



FRC 2015
8ème édition

LA RÉGION DE GENDARMERIE D'ALSACE
& LES OFFICIERS DE LA RÉSERVE CITOYENNE



8^{ème} FORUM DU RHIN SUPÉRIEUR SUR LES **CYBER**MENACES



ACTEUR AUJOURD'HUI SINON VICTIME DEMAIN

www.frc.alsace

8ÈME FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES



8ÈME FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

Discours d'ouverture

- **Colonel Denis HEYMANN**

Commandant en second de la Région de Gendarmerie d' Alsace

8ÈME FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

Discours d'ouverture

- **Jacques GARAU**

Secrétaire Général pour les Affaires Régionales et Européennes
à la préfecture de la région Alsace

8ÈME FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

Discours d'ouverture

- **Bernard STIRNWEISS**

Président de la CCI de la région Alsace

LES SPONSORS



NOTRE OBJECTIF

"Mobiliser les décideurs des PME-PMI d'Alsace afin que ceux-ci mettent en œuvre les actions nécessaires à leur entreprise, face aux risques numériques".

- **Animation : Gilbert GOZLAN**

Directeur Opérationnel Sûreté Réseau La Poste Nord & Est
Lieutenant-Colonel (RC) de la Gendarmerie d'Alsace
Président de l'association AD HONORES Réseau Alsace

PRÉSENTATION DU THÈME

Panorama et perspectives en cybercriminalité

- **Colonel Éric FREYSSINET**

Conseiller auprès du Préfet en charge de la lutte
contre les cybermenaces au Ministère de l'intérieur

- **Rappel sur les acteurs**
- **Considérations générales**
- **Nouvelles formes d'organisation criminelle**
- **Focus sous l'angle des botnets**
- **Perspectives**

SERVICES DE LUTTE CONTRE LA CYBERCRIMINALITÉ

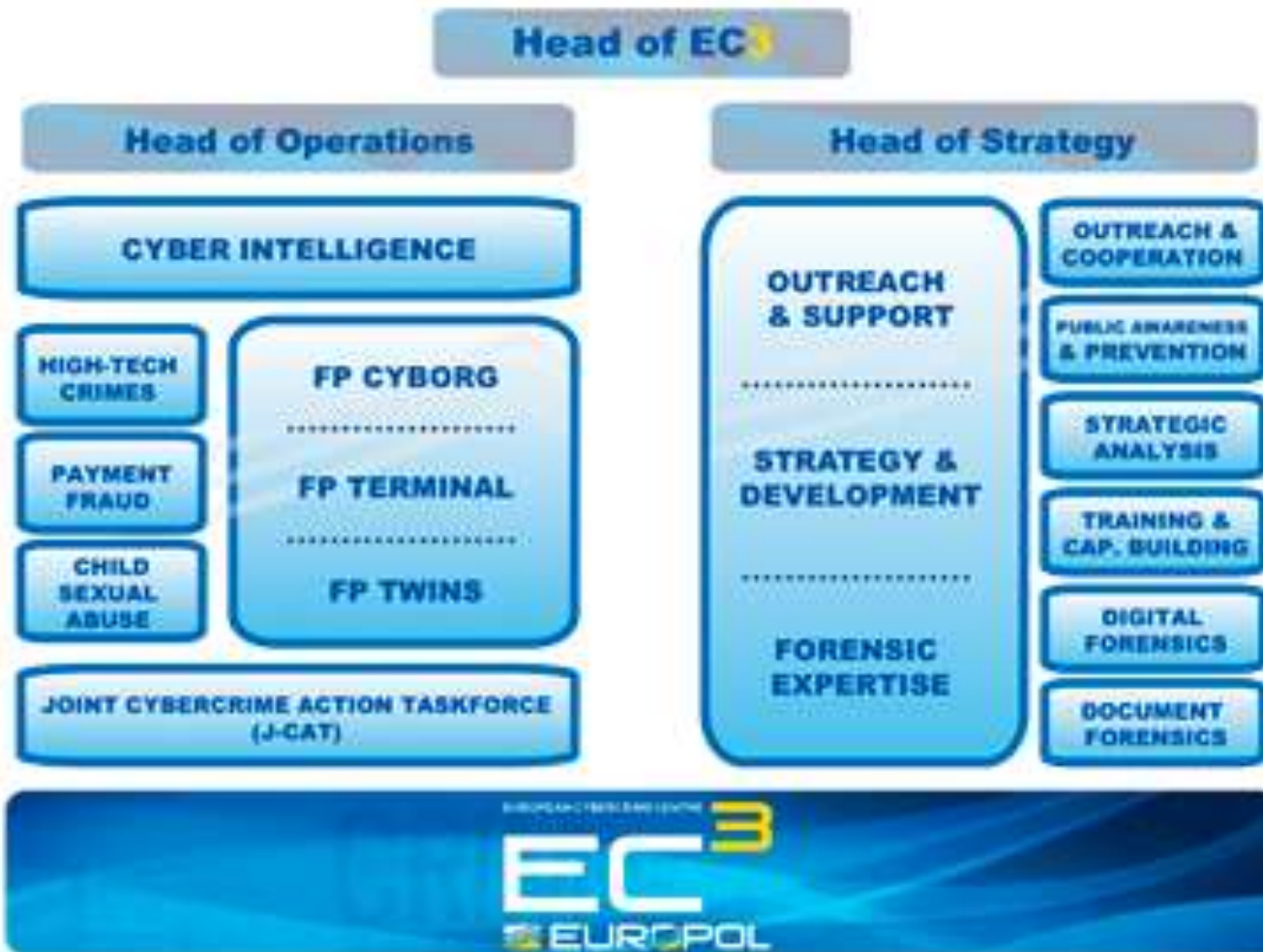


Investigateurs en cybercriminalité (ICC)

Enquêteurs en technologies numériques (NTECH)
Correspondantes en technologies numériques (CNTECH)



EUROPOL EC3



INTERPOL IGCI



► DIGITAL SECURITY

The crime threat in the digital age is constantly evolving as criminals exploit the speed, convenience and anonymity of the Internet to commit crime.

INTERPOL Digital Crime Centre

The ease with which criminals can now carry out their activities means there is even greater need to develop a common platform for exchanging specialized police information and collaborate in digital crime investigations.

The Digital Crime Centre will support member countries' operations and will house a digital forensics laboratory, which will be a centre of excellence for forensic technology for the law enforcement community.

Cyber Innovation and Outreach

While effective law enforcement action is a critical component of fighting the cyber threat, we also recognize the importance of engaging all stakeholders, particularly those in the technology sector, to work towards the goal of a safer cyberspace.

A critical function in the area of cyber innovation and outreach will be the formulation of INTERPOL's global cybersecurity strategy.

It is essential that we work in tandem with partners worldwide to tailor a law enforcement response which complements existing international strategies.

► INTERNATIONAL PARTNERSHIPS AND DEVELOPMENT

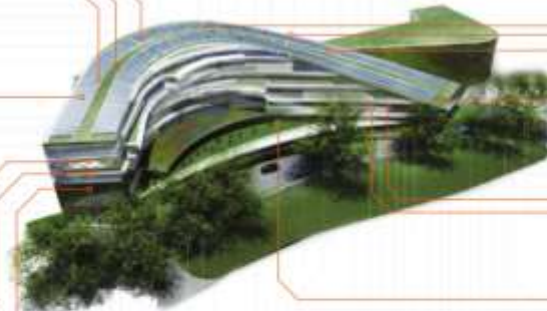
Transnational crime cannot be tackled in isolation; its scope and reach are too wide. Building strong partnerships with other organizations and the public and private sectors is essential to tackle challenges in common areas and strengthen security worldwide.

The exchange of knowledge and expertise with external partners is of mutual benefit, so consolidating existing alliances and forging new relationships is to the advantage of all those who seek to curb the activities of today's criminals. We have been embracing this opportunity for the past decade.

Reaching our true potential as an organization will require us to secure sustainable external funding and resources. We will identify new opportunities for revenue generation and will develop the legal, financial and administrative frameworks needed to support this effectively.



THE INTERPOL GLOBAL COMPLEX FOR INNOVATION



The Global Complex in Singapore is a state-of-the-art building, conforming to the highest environmental standards and will complement our General

THE INTERPOL GLOBAL COMPLEX FOR INNOVATION



► CAPACITY BUILDING AND TRAINING

The Global Complex will build on our established training activities and continue to drive international capacity building programmes for police, tailored to the needs of our member countries.

Core programmes ensure that frontline officers around the world are able to use INTERPOL's databases and search facilities to their full potential. We also design and implement classroom, field and online training programmes for staff at our National Central Bureaus, as well as for other law enforcement agencies and authorized users of our services.

In partnership with academia, we coordinate research into training technology and methodology, and facilitate the exchange of results and best practices. In future, an INTERPOL accreditation policy will ensure the transfer of this knowledge into police operations on the ground.

► OPERATIONAL AND INVESTIGATIVE SUPPORT

In order to reinforce our global 24/7 operational support to member countries, we are expanding the INTERPOL Command and Coordination Centre to a third time zone. A dedicated operations room in Singapore will complement the current sites in Europe and Latin America, and will also manage the deployment of specialized teams within the region, providing support at major incidents and events.

