CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Panorama de la cybercriminalité année 2015

Paris, 14 janvier 2016

Evénement organisé en partenariat avec :

Agir pour la Sécurité de l'Information : **Le CLUSIF…**

- Lieu de rencontre de **tous les professionnels** pour qui la SI est une préoccupation, leur mission
- Lieu de réflexion sur les **enjeux de la Sécurité de l'Information** pour aujourd'hui et pour demain
- Communauté de **partage des savoirs et des expériences**
- Communauté d'association en Région, les **CLUSIR**, et à l'étranger, les **CLUSI**
- **Plus de 20 ans de travaux** fédérés autour d'un même thème pour produire des **Méthodes et des Documents** aujourd'hui de référence

L'Esprit d'Echange !

Panorama Cybercriminalité : **Derrière le rideau**

- C'est avant tout un **Groupe de travail**
  - constitué par des Membres et des non-membres (experts externes)
  - des heures de veille, de discussions, de contradictions…

- C'est une **sélection d'événements** illustrant
  - l'émergence d'un « phénomène »
  - une tendance durable
  - des incidents et des accidents de la société numérique
  - un regard sur notre société et ses effets dans les mondes virtuels

- C'est un **moment de partage**
  - avec notre communauté
  - avec la société civile, les autorités et la presse

Panorama Cybercriminalité : **Que nous réserve 2016 ?**

- L'année 2015 aura été marquée par de tristes événements

- Les cyber-attaques contre les environnements pubics, grands publics au-delà des ressources numériques de nos entreprises nous font prendre conscience des besoins
  - tant de ***Cybersécurité***
  - que de ***Sécurité des Systèmes d'Information*** ...

En juin, nous vous présenterons le résultat de notre ***étude MIPS 2016***

Elle fera un point de situation sur la prise en compte de ses concepts par nos Entreprises et nos Collectivités territoriales

Les contributeurs au Panorama:

Un groupe de travail pluriel issu du privé et de l'administration.

- Air Caraïbes
- AP-HP Assistance Publique-Hôpitaux de Paris
- Cabestan-consultants
- CEIS
- CERT-IST
- CERT-LEXSI
- CERT Société Générale
- CERT-Solucom
- Garance Mathias Avocats
- Gras Savoye
- Hewlett Packard Enterprise
- HSC by Deloitte
- Huawei
- Intel Security / McAfee Labs & StoneSoft
- InventiPharma
- Michelin
- Prosica
- Red Team
- SCASSI
- Trend Micro

- Caisse Nationale de l'Assurance Maladie des Travailleurs Salariés (CNAM-TS)
- Ministère de l'Intérieur, Direction Centrale de la Police Judiciaire
- Ministère de l'Intérieur, Lutte contre les cybermenaces

Panorama 2015

Les images sont de droits réservés
Les informations utilisées proviennent de sources ouvertes
Les entreprises sont parfois citées par souci de précision. Leur nom a été vu dans les médias

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

Interventions, Panorama 2015 (1/4)

- Attaques astucieuses: Comment les cybercriminels nous ont-ils surpris en 2015 ?

  Fabien COZIC

  - Directeur d'enquêtes privées / Red Team Investigations

- 0-days : analyse des marchés noirs des outils d'attaques numériques

  Loïs SAMAIN

  - Consultant Cybersécurité / Cyberdéfense - CEIS

  Sujet présenté par Hervé SCHAUER

  - Directeur Général / HSC by Deloitte

Interventions, Panorama 2015 (2/4)

- Cyber-diplomatie : Chine, USA mais pas seulement …

  Loïc GUEZO

  - CyberSecurity Strategist – Trend Micro Inc.

- Djihad 2.0 - état des lieux, enjeux opérationnels et juridiques

  François PAGET

  - Secrétaire Général Adjoint du CLUSIF et animateur du groupe « Panorama »

  DCPJ

  - Sous-Direction de Lutte contre la Cybercriminalité / Division de l'anticipation et de l'analyse – Ministère de l'Intérieur

  Amélie PAGET

  - Consultante juridique SI – HSC by Deloitte

Interventions, Panorama 2015 (3/4)

- Objets connectés – 2015, l'année du piratage des voitures, et demain ? Etat des lieux et aspects juridiques

  Gérôme BILLOIS

  - Senior Manager / CERT-Solucom

  Garance MATHIAS

  - Avocat à la Cour / Mathias Avocats

- Nos téléphones mobiles : des cibles de premier plan
- Les conséquences d'une attaque

  Colonel Eric FREYSSINET

  - Conseiller auprès du Préfet, Conseiller du Gouvernement, chargé de la lutte contre les cybermenaces

Interventions, Panorama 2015 (4/4)

- (Malgré tout,) Quelques raisons de se réjouir

  François PAGET

  - Secrétaire Général Adjoint du CLUSIF et animateur du groupe « Panorama »

- Conclusion

  Monsieur le Préfet Jean-Yves LATOURNERIE

  - Conseiller du Gouvernement, Chargé de la lutte contre les cybermenaces, Ministère de l'Intérieur.

Attaques astucieuses:
Comment les cybercriminels nous ont-ils surpris en 2015 ?

Fabien COZIC

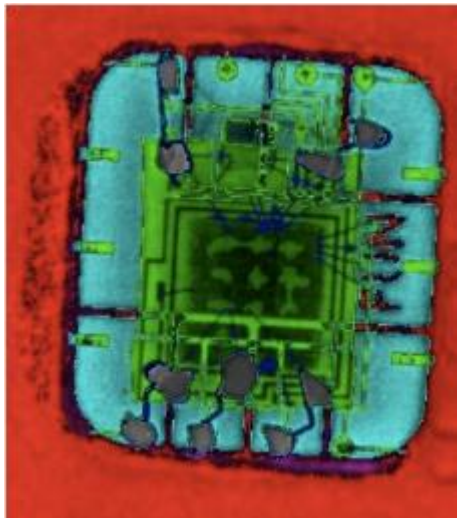
Directeur d'enquêtes privées – **Red Team Investigations**

Introduction

- Passage en revue de cas astucieux, de détournements et de hacks 2015
- Sélection non exhaustive et subjective de cas spectaculaires ou plus anecdotiques
- Révélateurs de tendances et symptomatiques des efforts d'améliorations des MO cybercriminels

Attaques astucieuses - Environnement bancaire

- La *Yes Card* Nouvelle Génération (France, Belgique Octobre 2015)
  - *Groupe de délinquance ordinaire amélioré par la présence d'un ingénieur*
  - *Liens avec le vol en 2011 en France d'un lot de cartes puis utilisées en Belgique*
  - *L'expertise du Centre Microélectronique de Provence fait apparaître la modification physique de la puce*
  - *Attaque de type « Chip in the Middle » -> la seconde puce se substitue au mécanisme de validation du code PIN pour autoriser l'opération de retrait*
  - *Préjudice estimé de 600,000 €uros, 5 personnes arrêtées*



Source : http://arstechnica.com/tech-policy/2015/10/how-a-criminal-ring-defeated-the-secure-chip-and-pin-credit-cards/

Attaques astucieuses - Environnement bancaire

- Rétro attaque de distributeurs de billets (Russie, République Tchèque, USA – Novembre 2015)
  - *Groupe cybercriminel organisé, réseau de mules et fine connaissance des process de validation et d'annulation des transactions au DAB*
  - *Exploitation d'une faille dans le système de transactions internationales et de POS compromis*
  - *Dépôts de fonds par des mules puis retrait immédiat des mêmes sommes*
  - *Opération de réversion sur des POS contrôlés par le réseau à l'étranger avec les informations des reçus de retrait*
  - *La banque identifie cette opération comme une annulation de retrait et recrédite les comptes*
  - *Près de 4 millions d'€uros de butin, aucune arrestation*

Source : http://www.forbes.com/sites/thomasbrewster/2015/11/23/visa-mastercard-atm-fraud-hackers-steal-millions-dollars/

Attaques astucieuses – Environnement Finance

- Le délit d'initié 2.0 (France, Ukraine, USA, Russie, îles Vierges, îles Caïmans, Malte, Chypre et Bahamas - Août 2015)
  - *Réseau de fraude international, hackers ukrainiens et courtiers internationaux*
  - *Les pirates pénétraient les serveurs d'agence de communiqués de presse*
  - *Les traders utilisaient ces informations inédites pour mener de juteuses opérations*
  - *Les premières victimes sont les entreprises visées par les opérations: Boeing, Caterpillar, Netflix, Ford,…*
  - *15000 informations volées en 5 ans, préjudice estimé $100 millions, une trentaine de traders impliqués*

Source : http://www.lemonde.fr/economie-mondiale/article/2015/08/11/des-traders-allies-a-des-hackeurs-ukrainiens-poursuivis-par-la-justice-americaine_4721336_1656941.html

Attaques astucieuses – Environnement Web

- XCode Ghost: tout est plus simple quand on contrôle la source (Chine, USA – Septembre 2015)
  - *Compromission du logiciel de création et de développement des applications pour l'AppStore*
  - *Malware placé sur un service chinois de partage de fichiers et téléchargé par des développeurs IOS via un XCode repacké*
  - *Les applications générées par ces versions corrompues ont ensuite été distribuées légitimement sur l'AppStore*
  - *Le malware est destiné à capturer des informations sur les appareils infectés pour les renvoyer vers des C&C contrôlés par les pirates*
  - *Grâce à ces informations, mise en place de scenarios de phishing pour dérober des mots de passe et établissement d'une tête de pont pour l'installation d'autres programmes malveillants.*

Source : http://tempsreel.nouvelobs.com/tech/20150921.OBS6188/des-hackers-dupent-apple-et-infectent-des-millions-d-iphone.html

Attaques astucieuses – Environnement Web

- Le Malware Turla envoie le cybercrime dans l'espace (Russie, Europe, USA, OTAN – Septembre 2015)
  - *APT ciblant des gouvernements à des fins d'espionnage notamment diplomatique*
  - *Actif depuis 2008 au moins, toujours en cours*
  - *Mode opératoire d'infection classique (emails forgés, pièces jointes infectées…)*
  - *La communication avec les C&C passe par des connexions satellites légitimes, des leurres utilisées pour relayer les instructions*
  - *Cette méthode cache la partie critique des communications pour empêcher leur interception*
  - *Les satellites choisis semblent couvrir uniquement l'Afrique, ce qui complique encore les investigations*

Source : https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky/

Attaques astucieuses – Environnement Web

- Dridex, le malware qui ne voulait pas mourir (France, UK, USA, - Décembre 2015)
  - *Botnet / Malware bancaire par Spam (fausses factures, reçus de paiement…) le plus utilisé en 2015*
  - *Exploitation par MS Office -> Macro*
  - *Assemblage directement sur le poste infecté, Certificat Comodo*
  - *Gains estimés £20 millions en Grande Bretagne*
  - *Considéré comme démantelé en Octobre 2015 – Arrestations + Coupure des serveurs par le FBI (US) et le NCA (UK)*
  - *Réapparaît en novembre 2015 ciblant essentiellement des victimes françaises et américaine*

[INFO] [SPAM] Le malware Dridex n'est pas mort

Comme chaque semaine, le CERT-XMCO vous partage une information ayant fait l'actualité la semaine dernière. Cette semaine, nous vous proposons l'article sur la réapparition du malware bancaire Dridex par le biais de multiples campagnes de spam.

Bulletin CXA-2015-3481	
Titre	Le malware Dridex n'est pas mort
Titre officiel	*Despite takedown, the Dridex botnet is running again*
Criticité	Elevée
Date	26 Octobre 2015
	En dépit de l'arrestation des responsables de l'équipe à l'origine du malware Dridex, de nombreux spams contenant aujourd'hui encore le malware circulent toujours.

Source : http://blog.xmco.fr/index.php?post/2015/11/02/Le-malware-Dridex-n-est-pas-mort

Attaques astucieuses – Environnement Matériels

- Fusils intelligents : tout dépend de qui l'a en main
  - *Le trick de l'année ! POC de Prise de contrôle à distance d'un fusil de gros calibre via WIFI*
  - *Calibre .300, $13,000 équiper du système Tracking Point d'assistance à la visée*
  - *Le WIFI intégré permet d'enregistrer le tir et de retransmettre en direct ce qui passe par la lunette*
  - *Signal non chiffré -> l'exploitation permet d'accéder à l'OS de l'arme et à altérer le mécanisme d'aide à la visée et au tir*
  - *Le hacker peut rooter le système et contrôler entièrement le système*

Source : http://www.wired.com/2015/07/hackers-can-disable-sniper-rifleor-change-target

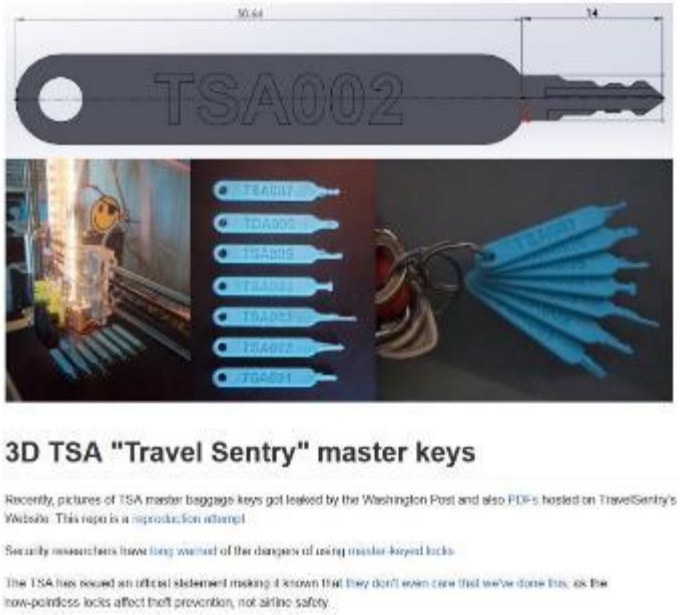
Attaques astucieuses – Environnement Matériels

- Déverrouiller les portes de garage est un jeu d'enfant (USA – Octobre 2015)
  - *RollJam intercepte les codes tournants émis par les systèmes d'ouverture à distance -> pas de chiffrement…*
  - *Le dispositif est caché dans un rayon de 10 mètres et intercepte le signal émis par l'usager*
  - *Le signal est stocké et peut être rejouer car non transmis au récepteur*
  - *Fonctionne également avec les portières de voiture*
  - *Le « jouet » peut transmettre au récepteur toutes les combinaisons possibles une fois un échantillon intercepté*
  - *Cas identifiés de cambriolages impliquant ce système aux USA*

Source : http://motherboard.vice.com/read/this-kids-toy-can-hack-garage-doors-in-seconds

Attaques astucieuses – Environnement Transports

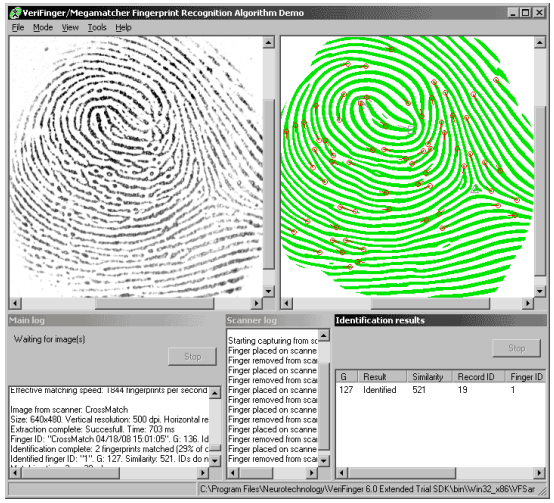
- La clé des contrôles de sécurité compromise
  - Après le 11/09/2001 ces clés permettent d'ouvrir tous les bagages
  - Un reportage du Washington Post montrant les Masterkeys
  - Reproduction à partir d'une photo puis impression 3D
  - Les modèles 3D ont été publiés sur GitHub



Source : http://www.zdnet.fr/actualites/les-clefs-des-verrous-tsa-dans-la-nature-39824778.htm

Attaques astucieuses – Environnement Identité

- Porter des gants pour protéger les systèmes ? (Allemagne – Janvier 2015)
  - Reconstitution d'une empreinte digitale à partir de photos HD
  - La cible était la ministre allemande de la Défense
  - Une réalisation du Chaos Computer Club
  - Utilisation de Verifinger pour récupérer la tracé
  - Mise en parallèle avec le hack du système Touch ID d'Apple en 2013



Source : http://www.nextinpact.com/news/91637-il-est-possible-reconstituer-empreinte-digitale-depuis-photos.htm

Attaques astucieuses:
Comment les cybercriminels nous ont-ils surpris en 2015 ?

Sources 1/2

- La *Yes Card* Nouvelle Génération
  - http://arstechnica.com/tech-policy/2015/10/how-a-criminal-ring-defeated-the-secure-chip-and-pin-credit-cards/
  - http://eprint.iacr.org/2015/963.pdf
- Rétro attaque de distributeurs de billets
  - http://www.forbes.com/sites/thomasbrewster/2015/11/23/visa-mastercard-atm-fraud-hackers-steal-millions-dollars/
- Le délit d'initié 2.0
  - http://www.lefigaro.fr/societes/2015/08/11/20005-20150811ARTFIG00340-etats-unis-une-trentaine-de-traders-impliques-dans-une-affaire-de-delit-d-inities.php
  - http://fr.reuters.com/article/technologyNews/idFRKCN0QG25X20150811
  - https://www.washingtonpost.com/news/the-switch/wp/2015/08/11/hackers-who-breached-corporate-wires-made-millions-off-insider-trading/
- XCode Ghost: tout est plus simple quand on contrôle la source
  - http://tempsreel.nouvelobs.com/tech/20150921.OBS6188/des-hackers-dupent-apple-et-infectent-des-millions-d-iphone.html
  - http://researchcenter.paloaltonetworks.com/2015/09/novel-malware-xcodeghost-modifies-xcode-infects-apple-ios-apps-and-hits-app-store/
- Le Malware Turla envoie le cybercrime dans l'espace
  - http://www.reuters.com/article/2014/03/07/us-russia-cyberespionage-insight-idUSBREA260YI20140307
  - https://www.blackhat.com/presentations/bh-dc-10/Nve_Leonardo/BlackHat-DC-2010-Nve-Playing-with-SAT-1.2-wp.pdf

Attaques astucieuses:
Comment les cybercriminels nous ont-ils surpris en 2015 ?

