CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Panorama de la cybercriminalité année 2013

Paris, 16 janvier 2014

Evénement organisé en partenariat avec :

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Le CLUSIF : agir pour la sécurité de l'information

Association **sans but lucratif** (créée en 1984)

~500 adhérents (pour 50% fournisseurs et prestataires de produits et/ou services, pour 50% RSSI, DSI, FSSI…)

Partage de l'information

Echanges homologues-experts, savoir-faire collectif, groupe de travail documentaire

Valoriser son positionnement

Retours d'expérience, visibilité créée,

Annuaires (formations, membres offreurs)

Anticiper les tendances

Le « réseau », faire connaître ses attentes auprès des offreurs

Promouvoir la sécurité

Logo pour vos actions commerciales, votre site web

Adhérer…

Groupes de travail

Les groupes actifs en 2014

- Codes malveillants : malware
- Evaluation Financière des Incidents de Sécurité - EFIS
- Fiches de sécurité pour la micro-informatique
- Gestion des vulnérabilités et de la conformité
- Incidents de sécurité et l'ISO/IEC 27035
- Panorama de la cybercriminalité
- PCI DSS V3.0
- Sécurité des Applications Web : Défense en profondeur des applications Web
- Sécurité des Outils de Communication
- Sécurité SCADA
- Security Guidelines
- SSI Santé

Espaces de travail actifs en 2014

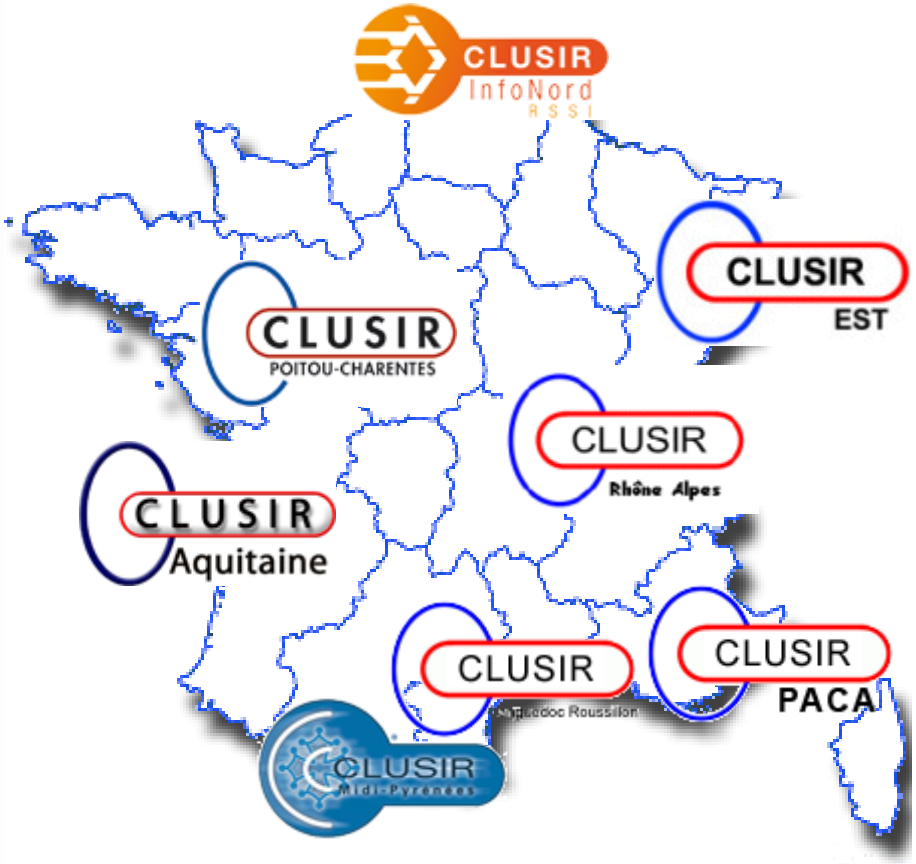
- Espace MEHARI
- Espace Menaces
- Espace RSSI

Suivez-nous sur facebook, twitter, linkedIn et abonnez-vous à nos flux RSS

Une collaboration à l'international…

Des créations en cours : Ethiopie, pays du Maghreb…

Des actions en région…



CLUSIR TAHITI

CLUSIR RÉUNION

Sélection des événements médias

Illustration

- d'une émergence,
- d'une tendance,
- d'un volume d'incidents.

Cas particuliers:

- impact ou enjeux,
- cas d'école.

Depuis 2009, élargissement au risque numérique (événements accidentels, faits de société).

D'un panorama à l'autre…

2012 – Cyber-conflits

2011 – Mobilité, la menace se précise

2010 – Hacktivisme. OS embarqués

2009 – Malware sur DAB. Web 2.0: le 5e pouvoir ?

2008 – Scareware & ransomware

2007 – Dangers autour de SCADA

2006 – Mules. Pump & dump

2005 – Rootkit Windows. Happy-slapping & cyberbullying

2004 – Spyware & robots

2003 – Skimming & phishing

2002 – Dangers de la WiFi

2001 – Virus P2P

Les informations utilisées proviennent de sources ouvertes

Les entreprises sont parfois citées par souci de précision et parce que leur nom a été communiqué dans les médias

Contributions au Panorama

Sélection réalisée par un groupe de travail pluriel issu du privé et de l'administration:

- BSSI
- CEIS
- CERT Devoteam
- CERT-IST
- CERT LEXSI
- CERT Soc.Gen
- CERT-Solucom
- Garance Mathias Avocats
- GRAS SAVOYE
- Hervé Schauer Consultants
- McAfee Labs
- McAfee Stonesoft
- OPEN
- Pinsent Masons LLP
- Trend Micro
- Verizon
- Direction Centrale de la Police Judiciaire \ OCLCTIC
- Gendarmerie Nationale \ STRJD
- Sûreté du Québec

Le choix des sujets et les propos tenus n'engagent pas les entreprises et organismes ayant participé au groupe de travail

Interventions, Panorama 2013 (1/3)

- Démystification ou comment s'affranchir du « PRISM » déformant de l'actualité

  Gérôme BILLOIS

  - Senior Manager – Solucom

- Les cybercriminels n'ont pas disparu...

  Fabien COZIC

  - Consultant Senior en cybercriminalité - CERT-LEXSI

  Colonel Éric FREYSSINET

  - Chef de la division de lutte contre la cybercriminalité - Pôle judiciaire de la Gendarmerie Nationale - STRJD

Interventions, Panorama 2013 (2/3)

- Le paradis cybercriminel existe-t-il sur terre ? Quelles sont les stratégies des Etats pour en obtenir la clé ?

  Diane MULLENEX

  - Avocat à la Cour – Pinsent Masons LLP

- 2013, l'année des monnaies virtuelles

  Barbara LOUIS-SIDNEY

  - Juriste - CEIS

  Garance MATHIAS

  - Avocat à la Cour – Cabinet d'Avocats Mathias

- Le droit à l'épreuve de la cybercriminalité. Quel arsenal juridique pour la France et l'Europe ?

  Garance MATHIAS

  - Avocat à la Cour – Cabinet d'Avocats Mathias

Interventions, Panorama 2013 (3/3)

- Nous aurions aussi aimé vous parler de…

Gérôme BILLOIS

- Senior Manager – Solucom

- Table ronde

Éric FREYSSINET

- Chef de la division de lutte contre la cybercriminalité – Pôle judiciaire de la Gendarmerie Nationale \STRJD

Olivier GUERIN (animateur de la table ronde)

- Chargé de mission - CLUSIF

Lazaro PEJSACHOWICZ

- Président du CLUSIF
- Chargé de mission auprès de la communauté des SSI – CNAMTS

Hervé SCHAUER

- Consultant en sécurité de l'information et dirigeant du cabinet éponyme

Agenda du Panorama 2013

- **Démystification ou comment s'affranchir du « PRISM » déformant de l'actualité**
- Les cybercriminels n'ont pas disparu...
- Le paradis cybercriminel existe-t-il sur terre ? Quelles sont les stratégies des Etats pour en obtenir la clé ?
- 2013, l'année des monnaies virtuelles
- Arsenal juridique français et européen : le droit à l'épreuve de la cybercriminalité
- Nous aurions aussi aimé vous parler de…
- Table ronde

Démystification *ou comment s'affranchir du PRISM déformant de l'actualité*

Gérôme BILLOIS, Senior Manager Solucom,
gerome.billois@solucom.fr **Twitter** @gbillois

Oui, 2 évènements majeurs ont rythmé l'année 2013…

Le rapport APT1 en février…

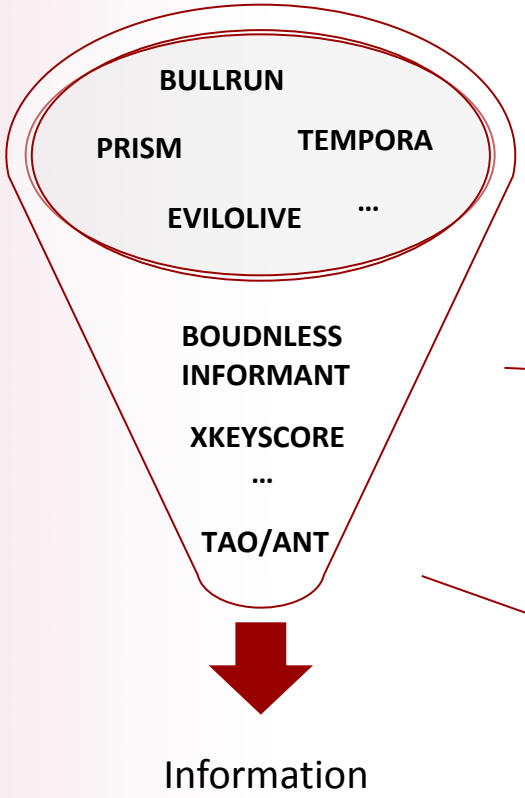
La première mise en cause détaillée d'une équipe d'attaquants chinois avec des moyens très importants…

- Probablement issue de l'armée
- Ayant été observée dans plus de 140 entreprises, sur 20 secteurs d'activité
- Une approche de réutilisation d'outils / d'infrastructure et de persistance dans les SI
- Capable de voler 6 To de données en quelques mois
- Disposant de réseaux de C&C de près de 1000 serveurs dans 13 pays

… qui met en lumière ce que la communauté sécurité observait au quotidien

- Une volonté claire d'espionnage économique / politique
- Des moyens importants dans la durée

La NSA et Snowden depuis juin : une formidable machine à espionner !



Des capacités de collectes démesurément larges

- 2.5 Milliards du budget annuel dédiés
- Câble sous-marin, accord plus ou moins forcé…

Des capacités d'analyse performantes

- 3 milliards de dollars de budget
- Des outils qui font rougir les spécialistes du Big Data

Des capacités d'interventions ciblées industrialisées

- Compromission du chiffrement / achat de 0-day
- Catalogue de services d'armes numériques

➔ Au final une surveillance généralisée… qui confirme ce que la communauté sécurité imaginait. C'est l'ampleur et l'industrialisation qui ont surpris !

Mais aussi un colosse au pied d'argile…

Plus de 1000 administrateurs du système d'information

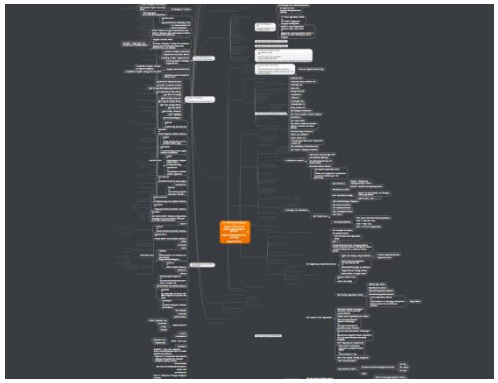
- Dont la plupart sont externes

Une difficulté à protéger l'accès aux documents

- La capacité à « emprunter » des identités en interne
- Un outil de DLP partiellement déployé
- Une traçabilité incomplète

Encore aujourd'hui, l'incapacité à savoir ce qui a été volé….

Un programme drastique de réorganisation interne mais aussi et surtout du renseignement plus largement.



Finalement, une opportunité pour les responsables sécurité ?

➔ Mise en lumière de la réalité des menaces

Oui, 2 évènements majeurs ont rythmé l'année 2013…

… mais ils ne doivent pas faire oublier les évolutions de la cybercriminalité dans son ensemble !

Les attaques « waterholing » ou la méthode du point d'eau

Une méthode simple : piéger un site web visité par les cibles

- Compromettre le site web
- Y déposer des pages / codes malveillants
- Attendre les visites et les infections des postes
- Exploiter les données collectées

… mais très efficace quand il est bien ciblé !