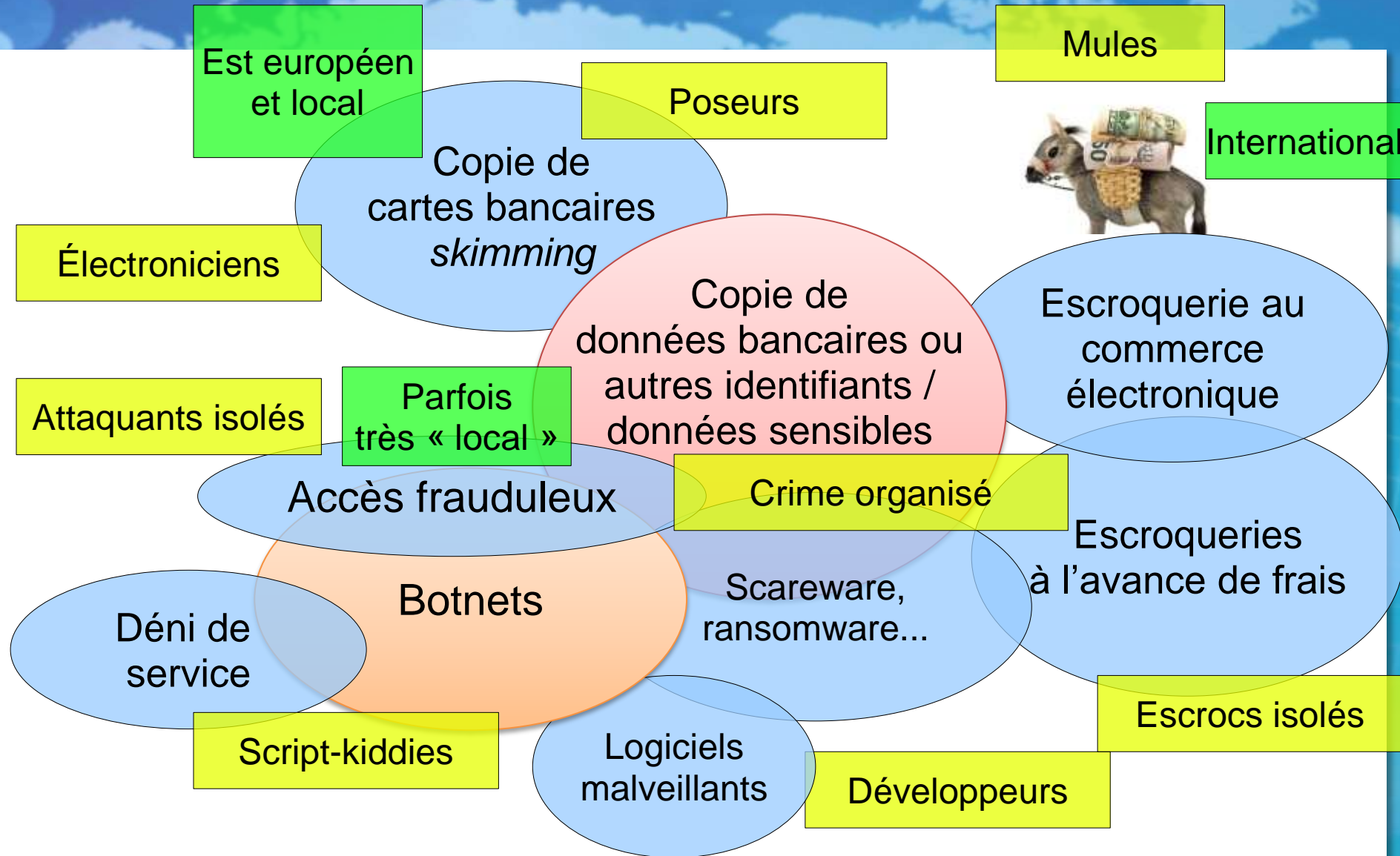
Specialists at the Global Complex will focus on identifying and addressing ways to combat emerging crimes and threats, raising awareness and forging initiatives with pertinent partners to coordinate enforcement action.

As Asia is a region vulnerable to natural disasters, a permanent platform for disaster victim identification (DVI) will be established at the Global Complex. By combining practical experience with scientific disciplines, we aim to enhance international standards in the DVI process, and expert staff will offer training to member countries.

SYNTHÈSE CYBERCRIMINALITÉ

- **Sur la base des trois piliers traités par Europol:**
 - Atteintes aux mineurs facilitées par Internet
 - Toujours un sujet très fort
 - Croissance des situations d'abus « sur commande »
 - Cartes bancaires, moyens de paiement
 - Stable, avec une adaptation des modes opératoires
 - En réalité ce sont toutes les formes d'escroquerie, quels que soient les moyens de paiement qui tiennent le haut du pavé
 - Atteintes aux STAD
 - Développement fort des menaces liées à des virus informatiques et les atteintes directes contre les systèmes d'information

ECOSYSTÈME DU CYBERCRIME FINANCIER



EVOLUTION DES FORMES DE CRIMINALITÉ ORGANISÉE

- **Intermédiaires:**

- Blanchiment
- Mules



- ▶ **Gestionnaires:**

- ▶ D'infrastructures (bulletproof)
- ▶ De services criminels divers
- ▶ De plateformes de discussion / marchés



- ▶ **Développeurs de:**

- ▶ Virus
- ▶ Plateformes de diffusion
- ▶ Vulnérabilités/ exploits

AUTOUR DES CARTES BANCAIRES

- **Virus contre terminaux de point de vente (TARGET)**

- Kit BlackPos serait développé par un jeune russe de 17 ans (ree4 / Sergey Taraspov) selon IntelCrawler



- **Virus installés dans des DAB pour les vider (Cf. CCC)**



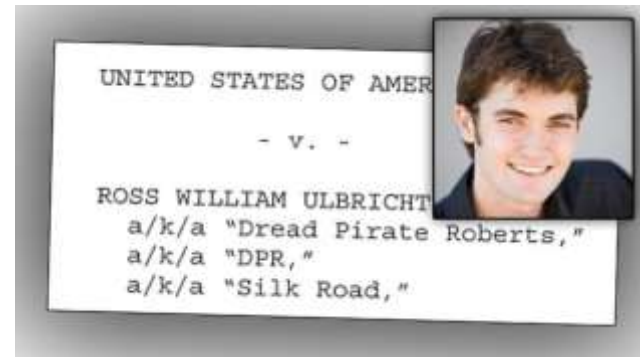
83883992



CAS EMBLÉMATIQUES – ACTEURS ISOLÉS



- **Paunch (Dmitry Fedotov?)**
Auteur de BlackHole (plateforme d'exploits)
Arrêté en octobre 2013 (RU)
Offrait de multiples autres services
- **SilkRoad / DPR (Ross William Ulbricht)**
Arrêté en octobre 2013 (SF, USA)
Complices en Irlande, Australie...



HAMEÇONNAGE PROVENANT DES IMPÔTS

impots.gouv.fr **impôt sur le revenu** 1

http://189.26.241.170/.site/fr/?http://www.impots.gouv.fr/portal/dgi/public/particu

Firefox pense que ce site est malveillant

Ce site a été signalé comme étant une contrefaçon !

impots.gouv.fr

ACTUALITE CONTACTS QUESTIONS FREQUENTES PLAN DU SITE POUR LA PRESSE NOUS CONNAITRE

PARTICULIERS

VOS IMPÔTS VOS PRÉOCCUPATIONS CALENDRIER VOS DROITS

Particuliers > Vos impôts > Formulaire de remboursement

1

Votre compte bancaire va-t-il être crédité... ou débité (de 178,80 €) ???

S'il vous plaît entrez votre nom et une carte de crédit / débit sur lequel le remboursement sera effectué. **2**

Nom

Numéro de la carte

Code PIN (utilisée au guichet automatique)

Soumettre Date 20/10/2009

Montant 178.80 euros **2**

2 **2**

1 **1** **1**

impôt sur le revenu

Ministère du budget, des comptes publics, de la fonction publique et de la réforme de l'Etat

Terminé YSlow (inconnu)

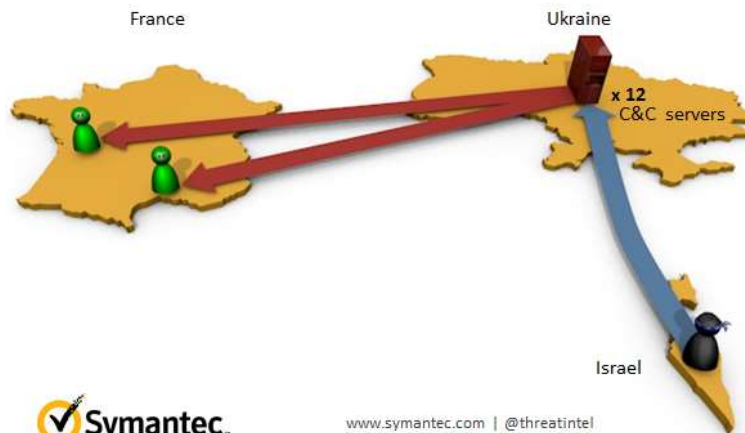
HAMEÇONNAGE

- Kits (achat, gratuit...)
- Hébergement des pages
- Diffusion des messages
- Revente des données