Sources 2/2

- Dridex, le malware qui ne voulait pas mourir
  - http://www.nationalcrimeagency.gov.uk/news/723-uk-internet-users-potential-victims-of-serious-cyber-attack
  - http://blog.xmco.fr/index.php?post/2015/11/02/Le-malware-Dridex-n-est-pas-mort
  - http://www.itespresso.fr/dridex-botnet-bancaire-coriace-vise-france-111869.html
- Fusils intelligents : tout dépend de qui l'a en main
  - http://news.discovery.com/tech/gear-and-gadgets/hackers-redirect-and-disable-sniper-rifle-remotely-150729.htm
- Déverrouiller les portes de garage est un jeu d'enfant
  - http://motherboard.vice.com/read/this-kids-toy-can-hack-garage-doors-in-seconds
  - http://fox59.com/2015/10/09/police-issue-warning-after-hackers-use-handheld-device-to-break-into-homes/
- La clé des contrôles de sécurité compromise
  - http://www.zdnet.fr/actualites/les-clefs-des-verrous-tsa-dans-la-nature-39824778.htm
  - https://github.com/Xyl2k/TSA-Travel-Sentry-master-keys/blob/master/LICENSE.md
- Porter des gants pour protéger les systèmes ?
  - http://www.nextinpact.com/news/91637-il-est-possible-reconstituer-empreinte-digitale-depuis-photos.htm

0-days : analyse des marchés noirs des outils d'attaques numériques

Loïs SAMAIN

Consultant Cybersécurité/Cyberdéfense - CEIS

 *@lsamain*

Sujet présenté par **Hervé SCHAUER**
Directeur Général / HSC by Deloitte

0-days: les chiffres clés

Somme record pour une faille 0-day en 2015 : 1,000,000 $

16% des annonces publiées sur les trois plus importantes plateformes de Blackmarket concernent les données et logiciels

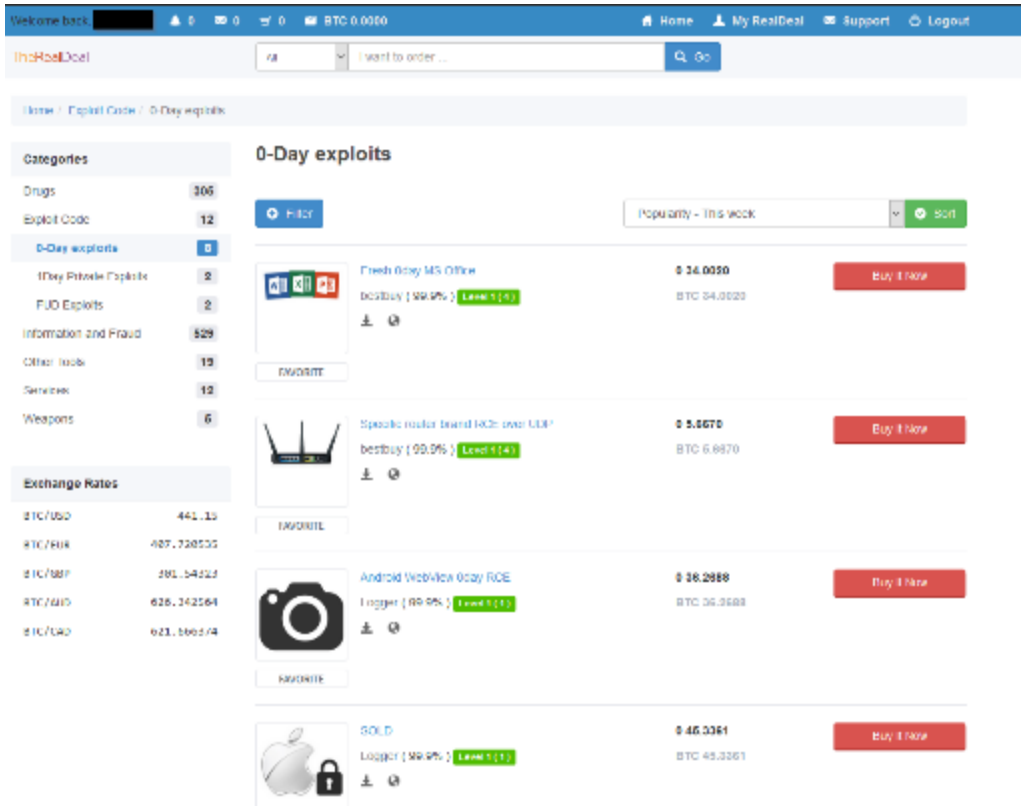
Les 0-day en 2015

Apparition d'un nouveau type de black-market:

Black-markets spécialisés dans le commerce de produits à très haute valeur ajoutée.

Exemple: **TheRealDeal**, marché spécialisé sur la vente de codes, 0-day et exploits

TheRealDeal



Les 0-day en 2015

Prix des vulnérabilités :

Plus le nombre de vulnérabilités est faible, plus le prix augmente…

Entre 500 et 40,000 $ en moyenne pour les failles 0-day

Exemple :

- OS Commerce : 2,000 $
- Microsoft Office: 15,000 $
- Piratage de compte iCloud: 17,000 $
- Record de l'année 2015 avec Zerodium et une faille i0S 9.1/9.2b à 1,000,000 $

Evolution de la législation aux Etats-Unis

- Evolution de l'arrangement de Wassenaar

En décembre 2013, le commerce de l'exploitation des vulnérabilités informatiques fait son entrée dans l'arrangement de Wassenaar, ainsi que différentes solutions de sécurité informatique.

- 5. A. 1. j. Systèmes IP de surveillance des communications du réseau ou de l'équipement, et composants spécialement conçus ;

- 4. A. 5. Systèmes, équipements et composants conséquents, spécialement conçus ou modifiés pour la production, l'exploitation, ou livraison de, ou la communication avec, « des logiciels d'intrusion » ;

- 4. D. 4. « Logiciel » spécialement conçu ou modifié pour la production, l'exploitation, ou la livraison de, ou la communication avec, des « logiciels d'intrusion » ;

- 4. E. 1. c. « Technologie » pour le « développement » des « logiciels d'intrusion »

Evolution de la législation aux Etats-Unis

- Evolution de l'arrangement de Wassenaar… et les Etats-Unis

Le 20 mai 2015: proposition d'une transposition dans la loi américaine de cette nouvelle version de l'arrangement de Wassenaar par le BIS (*Bureau of Industry and Security*)

Mais de nouvelles règles apparaissent au sein de cette transposition américaine, qui impactent la communauté de chercheurs en sécurité informatique.

Il est ajouté dans la liste des équipements contrôlés :

- *Les systèmes, équipements, composants et logiciels spécifiquement conçus pour la production, l'opération ou la fourniture, ou la communication avec des logiciels d'intrusion, dont les produits de test d'intrusion pour identifier les vulnérabilités des ordinateurs et des appareils capables de connexion réseau ;*
- ***Les technologies pour le développement de logiciels d'intrusion comprenant la recherche exclusive sur les vulnérabilités et l'exploitation des ordinateurs et des appareils capables de connexion réseau.***

Evolution de la législation aux Etats-Unis

- Evolution de l'arrangement de Wassenaar… et les Etats-Unis

Un fort levé de boucliers de la communauté :

- Google: https://googleonlinesecurity.blogspot.fr/2015/07/google-wassenaar-arrangement-and.html
- CISCO: http://blogs.cisco.com/gov/wassenaar
- Organisateurs de la Blackhat: https://www.blackhat.com/latestintel/07172015-wassenaar.html

Plus de 30 Etats membres aux Etats-Unis appliquent déjà cette règle actuellement.

En décembre 2015, une lettre signée par 125 membre de la Chambre des Représentants est adressée à la Maison Blanche en leur demandant d'entrer dans la discussion sur le sujet:
https://langevin.house.gov/sites/langevin.house.gov/files/documents/12-16-15_Langevin-McCaul_Wassenaar_Letter.pdf

Une nouvelle version de la transposition devrait être présenté au début de l'année 2016.

Evolution du marché des 0-day

- Bug bounty, un métier qui évolue

Des plateformes professionnelles de plus en plus reconnues

hackerone Fire Bounty bugcrowd™

Des primes qui explosent

Mozilla => la prime maximale est passée de 3,000 à 10,000 $

Microsoft => jusqu'à 15,000 $ de prime pour une faille sur son nouveau navigateur Edge (programme de 3 mois avant son lancement)

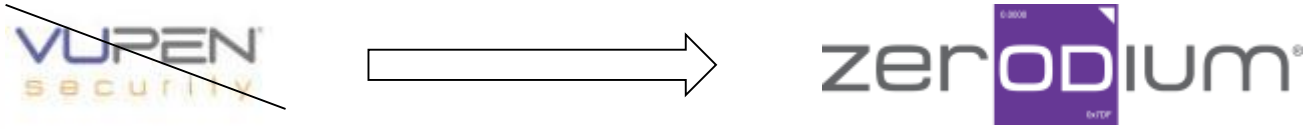
United Airlines => jusqu'à 1,000,000 de points Miles sur ses vols comme primes ☺

Et des sociétés de plus en plus hétérogènes

CLOUDFLARE. WU TESLA

Evolution du marché des 0-day

- Apparition d'un nouveau modèle : Zerodium (1/3)

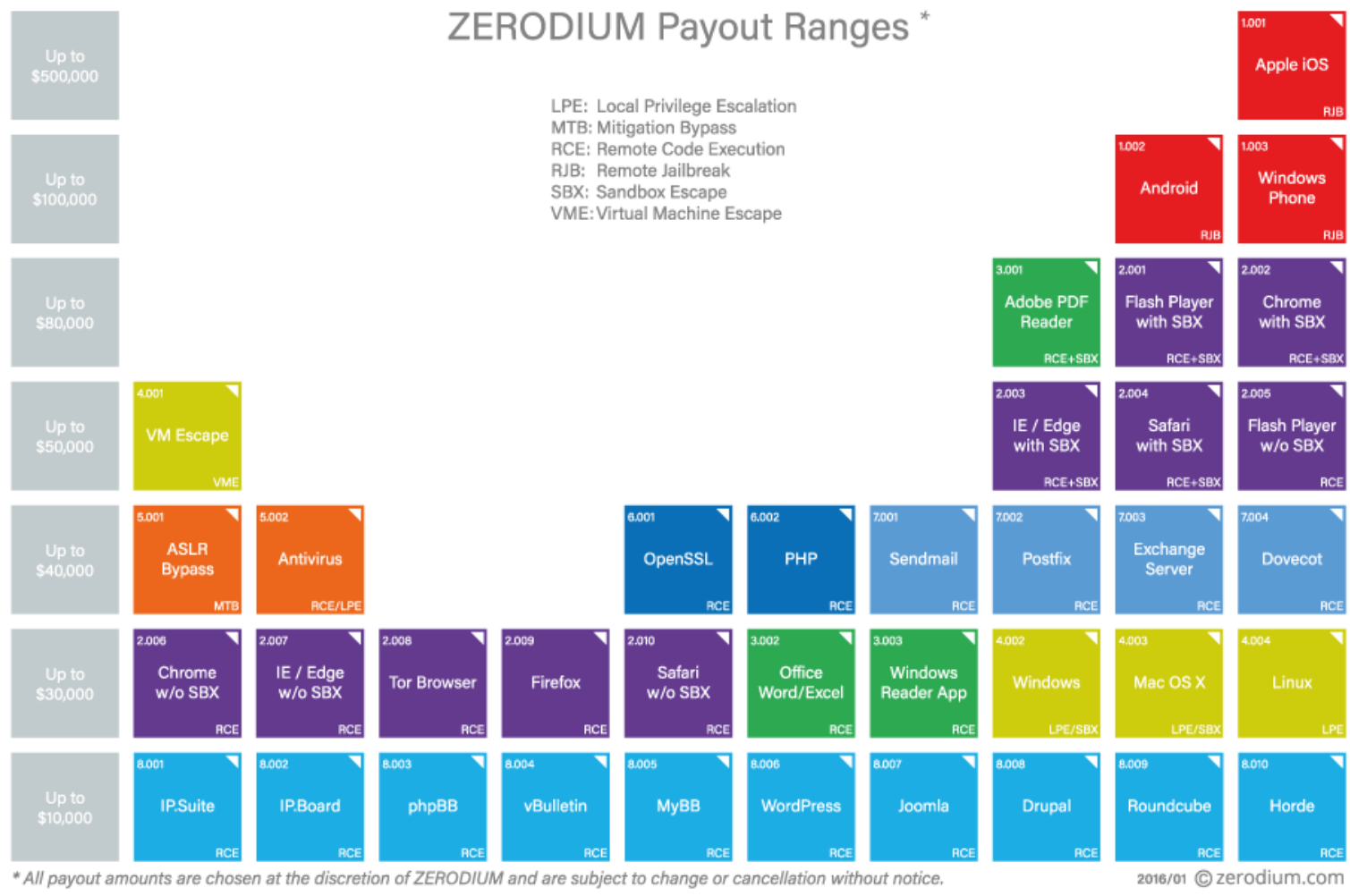


Zerodium: « *We created ZERODIUM to build a global community of talented and independent security researchers working together to provide the most up-to-date source of cybersecurity research and capabilities. To do so, ZERODIUM pays high rewards to researchers for their zero-day discoveries as we believe that this is the only effective way to capture high-end security research from all around the globe*. »

Les clients de Zerodium: « *ZERODIUM customers are major corporations in defense, technology, and finance, in need of advanced zero-day protection, as well as government organizations in need of specific and tailored cybersecurity capabilities.* »

Evolution du marché des 0-day

- Apparition d'un nouveau modèle : Zerodium (2/3)



Une tarification claire

Evolution du marché des 0-day

- Apparition d'un nouveau modèle : Zerodium (3/3)

Les annonces :

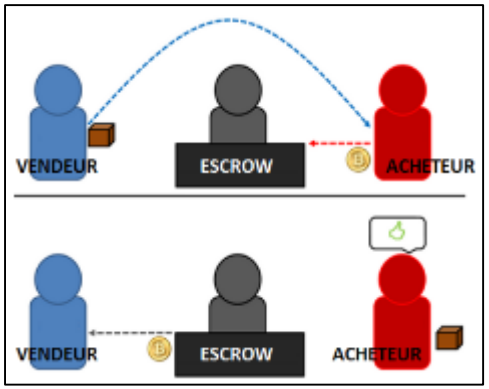
- En septembre 2015 : prime de 1,000,000 $ pour la découverte de nouvelles vulnérabilités dans iOS 9 permettant la compromission d'un appareil non encore jailbreaké.
  https://twitter.com/Zerodium/status/645955632374288384
- En Janvier 2016 : prime de 100,000 $ pour un exploit Flash devant contourner la sandbox de Flash Player et prendre à défaut une protection (heap isolation), récemment implémentée.
  https://twitter.com/Zerodium/status/684308378949033985

Evolution du marché des 0-day

- Un service de plus en plus professionnel

- Système d'escrow

Système de paiement faisant appel à une tierce personne neutre (rôle étant endossé majoritairement par les administrateurs) qui se rémunère en prélevant une commission sur les transactions.



Source: CEIS

- Transactions multi-signatures

Système imposant la signature de plusieurs clés privées pour réaliser la transaction. Par exemple, une équipe de 5 personnes pourra exiger la validation d'une transaction si au moins 3 personnes auront validé celle-ci.

Source: Bitgo.com

Cyber-diplomatie : Chine, États-Unis mais pas seulement …

Loïc GUEZO

CyberSecurity Strategist – Trend Micro Inc.

@lguezo

Emergence d'une cyber-diplomatie ?

- L'Internet via l'ICANN est au centre de (très) grandes manœuvres depuis … ?

2013, Protocole de Montevideo

Novembre 2015, 10th Internet Governance Forum (IGF)

Mi-décembre 2015, 193 membres des Nations Unies, de nombreuses ONG finalisent le plan de 2005 « UN World Summit on the Information Society (WSIS) » … et adoptent le document WSIS 10+

18 décembre 2015 à Wuzhen, en Chine se tient la 2nde « World Internet Conference » (WIC).

Source : http://www.circleid.com/posts/20151221_igf_wsis_10_wic_three_world_conferences_for_one_internet/

Emergence d'une cyber-diplomatie ?

- L'Internet via l'ICANN est au centre de (très) grandes manœuvres depuis … ?
- L'utilisation du cyber espace pour de nouvelles formes de confrontations étatiques (APT ?)

Une confrontation USA - Chine

- Points abordés lors des rencontres présidentielles

June 08, 2013

PRESIDENT OBAMA: Everybody ready? Well, I know we're a little behind, but that's mainly because President Xi and I had a very constructive conversation on a whole range of strategic issues, from North Korea to cyberspace to international institutions. And I'm very much looking forward to continuing the conversation, not only tonight at dinner but also tomorrow.

But I thought we'd take a quick break just to take a question from both the U.S. and Chinese press. So what I'll do is I'll start with Julie Pace and then President Xi can call on a Chinese counterpart.

