**.

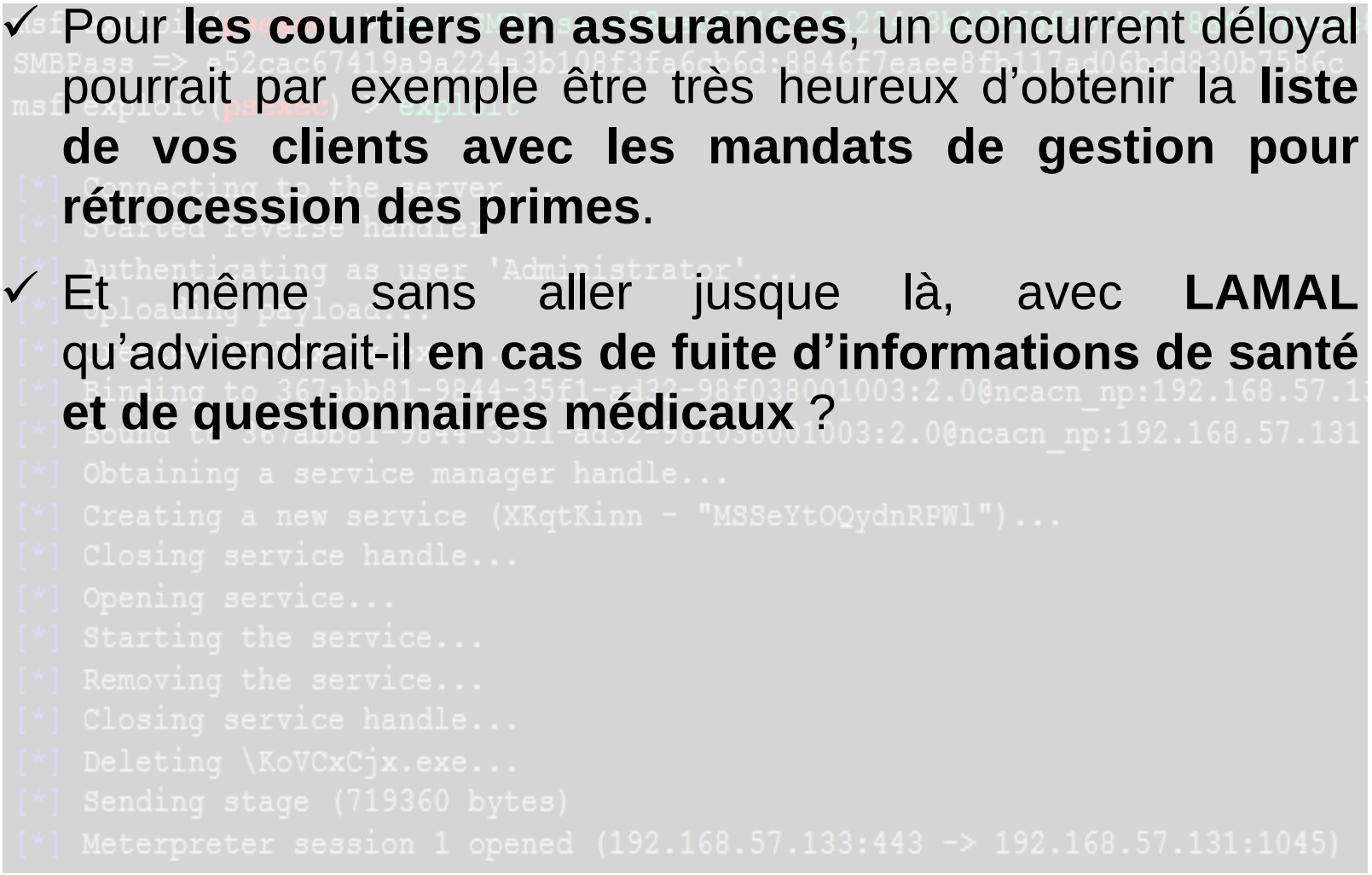


- ✓ **La disponibilité est probablement moins vitale pour vous que la confidentialité ou l'intégrité.**
- ✓ L'**intégrité** est en effet importante pour les assureurs, et potentiellement également pour l'ensemble des courtiers. Imaginez qu'**un pirate accède à vos emails et supprime les courriels de prise de contact des prospects** ?
- ✓ La **confidentialité est encore plus importe** dans votre secteur d'activités. Courtiers financiers, courtiers en assurances et assureurs ont tous un **devoir de confidentialité**.
- ✓ **Les courtiers financiers sont même soumis à la FINMA**, et ont ainsi les obligations que les banques en termes de confidentialité.

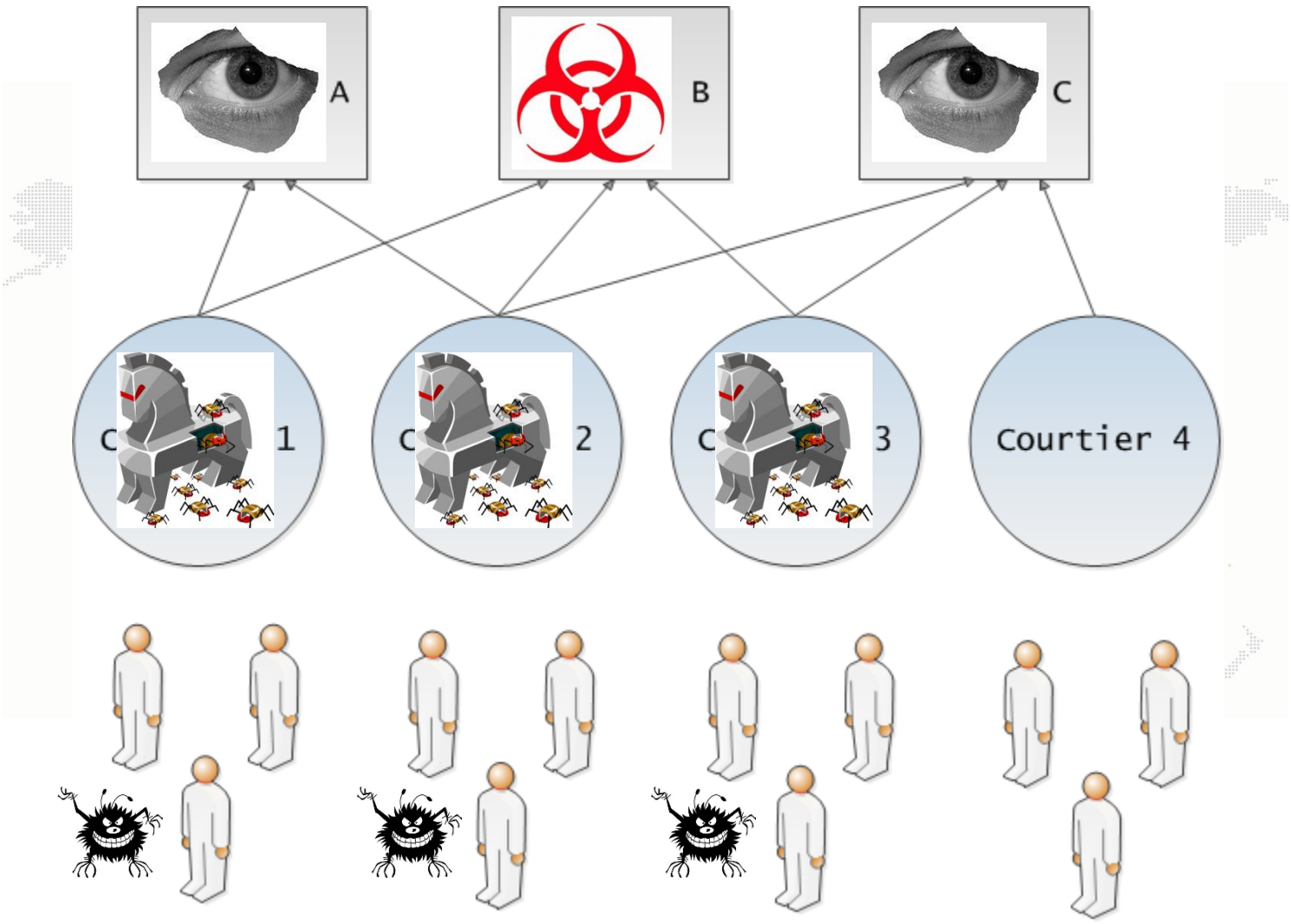
- ✓ Imaginez également que **Monsieur X prenne une police d'assurance pour sa maitresse Madame Y**… Et qu'**après piratage** de la plateforme des courtiers chez l'assureur, **l'adultère** soit **ébruité sur la toile** ?
- ✓ Les assureurs proposent parfois des **produis de défiscalisation**… Cela pourrait être **dommageable** que le **Fisc de certains pays tombent dessus**. D'autant plus que c'est à la mode ces dernières années, entre la Suisse, la France, les Etats Unis et l'Allemagne.
- ✓ Le **marché secondaire de l'assurance** vie est courant Etats-Unis, mais peut également se commercialiser en Suisse… Qu'adviendrait-il si **le client qui vient de racheter l'assurance décès parvient à savoir qui est l'assuré** ? Il pourrait envisager d'accélérer son trépas pour encaisser la prime et rentabiliser son investissement.