Recrudescence en 2013, y compris grand public

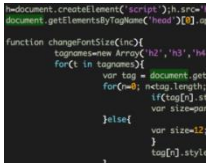
Retour sur l'attaque du Ministère du Travail US

Une cible : la communauté du nucléaire US

UNITED STATES DEPARTMENT OF LABOR

Page sur les compensations en cas d'exposition à des radiations

Un lieu à fort « rendement »



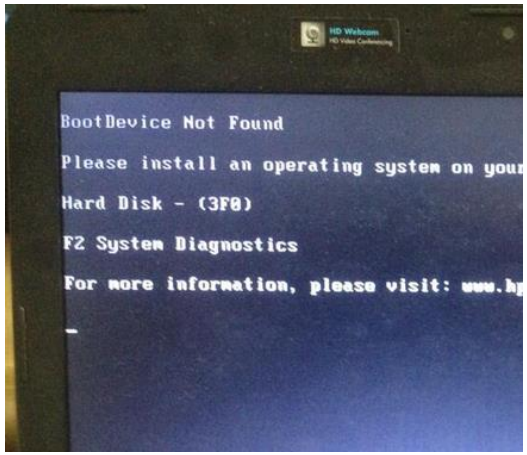
Une page piégée et un malware du groupe DeepPanda

Des postes infectés et des données qui fuitent

Les attaques « destructives » / « incapacitantes »

Un objectif : désorganiser une organisation en détruisant ses données et/ou ses postes de travail

- Compromettre le système d'information
- Déployer un malware « destructif » à grande échelle
- Effacer des données et/ou les disques durs des postes de travail et/ou chiffrer leur contenu (cas Cryptolocker)



… qui reste en développement :

Retour sur l'attaque Jokra visant la Corée du Sud en mars 2013

Une cible : la Corée du Sud, des banques et chaînes de TV

Un malware mal conçu mais bien déployé: DarkSeoul

Un réel impact : plus de 35 000 postes touchés

Les attaques « métiers »

Un objectif : cibler des actifs précis dans le SI pour réaliser des fraudes / actions malveillantes métiers

- Changement de plafond de retrait
- Réalisation de virements
- Collecte d'informations clés…

Un développement de plus en plus ciblé : retour sur quelques cas clés de 2013

Premier malware
SAP Carberp
➔ Key & screenlogger

Attaque de prestataires bancaires US/indiens
➔ 45 M$ détourné

Mais aussi

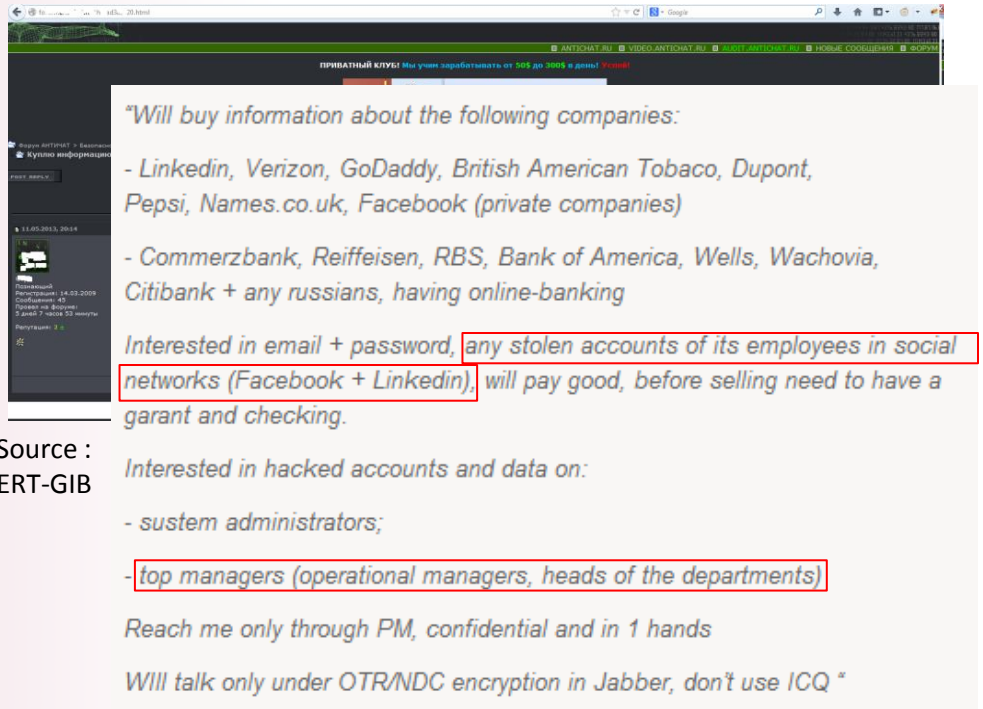
- Les distributeurs de billets / caisses enregistreuses (Target)
- Les terminaux portuaires à Anvers
- Des braconniers en Inde…

Les attaques « vie privée »

Un objectif : cibler les moyens de communication personnels des employés

- Email, messagerie instantanée, réseaux sociaux ou encore sites de stockage…

… pour voler de l'information ou mieux connaitre sa cible



"Will buy information about the following companies:

- Linkedin, Verizon, GoDaddy, British American Tobaco, Dupont, Pepsi, Names.co.uk, Facebook (private companies)

- Commerzbank, Reiffeisen, RBS, Bank of America, Wells, Wachovia, Citibank + any russians, having online-banking

Interested in email + password, any stolen accounts of its employees in social networks (Facebook + Linkedin), will pay good, before selling need to have a garant and checking.

Interested in hacked accounts and data on:

- sustem administrators;

- top managers (operational managers, heads of the departments)

Reach me only through PM, confidential and in 1 hands

WIll talk only under OTR/NDC encryption in Jabber, don't use ICQ "

Source : CERT-GIB

En 2013 :

- Evernote ➔ 5 millions de mots de passe
- Adobe ➔ 38 millions de comptes

Des mesures préventives de certains sites dont Facebook.

➔ Mais comment détecter ces attaques ?

En résumé…

Ce que 2013 nous rappelle

- Les menaces étatiques sont réelles et leurs ampleurs est plus que confirmée. Mais elles ne sont qu'une menace parmi d'autres !

- Les méthodes d'attaques se multiplient et se diversifient et elles visent de plus en plus les métiers des entreprises.

Mais qui sont les auteurs derrière ces attaques ?

Démystification – Références

- **Watering Hole**

US Dpt of Labor

http://threatpost.com/oil-energy-watering-hole-attacks-could-be-tied-to-dol-attacks/102366

http://www.theinquirer.net/inquirer/news/2265518/us-department-of-labor-website-hacked-by-a-chinese-group

http://www.alienvault.com/open-threat-exchange/blog/us-department-of-labor-website-hacked-and-redirecting-to-malicious-code

http://www.crowdstrike.com/sites/default/files/AdversaryIntelligenceReport_DeepPanda_0.pdf

iPhone Dev

http://threatpost.com/ios-developer-site-core-facebook-apple-watering-hole-attack-022013

NBC

http://www.theregister.co.uk/2013/02/22/nbc_hack/

Tibetan admin

http://www.securelist.com/en/blog/9144/Central_Tibetan_Administration_Website_Strategically_Compromised_as_Part_of_Watering_Hole_Attack

Démystification – Références

- **Attaques destructives/paralysantes**

http://www.northkoreatech.org/20

http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html?_r=013/03/21/malware-that-hit-south-korea-wasnt-so-sophisticated/

http://www.redorbit.com/news/technology/1113035548/cryptolocker-holds-250000-computers-ransom-122613/

http://www.zdnet.com/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin-7000024579/

- **Attaques métiers**

SAP

http://www.net-security.org/malware_news.php?id=2632

http://www.infoworld.com/d/security/new-malware-variant-suggests-cybercriminals-targeting-sap-users-230014

http://blog.trendmicro.com/trendlabs-security-intelligence/autocad-malware-leaves-victims-hackable/

http://www.theregister.co.uk/2013/06/18/drug_smugglers_using_hackers/

ATM Heist

http://www.ibtimes.co.uk/cyber-crime-bank-theft-45m-27-countries-466578

http://www.bankmuscat.com/en-us/AboutUs/Financials/Quarterly%20Reports/Quarterly%20results%20ended%2031%20March%202013.pdf

http://www.theverge.com/2013/5/13/4326336/cyber-caper-behind-the-scenes-of-the-45-million-atm-heist

http://www.bloomberg.com/news/2013-05-07/banks-say-fed-should-lead-in-cybersecurity-for-industry.html

Démystification – Références

- **Attaques métiers**

Autocad
http://blog.trendmicro.com/trendlabs-security-intelligence/autocad-malware-leaves-victims-hackable/
Port d'Anvers
http://www.theregister.co.uk/2013/06/18/drug_smugglers_using_hackers/
Tigre
http://blogs.computerworld.com/cybercrime-and-hacking/22976/cyber-poaching-hacking-gps-collar-data-track-and-kill-endangered-tigers
http://www.popsci.com/article/technology/poachers-try-hack-data-rare-tigers-gps-collar
ATM/POS
http://www.bankinfosecurity.com/target-were-debit-pins-compromised-a-6320
http://www.businessinsider.com/target-credit-card-hackers-2013-12

Démystification – Références

•**Attaque par des tiers**

Bit 9

http://www.darkreading.com/attacks-breaches/elite-chinese-cyberspy-group-behind-bit9/240161491
http://www.darkreading.com/attacks-breaches/bit9s-delicate-disclosure-dance-a-sign-o/240150201
http://krebsonsecurity.com/2013/02/security-firm-bit9-hacked-used-to-spread-malware/

Belgacom

http://cryptome.org/2013/09/belgacom-hack-en.htm
http://thehackernews.com/2013/11/snowden-reveals-gchq-planted-malware.html#

•**Vie privée**

http://www.theverge.com/2013/3/2/4056704/evernote-password-reset
http://blog.evernote.com/blog/2013/03/02/security-notice-service-wide-password-reset/
http://securityaffairs.co/wordpress/14877/cyber-crime/senior-management-considered-a-primary-target-by-modern-cybercrime.html
http://www.pcworld.com/article/2052180/adobe-reports-massive-security-breach.html
http://krebsonsecurity.com/2013/11/facebook-warns-users-after-adobe-breach/
http://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/
http://www.forbes.com/sites/oreillymedia/2013/11/14/adobes-breach-widens/
http://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/

Agenda du Panorama 2013

- Démystification ou comment s'affranchir du « PRISM » déformant de l'actualité
- **Les cybercriminels n'ont pas disparu...**
- Le paradis cybercriminel existe-t-il sur terre ? Quelles sont les stratégies des Etats pour en obtenir la clé ?
- 2013, l'année des monnaies virtuelles
- Arsenal juridique français et européen : le droit à l'épreuve de la cybercriminalité
- Nous aurions aussi aimé vous parler de…
- Table ronde

Les cybercriminels n'ont pas disparu

Colonel Éric Freyssinet

Pôle judiciaire de la Gendarmerie Nationale - STRJD

Chef de la division de lutte contre la cybercriminalité

Fabien Cozic

CERT-LEXSI

Consultant Senior en Cybercriminalité

Une année riche en arrestations

Nikita Kuzmin (Gozi)

Dmitry FedoRov Paunch (Blackhole & Cool)

Hamza Bendellaj aka Bx1 (Zeus & SpyEye)

Sven Olaf Kamphuis (DDoS de SpamHaus)

Ross Ulbricht aka Dread Pirate Roberts (Silkroad)

Des arrestations aux effets limités

- Les coups d'arrêt portés à ces activités sont temporaires et les services fermés rouvrent dans des délais très courts

Des arrestations aux effets limités

New Silk Road drug bazaar opens a month after FBI bust

BY NOEL RANDEWICH

SAN FRANCISCO | Thu Nov 7, 2013 3:41am EST

SECURITY | 12/20/2013 @ 10:56AM | 15 489 views

At Least Two Moderators Of 'Silk Road 2.0' Drug Site Forums Arrested

security silk road

Silk Road 2 Still Running After Moderator Arrests

*Posted Dec 23, 2013 by **John Biggs** (@johnbiggs)*

La cybercriminalité a gagné du terrain dans le monde réel

- Une tendance se confirme avec l'emploi de services cybercriminels par des criminels traditionnels

- Multiplication des cas impliquant l'utilisation de moyens numériques

Drug gang hacks into Belgian seaport, cops seize TONNE of smack

9 nabbed after shipping container system used to transport heroin, cocaine

By John Leyden, 18th June 2013

After a Kidnapping, Hackers Take On a Ruthless Mexican Crime Syndicate

By DAMIEN CAVE
Published: October 31, 2011

MEXICO CITY — The hackers' message, delivered via YouTube by a man wearing a red tie and a Guy Fawkes mask, was as bold and risky as anything produced by the Zetas, Mexico's most ruthless crime syndicate. But this time, the Zetas were the target.

SIGN IN TO E-MAIL
PRINT
REPRINTS

Connect With Us on Twitter
Follow @nytimesworld for international breaking news and headlines.
Twitter List: Reporters and Editors

World

They had kidnapped a geek with backup — a respected member of the hackers collective known as Anonymous.

"You have made a great mistake by taking one of us," said the video's masked figure. "Release him."

Or else, the message said, the names of government officials, taxi drivers and journalists who worked with the Zetas would be published online. The goal, they said, was the arrest of these suspected collaborators, but was there a possibility they might be killed by a rival cartel? Yes, said self-identified members of Anonymous, acknowledging the danger. Beyond that, might the hackers also be targeted? Were they afraid?