Escroqueries facilitées par des atteintes aux STAD et l'ingénierie sociale

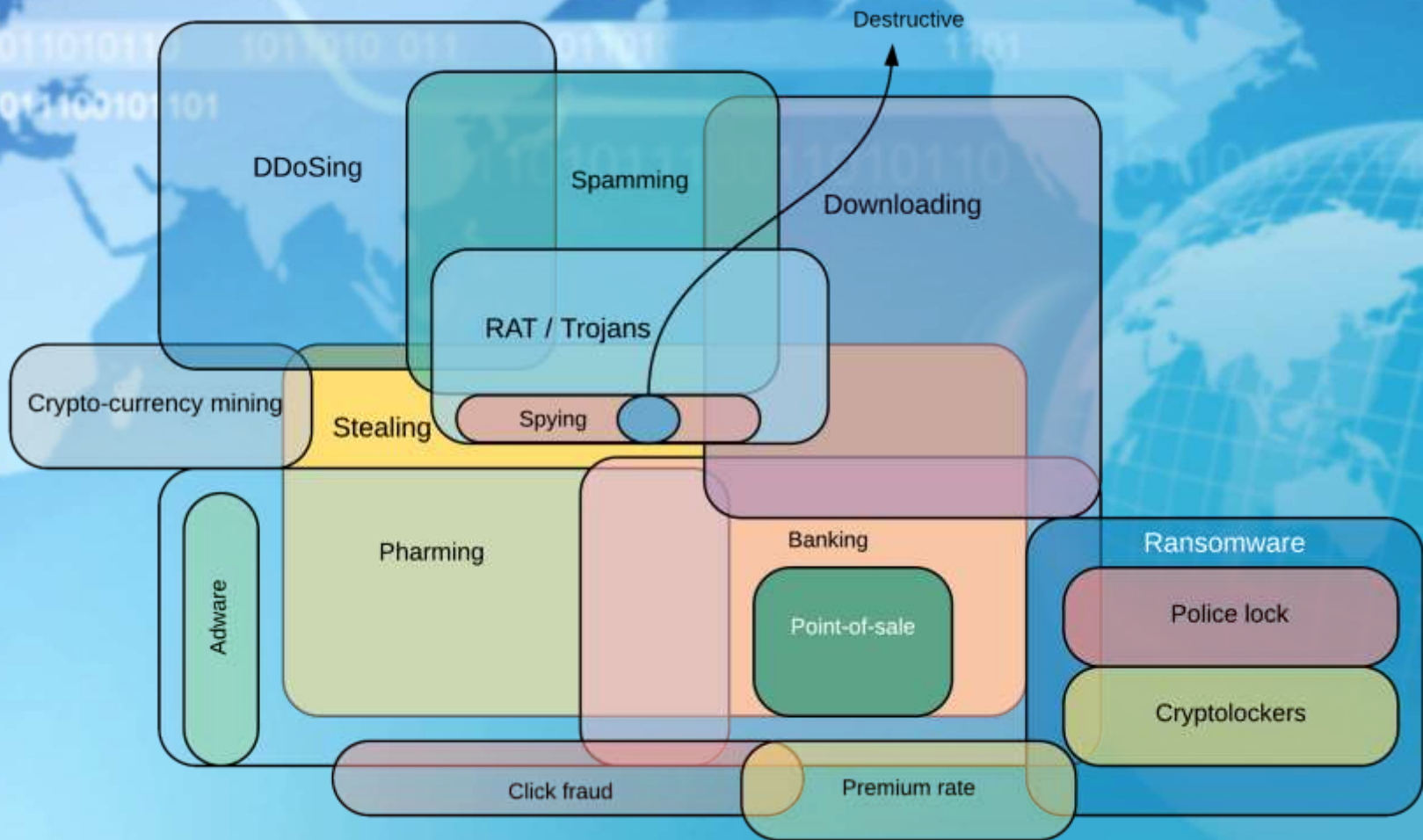
- **Phénomène des faux ordres de virement – FOVI**
 - Facilités par des virus
 - Facilités par des attaques contre des systèmes téléphoniques



BOTNETS – PRINCIPE GÉNÉRAL



CATÉGORIES DE BOTNETS



APPLICATIONS BANCAIRES TOUJOURS CIBLÉES (EN FAIT L'OTP PAR SMS)

02 Android Botnet Targets Middle East Banks

APR 14

I recently encountered a botnet targeting **Android** smartphone users who bank at financial institutions in the Middle East. The crude yet remarkably effective mobile bot that powers this whole operation comes disguised as one of several online banking apps, has infected more than 2,700 phones, and has intercepted at least 28,000 text messages.

The botnet — which I've affectionately dubbed “Sandroid” — comes bundled with Android apps made to look like mobile two-factor authentication modules for various banks, including **Riyad Bank**, **SAAB** (formerly the Saudi British Bank), **AlAhliOnline** (National Commercial Bank), **Al Rajhi Bank**, and **Arab National Bank**.



The fake Android bank apps employed by the Sandroid botnet.

LES TERMINAUX DE POINT DE VENTE

16 Breach at Goodwill Vendor Lasted 18 Months

SEP 14



C&K Systems Inc., a third-party payment vendor blamed for a credit and debit

21 Banks: Card Breach at Goodwill Industries

JUL 14

Heads up, bargain shoppers: Financial institutions are tracking what appears to be a series of credit card breaches nationwide. For its part, **Goodwill Industries International** is the **U.S. Secret Service** on an investigation into the

Headquartered in Rockville, Md., Goodwill International, Inc. is a network of 165 independent units in the United States and Canada with a presence in 15 countries. The organizations sell donated clothing, household items, and use the proceeds to fund job training programs, employment placement services and other community-based initiatives.

According to reports, the locations of Goodwill Industries are likely point of entry for the breach.



18 In Home Depot Breach, Investigation Focuses on Self-Checkout Lanes

SEP 14

The malicious software that unknown thieves used to steal credit and debit card numbers in the data breach at **Home Depot** this year was installed mainly on payment systems in the self-checkout lanes at retail stores, according to sources close to the investigation. The finding could mean thieves stole far fewer cards during the almost five-month breach than they might have otherwise.

Since news of the Home Depot breach first broke on Sept. 2, this publication has been in constant contact with multiple financial institutions that are closely monitoring daily alerts from **Visa** and **MasterCard** for reports about new batches of accounts that the card associations believe were compromised in the break-in. Many banks have been bracing for a financial hit that is much bigger than the exposure caused by the breach at Target, which lasted only three weeks and exposed 40 million cards.

But so far, banking sources say Visa and MasterCard have been reporting far fewer compromised cards than expected given the length of the Home Depot exposure.

Sources now tell KrebsOnSecurity that in a conference call with financial institutions today, officials at **MasterCard** shared several updates from the ongoing forensic investigation into the breach at the nationwide home improvement store chain. The card brand reportedly told banks that at this time it is believed that only self-checkout terminals were impacted in the breach, but stressed that the investigation is far from complete. *Continue reading* --



A self-checkout lane at a Home Depot in N. Virginia.

Avril/mai 2014

-> Révélé en septembre

Serait la même équipe que pour Target (la brèche n'était restée ouverte que 3 semaines).

<http://krebsonsecurity.com/2014/09/in-home-depot-breach-investigation-focuses-on-self-checkout-lanes/>

<http://krebsonsecurity.com/2014/09/breach-at-goodwill-vendor-lasting-18-months/>

DES VARIANTES SPÉCIALISÉES DE BOTNETS BANCAIRES

02 Brazilian 'Boleto' Bandits Bilk Billions



With the eyes of the world trained on Brazil for the 2014 FIFA World Cup, it seems a fitting time to spotlight a growing form of computer fraud that's giving Brazilian banks and consumers a run for their money. Today's post looks at new research into a mostly small-time cybercrime practice that in the aggregate *appears to have netted thieves the equivalent of billions of dollars over the past two years.*

At issue is the "boleto" (officially "Boleto Bancario"), a popular payment method in Brazil that is used by consumers and for most business-to-business payments. Brazilians can use boletos to complete online purchases via their bank's Web site, but unlike credit card payments — which can be disputed and reversed — payments made via boletos are not subject to chargebacks and can only be reverted by bank transfer.



A boleto.

Brazil has an extremely active and talented cybercrime underground, and increasingly Brazilian organized crime gangs are setting their sights on boleto users who bank online. This is typically done through malware that lies in wait until the user of the hacked PC visits their bank's site and fills out the account information for the recipient of a boleto transaction. In this scenario, the unwitting victim submits the transfer for payment and the malware modifies the request by substituting a recipient account that the attackers control.

Many of the hijacked boleto transactions are low-dollar amounts, but in the aggregate these purloined payments can generate an impressive income stream for even a small malware gang. On Tuesday, for example, a source forwarded me a link to a Web-based control panel for a boleto-thieving botnet (see screenshot below); in this operation, we can see that the thieves had hijacked some 383 boleto transactions between February 2014 and the end of June, but had stolen the equivalent of nearly USD \$250,000 during that time.

But a recent discovery by researchers at RSA, the security division of EMC, exposes far more lucrative and ambitious boleto banditry. RSA says the fraud ring it is tracking — known as the "Bolware" operation — affects more than 30 different banks in Brazil, and may be responsible for up to \$3.75 billion USD in losses. RSA arrived at this estimate based on the discovery of a similar botnet control panel that tracked nearly a half-million fraudulent transactions.

<http://krebsonsecurity.com/2014/07/brazilian-boleto-bandits-bilk-billions/>

Most Brazilian banks require online banking customers to install a security plug-in that hooks into the user's browser. The plug-ins are designed to help block malware attacks. But according to RSA, the Bolware gang's malware successfully disables those security plug-ins, leaving customers with a false sense of security when banking online.

The malware also harvests usernames and passwords from victim PCs, credentials that are thought to be leveraged in spreading the malware via spam to the victim's contacts. RSA said this fraud gang appears to have infected more than 192,000 PCs, and stolen at least 83,000 sets of user credentials.

| # | DATA | QUANT | VALOR | DATA ALTERADA | VALOR | VALOR | VALOR |
|----|---------------------|---------|---------|---------------------|---------|---------|---------|
| 1 | 2014-02-10 10:10:10 | 1000.00 | 1000.00 | 2014-02-10 10:10:10 | 1000.00 | 1000.00 | 1000.00 |
| 2 | 2014-02-10 10:10:10 | 1000.00 | 1000.00 | 2014-02-10 10:10:10 | 1000.00 | 1000.00 | 1000.00 |
| 3 | 2014-02-10 10:10:10 | 1000.00 | 1000.00 | 2014-02-10 10:10:10 | 1000.00 | 1000.00 | 1000.00 |
| 4 | 2014-02-10 10:10:10 | 1000.00 | 1000.00 | 2014-02-10 10:10:10 | 1000.00 | 1000.00 | 1000.00 |
| 5 | 2014-02-10 10:10:10 | 1000.00 | 1000.00 | 2014-02-10 10:10:10 | 1000.00 | 1000.00 | 1000.00 |
| 6 | 2014-02-10 10:10:10 | 1000.00 | 1000.00 | 2014-02-10 10:10:10 | 1000.00 | 1000.00 | 1000.00 |
| 7 | 2014-02-10 10:10:10 | 1000.00 | 1000.00 | 2014-02-10 10:10:10 | 1000.00 | 1000.00 | 1000.00 |
| 8 | 2014-02-10 10:10:10 | 1000.00 | 1000.00 | 2014-02-10 10:10:10 | 1000.00 | 1000.00 | 1000.00 |
| 9 | 2014-02-10 10:10:10 | 1000.00 | 1000.00 | 2014-02-10 10:10:10 | 1000.00 | 1000.00 | 1000.00 |
| 10 | 2014-02-10 10:10:10 | 1000.00 | 1000.00 | 2014-02-10 10:10:10 | 1000.00 | 1000.00 | 1000.00 |

The records kept by a boleto-stealing botnet. Next to the date and time is the account of the intended recipient of the transfer; the "data alterada" column shows the accounts used by the thieves to accept diverted payments. "Valor" refers to the amount, expressed in Brazilian Real.

