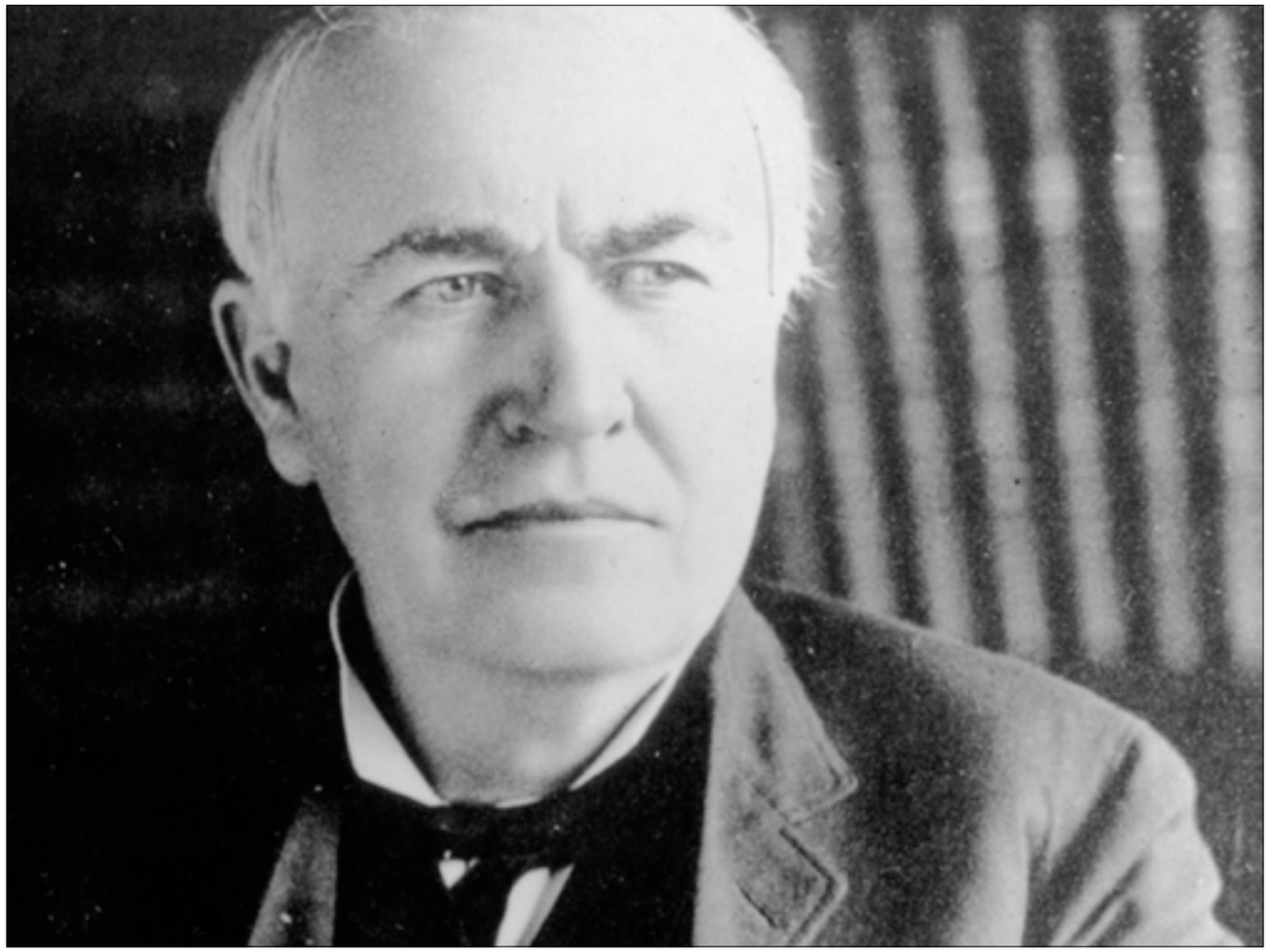
Actuellement, le niveau de cyber-sécurité mondial me fait un peu penser à la sécurité qu'il y avait au Far-West, vers le milieu du 19e siècle. En résumé, c'est plus ou moins la jungle. Je vous propose donc de faire une analogie entre des personnages tirés de cette période et ce que l'on peut observer en 2014.