Q Thank you, Mr. President. **How damaging has Chinese cyber-hacking been to the U.S.?** And did you warn your counterpart about any specific consequences if those actions continue? And also, while there are obviously differences between China's alleged actions and your government's surveillance programs, do you think that the new NSA revelations undermine your position on these issues at all during these talks?

And President Xi, did --

Source : https://www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china-

Une confrontation USA - Chine

- Points abordés lors des rencontres présidentielles

PRESIDENT OBAMA: Why don't you let the interpreter --

Q And President Xi, did you acknowledge in your talks with President Obama that China has been launching cyber attacks against the U.S.? Do you also believe that the U.S. is launching similar attacks against China? And if so, can you tell us what any of the targets may have been? Thank you.

PRESIDENT OBAMA: Well, Julie, first of all, we haven't had, yet, in-depth discussions about the cybersecurity issue. **We're speaking at the 40,000-foot level**, and we'll have more intensive discussions during this evening's dinner.

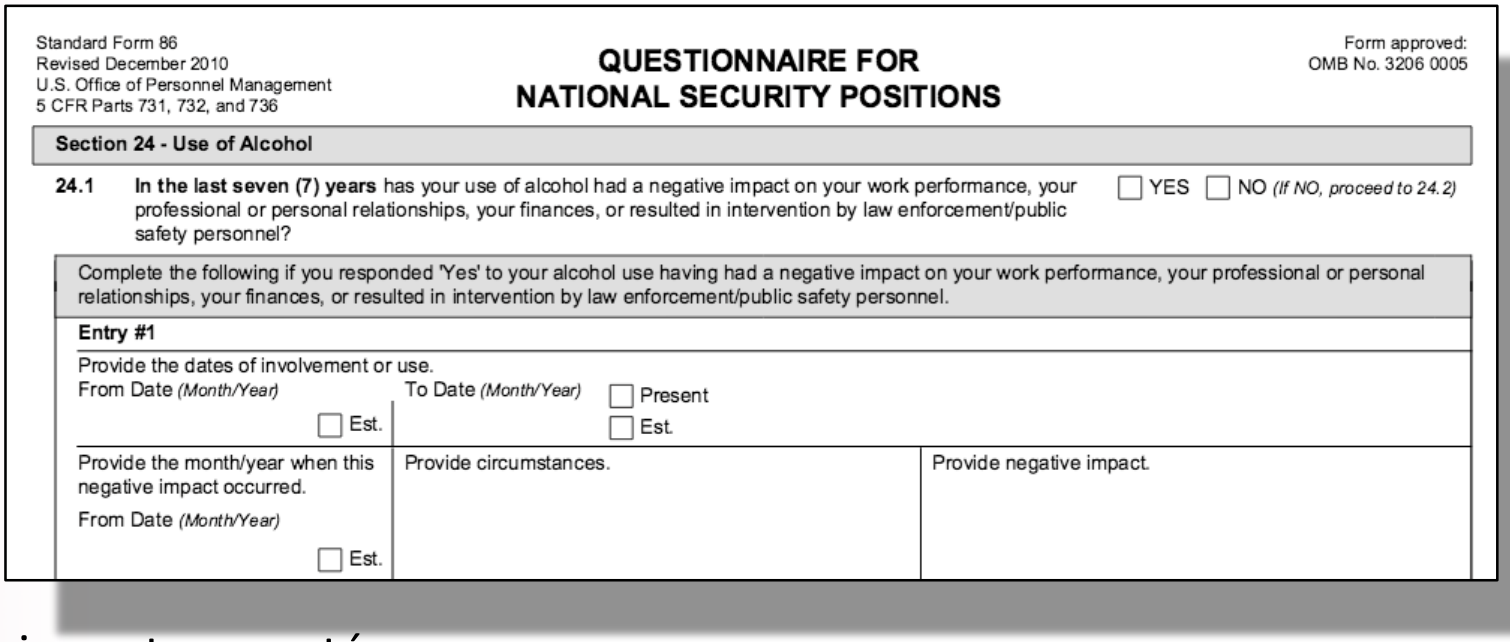
What both President Xi and I recognize is that because of these incredible advances in technology, that the issue of cybersecurity and the need for rules and common approaches to cybersecurity are going to be increasingly important as part of bilateral relationships and multilateral relationships (…)

PRESIDENT XI: (As interpreted.) As President Obama said, in our meeting this afternoon we just briefly touched upon the issue of cybersecurity. And the Chinese government is firm in upholding cybersecurity and we have major concerns about cybersecurity.

In the few days before President Obama and I meet today, **I note sharp increased media coverage of the issue of cybersecurity**. This might give people the sense or feeling that cybersecurity as a threat mainly comes from China or that the issue of cybersecurity is the biggest problem in the China-U.S. relationship.

OPM hack – juillet 2015

- Point fort : la nature des données volées *dont* empreintes digitales :
- OPM = U.S. Office of Personnel Management, donc données sensibles et complètes ! sur employés actuels, passés, consultants, externes …
- 19.7 (+1.8) millions de personnes concernée, 1.1 million d'empreintes



Standard Form 86
Revised December 2010
U.S. Office of Personnel Management
5 CFR Parts 731, 732, and 736

QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS

Form approved:
OMB No. 3206 0005

Section 24 - Use of Alcohol

24.1 **In the last seven (7) years** has your use of alcohol had a negative impact on your work performance, your professional or personal relationships, your finances, or resulted in intervention by law enforcement/public safety personnel? ☐ YES ☐ NO *(If NO, proceed to 24.2)*

Complete the following if you responded 'Yes' to your alcohol use having had a negative impact on your work performance, your professional or personal relationships, your finances, or resulted in intervention by law enforcement/public safety personnel.

Entry #1

Provide the dates of involvement or use.
From Date *(Month/Year)* ☐ Est. To Date *(Month/Year)* ☐ Present ☐ Est.

Provide the month/year when this negative impact occurred. From Date *(Month/Year)* ☐ Est.	Provide circumstances.	Provide negative impact.

- La Chine est suspectée…

Source : en fin de dossier

Arrestations en Chine

- Une première, qui tombe à pic, en septembre 2015

- Les arrestations ont lieu peu avant une visite d'état du Président Xi. Et apparaissent comme une volonté manifeste de diminuer les tensions avec Washington.
- Les arrestations « OPM » font partie d'un plus vaste programme de répression d'activités criminelles, avec des centaines d'arrestations.

Source : https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html

Une « Cyber Détente » ?

- Les présidents Xi et Obama trouvent un accord

« Xi and President Obama agreed that neither China nor the U.S. would engage in cyber espionage against the other for economic gain.

This week, more official meetings on cybercrime are taking place in Washington between Chinese and American officials, including China's Public Security Minister Guo Shengkun and U.S. Secretary of Homeland Security Jeh Johnson. »

Depuis septembre 2015 …

- Fermeté, des 2 côtés.

- « It has to stop. The question now is, are words followed by actions? »
- « Confrontation and friction are not the right choice for both sides, » he said. China has routinely insisted that it too is a victim of cyber hacking. »

Source : http://www.reuters.com/article/us-usa-china-idUSKCN0RO2HQ20150926

…, puis fin novembre 2015

- En marge, dans l'ombre de la COP21 …

The White House
Office of the Press Secretary

For Immediate Release — November 30, 2015

Remarks by President Obama and President Xi of China Before Bilateral Meeting

Le Bourget
Paris, France

9:48 A.M. CET

« Of course, as President Xi indicated, there are differences between our countries. That's natural. But on issues like cybersecurity and maritime issues, I think President Xi and I have developed a candid way of discussing these issues. And our teams have found ways to work through these tensions in a constructive fashion. And we hope to build on that today. »

Source : https://www.whitehouse.gov/the-press-office/2015/11/30/remarks-president-obama-and-president-xi-china-bilateral-meeting

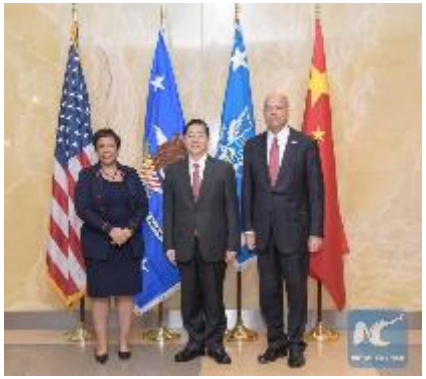
Ouverture économique, mais sur OPM précisément ?

- Le doute persiste sur la nature des personnes arrêtées, voire leur existence …

- A l'issue du séminaire ministériel du 1er décembre 2015, un accord est annoncé sur un alignement de la lutte contre la cyber criminalité.

- Le cas OPM aurait bien été abordé, mais sous un axe« criminel », non étatique…
- Aucune mention d'OPM dans le compte-rendu américain
- Rendez-vous pris pour Juin 2016, à Pékin

THE UNITED STATES DEPARTMENT of JUSTICE



- Rencontres, communications, prises de position … Diplomatie ?

Un refrain connu ?

- Le 31 décembre 2015, une attaque de 2009 envers Microsoft

- Ciblage de mails de leaders tibétains et minorité ouighoure. Mais aussi diplomates africains, japonais, avocats défenseurs des Droits de l'Homme, …
- Microsoft n'a pas alerté ses clients victimes.
- Provenance de l'AS4808, déjà associé depuis 2011 à l'attaque d' EMC Corp's, division sécurité de RSA que les Services US avaient publiquement attribués à la Chine

- Google, Yahoo, Facebook et désormais Twitter ont une politique de communication en cas de suspicion d'une attaque étatique…

Source : http://www.reuters.com/article/us-microsoft-china-insight-idUSKBN0UE01Z20151231

Et la Russie ?

- Un pacte sino-russe de non agression, signé 4 mois avant les rencontres avec les USA
- Ne signifie pas pour autant l'arrêt des opérations entre eux
- Volonté russe de suivre la Chine dans son activité de Gouvernance de l'Internet ? Surement car entre Ouverture et Souveraineté, Russie et Chine sont largement alignés sur l'idée de Souveraineté.

- De l' actualité en Ukraine (et en Crimée comme vers l'Ouest), principalement autour des systèmes ICS/SCADA, Energie …

Qui d'autre ?

- <u>L'Iran (et dans une moindre mesure la Corée) sont vus comme des risques cyber majeurs.</u>
  - L'effet « Syrie » : malgré une normalisation croissante avec l'Iran, les US ont une longue histoire conflictuelle et continuent l'affrontement sur de nombreux fronts (Moyen-orient, Syrie, Irak, Israël, Yemen…)
  - L'effet « Stuxnet » : l'Iran reste largement dépendant de ses alliés (et adversaires) quant aux technologies qu'il peutsereinement utiliser.
  - L'effet « Sony Pictures » : les Etats-Unis ont largement commenté leur faiblesse (auditions du Congrès notammen et forte reprise médiatique)

- La Corée et l'Iran ont bien entendu le message …

Et en Europe ?

- L'accord "Umbrella" (septembre 2015) : grande avancée, en permettant notamment de limiter le terrain de jeu des cybercriminels ; en assurant une meilleure collaboration entre LEA et meilleures garanties pour la protection des données.

- En France, en octobre 2015, est dévoilée la Nouvelle Stratégie Nationale pour la Sécurité du Numérique, par Manuel VALLS.

"Depuis plusieurs années, plusieurs Etats ont mis en oeuvre leur volonté politique et des moyens humains, techniques et financiers considérables afin de mener, à notre encontre, des opérations informatiques à grande échelle dans le cyberespace"

En France

David Martinon,

Ambassadeur pour la cyberdiplomatie et l'économie numérique

Ambassador for Cyberdiplomacy and the Digital Economy

Intronisation lors de la présentation de la Nouvelle Stratégie Nationale pour la Sécurité du Numérique

Quelques déclarations, actions : il était représentant spécial de la France pour les négociations internationales sur la société de l'information et l'économie numérique (WSIS)

La cyberdiplomatie est désormais un élément-clé de la vie politique, dont l'influence géopolitique* ; les gouvernements intègrent la dépendance croissante des économies au numérique.

Cyber-diplomatie : Chine, États-Unis mais pas seulement …

- OPM hack
  https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/
  http://www.theguardian.com/technology/2015/jul/09/opm-hack-21-million-personal-information-stolen
  https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html

- Identités des personnes arrêtées
  http://news.xinhuanet.com/english/2015-12/02/c_134875362.htm
  http://jeffreycarr.blogspot.fr/2015/12/who-has-chinese-government-arrested-for.html
  http://www.justice.gov/opa/pr/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary-outcomes-0

- Synthèse complète
  http://thediplomat.com/2015/12/has-u-s-cyber-pressure-worked-on-china/

- Russie
  http://www.darkreading.com/vulnerabilities---threats/advanced-threats/what-does-china-russia-no-hack-pact-mean-for-us-/d/d-id/1320365
  https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered

Cyber-diplomatie : Chine, États-Unis mais pas seulement …

- Qui d'autre ?
  http://uk.businessinsider.com/iran-is-emerging-as-one-of-the-most-dangerous-cyber-threats-to-the-us-2015-12
  http://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559
  https://ics.sans.org/blog/2015/12/21/takeaways-from-reports-on-iranian-activity-against-the-power-grid-and-a-dam#
  http://edition.cnn.com/2015/12/21/politics/iranian-hackers-new-york-dam/
  http://www.nbcnews.com/news/us-news/iranian-hackers-claim-cyber-attack-new-york-dam-n484611
  http://thehill.com/policy/cybersecurity/263135-fiorina-i-would-retaliate-for-chinese-russian-hacks

- Europe
  https://securityintelligence.com/news/out-in-the-rain-malware-makers-extradited-in-us-eu-umbrella-agreement/
  http://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/
  http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf
  https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf

- En France
  http://www.cnnumerique.fr/intervention-de-david-martinon-a-lonu-concernant-le-sommet-mondial-sur-la-societe-de-linformation-revue-a-10-ans/

Djihad 2.0

François PAGET

Secrétaire Général Adjoint du CLUSIF et animateur du groupe « Panaorama »

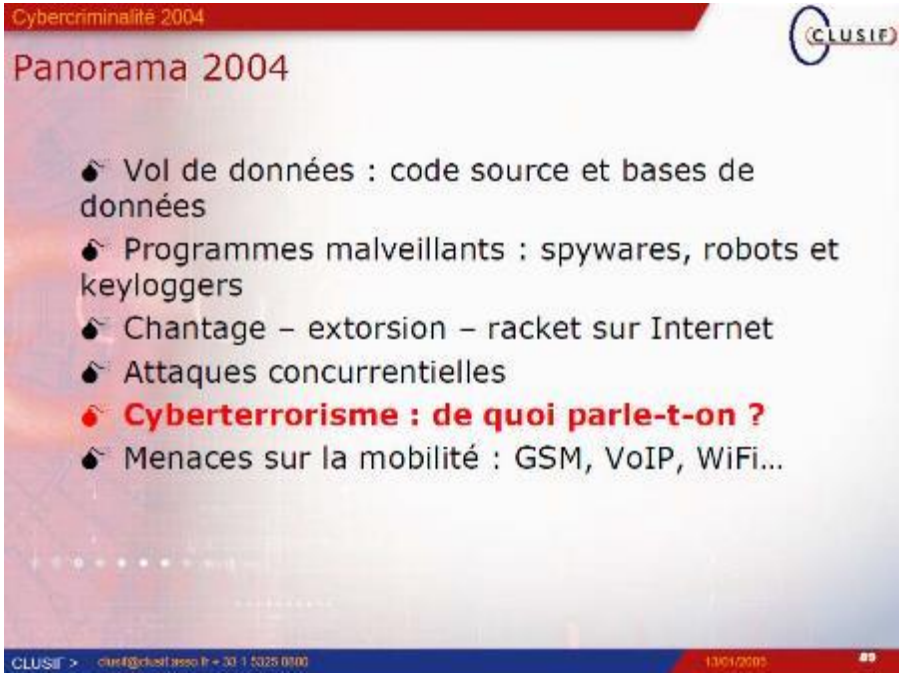
Une terrible année vient de s'achever

Janvier 2015

Novembre 2015

Internet est depuis longtemps utilisé par les terroristes

Le CLUSIF le disait déjà en 2004…



- ☑ Moyen de liaison,
- ☑ Moyen de propagande (web et forums),
- ☑ Moyen de financement,
- ☐ Moyen d'action directe,
- ☑ Renseignement d'opération (et présélection de cibles).