RSA notes that the miscreants responsible for the Bolware operation appear to have used just over 8,000 separate accounts to receive the stolen funds. That's roughly 7,997 more accounts than were used by the boleto bandits responsible for the diverted transactions in the boleto botnet control panel I discovered.

Researchers at RSA suggest that Brazilians who wish to transact in boletos online should consider using a mobile device to manage their boleto transactions, noting that boleto-thieving malware currently is not capable of altering the data stored in the barcode of each hijacked boleto order — at least for the time being.

"As the malware does not alter the barcode (for now), the safest approach is to use mobile banking applications available on smart phones (for now, immune to this malware) to read the barcode and to make payments," the company said in its report (PDF) on this crime wave.

FRAUDE AU CLIC – DES VARIANTES

25 Service Drains Competitors' Online Ad Budget

JUL 14



The longer one lurks in the Internet underworld, the harsher the reality that for nearly every legitimate business is an anti-business. Case in point: Today's online marketers exhaust the Google

AdWords is Google's paid advertising product, displaying ads on the top or the right side of your screen in search results. Advertisers bid on specific keywords, and those who bid the highest will have their ads show up first when Internet users search for those terms. In turn, advertisers pay Google a small amount each time a user clicks on one of their ads.

One of the more well-known forms of online ad fraud (a.k.a. "click fraud") involves Google AdSense publishers that automate the clicking of ads appearing on their own Web sites in order to inflate ad revenue. But fraudsters also engage in a practice where they try to attack competitors by running ads early in the day.

Enter "GoodGoogle," the nickname chosen by fraudsters operating on the Russian-language Internet. The software and hands-on customer service, created by a person whose name is not known, is used to click the appearance of competitors' ads.

"Are you tired of the competition in Google AdWords that take your first position and quality traffic,?" reads GoodGoogle's pitch. "I will help you get rid once and for all competitors in Google Adwords."



"Are you tired of the competition in Google AdWords that take your first position and quality traffic,?" reads GoodGoogle's pitch. "I will help you get rid once and for all competitors in Google Adwords."

(WebMoney, e.g.), and the seller offers support and a warranty for his work for the first three weeks.

Reached via instant message, GoodGoogle declined to specify how his product works, instead referring me to several forums where I could find dozens of happy customers to vouch for the efficacy of the service.

Nicholas Weaver, a researcher at the International Computer Science Institute (ICSI) and at the University California, Berkeley, speculated that GoodGoogle's service consists of two main components: A private botnet of hacked computers that do the clicking on ads, and advanced software that controls the clicking activity of the botneted computers so that it appears to be done organically from search results.

The service, which appears to have been in the offering since at least January 2012, provides customers both a la carte and subscription rates. The prices range from \$100 to \$1,000, small businesses can use GoodGoogle's software and service to sideline a handful of competitors's ads indefinitely. Fees are paid up-front and in virtual currencies (WebMoney, e.g.), and the seller offers support and a warranty for his work for the first three weeks.

but he also uses several Gmail accounts as points of contact. My guess is it will not be difficult for Google to shutter this operation, and possibly to identify this individual in real life.

<http://krebsonsecurity.com/2014/07/service-drains-competitors-online-ad-budget/>

CRYPTOLOCKERS

Actualités > Sécurité

Pris de remords, un hacker au bon cœur déchiffre les disques de ses victimes

Plégées par un Cryptolocker, les victimes ont pu retrouver leurs fichiers automatiquement il y a quelques jours. Le processus de déchiffrement était accompagné d'un message d'excuse.

Gilbert Kallenborn | 01net | le 04/06/15 à 11h24 | laisser un avis

J'aime 308 Recommander 308 Tweeter 57 +1 4



Voilà la preuve que certains pirates ont une âme et ne sont pas uniquement intéressés par l'appât du gain. La semaine dernière, un nouveau CryptoLocker commençait à se répandre sur la Toile et à chiffrer des disques durs. Mais le week-end dernier, l'auteur de ce malware, « Poka BrightMinds », a finalement changé d'avis. Dans un message publié sur [Pastebin](#), il explique être « désolé de ce qui s'est passé. Il n'a jamais été dans mon intention de publier ceci ». Puis il indique une adresse où les victimes pourront trouver leur clé de déchiffrement.

```
1 HI,
2
3 I am the author of the locker ransomware and I'm very sorry about that has happened. It was never my
4 intention to release this.
5
6 I uploaded the database to mega.co.nz containing "bitcoin address, public key, private key" as CSV.
7 This is a dump of the complete database and most of the keys weren't even used.
8 All distribution of new keys has been stopped.
```

Payment for private key

Choose a convenient payment method and click «Next»: **Bitcoin (most cheap option)**

bitcoin

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **2 BTC** to Bitcoin address [redacted] and specify the Transaction ID on the next page, which will be verified and confirmed.

[Home Page](#)
[Getting started with Bitcoin](#)

Time left
71 : 33 : 17

<< Back Next >>

BUGAT / DRIDEX



DRIDEX Infection Chain



DRIDEX arrives onto systems as malware downloaded by a malicious spam attachment.

The downloading is done through the malicious macro embedded in the .DOC attachment (detected as TROJ_WMSHELL.A).

Once DRIDEX is downloaded and installed, it injects malicious codes onto the system's browser, to steal online banking login credentials.

DRIDEX also performs form grabbing, screenshots and clickshots in order to steal more personal information from the affected system.

PRENONS UN PEU DE REcul



Javascript malveillant

- Sur des sites piratés
- Dans des bannières publicitaires



CLICKSOR



Exploit kits

Drive-by download

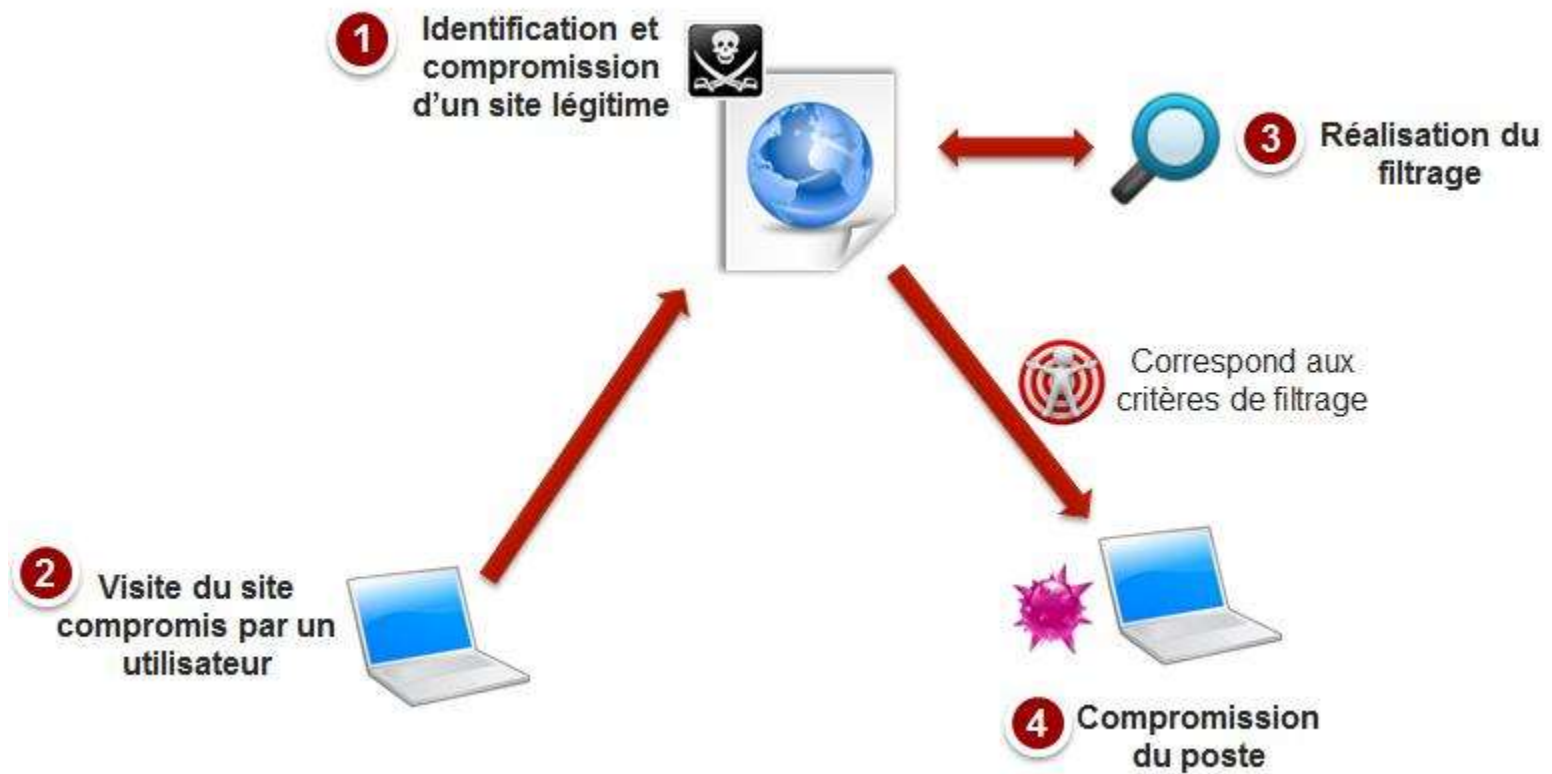


- Ransomware
- Autres malwares



Ticket de paiement
(+ données perso)

LE WATERHOLING – TECHNIQUE DU TROU D'EAU



AUTRES MODES DE DIFFUSION – PAR SMS

- <http://blog.fortiguard.com/android-malware-distributed-by-malicious-sms-in-france/>

• mato [REDACTED] Posté [REDACTED] 2012 - 08:53 #1

Newbie



Membre
1 messages
Marque: [REDACTED]
Modèle: STAR ADDICT

Bonjour,

Ce matin je reçois un message du 10052

*" Pour le bon fonctionnement de votre appareil, téléchargez la nouvelle mise à jours ANDROID Flash Player ci-dessous :
[http://tinyurl.com/\[REDACTED\]](http://tinyurl.com/[REDACTED])
"*

J'ai un [REDACTED] Star Addict, je ne sais pas si c'est un virus. Quand j'ai vérifié l'uri du téléchargement sa venait d'un serveur mail, et le whois me disait que sa venait d'arable.