HIGH-TECH BRIDGE
INFORMATION SECURITY SOLUTIONS

- ✓ Pour **les courtiers en assurances**, un concurrent déloyal pourrait par exemple être très heureux d'obtenir la **liste de vos clients avec les mandats de gestion pour rétrocession des primes**.
- ✓ Et même sans aller jusque là, avec **LAMAL** qu'adviendrait-il **en cas de fuite d'informations de santé et de questionnaires médicaux** ?



Sécurité de l'information

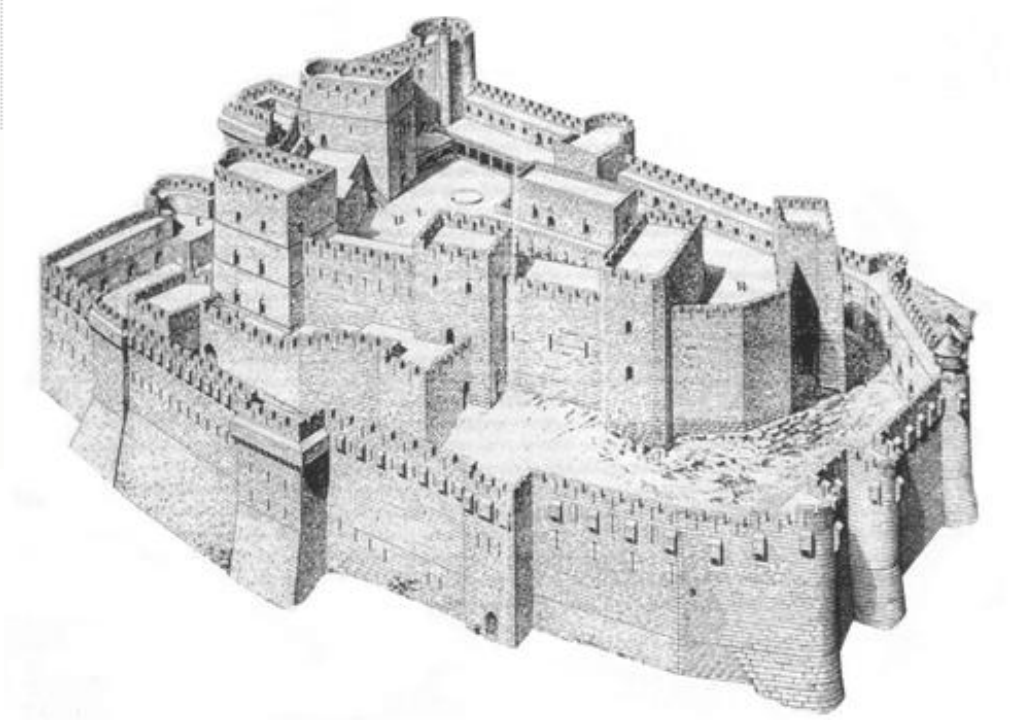


Sommaire

Les faiblesses récurrentes

HIGH-TECH BRIDGE
INFORMATION SECURITY SOLUTIONS

- ✓ À l'instar d'un château, **les défenses périmétriques se sont fortifiées au fil des années**…
- ✓ Mais pourquoi attaquer un **pont levis périlleux** lorsqu'il est possible de **passer simplement par une fenêtre** ?



Les faiblesses récurrentes

HIGH-TECH BRIDGE
INFORMATION SECURITY SOLUTIONS

- ✓ Dans la grande majorité des cas, **les hackers vont au plus simple en attaquant directement les points faibles** de leurs proies :
  - ➢ Le **réseau local** ne s'est pas autant fortifié que ses défenses périmétriques.
  - ➢ Les **utilisateurs** internes, rarement formés aux bonnes pratiques informatiques et aux concepts de base de la sécurité de l'information, constituent également une cible de prédilection. À titre d'exemple, **plus de 60'000 utilisateurs sont victimes de Phishing tous les mois** dans le monde.
  - ➢ Les sites Web sont souvent « mal codés » et restent également une cible de choix pour les cybercriminels.

Les faiblesses récurrentes

HIGH-TECH BRIDGE
INFORMATION SECURITY SOLUTIONS

- ✓ C'est donc principalement sur ces **3 axes** que vous devez articuler votre stratégie, et ainsi **obtenir une efficacité défensive maximale pour un minimum d'efforts**.