Source : https://www.clusif.asso.fr/fr/production/ouvrages/pdf/PanoCrim2k4-fr.pdf

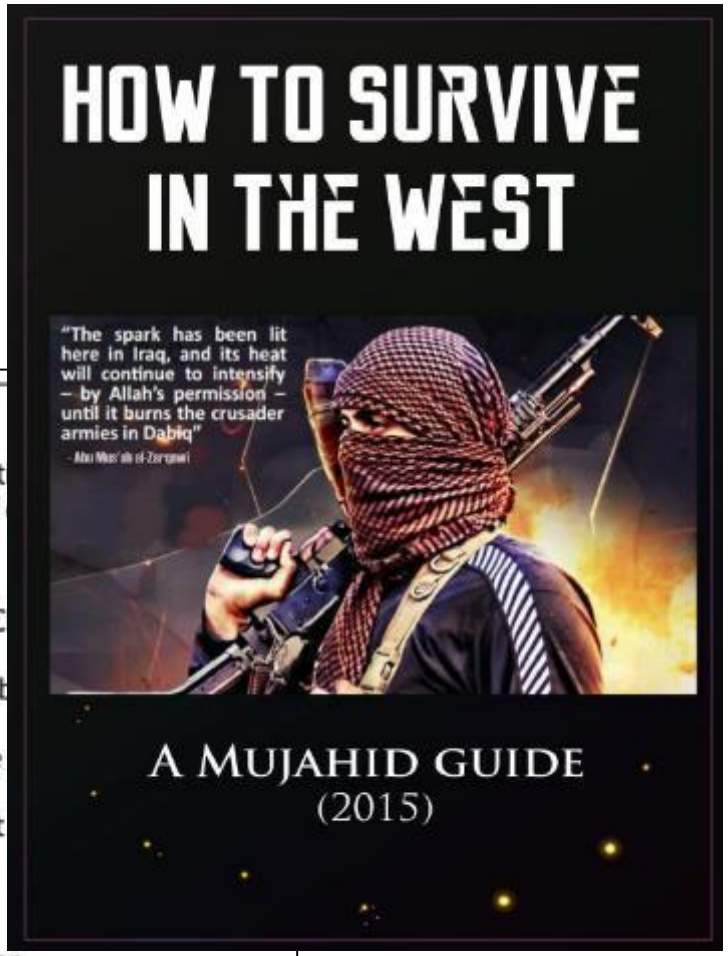
Réseaux sociaux et terrorisme

Hier : les forums,

Encore actuellement, et depuis plusieurs années : Facebook et Twitter,

Les conseils de l'état islamique en matière de communication

« Ayez à la maison une adresse IP irréprochable, utilisez TOR, méfiez vous des téléphones, et chiffrez vos conversations. »



Under the Radar

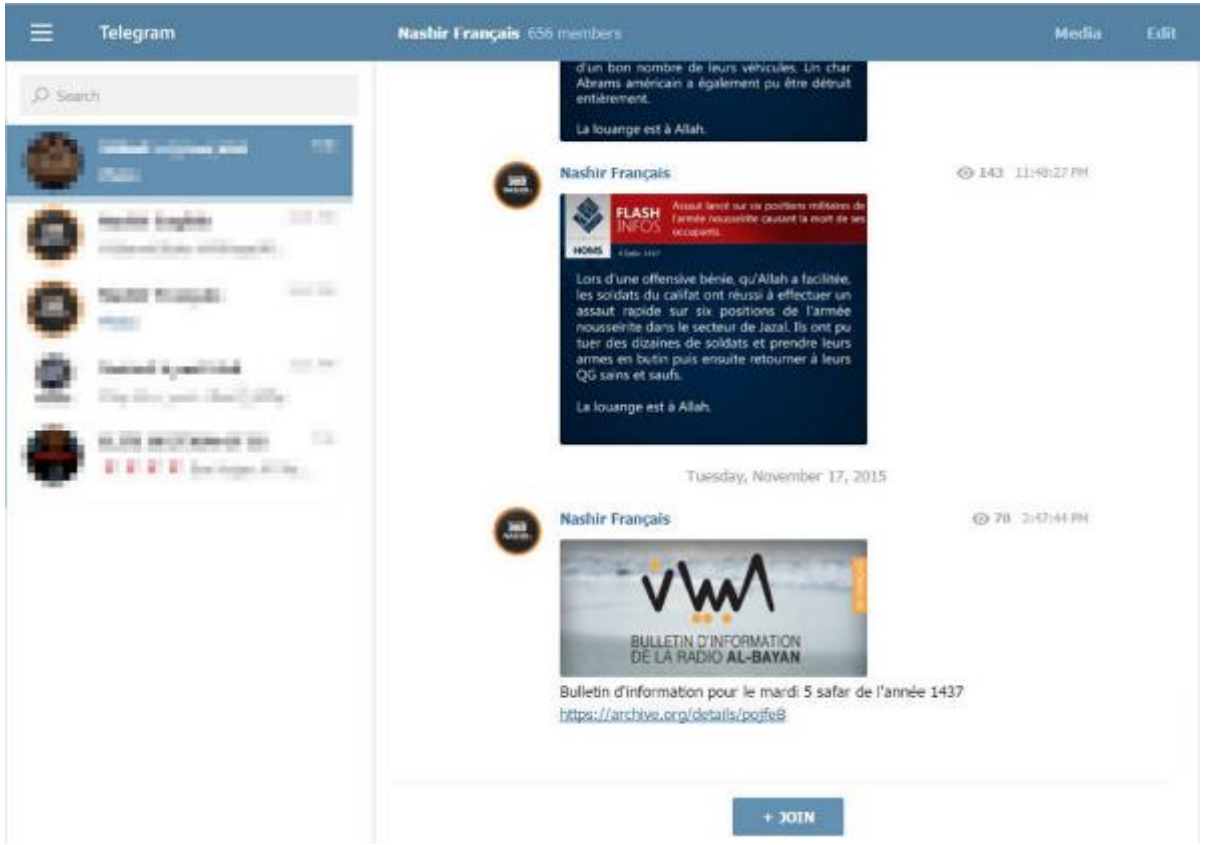
Islamic State issues regular tech tutorials intended to keep followers' communicat
government surveillance. This guide, circulated in January, ranks the encryption of

'Safest'	'Safe'	'Moderately safe'	'Unsafe'	
SilentCircle	Telegram	CoverMe	Viber	WeC
Redphone	Wickr	BBM	WhatsApp	Nimb
OSTel	Threema	iMessage	LINE	Hike
ChatSecure	Surespot	FaceTime	Tango	Chat
Signal (formerly Textsecure)		Hangouts	ooVoo	Kik
		Facebook Messenger	Kakao Talk	Voxer

Source SITE Intelligence Group & le Wall Street Journal

Réseaux sociaux et terrorisme

Hier : les forums,
Actuellement, et depuis plusieurs années : Facebook et Twitter,
Egalement aujourd'hui : Telegram.



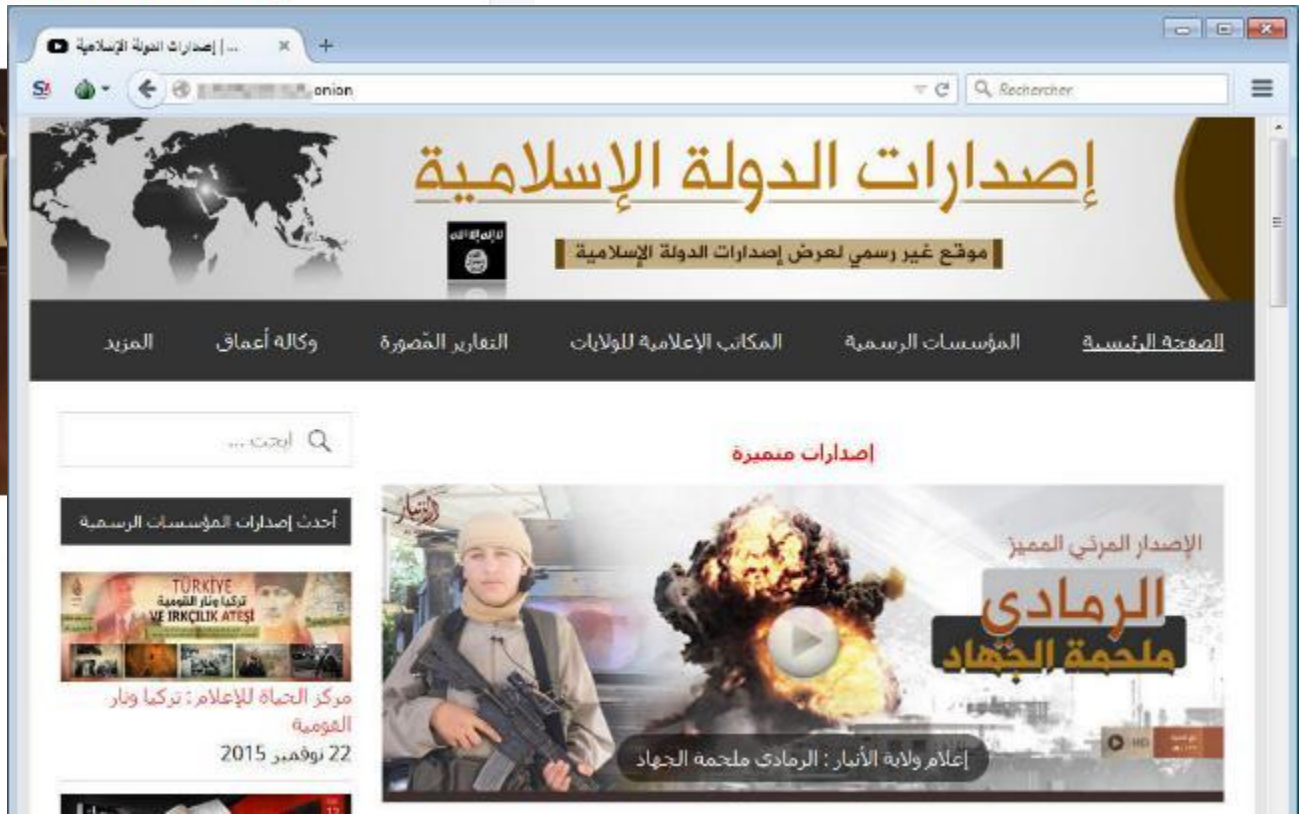
Réseaux sociaux et terrorisme

Baptisée *« application favorite des djihadistes»* par la presse américaine, Telegram tente à remplacer Twitter dans la boite à outil terroriste :

- Réseau social dominant en Russie, créé en 2013,
- Messages réguliers chiffrées,
- Permet l'échange de tous types de fichiers (photos, vidéos, documents et exécutables),
- Discussions (chats) secrètes avec chiffrement de bout en bout,
- Autodestruction des messages dans les conversations secrètes.

Le Darknet à l'heure du terrorisme

Quelques heures après les attentats de Paris, Al-Hayât arrive sur le Darknet



Réseaux sociaux : le côté pervers des suggestions…

Vous connaissez peut-être…

Cependant, Internet n'est jamais l'unique vecteur dans les trajectoires de radicalisation.

Source : http://apps.rue89.com/2014-dr/index.html

Le réveil d'Anonymous

#OpParis,
#OpISIS…

… un travail collectif, des approximations et des bévues…

GhostSec et Ghost Security Group

What is GhostSec's relationship to Anonymous? My understanding is that it's similar to LulzSec or AntiSec, a subgroup that uses Anon principles but broke away to get more things accomplished more quickly than a messy, chaotic hive mind can manage.

Digita Shadow, Ghost Security Group: We fight the same cause however Ghost Security Group and CtrlSec are not directly affiliated with Anonymous. We have chosen to step away from the Anonymous brand because our work is depending on collaborating with government officials so that our data may be acted on. Our official press release in regards to that can be viewed at http://ghostsecuritygroup.com.

Ransacker of GhostSec.org : GhostSec is a subgroup of Anonymous so we are part of the Anon family.

Source : http://thecryptosphere.com/2015/11/16/putting-isis-on-ice-an-interview-with-ghostsecpi-and-ghost-security-group/

GSG annonce coopérer avec les autorités américaines.
Celles-ci ne démentent pas formellement l'information.

Défacements

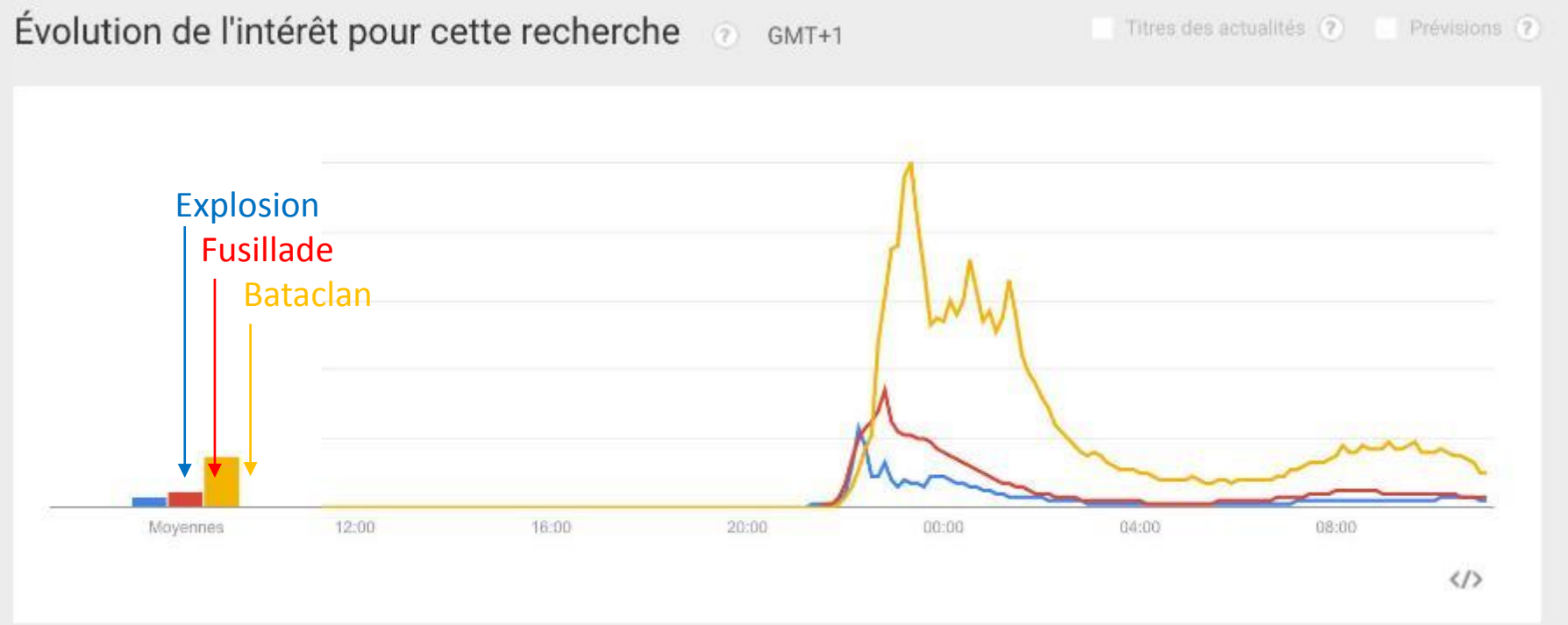
Après les défacements pro-ISIS de janvier, voici les défacements anti-ISIS de novembre

Janvier 2015

Novembre 2015

Google, sollicité et au cœur de l'évènement

Les recherches suivent le déroulement chronologique des informations.



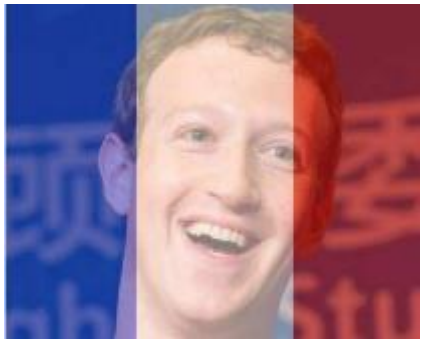
Source : Google Trends et http://www.slate.fr/story/109925/reseaux-sociaux-attentats-paris

L'aide précieuse de Twitter

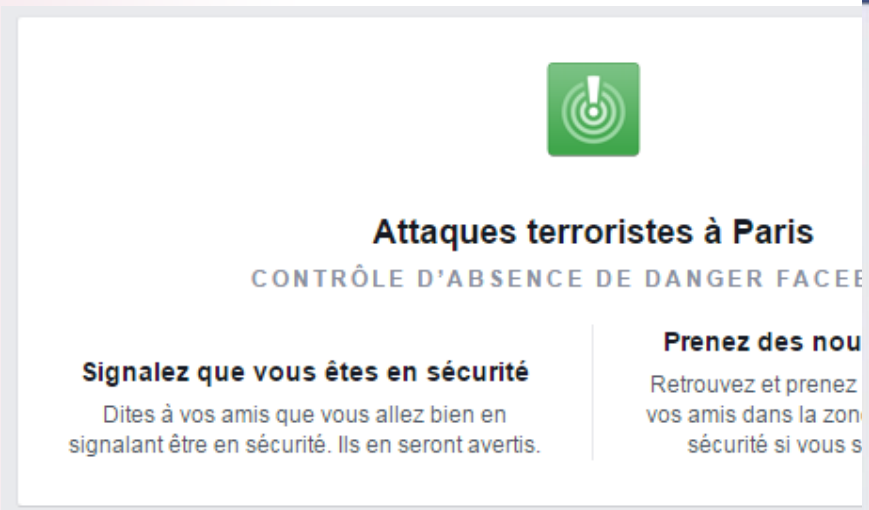
#Porte Ouverte #MonPlusBeauSouvenirDuBataclan, etc.

L'engagement de Facebook

Filtre bleu-blanc-rouge, bouton « Safety check »,



Délai de réaction face à des posts à éliminer.



Y a-t-il dans tout cela une arrière pensée mercantile ?