Je les téléchargez puis je les ouvert on aurait dit une image flash. Puis je l'ai désinstaller.

J'ai des chances d'avoir un virus ?

Car les permissions, prenait le réseau envoyez des sms etc...

Merci beaucoup!

FRAUDE AUX PABX/IPBX

- **Autocommutateurs**

- De plus en plus exclusivement technologie IP

- **Box ADSL**

- Détournement « physique »
- Via l'interface web du client suite à hameçonnage

- **Détournement auprès de l'opérateur possible dans certains pays**

- **Usurpations de numéros**



LES PERSPECTIVES

• Quelles menaces pour demain?

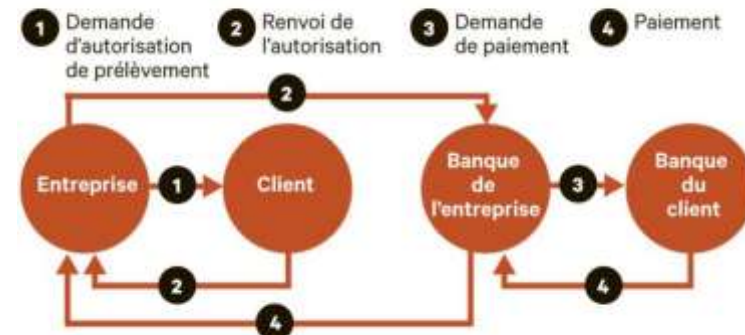
– Nouveaux services, nouvelles opportunités, aussi pour les délinquants, quelques exemples:

- Cloud computing et « big data »
- Cartes de paiement sans contact
- Internet des objets
- Prélèvements et virements SEPA
- Réseaux sociaux

– Poursuite de la professionnalisation

– Meilleure prise en compte des techniques d'évasion ou de camouflage

Le nouveau système de prélèvement SEPA



LES PERSPECTIVES

- **Quels besoins, évolutions nécessaires ?**
 - Développement de l'enquête sous pseudonyme
 - Notamment pour les atteintes aux systèmes de traitement automatisé de données, les escroqueries
- **Améliorer la prise en compte des plaintes et les contacts avec les victimes**
 - Développer la proximité, la réactivité et la collecte du renseignement directement auprès des victimes
- **Clarifier autant que de besoin le droit**
 - Définitions, procédures spéciales...
- **Renforcer les liens avec l'univers de la cybersécurité/cyberdéfense (public et privé)**

RAPPORT D'EUROPOL DE MARS 2015



<https://www.europol.europa.eu/content/massive-changes-criminal-landscape>

A service-oriented criminal underworld

The anticipated development of criminal networks engaged in 'traditional' organised crime activities, such as drug trafficking or the facilitation of illegal immigration, mirrors the evolution of criminal actors and criminal networks involved in cybercrime. Cybercriminals already operate as part of an online community which is complex and highly dynamic yet fragmented. Europol's iOCTA 2014 identifies crime-as-a-service as a key feature of the digital underground economy.

Data as a commodity

The increasing exploitation of Big Data and personal data will enable OCGs to carry out complex and sophisticated identity frauds on previously unprecedented levels.

For sale: your data

Nanotechnology and robotics

Nanotechnology and robotics will open up new markets for organised crime and deliver new tools for sophisticated criminal schemes.

The proliferation of virtual currencies

Virtual currencies increasingly enable individuals to act as freelance criminal entrepreneurs operating on a crime-as-a-service business model without the need for a sophisticated criminal infrastructure to receive and launder money.

E-waste

Without the necessary legislative and law enforcement responses, the illicit trade in e-waste is set to grow dramatically in the near future both in terms of quantities traded and the quality of the methods used by criminal actors engaging in this activity.

PRÉSENTATION DU THÈME

Témoignage

- **Caroline MARTIN**
Gérante de la société PLACE NET

FRC 2015 : ACTEUR AUJOURD'HUI OU VICTIME DEMAIN !

TABLES RONDES

- **Gestion d'une cyberattaque**
- **Usine 4.0 et objets connectés**
- **Sécurité des moyens de paiements**

TABLE RONDE 1

Gestion d'une cyberattaque



GESTION D'UNE CYBERATTAQUE

- **Daniel GUINIER**

Expert en cybercriminalité près la Cour pénale internationale de La Haye
Colonel (RC) de la Gendarmerie d' Alsace

- **Vincent HINDERER**

Directeur de mission - Expert cybersécurité
CERT LEXSI - Groupe LEXSI

- **Éric WIES**

Responsable du service informatique UFR MIM de l'université de Lorraine
Chef d'escadron (RC) de la Gendarmerie de Lorraine

GESTION D'UNE CYBERATTAQUE



Caractéristiques et dynamique d'une cyberattaque

Daniel GUINIER



CYBERATTAQUE : TENTATIVES DE DEFINITION

© 2015 D. Guinier

☐ Définition 2011 - *Cyber Security Strategy for Germany*

- "Attaque **informatique** préjudiciable à la sécurité **informatique** ..."

☐ Définition 2014 - *NATO AAP-06*

- "Action pour perturber, gêner, dégrader ou détruire l'information ... ou l'**ordinateur** et / ou le **réseau** lui-même"

Définitions très récentes encore orientées vers l'informatique ... comme il y a 25 ans.

Il s'agit en fait de la réalisation de **cybermenaces**, par l'exploitation de **vulnérabilités** de **cibles** constituées d'éléments du cyberspace, avec des **intentions malveillantes**, un préjudice pour les **victimes** et un avantage pour les **auteurs**.

Sans définition universelle et au vu de tentatives infructueuses, il paraît utile de comprendre ce qui constitue une cyberattaque.

CARACTERISTIQUES D'UNE CYBERATTAQUE

© 2015 D. Guinier

Attributs

Auteurs
Motifs
Buts
Compétences

Entité

Origine

Destination

Victimes
Cibles
Impacts
Compétences

Haut niveau

Hiérarchie

Intentions
Objectifs
Méthodes
Techniques
Outils
Vecteurs

Opérations

Poursuites

Plaintes
Qualifications
Enquête
Instruction
Expertise
Jugement

Bas niveau

Les options relèvent d'un catalogue structuré mis à jour.

DYNAMIQUE D'UNE CYBERATTAQUE

© 2015 D. Guinier

1 : Renseignement

Phase de préparation

Choix victime, recueil d'infos, scans :
adresses IP, ports, hôtes, etc.



2 : Conception

Stratégie d'infiltration, argumentaire "*digne de confiance*",
acquisition ou création de l'outil adéquat, test, validation



3 : Infiltration

Phase d'exécution

Distribution du code malveillant, redirection
vers serveur de l'attaquant : *Web, C2, infiltration*



4 : Exploration

Le "**kit d'exploit**" explore la cible pour trouver des **vulnérabilités** et ainsi pouvoir
former de **nouvelles portes d'entrée** avec **des outils plus avancés**



5 : Collecte

Le logiciel malveillant installé **collecte des infos** pour disposer de plus de
privileges, **apparaître comme légitime** et **établir la persistance**.



6 : Contrôle & commande

Liaison avec un **serveur de contrôle et commande (C2)**, permettant à
l'attaquant de **donner des instructions** et de **maintenir la persistance**



7 : Action

Action dissimulée possible : **contrôle des flux**, **exfiltration**, **effacement des traces**,
compromission avancée et **maintien de façon dormante**



8 : Crise



Phase de découverte - Phase de maîtrise

Mise en veille
ou retrait

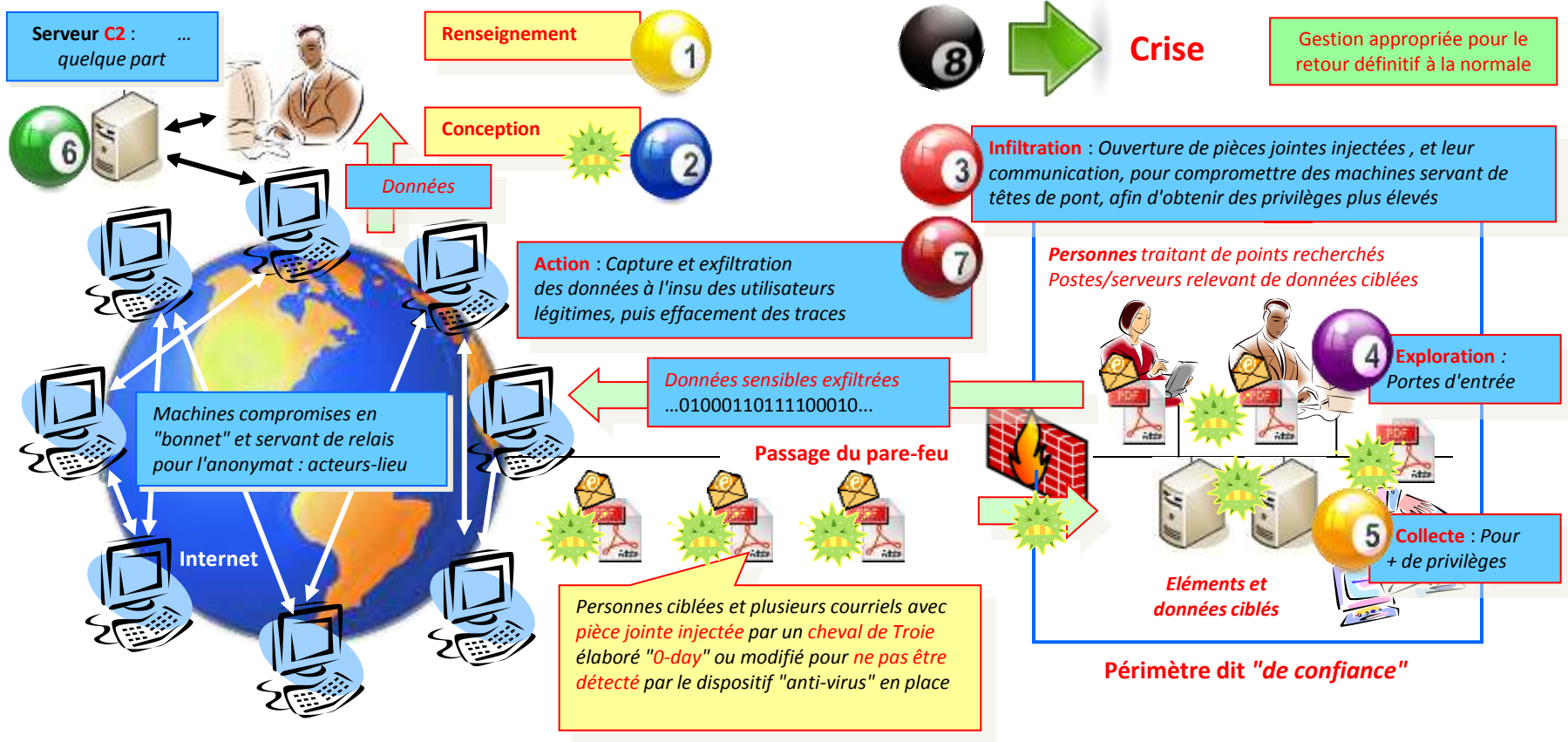
Gestion
de la crise

VOS DONNEES SONT VOLEES ... A VOTRE INSU

© 2012-2015 D. Guinier

Art. 323-3 du CP : Extraction et transmission frauduleuse de données
Art. 226-4-1 al. 2 du CP : Usurpation d'identité numérique