La cybercriminalité a gagné du terrain dans le monde réel

- Leurs domaines d'activité sont donc considérablement élargis par ces associations :
  - Trafics de stupéfiants
  - Trafics de biens
  - Traite d'êtres humains
  - Fraudes bancaires et financières
  - Etc.

L'hacktivisme newbie en berne…

- Anonymous Canal historique peut-il être déclaré légalement mort ?
  - Arrestations et condamnations de leaders majeurs
    - Topiary, Jeremy Hammond, Lauri Love, Matthew Flannery,…
  - Les condamnations très lourdes même pour des faits mineurs sont extrêmement dissuasives

Un pirate condamné à 183 000$ d'amende pour une minute d'attaque DDoS !

Eric Rosol, un pirate informatique de 38 ans ayant rejoint le mouvement Anonymous a été condamné à deux ans de probation fédérale et à 183 000…

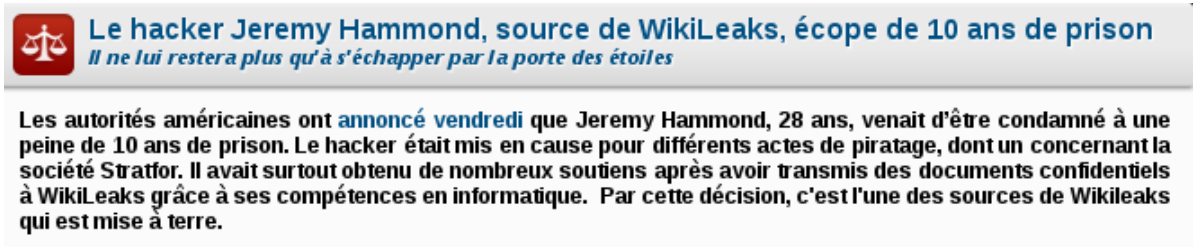
Undernews, le 13 décembre 2013 à 19h50

NEWS | IMAGES | VOICES | SPORT | TECH | LIFE | PROPERTY | ARTS + ENTS | TRAVEL | MO

OFFBEAT / Food & Drink / Health & Families / History / Gadgets & Tech / Motoring / Dating / Crosswords /

Technology > Life > Gadgets & Tech > News

LulzSec leader named as Matthew Flannery faces 12 years in jail after arrest in Australia



Le hacker Jeremy Hammond, source de WikiLeaks, écope de 10 ans de prison

Il ne lui restera plus qu'à s'échapper par la porte des étoiles

Les autorités américaines ont annoncé vendredi que Jeremy Hammond, 28 ans, venait d'être condamné à une peine de 10 ans de prison. Le hacker était mis en cause pour différents actes de piratage, dont un concernant la société Stratfor. Il avait surtout obtenu de nombreux soutiens après avoir transmis des documents confidentiels à WikiLeaks grâce à ses compétences en informatique. Par cette décision, c'est l'une des sources de Wikileaks qui est mise à terre.

… Mais a laissé des traces

- Les méthodes employées par le collectif ont été reprises et améliorées par les cercles cybercriminels
  - Augmentation de la part de l'ingénierie sociale
    - Vols de données personnelles pour le chantage et l'extorsion visant particuliers, entreprises et VIP
  - Les campagnes hacktivistes ont malgré elles facilité le passage de participants à la cybercriminalité
    - Appels frauduleux aux dons et aux souscriptions
    - Utilisation de moyens de paiement volés aux entreprises sous couvert d'un acte idéologique
    - Développement d'une offre d'attaques concurrentielles

… Mais a laissé des traces

- La dislocation du collectif Anonymous, amorcée fin 2012 s'est poursuivie en 2013
  - Des éléments isolés se retrouvent dans des dérives criminelles
  - Des sous-groupes se constituent et se développent sur fond de radicalisation des actions et d'élargissement des cibles potentielles

Paperblog.fr

… Mais a laissé des traces

- L'étendard est récupéré par des groupes étatiques ou para-étatiques pour mener leurs actions idéologiques
  - Cela ajoute à la confusion
  - Barrière supplémentaire pour l'attribution des attaques
  - Consécration des cyber-armées

Retour sur les tendances malware 2013

Malwares mobiles en augmentation

- Infection primaire via des liens frauduleux (93%) et propagation du lien par SMS
- Développement des botnets mobiles (Spam Soldier, 0bad,…)
- 99% sur Android
- Contrôle à distance par messagerie en ligne
- Contamination sur Pc via la synchronisation
- Communication avec les interfaces bancaires pour évaluer le solde disponible

Le mode d'infection par le marché applicatif est en baisse grâce aux dispositifs de vérification Android et Apple

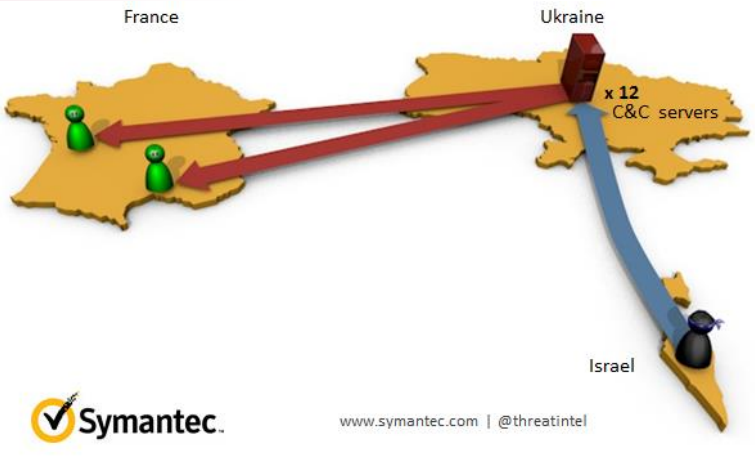
L'ingénierie sociale devient la clé de la compromission mobile

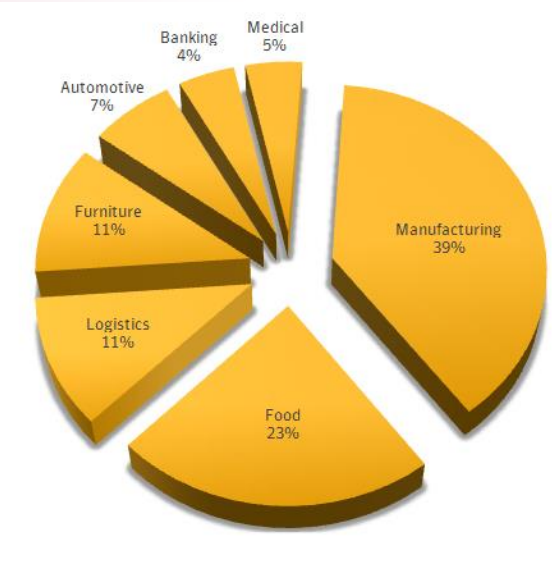
- De nouveaux malwares bancaires intègrent des modules pour détourner les appels de vérification des établissements bancaires
- Le contournement de la double authentification est la priorité des cybercriminels
- En autorisant l'installation de sources inconnues, l'utilisateur permet la contamination

Les ransomware sont la nouvelle grande tendance 2014

- Chiffrement des fichiers, disques et serveurs de particuliers et d'entreprises
- Le poste victime est verrouillé
- Le chiffrement peut être extrêmement fort pour ralentir le sauvetage des documents
- Demandes de rançon contre la clé de déchiffrement
- Paiement en monnaies virtuelles ou cartes prépayées
- Exemple de Cryptolocker (Chiffrement RSA 2048 bit !)

Groupes criminels et cyber-criminels main dans la main



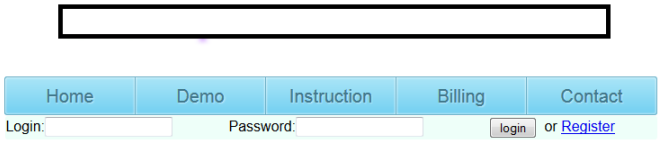


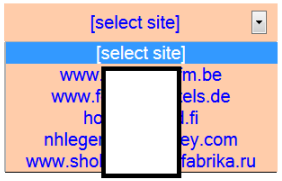
En août 2013, Symantec révèle « Francophoned »:

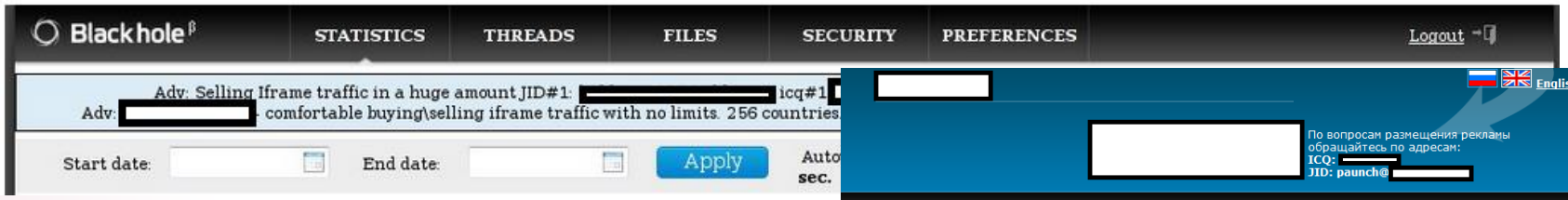
- Des groupes criminels agissant ici depuis Israël réalisent des opérations d'ingénierie sociale pour obtenir des virements
- Ils auraient obtenu l'aide de cybercriminels pour accompagner l'ingénierie sociale d'actions d'espionnage par virus informatique, via l'Ukraine

L'offre est disponible en ligne

On connaît les places de marché, mais de nouveaux services apparaissent sans cesse, tels des services de tests d'intrusion à réaliser soi-même







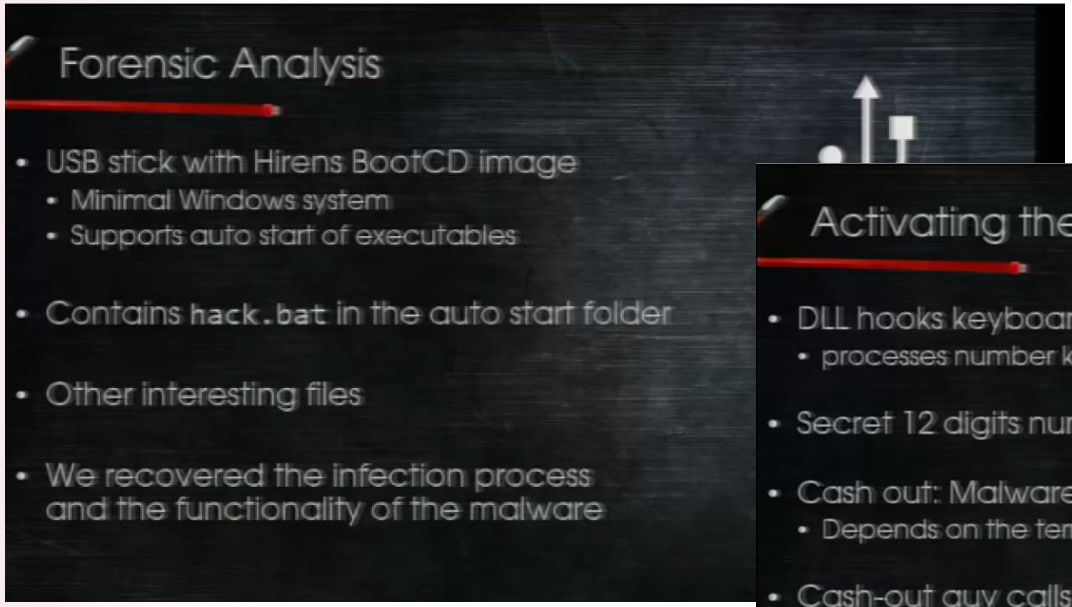
Paunch, l'auteur de Blackhole, intégrait la publicité pour ses autres services dans ses applications.