- ✓ **Pour l'aspect « utilisateur », votre meilleure arme est la connaissance**. Des **formations** ou des **conférences** comme celle d'aujourd'hui sont très efficaces. Des **simulations d'attaques par Cheval de Troie et Ingénierie Sociale** sont un excellent moyen de faire le point sur le niveau d'exposition de vos collaborateurs, et sur le risque qu'ils font encourir à l'entreprise.
- ✓ **Pour l'aspect « réseau interne »**, l'idéal est de faire appel à un expert au travers de prestations de **Consulting**, puis d'éprouver votre sécurité grâce à un **test d'intrusion interne**.

Les faiblesses récurrentes

HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

- ✓ Et finalement pour **l'aspect « site Web »,** l'idéal est d'éprouver son niveau de sécurité par le biais de simulations d'attaques spécifiques. **ImmuniWeb®** peut à ce titre vous être précieux, puisqu'il s'agit d'un SaaS unique alliant l'hybride d'un test de pénétration manuel à l'automatisation d'un scanner de vulnérabilité propriétaire. **Pour moins de 600 CHF, vous pouvez aujourd'hui sécuriser efficacement votre site Internet.**

- ✓ Pour de plus amples informations, veuillez consulter https://www.htbridge.com/immuniweb/.

Sommaire

Sommaire

HIGH-TECH BRIDGE
INFORMATION SECURITY SOLUTIONS

Conclusion

- ✓ Comme vous venez de le voir dans cette démonstration, **une simple faille sur le site Web d'un assureur peut permettre de compromettre l'ensemble des courtiers**, **et potentiellement permettre d'usurper leur identité chez d'autres assureurs**.
- ✓ Une telle attaques permettrait donc de **dérober des données confidentielles simultanément chez plusieurs assureurs**, tout en offrant l'opportunité de **nuire aux courtiers et à leur propres clients**.
- ✓ Cette attaque, comme beaucoup d'autres, **peut être évitée** si articulez votre réflexion autour de la **formation du personnel**, de la **sécurisation de votre site Web** et de la **fortification de votre réseau interne**.

Merci pour votre attention

Vos questions sont les bienvenues !

frederic.bourla@htbridge.com