C2 : Contrôle & Commande

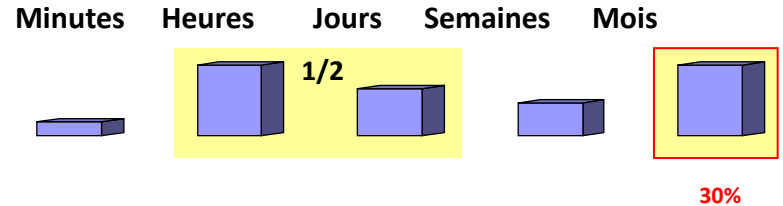


DELAIS USUELS D'UNE CYBERATTAQUE



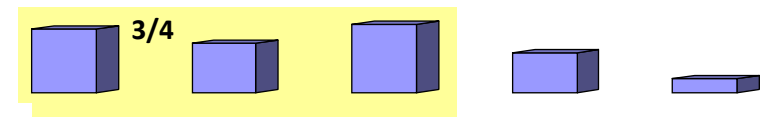
Auteurs

Délai de préparation



Délai d'exécution

Se prolonge jusqu'au retour à la normale



Victimes

Délai de découverte

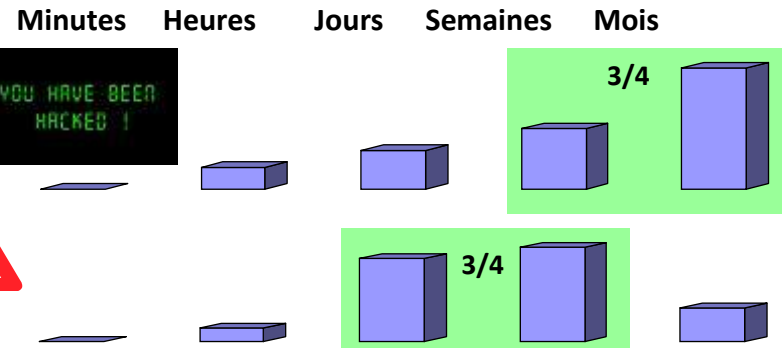
Moyen : 7,5 mois - Max. > 6 ans

Source : 2014 Mandiant Threat Report

Poursuites

Délai de maîtrise

Fin de crise lors du retour à la normale



Etat de crise

Etat de post-crise

Poursuites

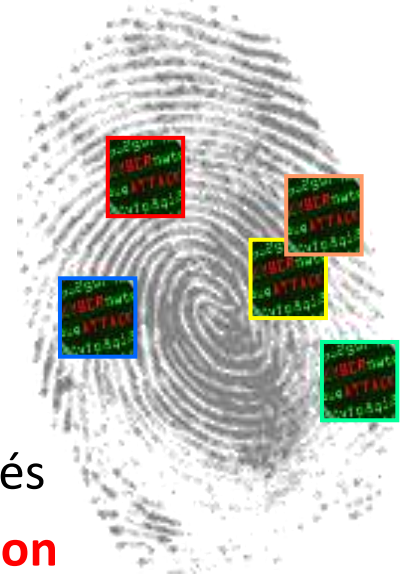
Année(s)

CONCLUSION

© 2015 D. Guignier

- **Le modèle** proposé montre qu'une cyberattaque peut être
 - **complètement caractérisée** par un tel catalogue et sa dynamique
 - **déTECTABLE à toute étape** pour obliger l'attaquant à revoir sa stratégie

- **Les traces** d'une cyberattaque forment des indices
 - **présents** dès les premières étapes, pour **la détection**
 - **observables** par la surveillance d'anomalies
 - **identifiables** par événements enregistrés et rémanence
 - **fragiles** et volatiles, à fixer au plus tôt de façon *ad hoc*
 - **analysables** avec des compétences et des outils appropriés
 - **corrélables** avec d'autres signaux faibles, pour **la prédiction**



Les éléments atteints constituent aussi une scène de crime avec de précieux indices sous forme de traces numériques à protéger.

"Nul ne peut agir sans laisser des marques multiples de son passage"

"Principe de Locard" - Dr. Edmond Locard (1877-1966)

GESTION D'UNE CYBERATTAQUE



Réaction à une cyberattaque, les bonnes pratiques en situation de crise

Vincent HINDERER



CRISES CYBER : RESPONSE = ! HANDLING

❑ Des crises (un peu) spécifiques

- Crise cyber = incident(s) grave(s), exploitant outils IT et/ou contre le(s) SIG/SII
- Souvent absent des risques identifiés => facteur de stress
- Impact productivité, image voire survie de l'entreprise
- Risque médiatique difficile à contrôler (effet Streisand, etc.)
- Attribution et condamnation complexes

❑ Différents acteurs pour Réponse vs. Gestion

- Rôles distincts
- Personnes distinctes (selon incident, taille entreprise, etc.)
- Compétences / profils distincts
- Accès / outillage distincts
- ...



INCIDENT HANDLING (IH) : OBJECTIFS



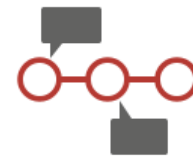
Objectifs

- Coordination et Planning de la réponse
- Communication: Liaison et Reporting
PoC interne (Direction, experts...)
et externe (fournisseur, autorités...)
- Logistique et scribe : i.e. outils, notes, synthèse, timeline...



Rappel : l'Incident Command System (US)

- Chaîne de commande unique
- Terminologie commune
- Objectifs -> Stratégies -> Tactiques
- Flexible et modulaire
- Etendue du contrôle (« span of control »)



IH : ORGANISER LA CELLULE DE CRISE



Cas particulier : quid si plus de confiance dans le SI ?

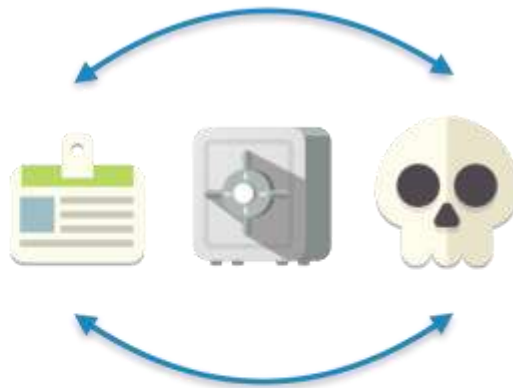
INCIDENT RESPONSE (IR) : OBJECTIFS

❑ Objectifs : mener les actions techniques

- D'analyses et investigations (dont forensics)
- De collecte et sauvegarde des preuves
- D'endiguement, de mitigation et de correction



Prepare



Respond



Restore



Learn

IR : QUELQUES PRÉCEPTES

☐ Poser les bonnes questions

- **When** : attaque ou non ? date de détection ? attaque encore en cours ?
- **What** : nature et criticité de l'incident ?
- **Where** : assets et services impactés ?
- **How** : déroulé de l'attaque ? incidents similaires ? concomittants ? préalables ?
- (**Who** : origine de l'attaque = le moins important)

☐ Rappel : bonnes pratiques en cas de compromission

- NE PAS SE PRECIPITER !
- Vérifier et respecter les processus
- Suivre les bonnes pratiques
- Se faire aider (expert, avocat, huissier, forces de l'ordre...)



IR : SAUVEGARDE DES PREUVES

☐ Sauvegarder : pendant analyse et containment

- **Prévenir** : informer les parties prenantes (internes et externes)
- **Légitimer** : types de preuve vs. actions envisagées (témoins, huissier, etc.)
- **Consigner** : conserver un déroulé des actions daté, authentifié
- **Stocker** : conservation physique, hors ligne, artéfacts et éléments de preuve
- **Porter plainte** : protéger l'entreprise et enclencher démarches (gel des données)

☐ Rappel : copie de disque

- NE PAS ETEINDRE LA MACHINE !
- déconnecter du réseau (attention aux *smartphones*)
- utiliser bloqueurs en écriture
- effectuer des copies multiples (au moins deux)
- faire intervenir un expert et/ou huissier (selon le cas)



RÉACTION CYBERATTAQUE : SYNTHÈSE

60% de préparation



Processus

Inventaire

Classification

Logs

Contacts

Simulation

...



30% de gestion d'incident



Coordination

Réponse

Surveillance

Amélioration continue

10% de chance !

The background features a light blue world map with a grid overlay. Binary code (0s and 1s) is scattered across the top and left sides. A white rectangular box with clipped corners is centered on the page.