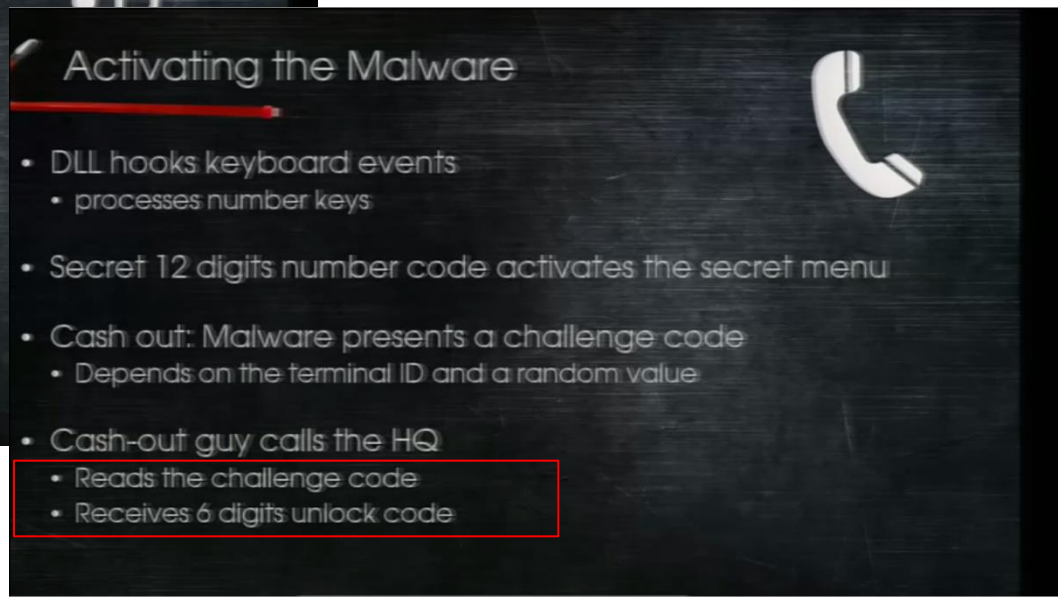
… et l'offre s'est encore professionnalisée

Hidden Lynx, un groupe chinois mis en lumière par Symantec

Piratage de DAB par le port USB

Ce n'est pas nouveau, mais est toujours observé de façon inquiétante selon des chercheurs qui se sont exprimés au CCC (à rajouter au questionnement autour de l'abandon de Windows XP par Microsoft en 2014)

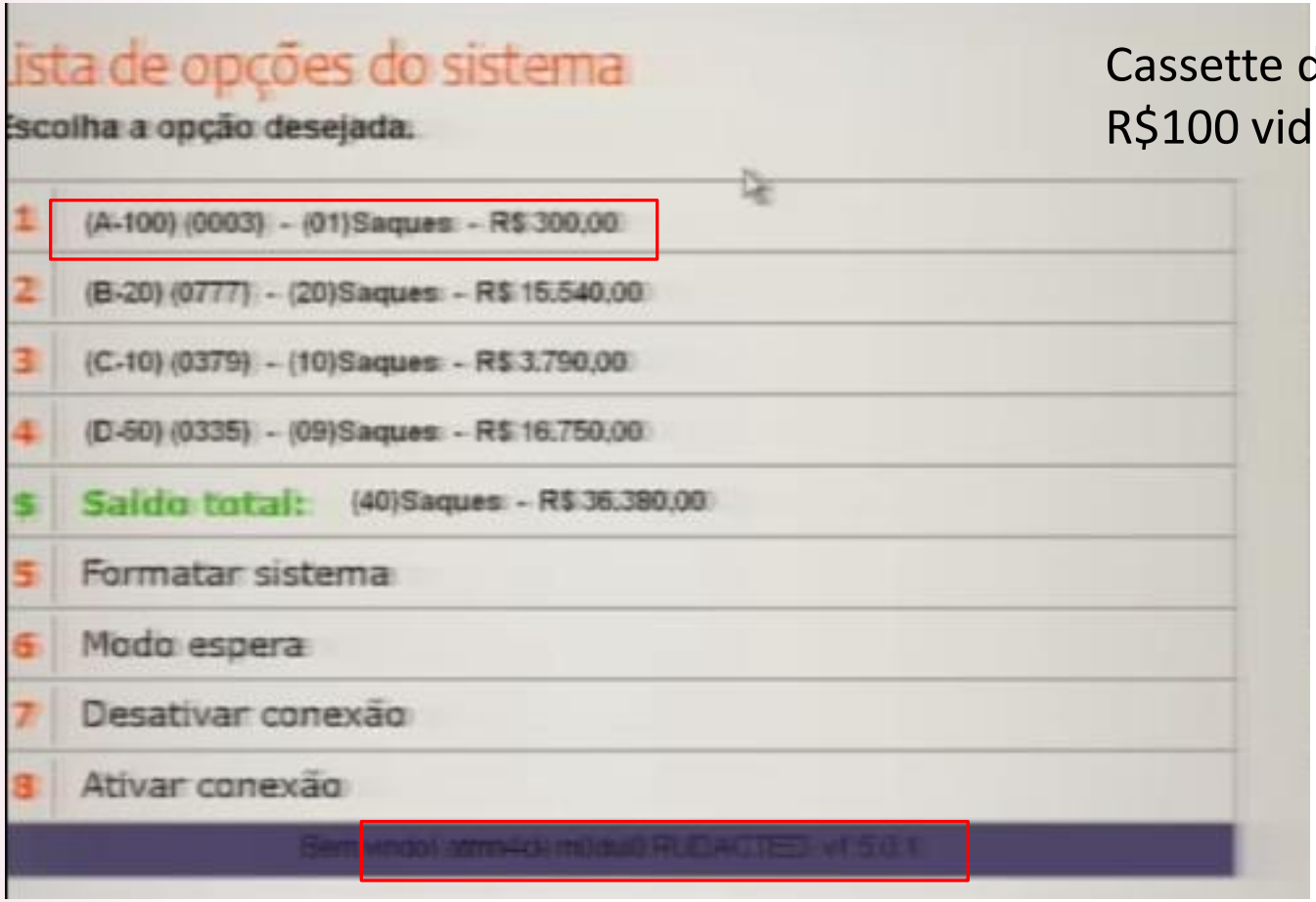




Double authentification

Piratage de DAB par USB

(suite de l'exposé par les chercheurs avec démonstration)



Cassette des billets de R$100 vidée

Version 1.5.0.1 !

Attaques contre le commerce de proximité

KrebsonSecurity
In-depth security news and investigation

20 DEC 13 Cards Stolen in Target Breach Flood Underground Markets

Credit and debit card accounts stolen in a recent data breach at retail giant Target flooding underground black markets in recent weeks, selling in batches of one mi and going for anywhere from $20 to more than $100 per card, KrebsOnSecurity has

Prior to breaking the story of the Target breach on Wednesday, Dec. 18, I spoke with a fraud analyst at a major bank who said his team had independently confirmed that Target had been breached after buying a huge chunk of the bank's card accounts from a well-known "card shop" — an online store advertised in cybercrime forums as a place where thieves can reliably buy stolen credit and debit cards.

about Target | careers | corporate responsibility | investors | press

home / press / releases / Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores

Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores

Issue has been identified and resolved

MINNEAPOLIS — December 19, 2013
Target today confirmed it is aware of unauthorized access to payment card data that may have impacted certain guests making credit and debit card purchases in its U.S. stores. Target is working closely with law enforcement and financial institutions, and has identified and resolved

Approximately 40 million credit and debit card accounts

this issue, so guests can shop with confidence. We regret any inconvenience this may cause," said Gregg Steinhafel, chairman, president and chief executive officer, Target. "We take this matter very seriously and are working with law enforcement to bring those responsible to justice."

Approximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013. Target alerted authorities and financial institutions immediately after it

Attaques contre le commerce de proximité

REUTERS EDITION: U.S.

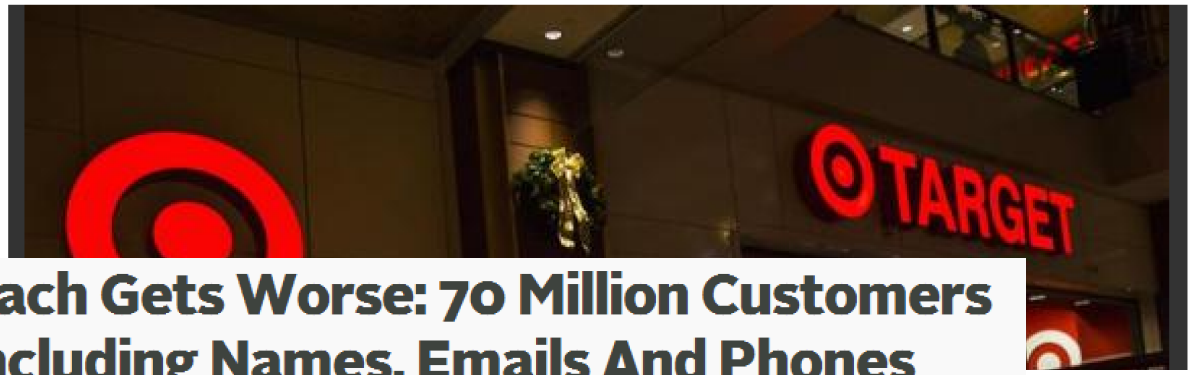
HOME BUSINESS MARKETS WORLD POLITICS TECH OPINION BREAKINGVIEWS

Exclusive: More well-known U.S. retailers victims of cyber attacks - sources

BY JIM FINKLE AND MARK HOSENBALL

BOSTON/WASHINGTON Sun Jan 12, 2014 4:26pm EST

9 COMMENTS | Tweet Share this Email Print



Target's Data Breach Gets Worse: 70 Million Customers Had Info Stolen, Including Names, Emails And Phones

Posted Jan 10, 2014 by Sarah Perez (@sarahintampa)

Références

- Cybercrime involved in drug smuggling (The Register)
http://www.theregister.co.uk/2013/06/18/drug_smugglers_using_hackers
- Cryptolocker (PC World)
http://www.pcworld.fr/internet/actualites,ransomware-cryptolocker-aurait-deja-infecte-plus-de-250-000-machines-a-travers-le-monde,544961,1.htm
- Malware mobiles, bilan 2013
http://www.cso.com.au/article/534711/seventy_percent_all_known_mobile_malware_variants_found_2013_kaspersky/
- FBI – Cyber Crimes Stories
http://www.fbi.gov/news/stories/story-index/cyber-crimes
- Black Hole exploit kit author's vertical market integration …
http://www.webroot.com/blog/2013/01/08/black-hole-exploit-kit-authors-vertical-market-integration-fuels-growth-in-malicious-web-activity/
- Hidden Lynx (Symantec)
http://www.symantec.com/connect/blogs/hidden-lynx-professional-hackers-hire
- Electronic bank robberies (CCC)
http://media.ccc.de/browse/congress/2013/30C3_-_5476_-_en_-_saal_2_-_201312271600_-_electronic_bank_robberies_-_tw_-_sb.html
- Cards stolen in Target breach flood underground markets
http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/
- Target confirms unauthorized access to payment card data in U.S. stores
http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores

Agenda du Panorama 2013

- Démystification ou comment s'affranchir du « PRISM » déformant de l'actualité
- Les cybercriminels n'ont pas disparu...
- **Le paradis cybercriminel existe-t-il sur terre ? Quelles sont les stratégies des Etats pour en obtenir la clé ?**
- 2013, l'année des monnaies virtuelles
- Arsenal juridique français et européen : le droit à l'épreuve de la cybercriminalité
- Nous aurions aussi aimé vous parler de…
- Table ronde

Le paradis cybercriminel existe-il sur Terre ?
Quelles sont les stratégies des Etats pour en obtenir la clé ?

Diane Mullenex

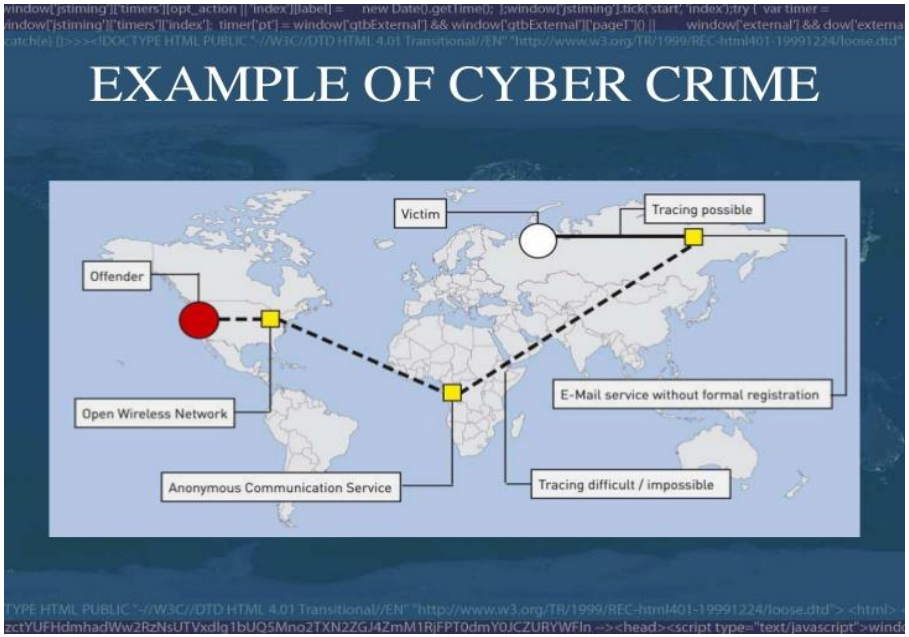
Pinsent Masons

Avocat à la Cour

Sollicitor England & Wales

Retour sur l'année 2013, quelles évolutions ?

- **Constat d'une multiplication de nouvelles formes de cyber attaques**
  - Vol d'informations confidentielles (attaques du groupe pirate APT1)
  - « Hacktivisme » (les descendants d'Anonymous)
  - Cyber guerre (les suites du virus Stuxnet)
  - Lanceurs d'alertes ou « Whistleblowing » (affaire Prism)
- **Les dangers du caractère international des cyber attaques**
  - La difficile mise en œuvre de procédures répressives à l'échelle internationale
  - Caractère transfrontalier des attaques



Les limites du droit international au bénéfice des cybercriminels

- **Approches législatives divergentes :**
  - Approches différentes sur la recevabilité ou non de la preuve électronique
  - Infractions différentes (nécessité de l'élément intentionnel ou pas)
  - Diversité des législations sur la compétence juridictionnelle
  - Conceptions divergentes des droits fondamentaux (vie privée)

- **Niveaux de ressources différents selon les pays :**
  - Absence de magistrats spécialisés dans de nombreuses juridictions
  - Manque de ressources et de capacité des structures chargées d'enquêter dans de nombreux pays en voie de développement (Etude UNODC, 2013)

Existe-t-il un paradis pour les cyber-criminels ?