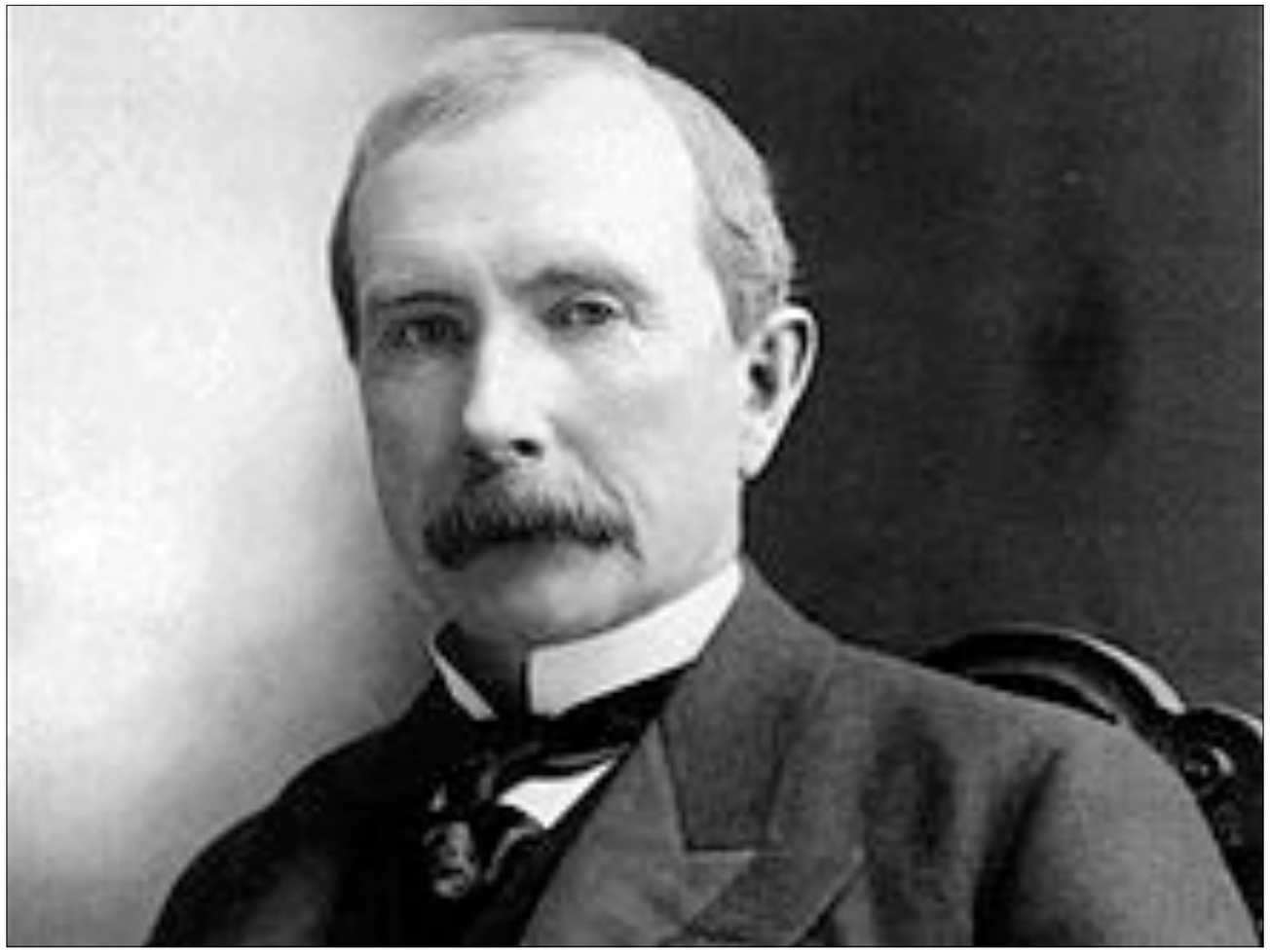
Voici donc quelques personnages typiques qui vont nous intéresser dans le quart d’heure à venir. On a la famille Ingals, qui vit paisiblement dans sa petite maison dans la prairie. On a Sentenza, ou Angel-Eyes, un mercenaire hors-la-loi insensible et sans scrupule. On a Thomas Edison, un inventeur et scientifique. On a John D. Rockfeller, un industriel. On a Bass Reeve, a US marshall, qui a arrêté plus de 3000 bandits. Et finalement, on a Abraham Lincoln, un président des Etats-Unis. Tous pourraient être des acteurs dans le monde de la cyber-sécurité en 2014.