Réseaux sociaux : entre fausses alertes et aide précieuse

Source : http://www.itele.fr/france/video/info-intox-demeler-le-vrai-du-faux-sur-les-attentats-de-paris-143626

Rumeurs et réalités…

Forbes / Tech

The Little Bla

SEP 26, 2014 @ 11:07 AM 119,758 VIEWS

ISIS Uses 'GTA 5' In New Teen Recruitment Video

Paul Tassi
CONTRIBUTOR
News and opinion about video games, technology and the internet

FOLLOW ON FORBES (1743)

FULL BIO >

Forbes / Tech

The Little Bla

NOV 14, 2015 @ 06:17 PM 658,940 VIEWS

How ISIS Terrorists May Have Used PlayStation 4 To Discuss And Plan Attacks [Updated]

Paul Tassi
CONTRIBUTOR
News and opinion about video games, technology and the internet

FOLLOW ON FORBES (1743)

FULL BIO >

Correction: *It has not been confirmed, as originally written, that a console was found as a result of specific Belgian terror raids. Minister Jambon was speaking about tactics he knows ISIS to be using generally.*

Source : http://www.forbes.com/sites/insertcoin/2015/11/14/why-the-paris-isis-terrorists-used-ps4-to-plan-attacks/

Rumeurs et réalités…

Source : http://www.metronews.fr/high-tech/info-et-intox-autour-du-virus-je-suis-charlie-qui-circule-sur-le-net/moao!RzlHjhcdfR0X/

Les forces de l'ordre, actives aussi sur les réseaux sociaux

Dihad 2.0 – Références

(en complément de celles déjà citées tout au long de cette intervention)

- Les réseaux sociaux, entre aide précieuse et grand n'importe quoi
  http://www.20minutes.fr/web/1731815-20151116-attentats-paris-reseaux-sociaux-entre-aide-precieuse-grand-importe-quoi
- Safety check
  http://www.lesechos.fr/tech-medias/hightech/021479513776-attentats-a-paris-pourquoi-facebook-a-declenche-safety-check-1175547.php
- Utilisation non avérée de la PS4
  http://www.numerama.com/politique/130839-non-rien-ne-dit-que-les-terroristes-de-paris-ont-utilise-des-ps4-pour-communiquer.html
- Le jeu Grand Theft Auto 5 a par contre été utilisé pour réaliser des vidéos de propagande
  http://www.dailymail.co.uk/news/article-2765414/Isis-use-video-game-Grand-Theft-Auto-5-recruit-children-radicalise-vulnerable.html
- Tentative d'endoctrinement via Clash of Clans
  http://www.larepublique77.fr/2015/11/17/apologie-du-terrorisme-tentative-dendoctrinement-via-un-jeu-video-en-reseau

SOUS-DIRECTION DE LUTTE CONTRE LA CYBERCRIMINALITÉ

DIVISION DE L'ANTICIPATION ET DE L'ANALYSE

Panorama de la cybercriminalité 2015

« DJIHAD 2.0 – ASPECTS OPÉRATIONNELS »

Jihad numérique : enjeux juridiques

Amélie PAGET

Consultante juridique SI – HSC by Deloitte

Multiplication des lois antiterroristes

12 lois depuis ces 15 dernières années

Versant administratif

- Renforcement des pouvoirs de police administrative
  - Lors de situations exceptionnelles : état d'urgence
  - En permanence

Versant judiciaire

- Procédure spéciale
- Multiplication des infractions
- Aggravation des peines

2 textes majeurs

Loi relative au renseignement

Loi prorogeant l'état d'urgence

Médiatisés et contestés

Surveillance de masse

Fiches S

Boîtes noires

État d'urgence

Notion

Régime d'exception

Applicable

- soit en cas de péril imminent résultant d'atteintes graves à l'ordre public
- soit en cas d'événement présentant, par leur nature et leur gravité, le caractère de calamité publique

Dans un périmètre donné

Pour une période donnée, prorogeable

6e application

- Décrété le 14 novembre 2015
- Prorogation législative à compter du 26 novembre 2015 pour 3 mois

Évolution de l'état d'urgence

Loi du 20 novembre 2015 prorogeant l'état d'urgence

→ Modification de la loi de 1955

Accès au système informatique au cours des perquisitions

- Accès à des données stockées sur un système informatique ou un équipement terminal, ou accessibles à partir du système initial
- Copie des données
- Saisie en cas de constat d'infraction

Contrôle d'Internet par le ministre de l'intérieur

- Interruption de tout service de communication au public en ligne provoquant à la commission d'actes de terrorisme ou en faisant l'apologie

État d'urgence

Projet de loi constitutionnelle de protection de la Nation

- Nouvel article 36-1 consacré à l'état d'urgence
- Modification de l'art. 34 pour permettre la déchéance des binationaux nés Français

Renseignement

Loi du 24 juillet 2015 relative au renseignement

→ Livre VIII : DU RENSEIGNEMENT

Art. L.801-1 et s. du Code de la sécurité intérieure

Télérama, 19/04/2015

La prévention du terrorisme justifie

- La mise en œuvre de moyens de recueil de renseignements
- Les mesures d'urgence absolue
- Le recours à des mesures renforcées en matière
  - D'accès aux données de connexion
  - D'interceptions de sécurité
  - D'information des agents

- A tout moment
- Sur autorisation préalable du Premier ministre après avis de la CNCTR
- Pour une durée maximale de 4 mois renouvelables

Renseignement

Accès administratif aux données de connexion

- Recueil auprès des opérateurs, FAI et hébergeurs
  - Des informations et données traitées ou conservées par leurs réseaux ou services
  - Des données techniques
- Recueil sur sollicitation du réseau et transmission en temps réel des données de localisation des équipements terminaux
- Utilisation d'un dispositif de géolocalisation en temps réel
- Utilisation d'un dispositif de recueil des données techniques
- <u>En matière de prévention de la lutte contre le terrorisme</u>
  - Recueil en temps réel des informations et documents sur les réseaux
  - Détection des connexions susceptibles de révéler une menace terroriste

Renseignement

Interceptions de sécurité

- Interception des correspondances électroniques
- En matière de prévention de la lutte contre le terrorisme

  Utilisation d'un matériel d'interception

Surveillance des communications internationales

Loi du 30 novembre 2015

- Interception des communications émises ou reçues à l'étranger

Renseignement

- Information des agents : ils peuvent
  - Échanger électroniquement avec toute personne susceptible de porter atteinte aux intérêts de la Nation
  - Extraire, acquérir ou conserver des données
  - En matière de prévention de la lutte contre le terrorisme : extraire, transmettre, acquérir et conserver des contenus provoquant à la commission d'actes de terrorisme ou en faisant l'apologie

- Déchiffrement
  - Les prestataires de cryptologie ont l'obligation de transmettre les convention de déchiffrement ou de procéder au déchiffrement dans les 72 heures

Renseignement

- La révélation de la mise en œuvre de technique de renseignement par une personne y concourant est punie d'un an d'emprisonnement et 15 000 euros d'amende

- Le refus de déférer aux demandes des agents est puni de 2 ans d'emprisonnement et de 150 000 euros d'amende

- Le refus de communiquer les informations ou documents, ou la communication de renseignements erronés sont punis de 2 ans d'emprisonnement et de 150 000 euros d'amende

Versant judiciaire

Depuis 2001, 10 textes consacrés à la lutte contre le terrorisme

Proposition de loi tendant à renforcer l'efficacité de la lutte antiterroriste

- Pouvoirs d'enquête
  - Saisie de données de messagerie électronique
  - Installation de dispositifs de captation de données informatiques et de dispositifs d'écoutes
- 2 infractions
  - Délit de consultation habituelle de sites terroristes
  - Délit d'entrave intentionnelle au blocage judiciaire ou administratif des contenus faisant l'apologie d'actes de terrorisme ou provoquant à ces actes

Sources

- Loi n° 2015-1501 du 20 novembre 2015 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et renforçant l'efficacité de ses dispositions
- Loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence
- Circulaire administrative pour la mise en œuvre du décret n° 2015-1475 du 14 novembre 2015
- Articles 16 et 36 de la Constitution
- Rapport au Président de la République du Comité constitutionnel, le 29 octobre 2007
- Discours du Président de la République devant le Congrès le 16 novembre 2015
- Projet de loi constitutionnelle de protection de la Nation n° 3381
- Loi n° 2015-912 du 24 juillet 2015 relative au renseignement
- Décision du Conseil constitutionnel n° 2015-713 DC du 23 juillet 2015
- Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales
- Décision du Conseil constitutionnel n° 2015-722 DC du 26 novembre 2015
- http://www2.assemblee-nationale.fr/static/14/lois/analyses_chiffrees_1.pdf
- http://www2.assemblee-nationale.fr/14/commissions-permanentes/commission-des-lois/controle-parlementaire-de-l-etat-d-urgence/controle-parlementaire-de-l-etat-d-urgence/donnees-de-synthese/mesures-administratives-prises-en-application-de-la-loi-n-55-385-du-3-avril-1955-depuis-le-14-novembre-2015-au-7-janvier-2016

Objets connectés

2015 l'année du piratage des voitures, et demain ?

Gérôme BILLOIS

Senior Manager – CERT-Solucom

@gbillois

Juillet 2015 : Une vidéo fait le tour du monde…

Comment cela est-il possible ?

Internet

Radio (GSM/Bluetooth/Wifi)

Climatisation

Portes

Sièges chauffants…

CAN-IHS

Console de bord

Processeur partie multimédia (OMAP)

Processeur échange réseaux CAN (v850)

CAN-C

Régulateur de vitesse (accélération, freinage…)

Volant

Boîte de vitesse

Assistant parking…

Étape 1 : prise de contrôle de la console de bord

Internet

Radio (GSM/Bluetooth/Wifi)

Climatisation

Portes

Sièges chauffants…

CAN-IHS

Console de bord

Processeur partie multimédia (OMAP)

Processeur échange réseaux CAN (v850)

CAN-C

Régulateur de vitesse (accélération, freinage…)

Volant

Boîte de vitesse

Assistant parking…

Après une analyse poussée et un jailbreak de la console de bord, découverte d'une faille permettant la prise de contrôle de la console, via le GSM également…

Étape 2 : prise de contrôle des fonctions de confort

Internet

Radio (GSM/Bluetooth/Wifi)

Climatisation

Portes

Sièges chauffants…

CAN-IHS

Console de bord

Processeur partie multimédia (OMAP)

Processeur échange réseaux CAN (v850)

CAN-C

Régulateur de vitesse (accélération, freinage…)

Volant

Boîte de vitesse

Assistant parking…

La prise de contrôle de la console de bord permet d'émettre « simplement » tous les ordres usuels vers les fonctions de confort et de désactiver les commodos

Étape 3 : rebond vers les fonctions de conduite

Internet

Radio (GSM/Bluetooth/Wifi)

Climatisation

Portes

Sièges chauffants…

CAN-IHS

Console de bord

Processeur
partie multimédia
(OMAP)

Processeur
échange réseaux
CAN (v850)

```
ROM:00067796    ld.w    [r6], r16
ROM:0006779A    add     r7, r16
ROM:0006779C    movea   0x100, r0, r10
ROM:000677A0    st.h    r10, 0xE[r16]   -- CnMCTRL - 0x100
ROM:000677A4    ld.w    [r6], r11
ROM:000677A8    add     r7, r11
ROM:000677AA    movea   0x200, r0, r12
ROM:000677AE    st.h    r12, 0xE[r11]
ROM:000677B2    mov     arg_can_module_index, r6
ROM:000677B4    mov     mod_id_plus_msg_buf_index, r7
ROM:000677B6    jarl    sub_718A4, lp
ROM:000677BA    mov     1, r20
ROM:000677BC    br      loc_677EA
```

CAN-C

Régulateur de vitesse
(accélération, freinage…)

Volant

Boîte de vitesse

Assistant parking…

La partie la plus complexe de l'attaque a consisté à tromper le processus de mise à jour afin d'installer un logiciel « maison » dans le contrôleur dédié aux réseaux CAN et d'envoyer des vrais/faux messages

Étape 4 : la voiture est intégralement compromise

Internet

Radio (GSM/Bluetooth/Wifi)

Climatisation

Portes

Sièges chauffants…

CAN-IHS

Console de bord

Processeur partie multimédia (OMAP)

Processeur échange réseaux CAN (v850)

CAN-C

Régulateur de vitesse (accélération, freinage…)

Volant

Boîte de vitesse

Assistant parking…

Il est maintenant possible de piloter la voiture à distance…

Mais tout cela a commencé bien avant 2015…
… et demande du temps et de l'expertise !

2010 / 2011 / 2012

-

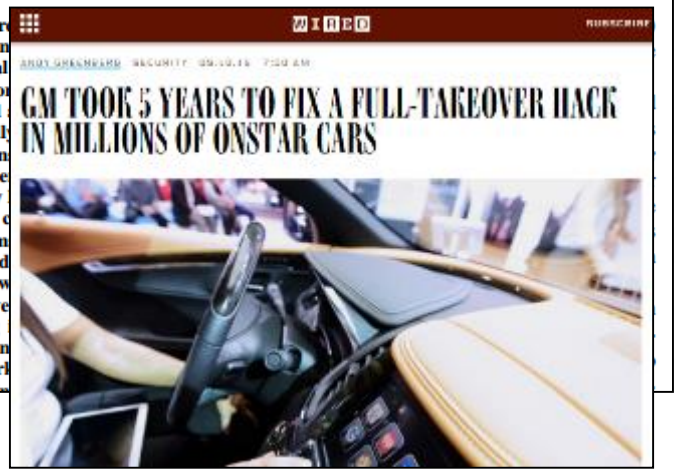
Les premières démonstrations par des équipes de recherche …non reprises publiquement

Experimental Security Analysis of a Modern Automobile

Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, and Tadayoshi Kohno
Department of Computer Science and Engineering
University of Washington
Seattle, Washington 98195–2350
Email: {supersat,aczeskis,franzi,shwetak,yoshi}@cs.washington.edu

Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage
Department of Computer Science and Engineering
University of California San Diego
La Jolla, California 92093–0404
Email: {s,dlmccoy,brian,d8anders,hovav,savage}@cs.ucsd.edu

***Abstract*—Modern automobiles are no longer mer**
ical devices; they are pervasively monitored and con
dozens of digital computers coordinated via internal
networks. While this transformation has driven majo
ments in efficiency and safety, it has also introduced
new potential risks. In this paper we experimentall
these issues on a modern automobile and demon
fragility of the underlying system structure. We de
that an attacker who is able to infiltrate virtually any
Control Unit (ECU) can leverage this ability to
circumvent a broad array of safety-critical system
range of experiments, both in the lab and in road
demonstrate the ability to adversarially control a w
of automotive functions and completely ignore drive
including disabling the brakes, selectively braking
wheels on demand, stopping the engine, and so on
that it is possible to bypass rudimentary networ



Mais tout cela a commencé bien avant 2015…
… et demande du temps et de l'expertise !

2010 / 2011 / 2012

-

Les premières démonstrations par des équipes de recherche …non reprises publiquement

2013 / 2014

-

Démonstration d'attaques avec accès physique (Toyota & Ford) et recherches additionnelles de Miller & Valasek

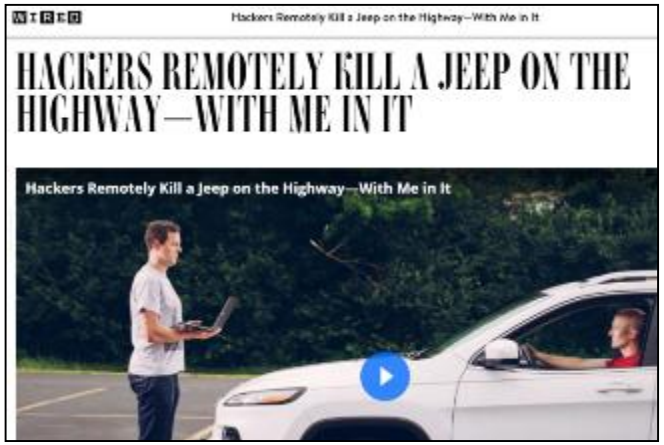
Véhicule	Surface d'attaque	Architecture réseau	Eléments pilotables informatiquement
2014 Jeep Cherokee	++	++	++
2015 Cadillac Escalade	++	+	+
2014 Ford Fusion	++	-	++
2014 Dodge Ram 3500	++	++	--
2014 BMW X3	++	--	++
2014 Chrysler 300	++	-	++
2014 Range Rover Evoque	++	-	++
2014 Toyota Prius	+	+	++
2010 Toyota Prius	+	+	++
2014 Infiniti Q50	++	+	+
2014 Audi A8	++	--	+

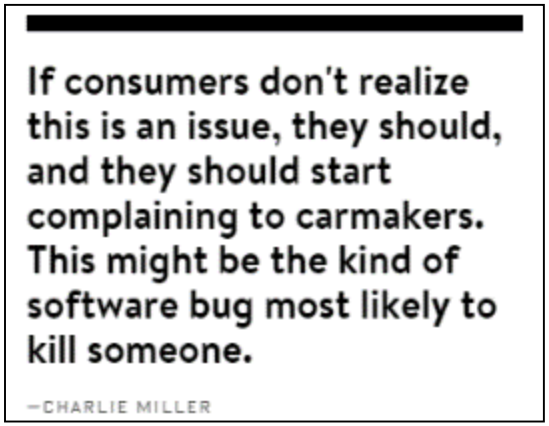
Mais tout cela a commencé bien avant 2015…
… et demande du temps et de l'expertise !

2010 / 2011 / 2012
-
Les premières démonstrations par des équipes de recherche
…non reprises publiquement

2013 / 2014
-
Démonstration d'attaques avec accès physique (Toyota & Ford) et recherches additionnelles de Miller & Valasek

2014 / 2015
-
Ciblage et réalisation d'attaques à distance sur une Cheep Cherokee par Miller & Valasek





Des impacts concrets… et d'ampleur !