- Difficultés d'investigation à l'échelle internationale (quelles procédures, quelles lois sont applicables aux cybercriminels ?)
- La souveraineté des Etats face aux lois internationales
- Une coopération transfrontalière limitée entre les polices nationales
- Les effets limités des accords ou traités multilatéraux
- L'absence de gouvernance réelle de l'internet

Réflexions sur la gouvernance de l'internet ?

- Libertés fondamentales versus sécurité de l'information ?

- L'internet peut-il ou a-t-il besoin d'être régulé ?
  - Les enjeux d'une gestion mondiale des réseaux
  - Un frein pour l'innovation ?
- Quel régime international appliquer (Antarctique, fonds sous-marins, etc.) ?
- Les effets déclencheurs des révélations sur le programme Prism
- Déclaration de Montevideo sur l'avenir de la coopération pour l'internet
  - Appel à la mondialisation des fonctions de l'IANA et de l'ICANN
  - Appel à la mise en place d'une coalition multi-acteurs pour la gouvernance de l'Internet.

La Convention internationale sur la cybercriminalité : une démarche positive à l'effectivité limitée

- « Convention de Budapest » adoptée le 23 novembre 2001
- 41 pays adhérents (36 pays européens et l'Australie, la République Dominicaine, le Japon, l'Ile Maurice et les USA)
- **Objectif :** poursuivre *"une politique pénale commune destinée à protéger la société contre le « cyber crime », notamment par l'adoption d'une législation appropriée et la stimulation de la coopération internationale"*.
- **Différentes catégories d'infractions :**
  - Infractions contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques
  - Infractions et falsifications informatiques
  - Infractions se rapportant au contenu (pornographie infantile et atteintes à la propriété intellectuelle)
- **Et en pratique ?**
  - Faible nombre de pays signataires : la Convention de Budapest a perdu sa vocation universelle

Cybercriminalité en 2013 aux Etats-Unis

- **Quelques affaires récentes:**
  - **Affaire Snowden** : *(Juin 2013, révélations sur Prism, le programme de surveillance de la NSA)*
  - **Affaire Silk Road** : *(Décembre 2013, démentellement d'un réseau de vente de stupéfiants par internet par enquête du FBI)*
  - **Affaire relative au vol de numéros de cartes de crédit** : *(Juillet 2013 : plus gros cas de piratage aux US : vol de 160 millions de numéros de cartes de crédit)*

- **Principales lois :**
  - Computer Fraud and Abuse Act (CFAA) de 1986
  - Electronic Communications Privacy Act (ECPA) de 1986
  - Cyber Security Enhancement Act (CSEA) de 2002

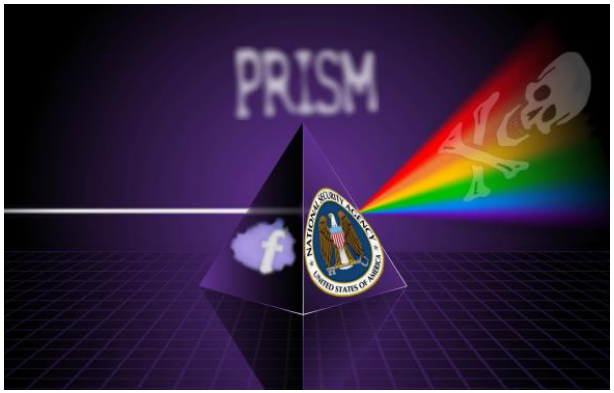
- **Les organismes d'enquête :**
  - La National Cyber Security Division (NCSD) du Department of Homeland Security (DHS)
  - La CATS (Cyber Action Teams) du FBI
  - La National security agency (NSA), au sein du département de la défense
  - L'USCYBERCOM

Règlementation américaine en matière de cybersécurité

- **Les dangers et abus des Etats Unis liés à la mise en œuvre de régime sécuritaires préventifs :**
  - Le Patriot Act
  - L'Espionnage Act
  - Remise en cause de la constitutionnalité du programme de la NSA

- **Les récents « efforts diplomatiques » :**
  - Instauration d'un dialogue avec la Chine pour la mise en place de règles en termes de cybercriminalité et d'espionnage commercial

- **Les lois ou projets de lois post-Prism**
  - Rapport d'étude sur les pratiques de la NSA remis au Président Obama en décembre 2013
  - Annonce de prochaines réformes :
    - Réforme des programmes de surveillance du renseignement américain, notamment la NSA
    - Limitation des écoutes téléphoniques



La lutte contre la cybercriminalité en Asie

- **Les récents efforts du Japon :**
  - Promotion de la coopération interétatique dans la lutte contre la cybercriminalité
  - En juillet 2012, le Japon a adhéré à la convention de Budapest sur la cybercriminalité (premier cocontractant de la région asiatique)
  - 2014- : "Global Program on Cybercrime Project for Southeast Asia" (UNODC, Office des Nations Unies contre la drogue et le crime)

- **Les politiques et stratégies mises en place en Chine :**
  - La Chine, un acteur du cyberespace devenu incontournable
  - Revendication par le Gouvernement chinois de la surveillance de ses citoyens et du monde extérieur
  - Rapport Mandiant et les révélations sur les cyber-attaques chinoises
  - Espionnage industriel

- **Affaires récentes en Chine:**
  - Piratage du jeu World of Warcraft (2 ans de prison)
  - Racket en ligne
  - Sites de vente de faux médicaments

Les enjeux pour 2014

- **Véritable prise de conscience de la vulnérabilité des données hackées ou interceptées en 2013**

- **La mise en œuvre d'actions nouvelles de lutte contre la cybercriminalité**
  - Une plus grande coopération entre les autorités internationales
  - Vers une harmonisation des réglementations et des procédures de lutte contre la cybercriminalité

- **De nouvelles initiatives en termes de gouvernance d'internet**
  - « Global Multistakeholder Meeting on the Future of Internet Governance », en avril 2014 à Sao Paulo

Références

- « *Etude approfondie sur le phénomène de la cybercriminalité et les mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face* », UNODC, janvier 2013

http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_F.pdf

- "*Le droit pénal face à la cyberdélinquance et à la cybercriminalité*", Jacques Francillon, 2012, Revue Lamy droit de l'immatériel

- « *Compétence et accès transfrontalier : quelles solutions* ? », 2012

http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2012)3F_transborder_repV27FR.pdf

- « *From nuclear war to Net War : Analogizing Cyber Attacks in International Law* », Scott J. Shackelford, 2009

http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1368&context=bjil

Agenda du Panorama 2013

- Démystification ou comment s'affranchir du « PRISM » déformant de l'actualité
- Les cybercriminels n'ont pas disparu...
- Le paradis cybercriminel existe-t-il sur terre ? Quelles sont les stratégies des Etats pour en obtenir la clé ?
- **2013, l'année des monnaies virtuelles**
- Arsenal juridique français et européen : le droit à l'épreuve de la cybercriminalité
- Nous aurions aussi aimé vous parler de…
- Table ronde

2013, année des monnaies virtuelles

Garance MATHIAS
Avocat à la Cour

Cabinet d'Avocats

Barbara LOUIS-SIDNEY
Juriste, CEIS

1. Qu'est-ce que la monnaie virtuelle ?

- Fonctions traditionnelles de la monnaie:
  - Monopole d'émission de la monnaie ayant un cours légal par les banques centrales
  - Unité de compte, c'est-à-dire une unité standardisée qui permet de mesurer la valeur des flux et des stocks de biens, de services ou d'actifs

1. Qu'est-ce que la monnaie virtuelle ?

Article L315-1 du Code monétaire et financier

I.-La monnaie électronique est une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement définies à l'article L.133-3 et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique.

II.-Les unités de monnaie électronique sont dites unités de valeur, chacune constituant une créance incorporée dans un titre.

1. Qu'est-ce que la monnaie virtuelle ?

- Par la Banque centrale européenne:
  - *« unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community. »*
- Par le bureau du département du Trésor, le FinCEN (Financial Crimes Enforcement Network) qui a publié le 18 mars 2013 ses analyses relatives aux monnaies virtuelles:
  - « *a medium of exchange that operates as currency in some environments, but does not have all the attributes of real currency* ».

2. Les monnaies virtuelles ont fait l'actualité 2013

Chute de Liberty Reserve: 28 mai 2013

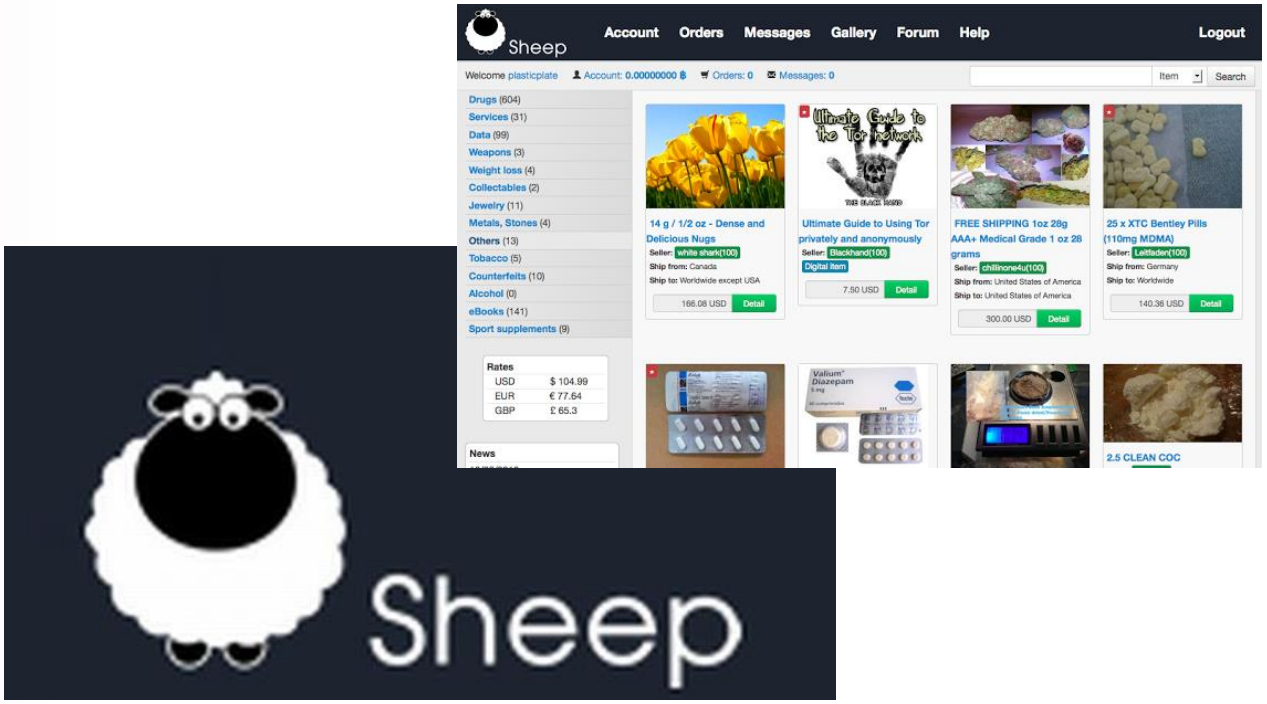
Liberty Reserve

Silk Road
anonymous marketplace

Fermeture du site Silk Road:
2 octobre 2013

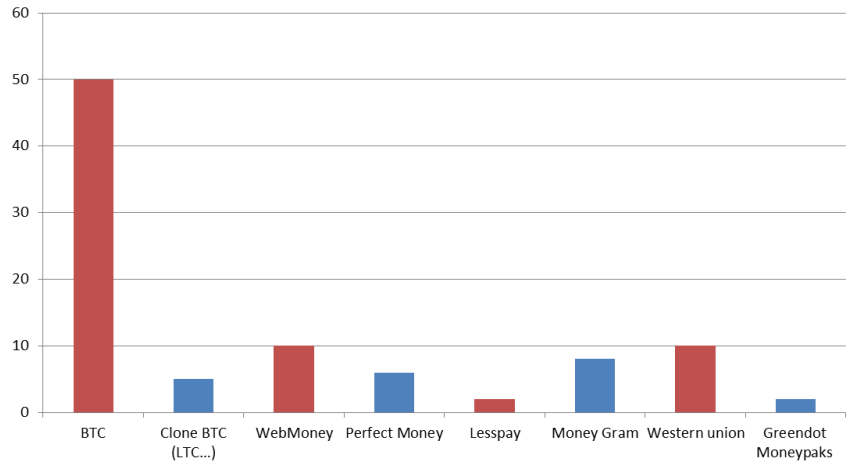
2. Les monnaies virtuelles ont fait l'actualité 2013

Fermeture après un vol de 40 millions de dollars en BTC



3. Pourquoi les monnaies virtuelles ?

Bitcoin plébiscité, pourquoi ?