Charles Ingalls est le membre de la famille qui utilise le plus les technologies de l'information. Il n'a jamais vraiment souffert de cyber-criminalité, à part une transaction bizarre qu'il a contestée auprès de l'émetteur de sa carte de crédit. Très récemment, un hors-la-loi a chiffré au moyen d'un virus toutes les données stockées dans son NAS, y compris les photos de famille, et il demande une rançon à payer en Bitcoin en échange de la clef de déchiffrement. Caroline Ingalls, quant à elle, ne sait pas toujours si elle doit répondre à certains e-mails envoyé par des inconnus lui demandant d'entrer son numéro de carte de crédit, ou son mot de passe sur un formulaire web un peu louche. Ce qu'elle ignore, par contre, c'est que son mari jaloux a installé un logiciel espion sur son iPhone 5, car ses relations avec le voisin ne sont pas très claires. Finalement, l'ainée des filles, Mary, passe beaucoup de temps sur Internet. Récemment, un inconnu lui a demandé de dévoiler sa poitrine via la webcam, et les autres filles du village se sont moquées de sa dernière robe sur son mur Facebook, ce qui fait qu'elle n'a plus eu le cran d'aller à l'école pendant quelques jours.

Sentenza, appelé également Angel-Eyes, est un bandit des grands chemins, expert en piratage informatique. Il n’a aucun scrupule à piller des sites webs, vendre des vulnérabilités au plus offrant, programmer du malware, travailler en tant que mercenaire pour d’autres desperados, voire même pour le gouvernement, parfois. La seule motivation qui le pousse est de gagner le plus d’argent le plus vite possible. Une fois attrapé, il finira sa carrière de deux façons possibles: soit il acceptera de travailler pour les US marshalls en échange de leur clémence, soit il sera pendu haut-et-court.



Thomas Edison est un ingénieur, un inventeur, un scientifique. Il tente par tous les moyens, et en dépensant un énergie folle, de développer de nouvelles technologies susceptibles d’améliorer la sécurité du Far-West. La plupart de ses découvertes ne servent en fait pas à grand chose, et restent dans des tiroirs, soit parce qu’elles résolvent des problèmes qui n’existent pas encore, soit parce qu’elles sont trop chères à mettre en oeuvre. Néanmoins, rarement, et avec un peu de chance, il est capable de produire des résultats réellement innovants qui changeront la face du monde. Ce qui lui importe le plus, c’est la reconnaissance de ses pairs.