Image : à l'échelle internationale

Financier : rappel de 1,4 million de véhicules « via des clés USB »…

Une multiplication des annonces…
… plus ou moins fantaisistes et anxiogènes

N'oublions pas qu'il sera toujours plus facile de couper les freins d'une voiture en coupant physiquement l'arrivée du liquide de frein…

Pas encore de cas d'attaques malveillantes avérées…

…même si cela reste possible

Teslacrypt portera peut-être un jour vraiment son nom…


Partager
Contact
Recherche
French
EURO NCAP
Euro NCAP · Notations et récompenses · Sécurité des véhicules · Média · Pour ingénieurs
Protection des adultes
82%
Protection des enfants
77%
Protection des piétons
66%
Protection cyber
71%
Total 9.3 Pts (points) / 71%
BON
SATISFAISANT
MOYEN
FAIBLE
MÉDIOCRE
Capacité de mise à jour transparente et de confiance
2.3 Pts
Résistance au déni de service
3 Pts
Isolation des fonctions « conduite » et « loisir »
3 Pts
Des critères « cyber » à intégrer aux évaluations de sécurité ? Pourquoi pas !

Au-delà des voitures, de plus en plus d'objets connectés…
…et de plus en plus de failles en 2015 !

Les jouets connectés : Barbie et Vtech (et bientôt BB8 ?)

Le domicile connecté : télévision, babymonitor et réfrigérateur

Au-delà des voitures, de plus en plus d'objets connectés…
…et de plus en plus de failles en 2015 !

Les équipements médicaux :
pompes à insuline

Les armes : fusils de sniper

Et les avions ? Une polémique toujours en cours…

Sommes-nous tous concernés ? Oui !

Distinguer les 4 dimensions de la sécurité des objets connectés

Mars 2015 – Méthodologie Propriété de Solucom

La nécessité de réagir… sans reproduire les erreurs du passé

Intégrer la sécurité à la conception… **Évidemment !**

Protéger notre vie privée… **Absolument !**

Mais sans oublier de prendre en compte les spécificités des objets connectés !

Aujourd’hui les objets connectés…

Demain, les objets « autonomes » !

Des usages qui se rapprochent de nous…
et qui augmentent encore les enjeux de sécurité !

Et qui posent aussi de complexes questions juridiques !

Sécurité des objets connectés

- Video
http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
- Pacemaker
http://motherboard.vice.com/read/hackers-killed-a-simulated-human-by-turning-off-its-pacemaker
- Pompe à insuline
http://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/
- Hello Barbie
https://bluebox.com/hello-barbie-app-hello-security-issues/
- Baby Monitor
http://fusion.net/story/192189/internet-connected-baby-monitors-trivial-to-hack/
- TV Ransomware
http://www.symantec.com/connect/blogs/how-my-tv-got-infected-ransomware-and-what-you-can-learn-it
- Sniper
http://www.wired.com/2015/07/hackers-can-disable-sniper-rifleor-change-target/
- Réfrigérateur
http://www.theregister.co.uk/2015/08/24/smart_fridge_security_fubar/
- PDG Volvo
http://fortune.com/2015/10/07/volvo-liability-self-driving-cars/
http://www.automobilemag.com/features/news/volvo-will-accept-full-liability-for-its-autonomous-vehicles/
- Sphero BB-8
http://www.tomsguide.fr/actualite/sphero-bb8-faille,49809.html

Sécurité des objets connectés

- Rappel Chrysler

http://www.reuters.com/article/us-fiat-chrysler-recall-idUSKCN0PY1U920150724
http://www.safercar.gov/rs/chrysler/pdfs/FCA_Consent_Order.pdf
http://www.theguardian.com/technology/2015/aug/18/security-flaw-100-car-models-exposed-scientists-volkswagen-suppressed-paper?CMP=Share_AndroidApp_Gmail&utm_content=buffer2055a&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

http://www.wired.com/2015/08/bmw-benz-also-vulnerable-gm-onstar-hack?utm_content=bufferaa30d&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer
http://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/
http://www.securityinsider-solucom.fr/2015/03/cara-les-4-dimensions-de-la-securite.html
http://pro.clubic.com/it-business/securite-et-donnees/actualite-790182-piratage-vtech-lufc-attaque.html
http://jalopnik.com/mercedes-google-volvo-to-accept-liability-when-their-1735170893

- Historique des voitures connectées

http://techcrunch.com/2015/10/23/connected-car-security-separating-fear-from-fact/
http://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars/
http://www.autosec.org/pubs/cars-usenixsec2011.pdf
http://www.theguardian.com/technology/2013/jul/26/scientist-banned-revealing-codes-cars

Objets connectés

Quels enjeux juridiques ?

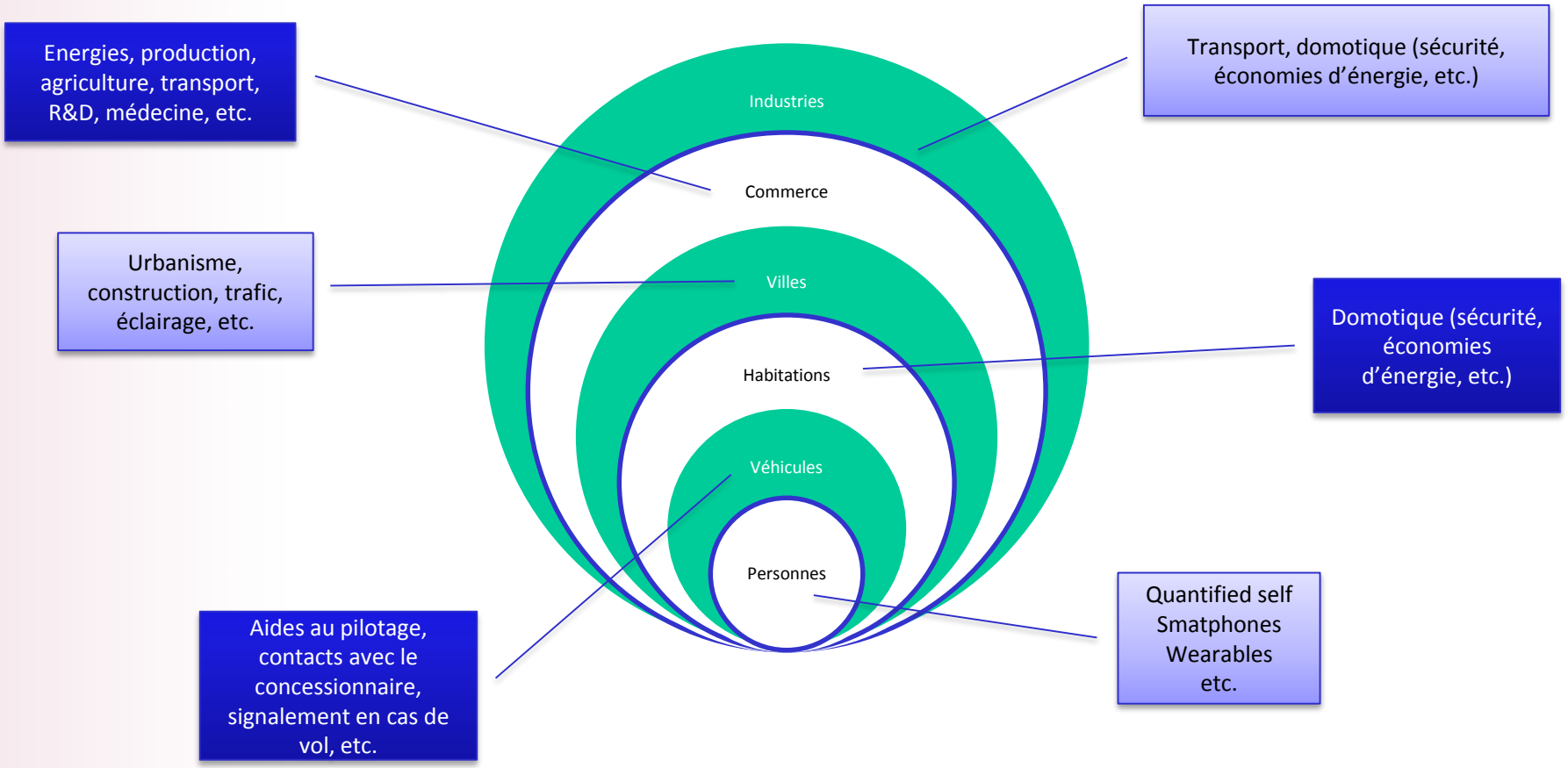
Garance Mathias

Avocat à la Cour

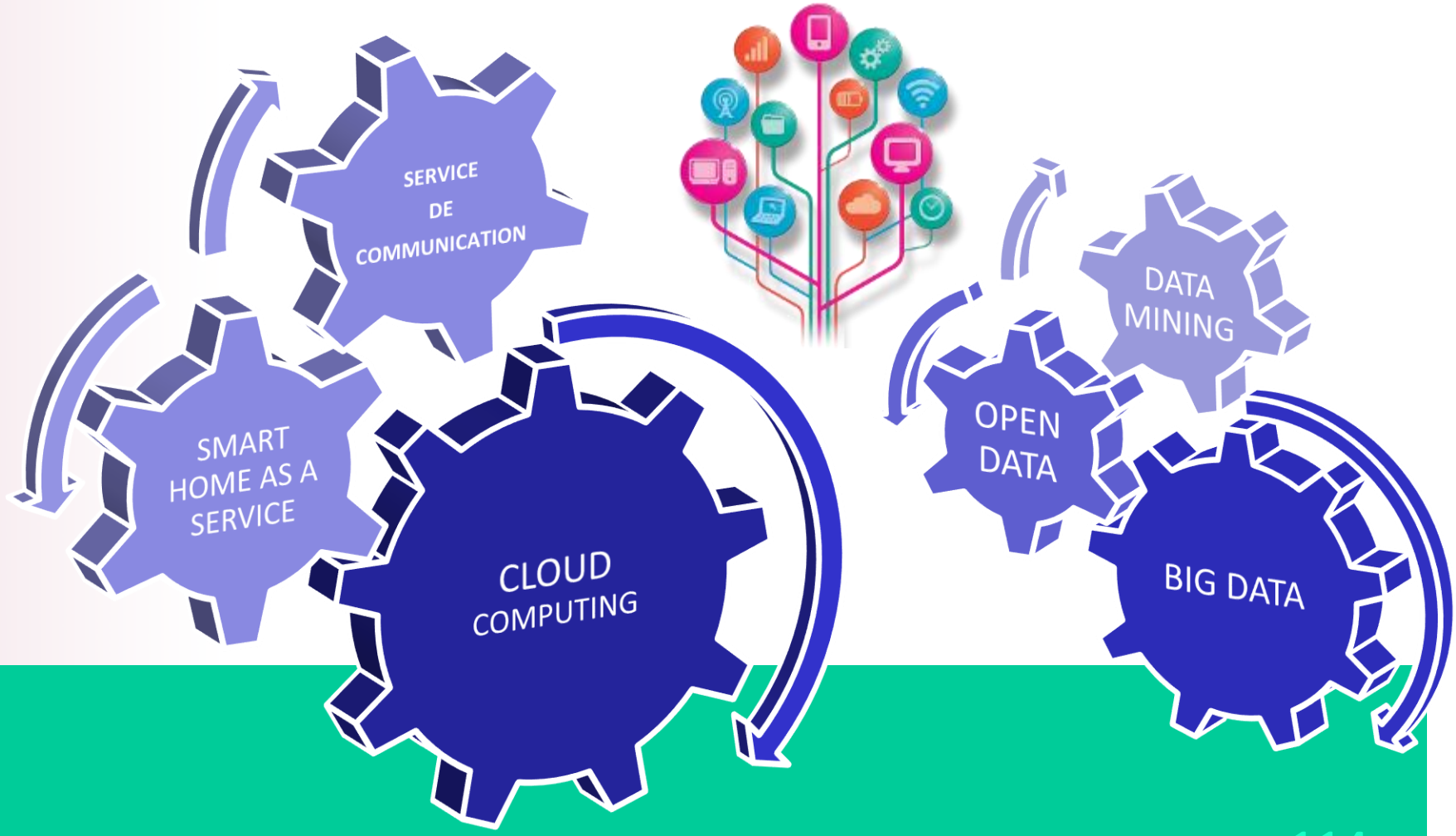
Mathias Avocats

@garancemathias

TOUS CONCERNÉS PAR LES OBJETS CONNECTÉS !



ECOSYSTEME DES OBJETS CONNECTÉS



LE DROIT S'IMPOSE À TOUS LES ACTEURS !

Le cloud est une externalisation.

- En ce sens, il s'agit d'un choix stratégique de l'entreprise.

Ce choix doit prendre en compte de nombreux enjeux juridiques :

- Droit applicable !
- Transparence & compréhension du « qui fait quoi »
- Localisation, propriété serveurs, liens contractuels en cascade, etc.
- Données à caractère personnel
- Sous-traitance (chaîne contractuelle)
- Savoir-faire & Propriété intellectuelle
- Responsabilités (continuité de service, etc.)
- Maintenance (curative / préventive / évolutive)

➔ Gestion des contrats en amont !

FOCUS DATA : QUELS REFLEXES POUR UNE GESTION DE RISQUE ?

Minimisation des données:

- En amont: personnel chargé de la conception → paramétrer les traitements, restreindre les possibilités de collecte
- En aval: personnel chargé de la collecte des données (clients, prospects, salariés, etc.)

Protection des droits des personnes:

- En amont:
  - Revoir la politique de rédaction des contrats avec les partenaires et les clients
  - Former les salariés avec des mises en situation
- En aval: s'assurer de l'effectivité des droits par l'évaluation des politiques

Sécurité des traitements:

- En amont:
  - Sensibiliser les salariés chargés de la sécurité du SI en interne et instaurer des bonnes pratiques, des procédures, des politiques et définir des méthodologies
  - Être vigilant quant aux mesures de sécurité des données mises en œuvre par les sous-traitants,
  - Négocier les conditions de sécurité avec les partenaires si elles ne sont pas satisfaisantes
- En aval:
  - Pratiquer des audits
  - Évaluer les politiques de sécurité

Documentation attestant de la conformité

- analyse d'impact pour les traitements à risques
- privacy by design (protection dès la conception) ou by default (protection par défaut)

Mesures de sécurité

Audits

COMMENT RÉAGIR APRÈS L'ATTAQUE ?

Si l'on soupçonne une attaque, sa prise en charge passe par notamment:

- L'identification de l'auteur (pirate, hacktivisme, etc.)
- L'identification de la victime: c'est l'entité responsable hiérarchique ou fonctionnelle de celle-ci qui décide d'intenter, ou non, d'éventuelles poursuites
- L'identification du bien altéré:
  - Un système d'exploitation ou un logiciel,
  - L'image ou la réputation d'une personne morale ou physique,
  - Une divulgation d'informations confidentielles ou une fuite de données personnelles,
  - Une autre cible. Face à la technique du rebond, la personne intermédiaire se retrouve dans le rôle de l'attaquant (involontaire). Elle doit pouvoir faire preuve de sa bonne foi en démontrant qu'elle avait correctement protégé son système.

L'analyse de l'impact: c'est au regard de cette évaluation que se décideront les éventuelles poursuites (au civil ou au pénal).

ET EN PRATIQUE ? Illustration des enjeux avec VTech

Faille de sécurité du fabricant de jouets Vtech qui concernerait 4,8 millions de consommateurs:

- Email, nom, prénom, mots de passe, genre, etc.
- Dates de naissance de 200 000 enfants
- Photographies des parents et des enfants

ET EN PRATIQUE ? Illustration des enjeux avec VTech

- **Plainte UFC-Que Choisir**

- Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès (**article 34 de la loi**).

- **Article 226-17 du Code pénal** : « *Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende* ».

Objets connectés – enjeux juridiques

- Security and Resilience of Smart Home Environments, Good practices and recommendations

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/smart-homes/security-resilience-good-practices

- Un Noël très connecté

http://www.cnil.fr/les-themes/conso-pub-spam/fiche-pratique/article/un-noel-tres-connecte/

- Piratage VTECH – L'UFC-Que Choisir dépose plainte

http://www.quechoisir.org/telecom-multimedia/internet/communique-piratage-vtech-l-ufc-que-choisir-depose-plainte

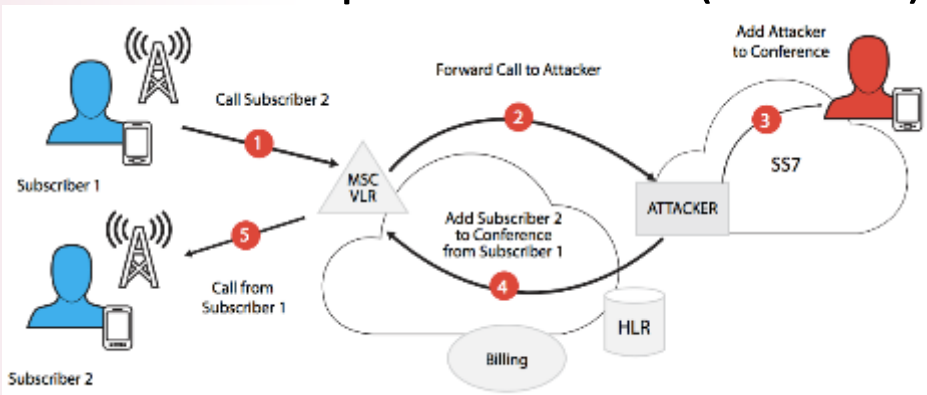
Nos téléphones mobiles : des cibles de premier plan

Col. Éric Freyssinet

Conseiller auprès du Préfet, Conseiller du Gouvernement, chargé de la lutte contre les cybermenaces

Des vulnérabilités au cœur du réseau (protocole SS7) ?

- Ces classes d'exploitation de SS7 ne sont pas nouvelles, mais ont suscité publications, présentations et réactions en 2014 et 2015
- Les vulnérabilités présentées en décembre 2014 permettraient de rediriger des communications ou d'intercepter des SMS (chiffrés)



A survey of a handful of large mobile operators on each continent showed that hackers have been exploiting a key signalling protocol for routing cellular calls known as SS7, to track the location of certain mobile users and in some cases, listen in on calls.