Source : Livre blanc CEIS – « Monnaies virtuelles et cybercriminalité »

Bitcoin and Tor, a perfect team

When using Bitcoin together with Tor you are combining the best online money with the best encryption and privacy technology available.
Its simply not possible to know you arent under surveilance when using normal internet websites for managing your Bitcoins.
Only a shared Bitcoin Web Wallet hosted as a Tor hidden service will provide you maximum anonymity and privacy!

Source : OnionWallet

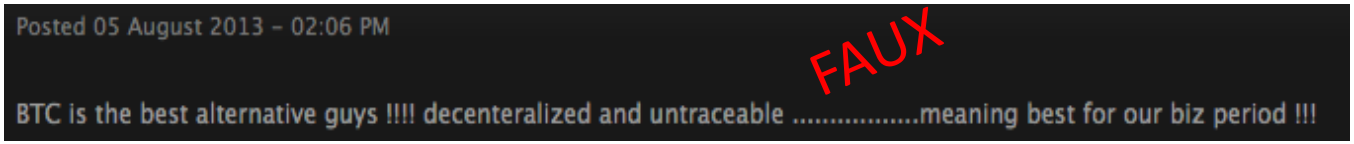
Les cybercriminels ont besoin de cet outil flexible, convertible en dollars, anonyme et hors du champ des autorités.

3. Pourquoi les monnaies virtuelles ?

L'anonymat : une monnaie anonyme…

Les adresses BTC sont anonymes

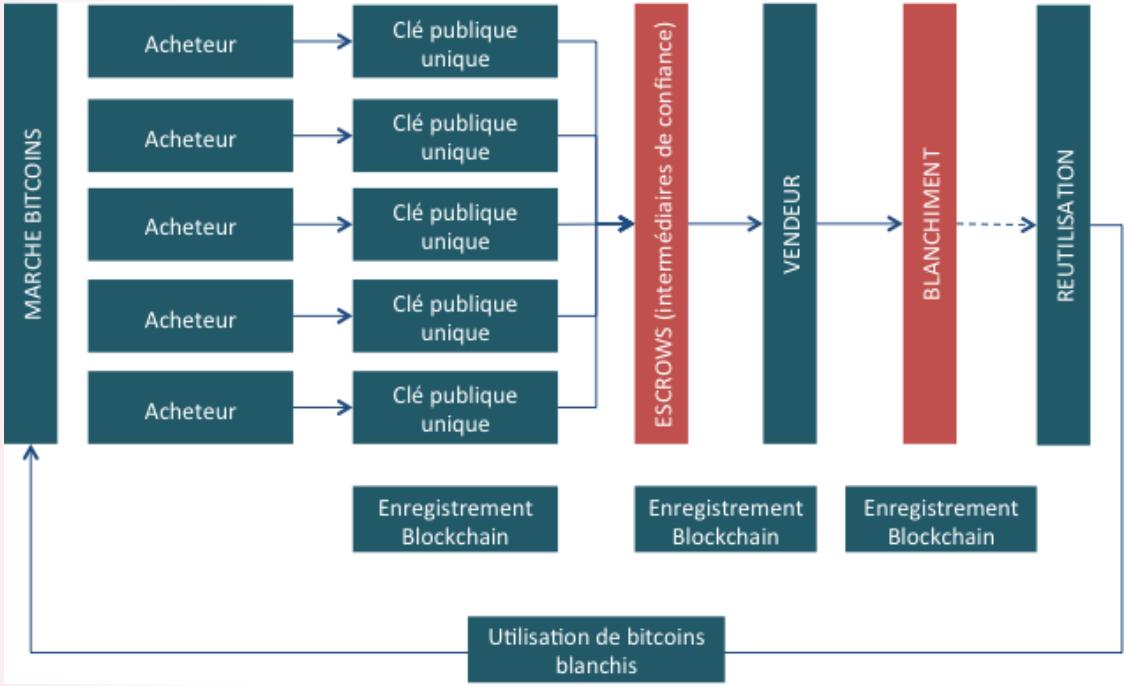
…mais traçable



Les transactions via Bitcoin sont publiques par défaut. Elles sont enregistrées dans un historique public (***blockchain***) afin d'éviter la dépense multiple d'une seule et même unité et d'instaurer la confiance nécessaire au développement de la monnaie et de palier ainsi l'absence d'autorité centrale.

3. Pourquoi les monnaies virtuelles ?

Aller plus loin : le blanchiment de bitcoins



Point de vulnérabilité

Source : Livre blanc CEIS – « Monnaies virtuelles et cybercriminalité »

Your anonymous Tor Bitcoin Wallet and Laundry

OnionWallet Features:

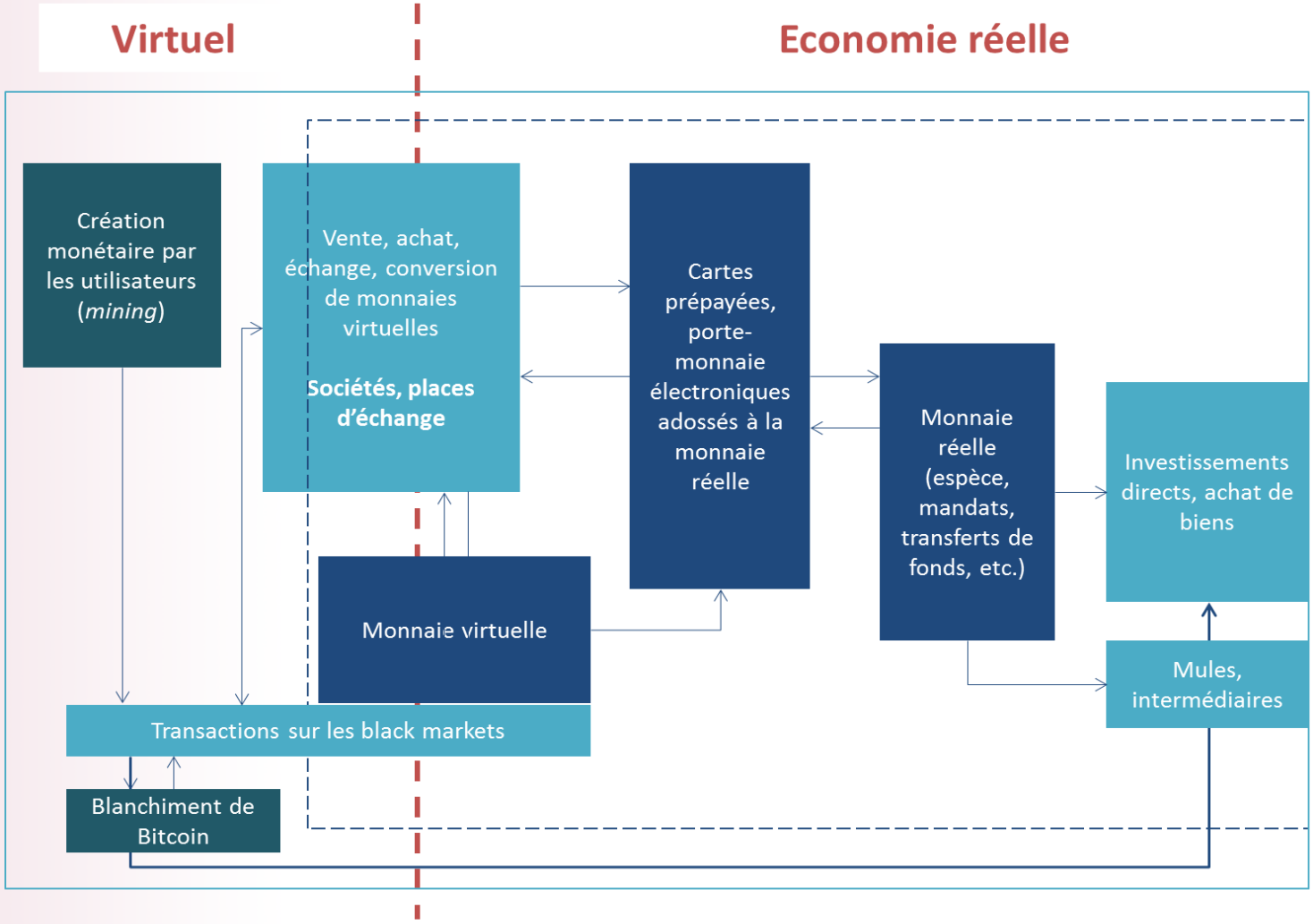
- **Free Bitcoin Mixer! You will always get get completely different Bitcoins on withdrawals with no "taint" to your recieving address.**
- Safe storage: we keep most of the bitcoins in secure encrypted offline storage.
- Protect your funds with a transaction PIN.
- Anonymous registration: We dont need any private data.
- Very simple user interface, no complicated options and settings.
- Transaction fee: only 0.001 Bitcoins which is fully paid to the network.

Source : OnionWallet (SCAM)

Vers un bitcoin anonyme et sécurisé ?

3. Pourquoi les monnaies virtuelles ?

Une monnaie décorrélée de l'économie réelle mais convertible en $



Source : Livre blanc CEIS – « Monnaies virtuelles et cybercriminalité »

3. Pourquoi les monnaies virtuelles ?

Une monnaie sans garde-fous

- Statut juridique incertain
- Question clé : est-ce que Bitcoin est une monnaie ?
- Quel est le statut de l'échangeur ?
- L'encadrement des monnaies virtuelles, pilier de la lutte contre la cybercriminalité ?
- Comment les Etats abordent-ils la question ?

4. Une nécessaire réglementation

La plate-forme Mt.Gox, après avoir été mise en demeure de se conformer à la réglementation, a demandé et obtenu le 13 août 2013 une licence de Money Service Business qui lui permet de fournir aux Etats-Unis une activité de transfert de fonds, surveillée au titre de la lutte contre le blanchiment et le financement du terrorisme.

4. Une nécessaire réglementation

Et en France ? Contrôle par l'Autorité de contrôle prudentiel et de résolution et par la Banque de France

Article L522-6

I.-Avant de fournir des services de paiement, les établissements de paiement doivent obtenir un agrément qui est délivré par l'Autorité de contrôle prudentiel et de résolution, après avis de la Banque de France au titre du troisième alinéa du I de l'article L.141-4. Cet agrément ne peut être accordé qu'à une personne morale.

II.-Pour délivrer l'agrément à un établissement de paiement, l'Autorité de contrôle prudentiel et de résolution vérifie que, compte tenu de la nécessité de garantir une gestion saine et prudente de l'établissement de paiement, celui-ci dispose pour son activité de prestation de services de paiement :

a) D'un solide dispositif de gouvernement d'entreprise, comprenant notamment une structure organisationnelle claire avec un partage des responsabilités bien défini, transparent et cohérent ;

b) De procédures efficaces de détection, de gestion, de contrôle et de déclaration des risques auquel il est ou pourrait être exposé et d'un dispositif adéquat de contrôle interne, y compris des procédures administratives et comptables saines ;

Ce dispositif et ces procédures sont proportionnés à la nature et à la complexité des services de paiement fournis par l'établissement de paiement.

(…)

Article L141-4

I.-La Banque de France veille au bon fonctionnement et à la sécurité des systèmes de paiement dans le cadre de la mission du Système européen de banques centrales relative à la promotion du bon fonctionnement des systèmes de paiement prévue par l'article 105, paragraphe 2 du traité instituant la Communauté européenne.

L'opposabilité aux tiers et la mise en œuvre des droits des banques centrales nationales membres du Système européen de banques centrales et de la Banque centrale européenne sur les instruments financiers, effets, créances ou sommes d'argent nantis, cédés en propriété ou autrement constitués en garantie à leur profit ne sont pas affectées par l'ouverture des procédures prévues au livre VI du code de commerce ou toute procédure judiciaire ou amiable équivalente sur le fondement d'un droit étranger, ni par aucune procédure civile d'exécution prise sur le fondement du droit français ou d'un droit étranger, ni par l'exercice d'un droit d'opposition.

La Banque de France s'assure de la sécurité des moyens de paiement tels que définis à l'article L.311-3, autres que la monnaie fiduciaire, et de la pertinence des normes applicables en la matière. Si elle estime qu'un de ces moyens de paiement présente des garanties de sécurité insuffisantes, elle peut recommander à son émetteur de prendre toutes mesures destinées à y remédier. Si ces recommandations n'ont pas été suivies d'effet, elle peut, après avoir recueilli les observations de l'émetteur, décider de formuler un avis négatif publié au Journal officiel. (…)

4. Une nécessaire réglementation

Banque de France – Focus – 5 Décembre 2013 « Les dangers liés au développement des monnaies virtuelles: l'exemple du bitcoin »

Le BTC ne peut pas être qualifié de monnaie ayant cours légal dans la mesure où il est possible de le refuser en paiement sans contrevenir aux dispositions de l'article R642-3 du Code pénal:

- *Le fait de refuser de recevoir des pièces de monnaie ou des billets de banque ayant cours légal en France selon la valeur pour laquelle ils ont cours est puni de l'amende prévue pour les contraventions de la 2e classe*.

Le BTC n'est pas non plus assorti d'une garantie légale de remboursement à tout moment et à la valeur nominale.