Se protéger des menaces connues

SE PROTÉGER DES MENACES CONNUES

MENACES INFORMATIQUES

- **Malware**

- Mise à jour (système et applications)
- Anti-virus, pare-feu, outils de sécurité

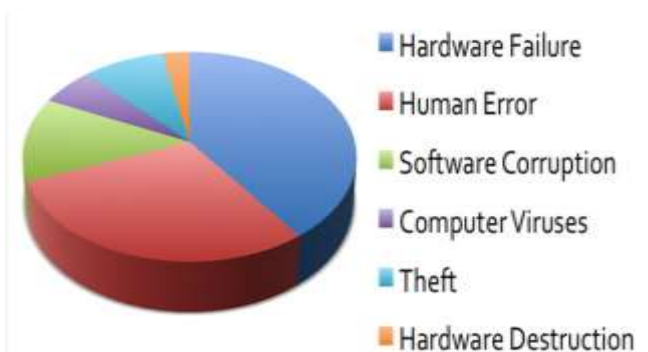
- **Perte de données**

- Sauvegarde, PRA/ PCA

- **Intrusion sur les réseaux**

- **Utilisation frauduleuse d'un poste de travail**

- **Accès illicite aux données**



SE PROTÉGER DES MENACES CONNUES AUTRES MENACES

- **Atteinte à l'image**
 - Photos, vidéos volées
- **Menace sur les personnes**
 - Utilisation du Web pour trouver des personnes
- **Rançons**
 - Virus "gendarmerie"
 - Cryptlocker
- **Ordre de virement**
 - Utilisation de renseignement pour détournement



The background features a light blue world map with a grid overlay. Scattered across the map are various binary strings (0s and 1s) in different colors and sizes, creating a digital or data-themed aesthetic. The text is centered within a white, rounded rectangular box.

Se protéger des menaces inconnues

SE PROTÉGER DES RISQUES INCONNUS

- **Localiser ses données**
 - Poste de travail
 - Photocopieur
 - Cloud
- **Connaître ses processus**
 - Qui a accès à quoi
 - Qui a le droit de faire quoi, et dans quelles circonstances
- **Connaître ses collaborateurs**
 - Quand ils arrivent ... et quand ils partent !



EVITER LA CYBERATTAQUE

- **Sensibilisation**
 - A tous les étages de l'entreprise
- **Maintenir la vigilance**
 - Visiteurs ? Sondages ?
 - Nouveau processus ?
 - Mails douteux ?
- **Obtenir un comportement**
 - minimisant les risques
- **Maintenir un système d'information à jour !**



GESTION D'UNE CYBERATTAQUE



QUESTIONS
RÉPONSES

TABLE RONDE 2

Usine 4.0 et objets connectés



USINE 4.0 ET OBJETS CONNECTÉS

- **Adjudant Chef Patrick WOLFERT**

Enquêteur en Nouvelles Technologies, Cellule d'identification criminelle,
Bureau Départemental de Renseignements et d'Investigations Judiciaires

- **Cécile DOUTRIAUX**

Avocate au barreau de Strasbourg

Chef d'Escadron (RC) de la Réserve Citoyenne de la Gendarmerie

Membre de la Chaire Cyberdéfense et Cybersécurité des écoles de Saint-Cyr Coëtquidan

- **Jean Christophe MATHIEU**

Responsable sécurité des solutions et produits Siemens France

- **Cédric LEVY-BENCHETON**

Expert en réseau et sécurité de l'information à l'ENISA

USINE 4.0 ET OBJETS CONNECTÉS

Les supports nomades

Adjudant Chef Patrick WOLFERT

LA FRAGILITÉ DES DONNÉES STOCKÉES

- Des solutions d'extraction et d'analyse des données stockées dans les outils nomades existent.
- Elles peuvent être soit logicielles ou matérielles.
- Les données récupérées donnent des informations pouvant avoir un impact grave voire dramatique sur la sécurité.
- La localisation d'un objet ou d'un lieu devient facile, mais plus encore...



Information de hachage d'image

⚠ Aucune information de hachage de référence n'est disponible pour ce projet.















Calculer

Infos appareil

| | | | |
|---------------------------------|--|-----------------|--|
| Apple ID | s600_w221@mail.ru | Apple ID | mamuka2221@mail.ru |
| Last Used ICCID | 8933250010062649330 | ICCID | 8933250010062649330 |
| Phone Number | 33106836933 | | |
| Fonction modem | | | |
| Heure de la dernière activation | 26/05/2015 23:28:03(UTC+0) | | |
| Interfaces réseau | | | |
| IP réseau Internet | 185.13.106.92:58930 at 2015-05-31 14:57:34 | IP réseau local | 10.110.191.20:58930 at 2015-05-31 14:57:34 |
| iPhone (2) | | | |
| ICCID | 8933250010062649330 | Device Name | iPhone (2) |
| Product Version | 8.2 | Display Name | iPhone (2) |
| IMEI | 355902060669221 | Phone Number | +33 1 06 83 69 33 |
| Serial Number | C34NL3LDG5MN | Product Type | iPhone2,2 |
| Unique Identifier | 81022FC2783D77380C2B00F55ECC15515554F7CE | Product Name | iPhone 6 |
| Is Encrypted | False | | |

Infos appareil :

Données de téléphone

| | | | | | | | | |
|--|--|--|---|--|---|--|--|--|
| Applications installées  35 (0) | Calendrier  40 (8) | Chaînes modelées  1 (1) | Chats  24 (15) | Comptes d'utilisateur  17 (0) | Contacts  237 (23) | Cookies  851 (17) | Historique Web  130 (0) | Journal des appels  235 (1) |
| Messages MMS  1 (1) | Messages SMS  28 (15) | Notes  5 (2) | Réseaux sans fil  25 (0) | Signets Web  10 (1) | | | | |

Fichiers de données

| | | | | | |
|---|--|--|--|---|--|
| Audio  1 (0) | Bases de données  117 (0) | Configurations  691 (0) | Images  322 (0) | Texte  2 (0) | Vidéos  4 (0) |
|---|--|--|--|---|--|

Rechercher dans le tableau ✕ Avancé

| ✓ | # | ☆ | ✖ | 📄 | Heure de création | Heure de modification | Titre | Corps |
|---|---|---|---|---|----------------------------|----------------------------|-------------------------|--------------------------------|
| ✓ | 1 | | | | 24/05/2015 09:17:57(UTC+0) | 24/05/2015 16:43:14(UTC+0) | C | C |
| ✓ | 2 | | | | 31/03/2015 23:54:21(UTC+0) | 31/03/2015 23:55:07(UTC+0) | 078905 | <div> </div><div> </div> |
| ✓ | 3 | | | | 10/03/2015 20:41:34(UTC+0) | 17/04/2015 19:49:11(UTC+0) | Mail-Mamuka2221@mail.ru | Mail-Mamuka2221@mail.ru<div>st |
| ✓ | 4 | | 🚫 | | | | | Mail-Mamuka2221@mail.ru<div>st |
| ✓ | 5 | | 🚫 | | | | | local://local/store |

Éléments : 5/5 Sélectionné : 5

Note Aller à ▾

Titre: Mail-Mamuka2221@mail.ru
Heure de création: 10/03/2015 20:41:34(UTC+0)
Heure de modification: 17/04/2015 19:49:11(UTC+0)
Source:

Synthèse 🗑️ 📄

Corps 🗑️ 📄 **HTML** Texte

Mail-Mamuka2221@mail.ru
s600221

iD-Ss600221

Skype- mamuka2221
s600221

Почта: mamuka_akob

Pièce jointe

Carte

Position:
Adresse:
Adresse sur la carte:



Rechercher dans le tableau Avancé

Emplacements (6)

| | | | |
|----|---|---------------------|-----------------------|
| 49 | ? | 06/02/2015 16:57:56 | (48.582358, 7.744869) |
| 50 | ? | 06/02/2015 16:57:56 | (48.582358, 7.744869) |
| 51 | ? | 06/02/2015 16:57:33 | (48.582386, 7.744828) |
| 52 | ? | 06/02/2015 16:57:33 | (48.582386, 7.744828) |
| 53 | ? | 06/02/2015 16:57:32 | (48.582386, 7.744828) |
| 54 | ? | 06/02/2015 16:57:32 | (48.582386, 7.744828) |

Emplacement Aller à ▾

Nom: FullSizeRender.jpg
 Description:
 Type:
 Horodateur: 06/02/2015 16:57:32
 Précision:
 Confiance:
 Carte:
 Catégorie: Emplacements des fichiers multimédia

Source

Images Aller à ▾

Détails Événements (0)

48° 34' 59.57" N 07° 44' 40.52" E
Cartes en ligne
100 m

SÉCURISER L'INFORMATIQUE MOBILE

- Chiffrement des données stockées.
- Sécuriser les terminaux mobiles / Verrouillage des appareils.
- Prévoir régulièrement des purges de données non utilisées.
- Utiliser un stockage dématérialisé.

USINE 4.0 ET OBJETS CONNECTÉS

Les objets connectés

Maître Cécile DOUTRIAUX

ÉTAT DES LIEUX

- **Chiffres :**

15 milliards d'IdO en 2015, 50/80 milliards en 2020

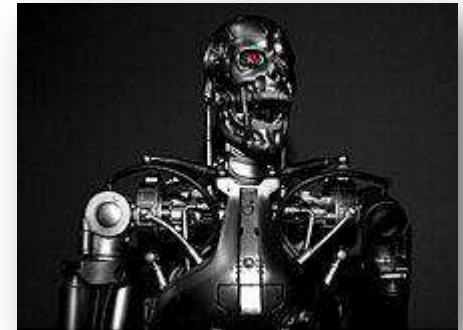
- **Quelle confiance pour les Objets connectés ?**

78% des français inquiets pour leur vie privée

- **Enjeux juridiques et éthiques :**

Un nouveau paradigme de société ?

- **IdO : opportunité ou danger ?**



DES OPPORTUNITÉS POUR LES ENTREPRISES PRODUCTRICE OU UTILISATRICE D'OBJETS CONNECTÉS

- Adaptation de l'offre à la demande des clients
- Une meilleure connaissance du parc industriel
- Un suivi en temps réel des moyens de production : maintenance et réparations

→ Gains de productivité et économies



DES RESPONSABILITÉS ACCRUES POUR LES ENTREPRISES

- **En cas de dommage causé par l'objet connecté : qui est responsable ?**

- Le gardien (1384 Code Civil)
- Le fabricant (1386-1 Code Civil)

L'entreprise responsable des données
personnelles

(Loi n°78-17 du 6 janvier 1978)



DES OPPORTUNITÉS POUR LES SALARIÉS

- Plus de sécurité sur les chaînes de production
- Optimisation du geste métier
- D'avantage de gains
- Un nouveau levier de bien-être au travail ?