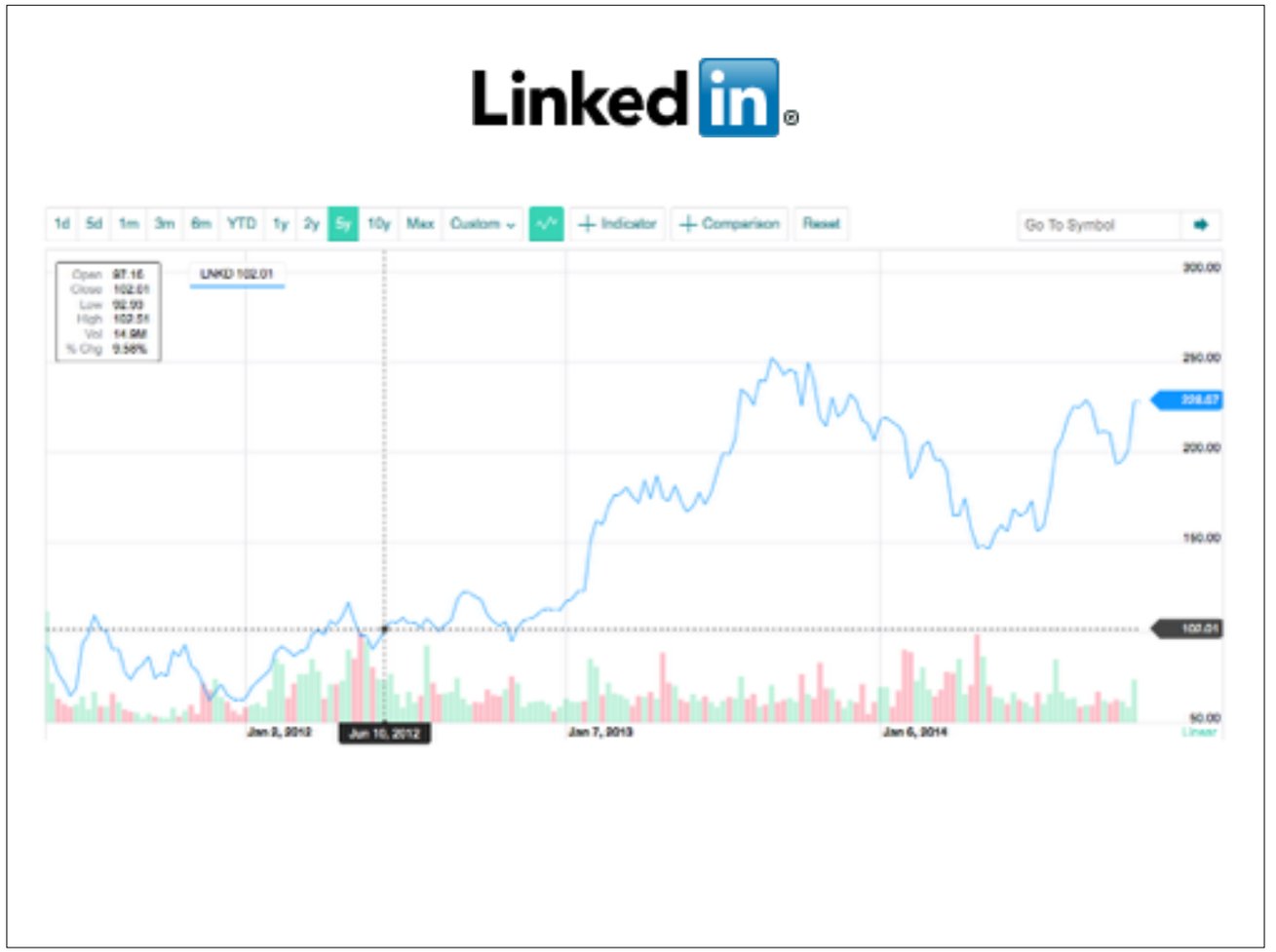


John D. Rockfeller a monté un empire industriel dans le domaine des nouvelles technologies. Il vend d'ailleurs également des solutions de sécurité plus ou moins efficaces à qui veut bien les acheter. Tant que cela paye… Il souffre lui-même régulièrement des activités de cyber-criminels, qui sont payés par ses concurrents, ou qui cherchent à lui voler des secrets industriels, ou encore à parasiter son business. Parfois, c'est carrément des pays étrangers qui cherchent à lui nuire via les infrastructures électroniques qui forment la colonne vertébrale de son empire. Il engage donc des sommes importantes pour se défendre, ce qui n'empêche pas que parfois, les cyber-criminels arrivent à leur fin. Cependant, il est peu probable qu'il fasse faillite à cause de ces problèmes de cyber-sécurité.

De manière générale, il est très difficile d'identifier l'impact d'un gros incident de cyber-sécurité sur la valorisation d'une entreprise. Voici trois exemples très différents.

Le 17 mars 2011, une division de EMC, RSA, à annoncé qu'elle a subi une attaque très sophistiquée visant a permis aux cyber-criminels de récupérer des données cruciales à la sécurité du système SecurID, qu'elle commercialise et qui protège un grand nombre d'entreprise dans le monde entier.

Une attaque est survenue entre le 17 et le 19 avril 2011 dans le réseau de jeu online Sony Playstation Network. Avec un total de plus de 77 millions d'utilisateurs, le nombre d'identifiants et de données volées en fait la plus grande faille de ce réseau connue depuis son lancement en 2006. De lourdes pertes financières se comptant en milliards de dollars ont été recensées et un bon nombre d'actions en justice ont été engagées contre la firme.