Across a range of operators, 0.08% of SS7 packets being sent across a network in Africa were deemed suspicious. In Asia the rate was 0.04% and in the Americas it was 0.025%, according to research by Dublin based research firm Adaptive Mobile.

While these are low percentages they relate to the millions of SS7 packets being sent every day.

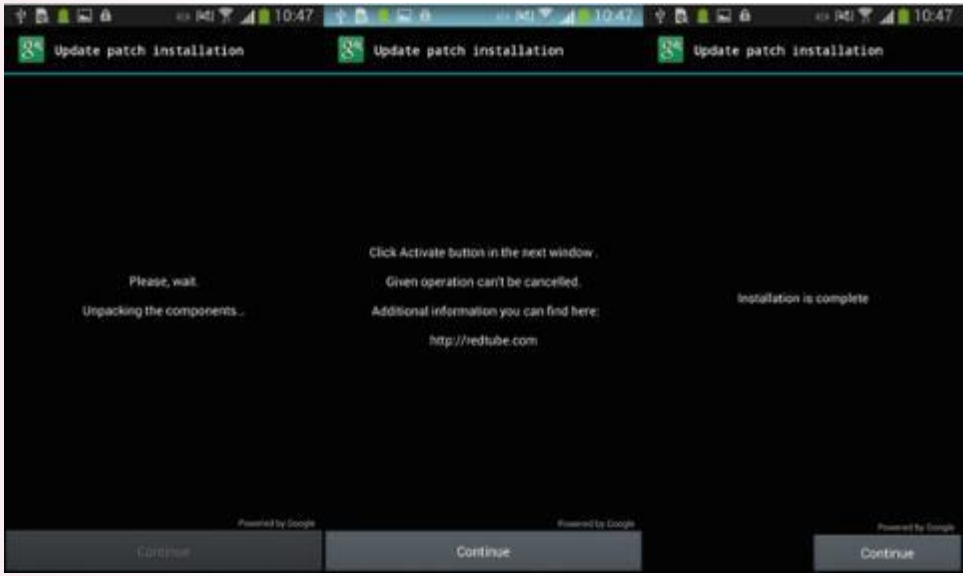
"That can add up to tens of thousands a day which can mean someone being tracked or some fraud transactions," says Cathal Mc Daid, head of Adaptive Mobile's cyber security unit. "These are low-volume, high-impact events."

Beaucoup d'informations chiffrées sont apportées par des fournisseurs de solutions de sécurité pour les opérateurs

Source : http://www.forbes.com/sites/parmyolson/2015/10/14/hackers-mobile-network-backbone-ss7/

Logiciels malveillants pour mobiles

- Toujours des évolutions
- Avec « PornDroid », le blocage du téléphone Android se fait par le changement du code de déverrouillage de l'écran



Source : http://www.pcworld.com/article/2983138/security/android-ransomware-changes-a-devices-pin-code.html (via ESET)

Les plates-formes de développement pour rebondir

- XCodeGhost exploite la plateforme Xcode de développement iOS pour se déployer
- L'application XCode modifie les librairies CoreServices qui sont intégrées automatiquement dans le code des applis mobiles

Depuis mars 2015

Par ex:

CoreServices

Classe UIWindow

Available on the iPhone App Store

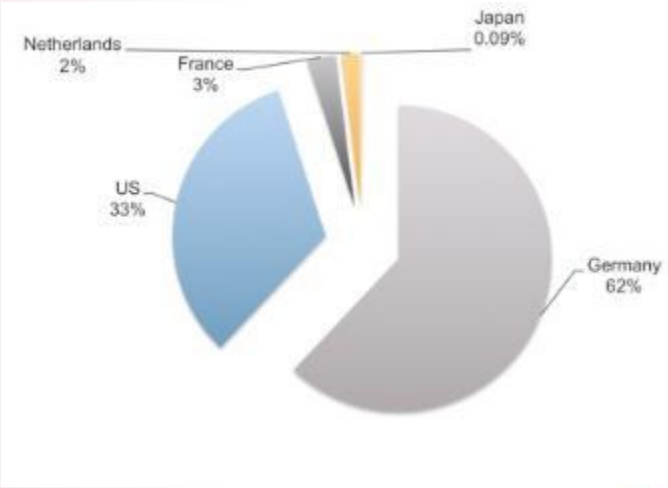
+39 applications

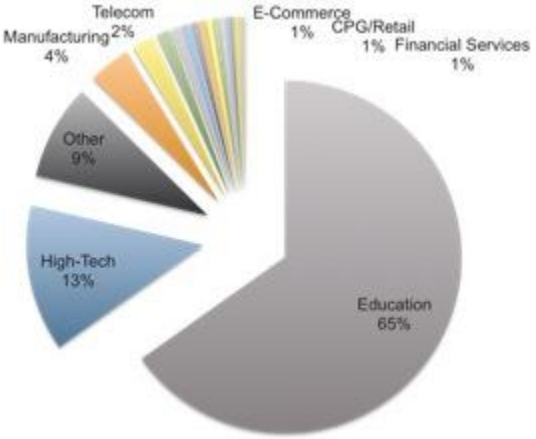
voire +3400…

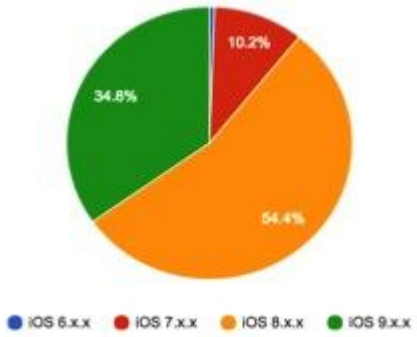
Vol de mots de passe, ouverture d'URLS…

Source : http://researchcenter.paloaltonetworks.com/2015/09/novel-malware-xcodeghost-modifies-xcode-infects-apple-ios-apps-and-hits-app-store/ (Palo Alto)

Et plusieurs semaines après, XCodeGhost continue de faire des dégâts







Source : https://www.fireeye.com/blog/threat-research/2015/11/xcodeghost_s_a_new.html (FireEye)

Nos téléphones mobiles : des cibles de premier plan

- PornDroid

http://www.pcworld.com/article/2983138/security/android-ransomware-changes-a-devices-pin-code.html (via ESET)

- XCodeGhost

http://researchcenter.paloaltonetworks.com/2015/09/novel-malware-xcodeghost-modifies-xcode-infects-apple-ios-apps-and-hits-app-store/

http://researchcenter.paloaltonetworks.com/2015/09/malware-xcodeghost-infects-39-ios-apps-including-wechat-affecting-hundreds-of-millions-of-users/

http://researchcenter.paloaltonetworks.com/2015/09/update-xcodeghost-attacker-can-phish-passwords-and-open-urls-though-infected-apps/

http://researchcenter.paloaltonetworks.com/2015/09/more-details-on-the-xcodeghost-malware-and-affected-ios-apps/

https://www.fireeye.com/blog/threat-research/2015/11/xcodeghost_s_a_new.html

- Vulnérabilité SS7

https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/german-researchers-discover-a-flaw-that-could-let-anyone-listen-to-your-cell-calls-and-read-your-texts/

http://www.bbc.com/news/technology-34536921

http://www.adaptivemobile.com/blog/russia-ukraine-telecom-monitoring

http://www.cellusys.com/2015/10/20/8-ss7-vulnerabilities-you-need-to-know-about/

Les conséquences d'une attaque

Col. Éric Freyssinet

Conseiller auprès du Préfet, Conseiller du Gouvernement, chargé de la lutte contre les cybermenaces

Conséquences de l'attaque contre TARGET

- Licenciements et millions de dollars de dédommagement
- Au final, le coût pour l'entreprise serait de 252 M$ (dont 90 pour assurances)

Target CEO: Fired for More than Security

Target Could Be Liable for $3.6 Billion from Security Breach

Target to Settle Claims Over Data Breach

Retailer to pay Visa issuers up to $67 million, is working with MasterCard on similar deal

The exact amount of fraud that resulted from the Target breach still isn't known. Trade groups representing community banks and credit unions estimate that they spent more than $350 million to reissue credit and debit cards and deal with other issues tied to the

RISK & ANALYTICS

Target's $100M EMV Migration Shows Just How Tight the Deadline Is

Why it took the US so long to adopt the credit card technology Europe has used for years

Source : http://www.wsj.com/articles/target-reaches-settlement-with-visa-over-2013-data-breach-1439912013

Conséquences de l'attaque contre OPM

- Le vol de données d'un service d'habilitation du personnel entraîne des réactions en cascade

National Security

Chinese breach data of 4 million federal workers

By Ellen Nakashima June 4 Follow @nakashimae

Hackers working for the Chinese state breached the computer system of the Office of Personnel Management in December, U.S. officials said Thursday, and the agency will notify about 4 million current and former federal employees that their personal data may have been compromised.

The hack was the largest breach of federal employee data in recent years. It was the second major intrusion of the same agency by China in less than a year and the second significant foreign breach into U.S. government networks in recent months. Last year, Russia compromised White House and State Department e-mail systems in a campaign of cyberespionage.

07/2014
… 06/2015

09/2015

National Security

CIA pulled officers from Beijing after breach of federal personnel records

Source : https://www.washingtonpost.com/world/national-security/cia-pulled-officers-from-beijing-after-breach-of-federal-personnel-records/2015/09/29/1f78943c-66d1-11e5-9ef3-fde182507eac_story.html

Les enfants ciblés

- Une série d'attaques en 2015 cible des plates-formes contenant des données concernant majoritairement les plus jeunes
- En fait les familles et leurs moyens de paiement aussi

VTech toymaker hacked – millions of families have their personal info exposed

By: Graham Cluley | comment : 0 | November 30, 2015 | Posted in: Industry News

VTech, a leading maker of electronic learning toys, has suffered a serious security breach, with hackers acces a database containing information about customers and their children.

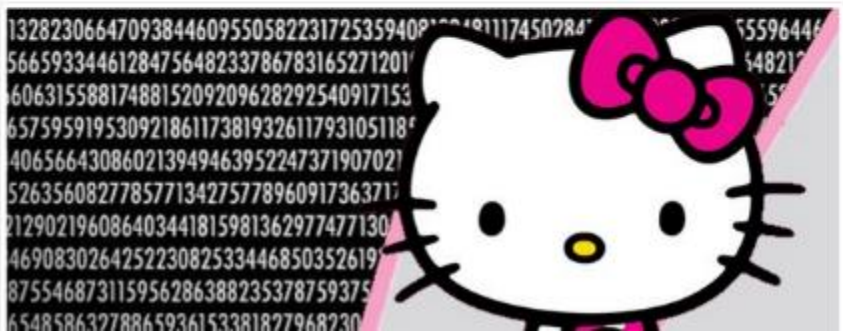
As a result, data including users' email addresses, home addresses, security questions and answers, children names and dates of birth, and easily-reversible passwords have been accessed.

Millions of Hello Kitty fans have their data exposed online

By: Graham Cluley | comment : 1 | December 21, 2015 | Posted in: Industry News

If you're a lover of Hello Kitty, My Melody, and (my favourite) Keroppi the frog then you might want to rub the cuteness out of your eyes, and wake up to the real world of information security.

Fresh on the heels of revealing that 13 million MacKeeper customers had had their sensitive account details left lying around on a publicly accessible database, researcher Chris Vickery had discovered a database containing the details of some 3.3 million users of the Sanrio Town online community.

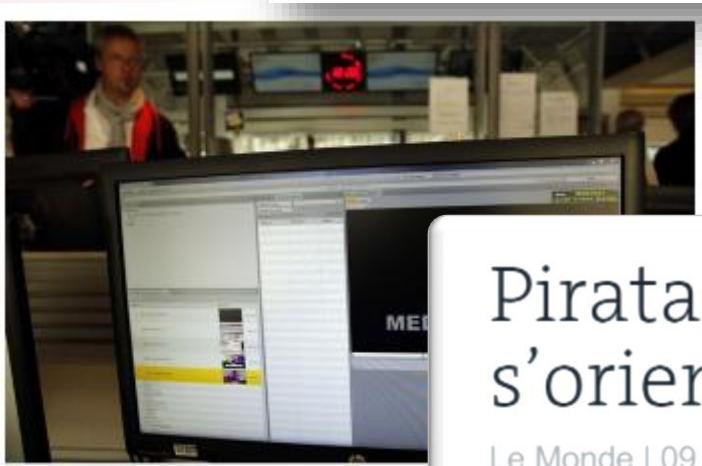


Source : http://www.hotforsecurity.com/blog/millions-of-hello-kitty-fans-have-their-data-exposed-online-13154.html

Conséquences de l'attaque contre TV5 Monde

- D'abord et avant tout une prise de conscience du risque de destruction d'un système d'information
- Gros investissements par la suite pour sécuriser
- PDG mobilisé pour partager son expérience

L'attaque subie par la chaîne francophone internationale en avril lui aura coûté plus d'une dizaine de millions d'euros. De quoi obliger TV5 à tailler dans son budget 2016.



Le 8 avril 2015, la chaîne de télévision francophone TV5 Monde
Christophe Ena/AP/SIPA

La publicité sur internet "s'effondre"

Les malheurs de la chaîne ne s'arrêtent pas là. Le site web, dont l'audience déjà en chute libre depuis plusieurs années (cf. ci-dessous), a été

Piratage de TV5 Monde : l'enquête s'oriente vers la piste russe

Le Monde | 09.06.2015 à 18h43 • Mis à jour le 11.06.2015 à 19h00 |

Source : http://bfmbusiness.bfmtv.com/entreprise/piratage-de-tv5-monde-une-facture-tres-salee-922231.html

Ashley Madison

- Perte d'image et conséquences importantes pour les tiers

What did hackers take from Ashley Madison and why?

The Ashley Madison hackers have posted personal information like e-mail addresses and account details from 32 million of the site's members. The group has two motivations: First, they've criticized Ashley core mission of arranging affairs between marrie individuals. Second, they've attacked Ashley Ma business practices, in particular its requirement pay $19 for the privilege of deleting all their data site (but, as it turns out, not all

Le premier hack contre Mr Tout-le-monde

Si tous les internautes ne sont pas partis chasser les infidèles fréquentant Ashley Madison, beaucoup d'Américains se sont cependant moqué de la situation de ces personnes hackées ou ont soutenu l'acte de The Impact Team.

Suicides, démission, chantage : les conséquences tragiques du piratage du site de rencontres Ashley Madison

Le Monde | 10.12.2015 à 09h35 |

Données traitées par les sites de rencontre : 8 mises en demeure

28 juillet 2015

A la suite de contrôles effectués auprès de plusieurs sites de rencontre ayant révélé de nombreux manquements à la loi Informatique et Libertés, notamment sur les informations sensibles fournies par leurs clients, la Présidente de la CNIL met en demeure huit acteurs du secteur.

- Mais ce n'est pas nouveau !

Source : http://fortune.com/2015/08/26/ashley-madison-hack/

Les conséquences d'une attaque - synthèse

- Les conséquences souhaitées par les attaquants
  - *Nuire (à la réputation, au fonctionnement)*
  - *Récupérer des informations*
- Mais aussi des conséquences non recherchées
  - Economiques
  - Sociales
- Des conséquences nécessaires
  - Déposer plainte
  - Préparer les éléments de preuve, évaluer le préjudice…
  - Réparer
  - … Et en tirer des leçons
- Et donc il vaut mieux s'y préparer:
  - Prévenir les risques (en être conscient, prendre des mesures préventives)
  - Être capable de détecter une survenance
  - Être en mesure de maîtriser voire diminuer l'impact

Les conséquences d'une attaque 1/2

- TARGET

http://www.tomshardware.com/news/target-security-hacking-fines-3.6-billion,25516.html
http://www.businessinsider.com/target-ceo-fired-for-more-than-security-2014-5?IR=T
http://www.wsj.com/articles/target-reaches-settlement-with-visa-over-2013-data-breach-1439912013
http://www.paymentssource.com/news/risk-analytics/targets-100m-emv-migration-shows-just-how-tight-the-deadline-is-3022176-1.html

- OPM

https://www.washingtonpost.com/news/morning-mix/wp/2014/07/09/report-chinese-hacked-into-the-federal-governments-personnel-office/
https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html
https://www.washingtonpost.com/world/national-security/in-a-series-of-hacks-china-appears-to-building-a-database-on-americans/2015/06/05/d2af51fa-0ba3-11e5-95fd-d580f1c5d44e_story.html
https://www.washingtonpost.com/world/national-security/cia-pulled-officers-from-beijing-after-breach-of-federal-personnel-records/2015/09/29/1f78943c-66d1-11e5-9ef3-fde182507eac_story.html

- TV5 Monde

http://bfmbusiness.bfmtv.com/entreprise/piratage-de-tv5-monde-une-facture-tres-salee-922231.html
http://www.lemonde.fr/pixels/article/2015/06/09/piratage-de-tv5-monde-l-enquete-s-oriente-vers-la-piste-russe_4650632_4408996.html
http://www.20minutes.fr/medias/1747847-20151210-piratage-tv5-monde-apres-cyberattaque-chaine-investit-protection

Les conséquences d'une attaque 2/2

- Ashley Madison

http://fortune.com/2015/08/26/ashley-madison-hack/
https://www.quora.com/What-are-some-less-obvious-consequences-of-the-Ashley-Madison-hack
http://www.lesinrocks.com/2015/08/20/actualite/pourquoi-il-ne-faut-pas-rire-du-hack-dashley-madison-11768231/
http://www.lemonde.fr/pixels/article/2015/12/10/suicides-demission-chantage-les-consequences-tragiques-du-piratage-du-site-de-rencontres-ashley-madison_4828391_4408996.html
http://www.cnil.fr/nc/linstitution/actualite/article/article/donnees-traitees-par-les-sites-de-rencontre-8-mises-en-demeure/