4. Une nécessaire réglementation

Paradoxe :

- Agrément des plate-formes de conversion qui peuvent permettre l'achat ou la vente de BTC;
- Absence de réglementation de l'utilisation du BTC sur Internet

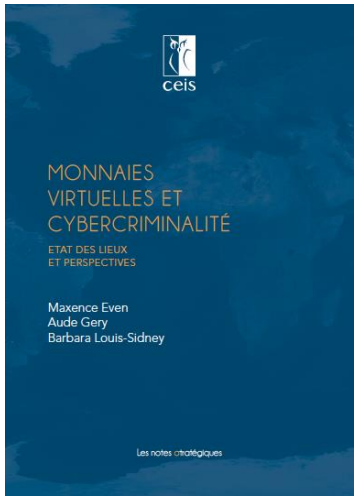
5. Quelles perspectives ?

L'autorégulation

- Respecte la philosophie sous-tendant l'utilisation de monnaies virtuelles
- Conserver l'absence d'intervention étatique ou d'institutions bancaires
- Monnaie virtuelle victime des activités cybercriminelles ?
- La *Digital Asset Transfer Authority (DATA)*

Objectif : *"développer la confiance du public et des autorités en devenant le référent en matière de standards pour des transactions sûres et responsables"*

Monnaies Virtuelles – Références



Livre blanc : Monnaies virtuelles et cybercriminalité - CEIS
Lien à venir
Zerocoin
http://zerocoin.org/
OnionWallet (SCAM)
Code monétaire et financier (art.L315-1; L522-6, L141-4), Code pénal (R642-3)
http://www.legifrance.gouv.fr/
Banque Centrale européenne
http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
Financial Crimes Enforcement Network (FinCen)
http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html
Liberty Reserve Silk Road sheep marketplace
http://www.libertyreserve.com/index.html
http://www.ice.gov/doclib/news/library/speeches/131218silkRoad.pdf
http://www.bbc.co.uk/news/technology-24373759
http://www.01net.com/editorial/609576/le-casse-du-siecle-sur-internet-76-millions-d-euros-voles-a-des-dealers/
Plate-Forme MT.GOX
https://www.mtgox.com/
Focus Banque de France -5.12.2013 « Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin »
http://www.banquefrance.fr/fileadmin/user_upload/banque_de_france/publications/Focus-10-stabilite-financiere.pdf

Agenda du Panorama 2013

- Démystification ou comment s'affranchir du « PRISM » déformant de l'actualité
- Les cybercriminels n'ont pas disparu...
- Le paradis cybercriminel existe-t-il sur terre ? Quelles sont les stratégies des Etats pour en obtenir la clé ?
- 2013, l'année des monnaies virtuelles
- **Arsenal juridique français et européen : le droit à l'épreuve de la cybercriminalité**
- Nous aurions aussi aimé vous parler de…
- Table ronde

Arsenal juridique français et européen : le droit à l'épreuve de la cybercriminalité

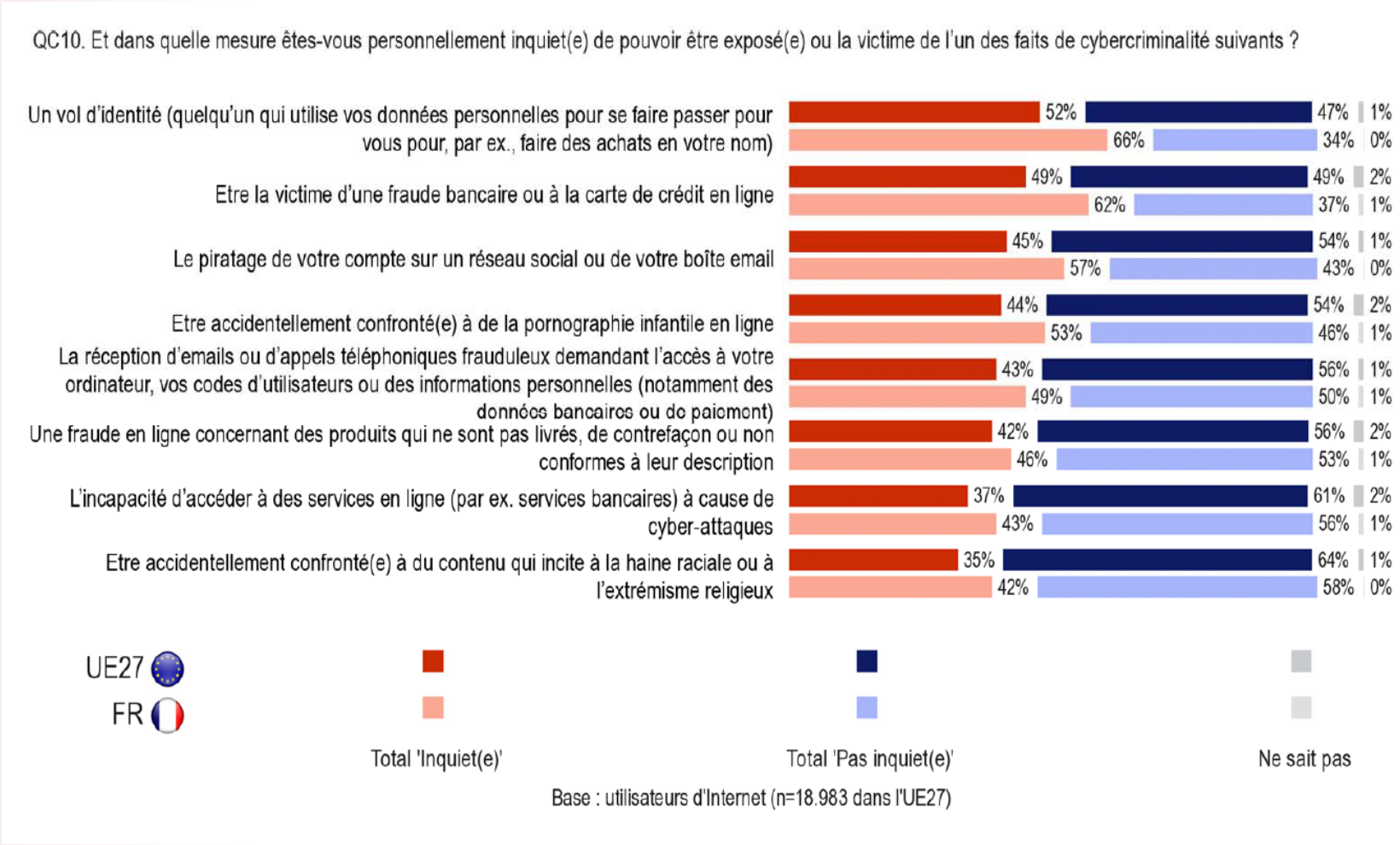
Garance MATHIAS

Avocat à la Cour

Cabinet d'Avocats

www.avocats-mathias.com

Craintes des français et des européens



Source: Commission Européenne – Eurobaromètre 2013

Environnement stratégique de la France et de l'Europe

- Nouveaux défis en matière de sécurité
- Volatilité régionale et mondiale accrue
- Conséquences de la crise financière…

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Union Européenne: une année 2013 riche en projets

Un plan de cybersécurité de l'UE pour protéger l'Internet ouvert et les libertés en ligne

Centre européen de lutte contre la cybercriminalité

Création du Centre européen de lutte contre la cybercriminalité (EC3) le 11 janvier 2013 à La Haye

« *Le centre de lutte contre la cybercriminalité accroîtra fortement la capacité de l'EU à combattre la cybercriminalité et à défendre un Internet libre, ouvert et sûr. Les cybercriminels sont intelligents et prompts à mettre les nouvelles technologies au service d'intentions criminelles. L'EC3 nous aidera à les surpasser en intelligence et en vitesse afin de prévenir et de combattre leurs actes criminels.* » a déclaré la commissaire Malmström.

Commission Européenne, Communiqué de presse, 09.01.2013

Stratégie de la Commission européenne

Communication de la Commission européenne en date du 7 Février 2013

« Stratégie de cybersécurité de l'UE: un cyberespace ouvert, sûr et sécurisé »

La vision de l'UE s'articule autour de 5 priorités stratégiques:

- Parvenir à la cyber-résilience;
- Faire reculer considérablement la cybercriminalité;
- Développer une politique et des moyens de cyberdéfense liée à la politique de sécurité et de défense commune (PSDC);
- Développer les ressources industrielles et technologiques en matière de cybersécurité;
- Instaurer une politique internationale de l'UE cohérente en matière de cyberespace et promouvoir les valeurs essentielles de l'UE.

Proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union (SRI) présentée le 7 février 2013

- Obliger les Etats membres
  - à adopter une stratégie en matière de SRI et à mettre en place une autorité de SRI;
  - à désigner une Equipe d'Intervention en cas d'Urgence Informatique;
  - à coopérer avec les autres Etats Membres et la Commission afin de diffuser des messages d'alerte rapide sur les risques et incidents.
- Obliger les administrations publiques et « certains acteurs du marché »
  - à adopter des pratiques en matière de gestion des risques;
  - à rapporter les incidents de sécurité majeurs de leurs services essentiels.

Le Règlement européen dit « data breach »

- Règlement n°611/2013 du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel
- Entrée en vigueur: 25 août 2013
- Objectifs:
  - Harmonisation des procédures de notification des violations aux autorités de protection des données personnelles et aux personnes concernées;
  - Impose aux autorités compétences de mettre à disposition des fournisseurs de service de communications électroniques un moyen électronique sécurisé de notification.

Directive du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information

Les Etats membres doivent ériger en infraction les 5 types d'agissements suivants:

- *l'accès illégal à tout ou partie des systèmes d'information*, à savoir l'accès commis en violation d'une mesure de sécurité ;
- *l'atteinte illégale à l'intégrité d'un système d'information*, à savoir le fait de provoquer une perturbation grave ou une interruption du fonctionnement d'un système, en introduisant, effaçant, altérant, ou rendant inaccessibles des données informatiques ;
- *l'atteinte illégale à l'intégrité des données*, à savoir le fait d'endommager, de détériorer, de supprimer ou de rendre inaccessibles des données informatiques d'un système ;
- *l'interception illégale* (par des moyens techniques de transmissions non publiques) *de données informatiques* à destination, en provenance ou à l'intérieur d'un système d'information ;
- enfin *la mise à disposition* (production, vente, importation, diffusion) *d'outils* (logiciels ou codes d'accès) utilisés dans l'intention de commettre l'une des infractions visées ci-dessus.

Transposition au plus tard en 2015.

Paquet sur la « Protection des données personnelles »

- Proposition de règlement sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel, et libre circulation de ces données
  - Objectif: instaurer le cadre général de la protection des données personnelles applicable au secteur privé et public

- Proposition de directive sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et libre circulation de ces données
  - Objectif: fixer les règles applicables aux traitements de données personnelles en matière de police et de justice

Paquet sur la « Protection des données personnelles »

La position adoptée le 21 octobre 2013 par la Commission des libertés civiles, de la justice et des affaires intérieures (LIBE)

<u>Focus sur l'obligation de notification des fuites de données</u>

Protection du secret d'affaires

- Le 28 Novembre 2013, la Commission européenne a présenté une proposition de directive « sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites »

- Objectif: établir un niveau suffisant et harmonisé de protection et de recours au sein du marché intérieur en cas d'appropriation illicite d'un secret d'affaires

Proposition de Règlement du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur

- Publiée le 4 juin 2012
- Objectifs:
  - susciter une confiance accrue dans les transactions électroniques au sein du marché intérieur;
  - garantir la reconnaissance juridique transnationale de l'identification, de l'authentification et des signatures électroniques et des services de confiance associés;
  - établir un cadre juridique clair afin de remédier au cloisonnement et au manque d'interopérabilité, de développer la citoyenneté numérique et de prévenir la cybercriminalité.

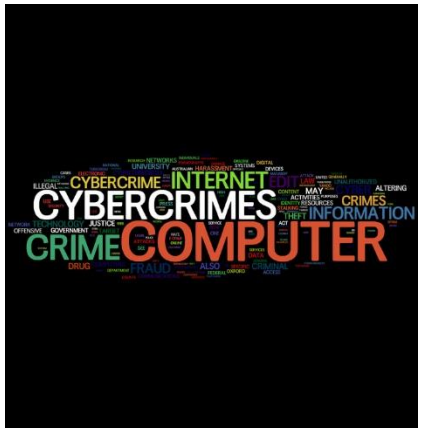
CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Réflexions françaises en matière de lutte contre la cybercriminalité

Nouveaux dispositifs de lutte

Livre blanc sur la défense et la sécurité nationale du 29 avril 2013

Cybercriminalité clairement identifiée comme une menace majeure pour la sécurité nationale (OIV prises pour cibles, espionnage, etc.)



"***La Cybersécurité est l'une des priorités de notre stratégie de défense et de sécurité nationale pour se protéger d'une attaque informatique majeure pouvant désormais constituer un véritable acte de guerre***"

Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale

- Pas d'examen par le Conseil constitutionnel

Loi de Programmation Militaire 2014-2019

Focus sur l'article 20 :

- Accès administratif aux données de connexion (L.246-1 du Code de la Sécurité intérieure)
  - « *(…) les informations ou documents mentionnés à l'article L. 246-1 peuvent être recueillis sur **sollicitation du réseau** et transmis **en temps réel** par les opérateurs aux agents mentionnés au I de l'article L. 246-2* ».