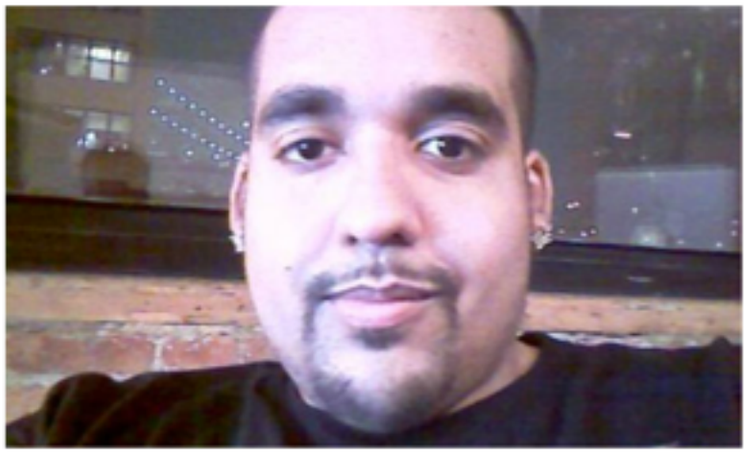
Le 5 juin 2012, 6.5 millions de mots de passe sont volés par des cyber-criminels russes chez LinkedIn. Avant cet incident, l’entreprise n’avait pas de CISO.

Bass Reeves est un US marshall, qui a voué sa vie à combattre les cyber-criminels. Il en a arrêté des milliers, et n’a jamais hésité à collaborer avec certaines de ses cibles en échange d’une remise de peine. Il a néanmoins l’impression que, faute de moyens suffisants et d’une législation adaptée, et à cause des problèmes de frontières, ses efforts restent vains, et le Far-West reste une jungle cybernétique impitoyable où règne encore et toujours la loi du plus fort.

LulzSec leader Sabu was working for us, says FBI

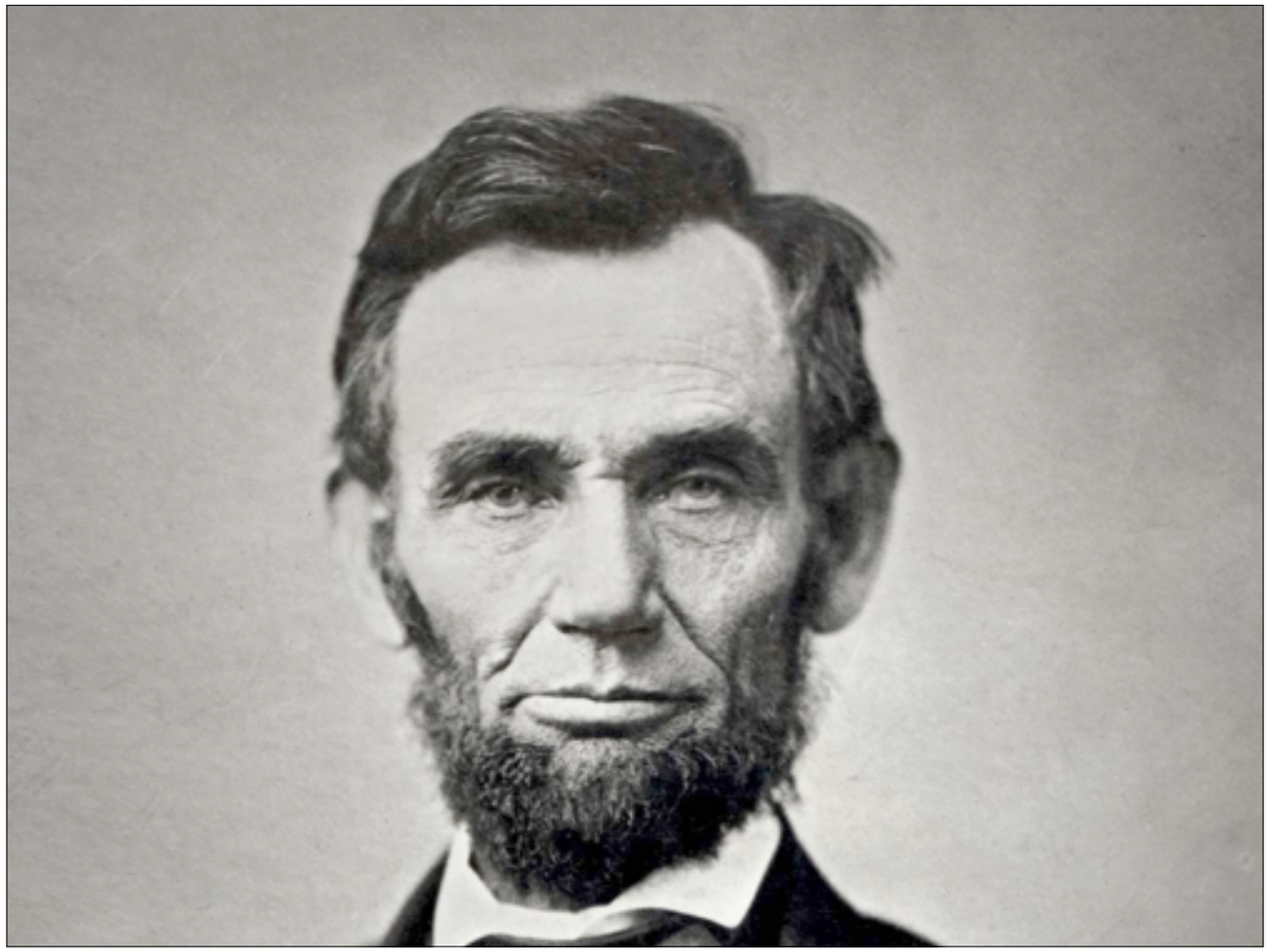
Hacker – real name Hector Xavier Monsegur – helped US authorities bring charges against five others