- Les plus jeunes ciblés

http://www.hotforsecurity.com/blog/millions-of-hello-kitty-fans-have-their-data-exposed-online-13154.html
http://www.hotforsecurity.com/blog/vtech-toymaker-hacked-millions-of-families-have-their-personal-info-exposed-13061.html

(Malgré tout,) Quelques raisons de se réjouir

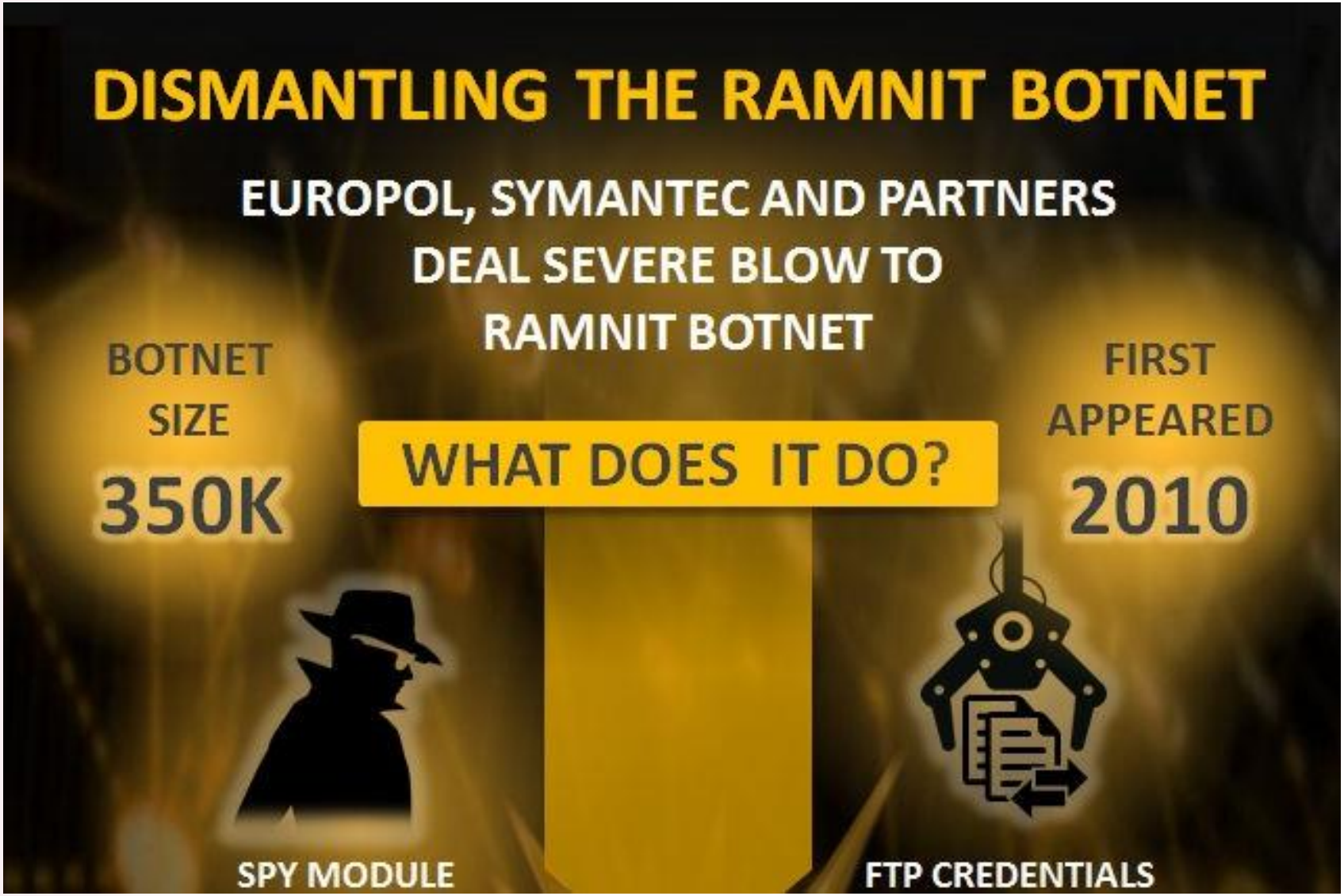
François PAGET

Secrétaire Général Adjoint du CLUSIF et animateur du groupe « Panorama »

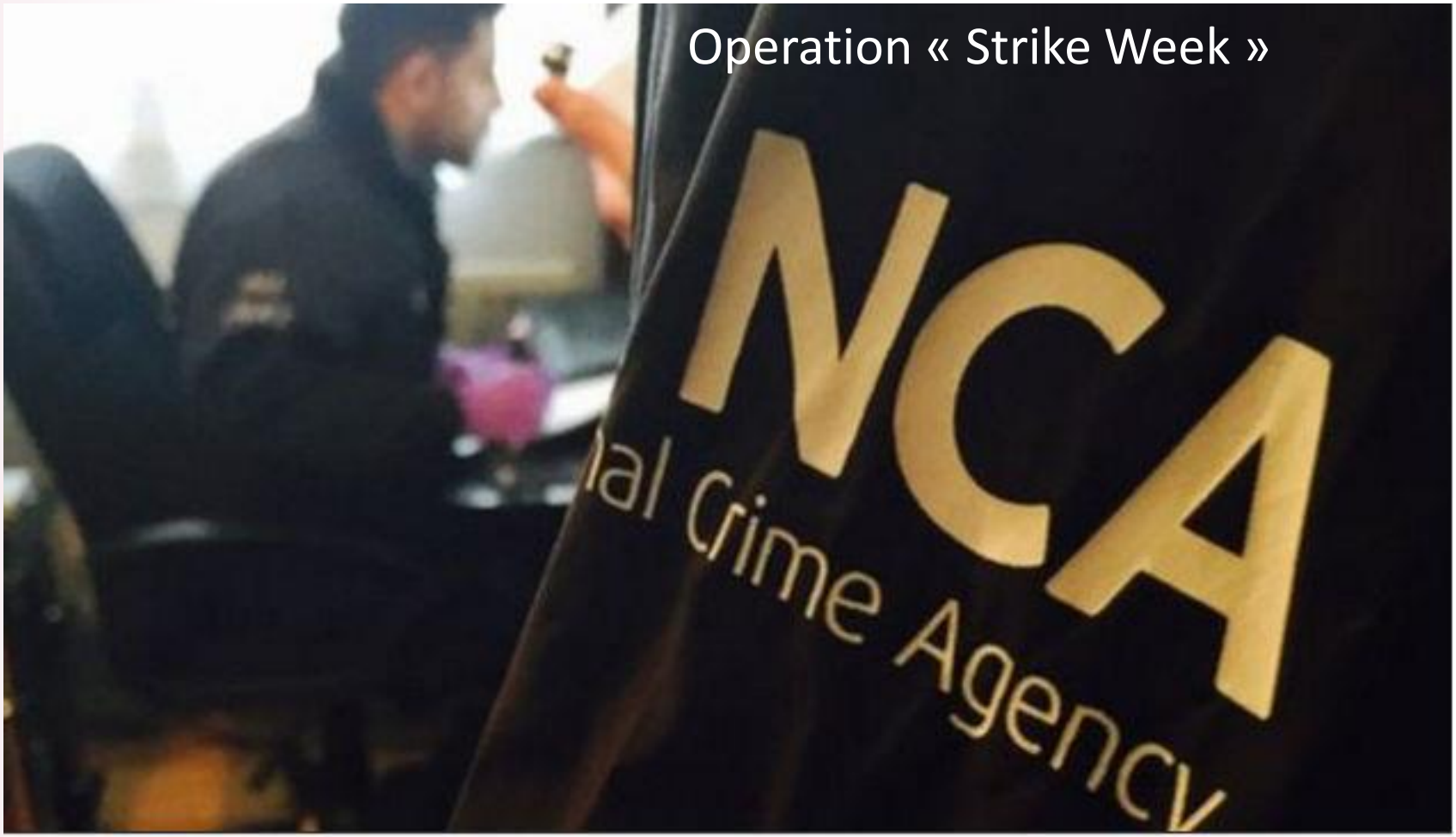
(Les captures d'écrans qui suivent proviennent de sources ouvertes et la présomption d'innocence s'applique, bien évidemment, à toutes les personnes citées ou représentées sur ces slides.)

Janvier 2015

Février 2015



Mars 2015



The UK's National Crime Agency has arrested 56 suspected hackers as part of a "strike week" against cybercrime.

Mars 2015

Sheep Marketplace Admin Arrested in $40 Million Bitcoin Theft

by Traderman on March 29, 2015

details regarding the whereabouts of Jiřikovský, u nabbed Jiřikovský and his wife, Eva Bartosova. Both are suspected of money laundering, pending the conclusion of an ongoing investigation by authorities in the Czech Republic. The entire investigation began when clerks at a Czech bank, noticed large transfer taking place on the account of Jiřikovský's wife. When employes at the bank

Avril 2015

Forbes / Security

20 Stocl

APR 13, 2015 @ 03:28 AM 20,110 VIEWS

Alleged 'Nazi' Android FBI Ransomware Mastermind Arrested In Russia

Статистика Боты Команды Отчеты Опции

Сообщения (0) Коллектор (0)

Команды

Сценарий для ботов.

Создать новую команду | Сбросить | Удалить

#	Название	Содержимое	Дата создания	Статус	Q / OK / %	Комментарий
	script_606..	getMessages	16:08:40 31.01.2014	В процессе	1 / 0 / 0%	
	send_sms_8..	sendSMS 900 8478	16:04:04 31.01.2014	В процессе	1 / 0 / 0%	
	send_sms_1..	sendSMS 900 31155	16:02:09 31.01.2014	В процессе	1 / 0 / 0%	
	send_sms_6..	sendSMS 900 8450	15:49:09 31.01.2014	Выполнено	1 / 1 / 100%	
	script_924..	sendSMS 79262000900..	15:31:08 31.01.2014	В процессе	9783 / 1382 / 14%	
	script_613..	sendSMS 900 1505	15:28:55 31.01.2014	В процессе	9783 / 2626 / 27%	

Avril 2015

Mai 2015

Silk Road

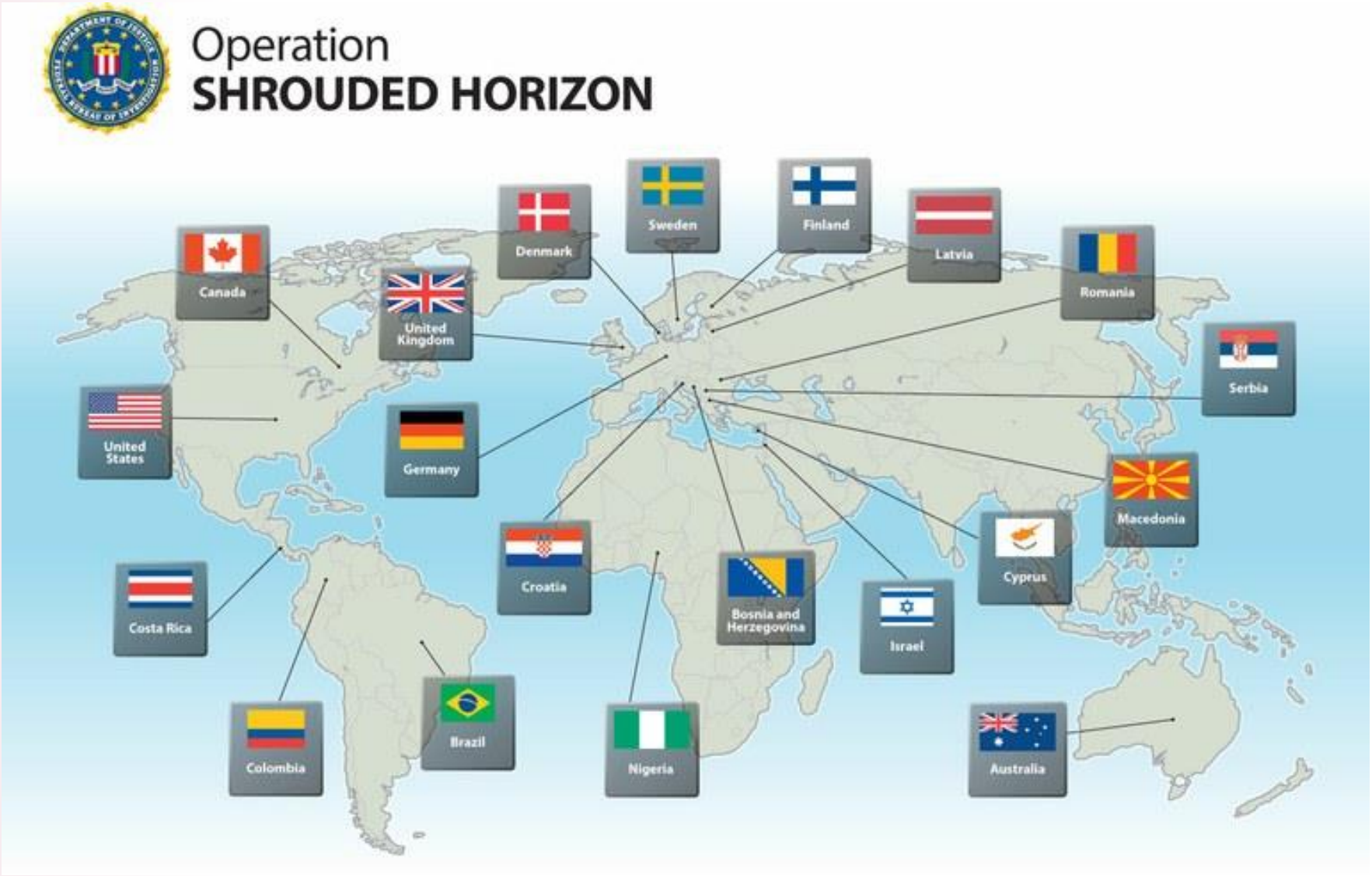
Silk Road operator Ross Ulbricht sentenced to life in prison

Thirty-one-year-old behind illegal online drug emporium handed five sentences – including two for life – to be served concurrently with no chance of parole

Ross Ulbrict was arrested and charged in 2013 with being Silk Road's pseudonymous founder 'Dread Pirate Roberts'.

Juin 2015

Juillet 2015



Juillet 2015

2 Florida men charged in illegal bitcoin operation

Août 2015

Août 2015

Septembre 2015

Authorities arrest creators of Dridex and Citadel banking Trojans

"Aquabox" author of trojan citadel and the author of "Dridex botnet",aka Cridex,were arrested

Octobre 2015

Alleged Head of Multimillion-Dollar Illegal Sports Betting Ring Arrested in Santa Clarita

POSTED 1:36 PM, OCTOBER 28, 2015, BY ANTHONY KURZWEIL AND COURTNEY FRIEL, *UPDATED AT 03:50PM, OCTOBER 28, 2015*

The man accused of heading a multimillion-dollar illegal sports betting ring was taken into custody Wednesday morning during a raid on his Santa Clarita home, authorities said.

Novembre 2015

TalkTalk hack: Met Police arrests fifth suspect in relation to breach

by Jason Murdock 25 Nov 2015

Décembre 2015

Europol s'attaque
au botnet Dorkbot

Succès police

- Janvier
  http://thehackernews.com/2015/01/two-lizard-squad-hackers-arrested-after.html
- Février
  https://www.europol.europa.eu/content/botnet-taken-down-through-international-law-enforcement-cooperation
- Mars
  http://www.nationalcrimeagency.gov.uk/news/news-listings/560-57-arrested-in-nationwide-cyber-crime-strike-week
  http://themerkle.com/news/sheep-marketplace-admin-arrested-in-40-million-bitcoin-theft/
- Avril
  http://www.forbes.com/sites/thomasbrewster/2015/04/13/alleged-nazi-android-fbi-ransomware-mastermind-arrested-in-russia/
  https://www.europol.europa.eu/content/international-operation-dismantles-criminal-group-cyber-fraudsters-0
- Mai
  http://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced
- Juin
  http://thehackernews.com/2015/06/zeus-spyeye-banking-malware.html

Succès police

- Juillet
  https://www.fbi.gov/news/stories/2015/july/cyber-criminal-forum-taken-down
  http://www.wptv.com/news/region-c-palm-beach-county/west-palm-beach/2-florida-men-charged-in-illegal-bitcoin-operation
  http://www.abcactionnews.com/news/2-florida-men-charged-in-illegal-bitcoin-operation
- Aout
  http://www.computerworld.com/article/2955989/financial-it/mt-gox-ceo-karpeles-arrested-in-japan.html
  http://www.nationalcrimeagency.gov.uk/news/691-operation-vivarium-targets-users-of-lizard-squad-s-website-attack-tool
- Septembre
  xakfor.net/threads/Правоохранители-арестовали-создателей-citadel-и-dridex.13641/
- Octobre
  http://ktla.com/2015/10/28/alleged-head-multi-million-dollar-illegal-sports-betting-ring-arrested-in-santa-clarita
- Novembre
  http://www.v3.co.uk/v3-uk/news/2431859/talktalk-ceo-receives-ransom-note-following-significant-and-sustained-cyber-attack
- Decembre
  https://www.europol.europa.eu/content/europol-works-international-partners-target-dorkbot-botnet

Conclusion

Monsieur Jean-Yves LATOURNERIE

Conseiller du Gouvernement, chargé de la lutte contre les cybermenaces / Ministère de l'Intérieur