- Auprès de qui ?
  - « *(…) des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique* ».

- Quels documents ?
  - « *(…) des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelant, la durée et la date des communications.* »

Arsenal juridique français et européen : le droit à l'épreuve de la cybercriminalité – Références

- FBI – Cyber Crimes Stories

http://www.fbi.gov/news/stories/story-index/cyber-crimes

- Commission Européenne, Communiqué de presse sur la création de l'EC3, 09.01.2013

http://europa.eu/rapid/press-release_IP-13-13_fr.htm

- Communication de la Commission européenne en date du 7 février 2013

http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_fr.pdf

- Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_fr.pdf

- Règlement n° 611/2013 de la Commission du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:fr:PDF

- Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:FR:PDF

- Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:FR:PDF

- Proposition de directive sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et libre circulation de ces données

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:FR:PDF

- Proposition de directive du Parlement européen et du Conseil sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0813:FIN:FR:PDF

- Proposition de Règlement du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:FR:PDF

- Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&dateTexte=&categorieLien=id

Agenda du Panorama 2013

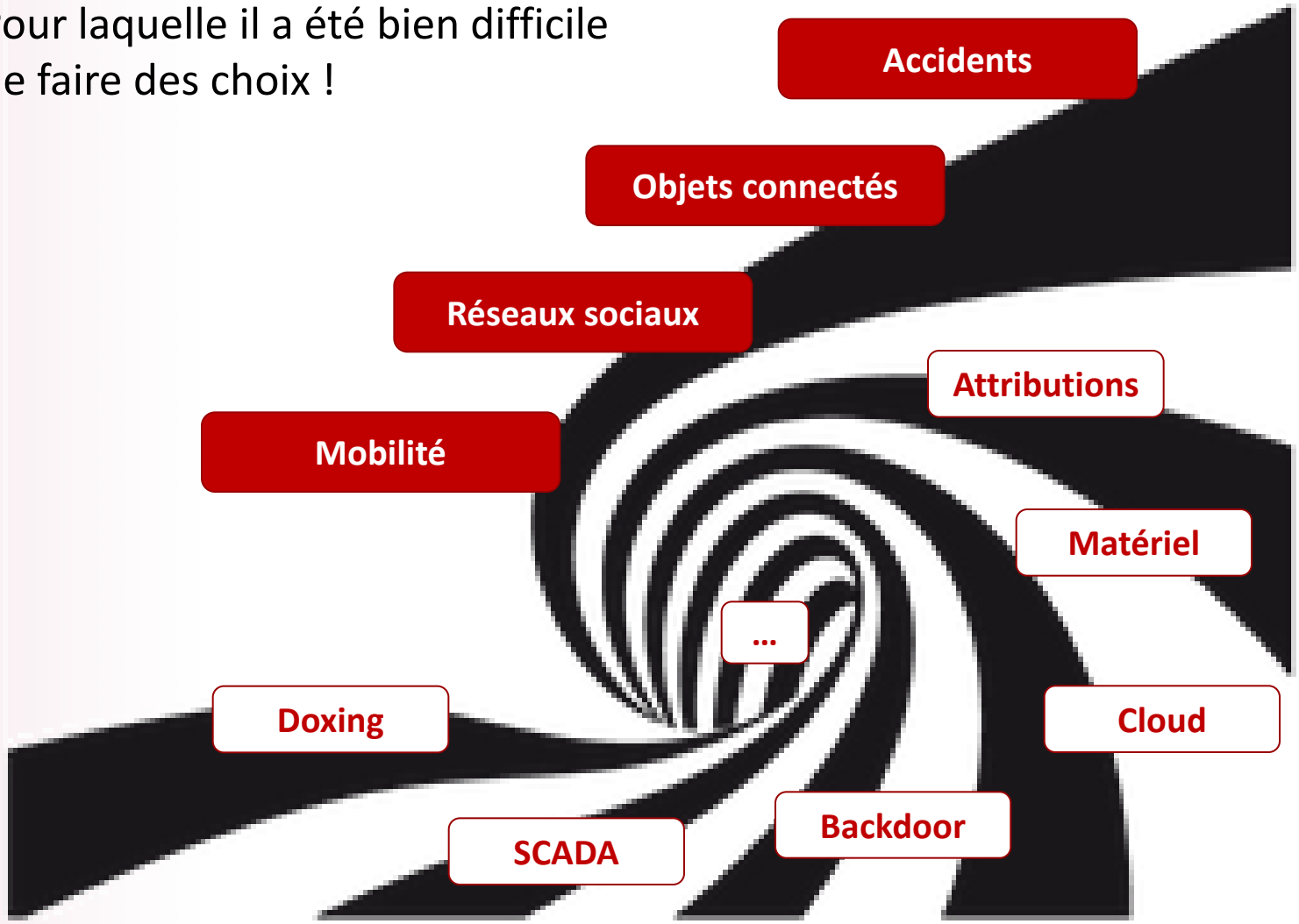
- Démystification ou comment s'affranchir du « PRISM » déformant de l'actualité
- Les cybercriminels n'ont pas disparu...
- Le paradis cybercriminel existe-t-il sur terre ? Quelles sont les stratégies des Etats pour en obtenir la clé ?
- 2013, l'année des monnaies virtuelles
- Arsenal juridique français et européen : le droit à l'épreuve de la cybercriminalité
- **Nous aurions aussi aimé vous parler de…**
- Table ronde

Nous aurions aussi aimé vous parler de…

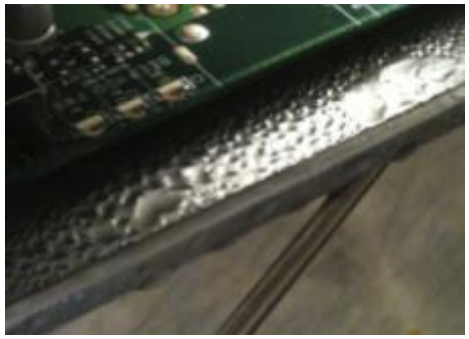
Gérôme BILLOIS, Senior Manager Solucom,
gerome.billois@solucom.fr **Twitter** @gbillois

2013… une année extrêmement riche

Pour laquelle il a été bien difficile de faire des choix !



Des accidents en pagaille



En 2013, toujours beaucoup de câbles coupés et de bug logiciels mais aussi des évènements plus « **originaux** » !

Le **cloud** de Facebook crée un nuage dans le datacenter…

… des **formules 1** sont clouées au sol à Barcelone…

… tandis que la **station spatiale internationale** tourne autour de la terre sans communication

➔ **Prévoir des incidents même lorsque tout a été testé**

Des objets toujours plus connectés…

Quel est le **point commun** entre tous ces objets ?

Oui, ils sont tous connectés, mais surtout ils recèlent tous **des vulnérabilités** !

Hue Blackout

Foscam hack

ECU Hack

Jailbreak

➔ Des premières **mises en cause des fabricants**… pour des cas graves

Les réseaux sociaux fréquemment usurpés…

Derrière ces attaques, la Syrian Electronic Army, un DJ anglais ou encore des plaisantins…

➔ Des solutions existent ! Pensez-y, les réseaux sociaux sont aujourd'hui considérés comme un canal de communication « officiel »

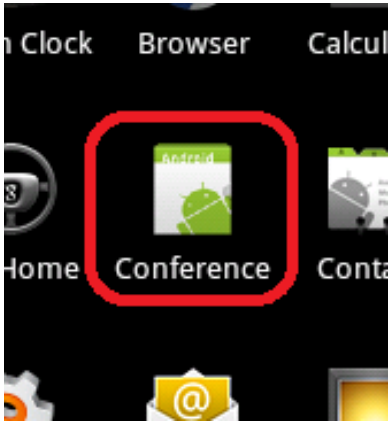
Mobilité, smartphones et tablettes

Toujours une pluie d'actualités sur ces thèmes…

…mais des menaces qui se précisent

Des malwares de plus en plus **sophistiqués**

→ Obad.a se rapproche des malwares Windows

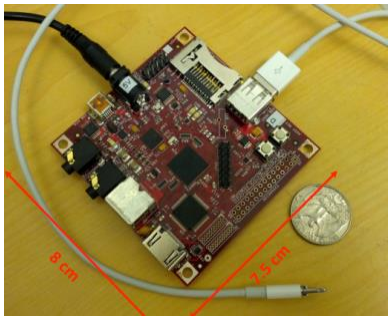


Des **attaques ciblées** « applicatives »

→ Chuli.a : Des activistes tibétains visés sur Androïd

Des attaques « **physiques** »

→ MacTans et son faux chargeur vise les iPhone/iPad



Les périphériques mobiles restent un domaine en développement pour les cybercriminels

Des sujets clés de 2013…

… à suivre de près en 2014 !

Nous aurions aussi aimé parler de… – Références

• Accident

http://www.theregister.co.uk/2013/06/08/facebook_cloud_versus_cloud/
http://pro.01net.com/editorial/587351/f1-les-essais-de-presaison-perturbes-par-un-bug-logiciel/
http://www.v3.co.uk/v3-uk/the-frontline-blog/2249029/nasa-briefly-loses-contact-with-international-space-station
http://www.theregister.co.uk/2013/06/08/facebook_cloud_versus_cloud/
http://www.opencompute.org/blog/learning-lessons-at-the-prineville-data-center/
http://en.wikipedia.org/wiki/International_Space_Station#Communications_and_computers

• Objets connectés

http://www.gizmodo.fr/2013/08/05/hacker-toilettes.html
http://bits.blogs.nytimes.com/2013/08/11/taking-over-cars-and-homes-remotely/?hp&_r=3
http://readwrite.com/2013/11/13/hacking-the-connected-home-when-your-house-watches-you#feed=/tag/internet-of-things&awesm=~or8pVfXE38smrB
http://www.futura-sciences.com/magazines/high-tech/infos/actu/d/technologie-skyjack-transformer-drone-pirate-air-50765/#xtor=AL-27-1[ACTU]-50765[SkyJack--ou-comment-transformer-un-drone-en-pirate-de-l--air
http://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/
http://www.eetimes.com/document.asp?doc_id=1319903&
http://conference.hitb.org/hitbsecconf2013ams/materials/D2T1%20-%20Sergey%20Shekyan%20and%20Artem%20Harutyunyan%20-%20Turning%20Your%20Surveillance%20Camera%20Against%20You.pdf
http://www.saurik.com/id/16
http://www.edn.com/design/automotive/4423428/2/Toyota-s-killer-firmware--Bad-design-and-its-consequences
http://illmatics.com/car_hacking.pdf

Nous aurions aussi aimé parler de… – Références

• Réseaux sociaux

http://rt.com/usa/hackers-associated-press-obama-282/
http://gizmodo.com/5985353/exclusive-the-burger-king-and-jeep-hacker-is-probably-this-dj-from-new-england
http://mashable.com/2013/02/18/burger-king-twitter-account-hacked/
http://www.20minutes.fr/search?q=twitter+pirat%C3%A9
http://theonion.github.io/blog/2013/05/08/how-the-syrian-electronic-army-hacked-the-onion/
http://21stcenturywire.com/2013/04/24/white-house-attacked-obama-injured-ap-tweet-hoax-crashes-us-stock-market/

• Mobile

http://www.infosecurity-magazine.com/view/36211/mobile-security-woes-escalate-a-whopping-733/
http://www.securelist.com/en/blog/8106/The_most_sophisticated_Android_Trojan
https://media.blackhat.com/us-13/US-13-Lau-Mactans-Injecting-Malware-into-iOS-Devices-via-Malicious-Chargers-WP.pdf
https://media.blackhat.com/us-13/US-13-Lau-Mactans-Injecting-Malware-into-iOS-Devices-via-Malicious-Chargers-Slides.pdf
http://www.scmagazineuk.com/targeted-attack-tied-to-tibet-leads-to-malicious-android-app-download/article/286036/
http://www.securelist.com/en/blog/208194186/
http://www.darkreading.com/attacks-breaches/luckycat-apt-campaign-building-android-m/240004623
http://www.securelist.com/en/blog/8131/Obad_a_Trojan_now_being_distributed_via_mobile_botnets

Agenda du Panorama 2013

- Démystification ou comment s'affranchir du « PRISM » déformant de l'actualité
- Les cybercriminels n'ont pas disparu...
- Le paradis cybercriminel existe-t-il sur terre ? Quelles sont les stratégies des Etats pour en obtenir la clé ?
- 2013, l'année des monnaies virtuelles
- Arsenal juridique français et européen : le droit à l'épreuve de la cybercriminalité
- Nous aurions aussi aimé vous parler de…
- **Table ronde**

Table ronde

Colonel Éric FREYSSINET
Chef de la division de lutte contre la cybercriminalité - Pôle judiciaire de la Gendarmerie Nationale - STRJD

Olivier GUERIN *(animateur de la table ronde)*
Chargé de mission - CLUSIF

Lazaro PEJSACHOWICZ
Président du CLUSIF
Chargé de mission auprès de la communauté des SSI – CNAMTS

Hervé SCHAUER
Consultant en sécurité de l'information et dirigeant du cabinet HSC