Charles Arthur, **Dan Sabbagh** and **Sandra Laville**
theguardian.com, Wednesday 7 March 2012 09.04 GMT



Hector Xavier Monsegur, AKA Sabu, who is allegedly the mastermind of hacking group LulzSec

Le leader des LulzSec, Hector Sabu, a aidé le FBI à arrêter les autres membres de ce gang durant 6 mois après son arrestation.



Abraham Lincoln est le président actuel des Etats-Unis, et il est donc responsable de la cyber-sécurité de ses concitoyens. Il dispose d'un budget de plusieurs dizaines de milliards de $ à ces fins: une partie vise à développer une meilleure défenses des intérêts américains dans le domaine des nouvelles technologies. Une autre partie vise carrément le domaine offensif: il fait fabriquer des outils très perfectionnés lui permettant d'espionner ses ennemis et ses amis. En fait, il a remarqué qu'il est beaucoup moins coûteux et plus efficace de faire fabriquer un virus informatique capable de saboter une usine d'enrichissement d'uranium en Iran que d'user de moyens diplomatiques ou militaires conventionnels. Par chance, les entreprise américaines ont un leadership incontestable dans le domaines des TIC, ce qui lui simplifie la tâche. Il n'hésite pas à travailler avec qui bon lui semble, au nom de la raison d'état.


HERO
OR
TRAITOR?


Gauss
DuQu
Stuxnet
Flame

Et le futur?


The Joy of Tech
by Nitrozac & Snaggy
WHAT IT'S LIKE WHEN YOU READ A NEWSPAPER...
WHAT IT'S LIKE WHEN YOU READ NEWS ONLINE...
AD NETWORK GUY
THE NSA
ANOTHER AD NETWORK GUY
AMAZON
ANOTHER NSA GUY
FACEBOOK
pulse
NEWS APPS
MORE AD NETWORK FOLKS!
YAHOO!
TWITTER
GOOGLE GUYS
YOUR ISP
AND DON'T FORGET YOUR SPOUSE CHECKING YOUR HISTORY!


Donnée médicales
Internet des objets
ShellShock
{bashbug}
Notion de vie privée à géométrie très variable
Big-Data
Cloud

Merci!

Toute ressemblance avec des faits réels n'est que pure et fortuite coïncidence

http://crypto.junod.info
@cryptopathe