DES NOUVEAUX RISQUES POUR LES SALARIÉS

- Analyse des performances ou surveillance ?
- Un dispositif déclaré, justifié et proportionné avec une information collective et individuelle des salariés (Code du travail)
- Consentement ou abus de pouvoir ?
(Loi 78-17 du 6 janvier 1978)



CONCLUSION ET PERSPECTIVES

instaurer la confiance pour assurer le développement des Objets connectés

- Impact du règlement européen des données personnelles sur les objets connectés ?
- Un droit à la « désactivation des puces »?



USINE 4.0 ET OBJETS CONNECTÉS

Analyse des menaces IoT vue par l'ENISA

Cédric LEVY-BENCHETON

USINE 4.0 ET OBJETS CONNECTÉS



QUESTIONS
RÉPONSES

8ÈME FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES



TABLE RONDE 3

Sécurité des moyens de paiement en ligne



SÉCURITÉ DES MOYENS DE PAIEMENT EN LIGNE

- **Ludovic HAYE**

Consultant IT à l'international

Chef d'Escadron (RC) de la Gendarmerie d'Alsace

- **Jean-Luc DELANGLE**

Conseiller au CREOGN

Lieutenant Colonel (RC) de la Gendarmerie d'Ile de France

SÉCURITÉ DES MOYENS DE PAIEMENT EN LIGNE

La sécurité des moyens de paiement

Ludovic HAYE

SÉCURITÉ DES MOYENS DE PAIEMENT EN LIGNE

- Introduction
- Les différents moyens de paiement
- Les dangers potentiels
- Les bonnes pratiques et les nouveautés
- Conclusion



LES DIFFERENTS MOYENS DE PAIEMENT

- **Payer en ligne par carte bancaire**
- **Par e-carte bleue**
- **Les tiers de confiance: Google Checkout ou Paypal**
- **Les autres modes de paiement (Bitcoin, téléphone surtax., chèques etc.)**
- **Les bonnes pratiques**

LES DANGERS POTENTIELS

- PHISHING
- FOVI
- Usurpation d'identité
- Risques partagés
- Les inéluctables :
(site malhonnête, vol a posteriori
des fichiers clients, poste d'achat infecté, ...)



LES BONNES PRATIQUES ET LES NOUVEAUTES

- Sites qui inspirent confiance (label)
- Ne jamais transmettre ses coordonnées bancaires
- En https (cadenas) avec activation du cryptage
- Préférez les URL de vos favoris plutôt qu'un e-mail
- Utilisez les rubriques “Mon compte – Mon espace”
- Etui de carte anti-NFC
- **SIGNALEZ tout site / mail qui vous parait suspect.**

(<https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action>)



LES PROTECTIONS

- Les navigateurs anti-phishing (Firefox, OpenDNS)
- Le SSL (Secure Socket Layer) Crypt + certif
- Le 3D secure (AFC)
- Les cartes à cryptogrammes dynamiques
- Authentification vocale



CONCLUSION

**Plus de 7 Millions de
Victimes d'actes de
Cybercriminalité !**

AGISSONS !

**NE CÉDEZ PAS
AU CHANTAGE !** NE FAÎTES PAS
DE VIREMENT
INTERNATIONAUX

**VOUS N'AVEZ PAS
GAGNÉ AU LOTO !**

**UNE VIDÉO SUR INTERNET
PEUT ÊTRE RETIRÉE !**

**ÉVITEZ WESTERN UNION
ET LES MANDATS CASH**



SÉCURITÉ DES MOYENS DE PAIEMENT EN LIGNE

Les monnaies virtuelles et les bitcoins

Jean-Luc DELANGE

LE BITCOIN

- **Est-ce une monnaie ?**
- **Des avantages espérés**
- **Des risques avérés**
- **Un intérêt pour le monde criminel**

VOLATILITÉ DU BITCOIN

(BTC en € - source www.bitcoincours.com)

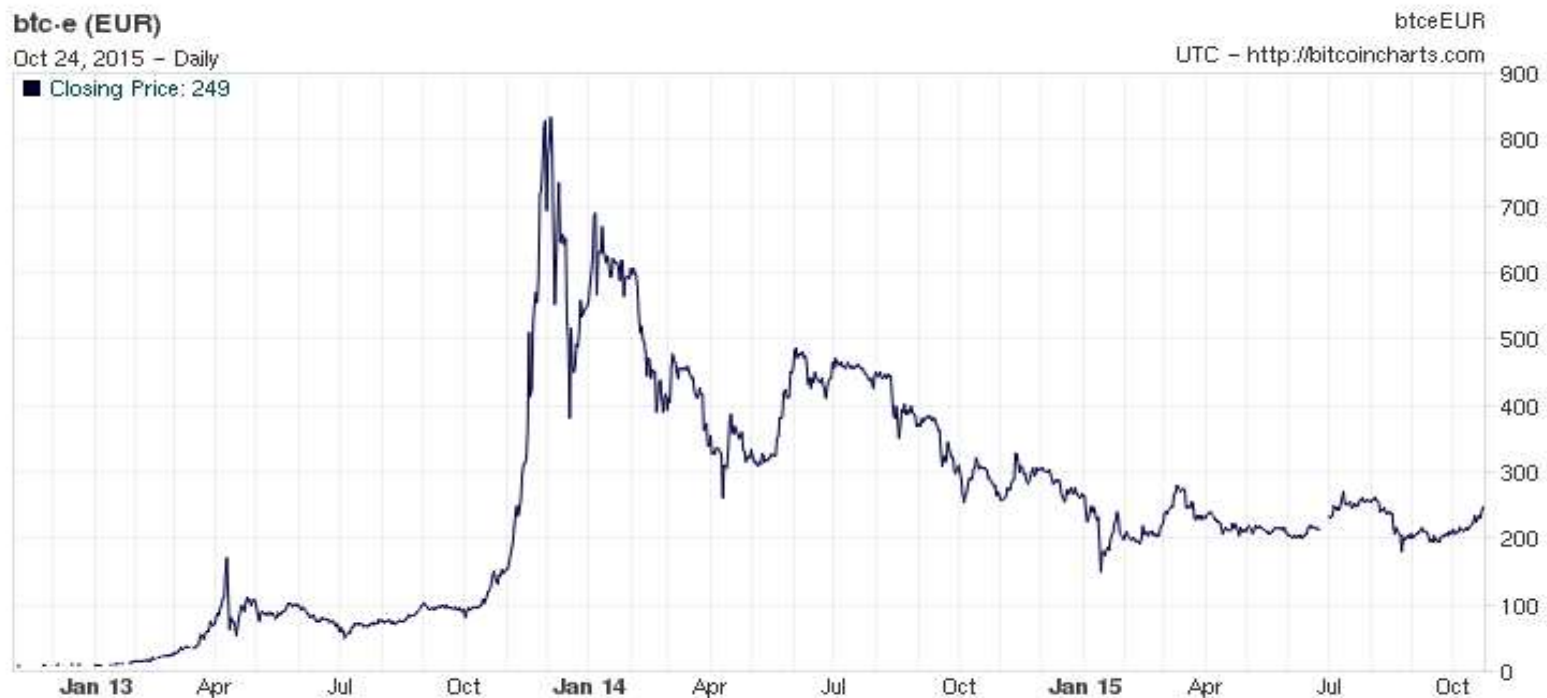
cours du bitcoin historique depuis fin 2011 | BTC EUR

[M](#) [e](#) [t](#) [f](#) [p](#) [G+](#) +2. Recommander ce contenu sur Google

btc-e (EUR)

Oct 24, 2015 - Daily

■ Closing Price: 249



SÉCURITÉ DES MOYENS DE PAIEMENT EN LIGNE



QUESTIONS
RÉPONSES



CONFÉRENCE DE CLÔTURE

- **Marc WATIN AUGOUARD**

Ancien inspecteur général des armées

Directeur du centre de recherche de l'école des Officiers de la Gendarmerie Nationale

LE SALON EUROPÉEN DE LA CONFIANCE NUMÉRIQUE



8^{ème} Forum International de la Cybersécurité – FIC 2016

La sécurité des données

Le 25 et 26 janvier 2016



REMERCIEMENTS

- L'association AD HONORES Réseau Alsace



REMERCIEMENTS : L'ÉQUIPE

LT Nadia BOUGHANI

Cécile DOUTRIAUX

Emmanuelle HAASER

Perle KREBS

Daniel GUINIER

Ludovic HAYE

Johan MOREAU

Philippe WITTIG

Didier SCHERRER

Éric WIES

LCL Olivier CAPELLE



REMERCIEMENTS

- **L'équipe de l'INEDIT THEATRE**

Camille COMPARON

Marko MEYERL

- **L'illustrateur**

Laurent SALLES

FICHE D'ÉVALUATION



Prénom :

Nom :

Fonction :

Entreprise :

Accueil

Je suis satisfait des conditions d'accueil du forum :

++ + - --

Table ronde « Gestion d'une cyberattaque »

Ce sujet est utile à l'exercice de mon métier :

J'ai trouvé réponse à mes questions :

Table ronde « L'usine 4.0 et objets connectés »

Ce sujet est utile à l'exercice de mon métier :

J'ai trouvé réponse à mes questions :

Table ronde « Sécurité des moyens de paiement en ligne »

Ce sujet est utile à l'exercice de mon métier :

J'ai trouvé réponse à mes questions :

Bilan Global

J'apprécie que des supports pédagogiques me soient fournis à l'issue du forum :

Je suis globalement satisfait de ce forum sur les cybermenaces :

Ce forum a répondu à mes attentes :

Je recommanderai ce forum à mon entourage :

J'ai participé au forum l'année dernière ?

oui non

Si oui, j'ai mis en place une (des) action(s) de prévention dans votre entreprise ?

oui non

Lesquelles ?

Je souhaite voir noter au 9^{ème} forum en 2016, le(s) thème(s) suivant(s) :

Merci de renvoyer ce document complété lors de votre visite de la salle.
Les informations demandées sont à destination exclusive de l'équipe de l'organisation du forum.

FRAC 2015

RENDEZ-VOUS

**9^{ème} Forum du Rhin Supérieur
sur les Cybermenaces**

8 novembre 2016

www.frc.alsace