FRC 2015
8ème édition

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

AD HONORES
Réseau ALSACE

8ème FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

www.frc.alsace

8ÈME FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

2009

2010

2011

2012

2013

2014

2015

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

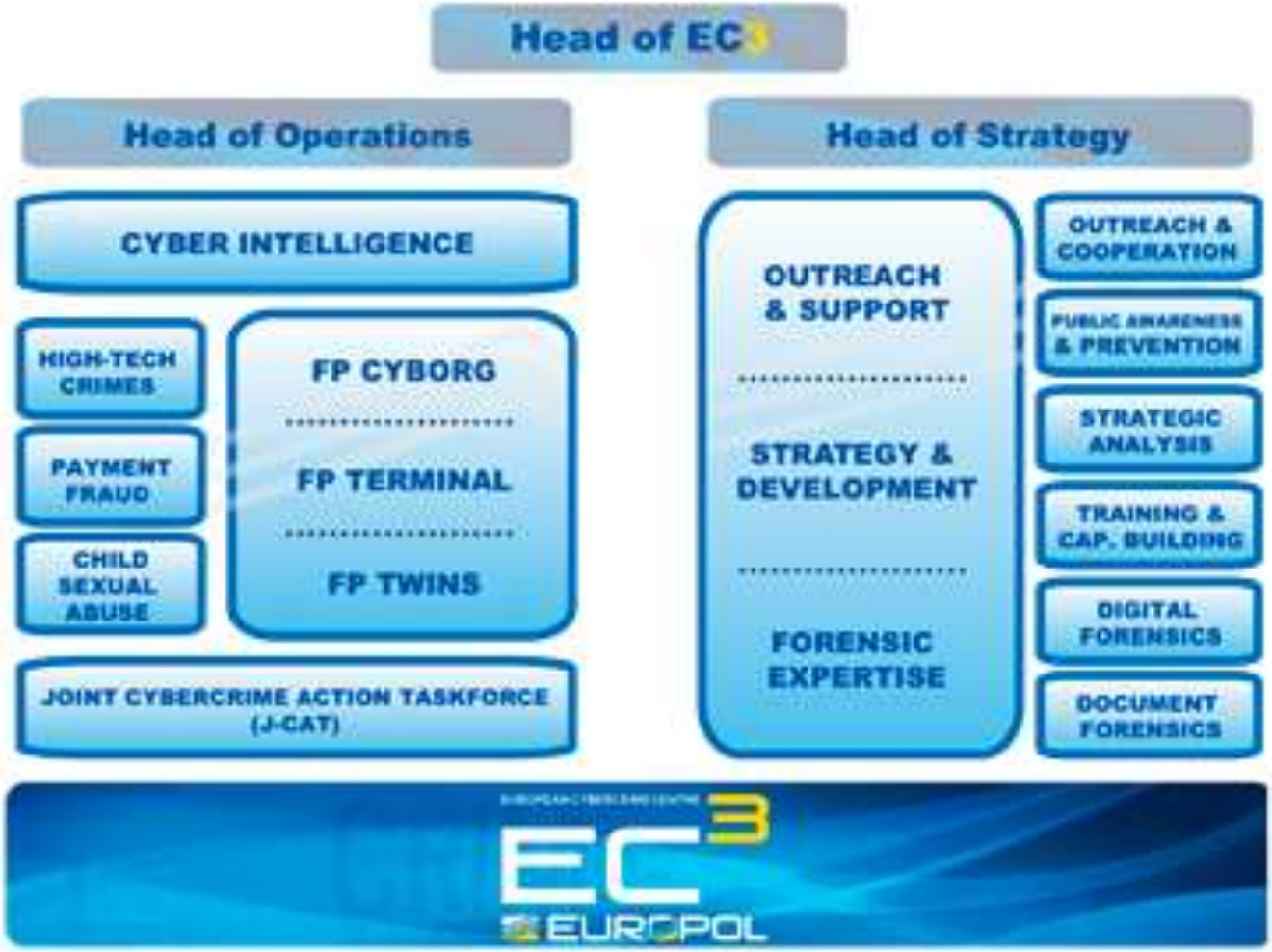
- Rappel sur les acteurs
- Considérations générales
- Nouvelles formes d’organisation criminelle
- Focus sous l’angle des botnets
- Perspectives

SERVICES DE LUTTE CONTRE LA CYBERCRIMINALITÉ

Investigateurs en cybercriminalité (ICC)

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

EUROPOL EC3


Head of EC3
Head of Operations
Head of Strategy
CYBER INTELLIGENCE
HIGH-TECH CRIMES
PAYMENT FRAUD
CHILD SEXUAL ABUSE
FP CYBORG
FP TERMINAL
FP TWINS
JOINT CYBERCRIME ACTION TASKFORCE (J-CAT)
OUTREACH & SUPPORT
STRATEGY & DEVELOPMENT
FORENSIC EXPERTISE
OUTREACH & COOPERATION
PUBLIC AWARENESS & PREVENTION
STRATEGIC ANALYSIS
TRAINING & CAP. BUILDING
DIGITAL FORENSICS
DOCUMENT FORENSICS
EC3
EUROPOL

INTERPOL IGCI

THE INTERPOL GLOBAL COMPLEX FOR INNOVATION

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

▸ 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

Est européen et local

Poseurs

Mules

International

Copie de cartes bancaires *skimming*

Électroniciens

Copie de données bancaires ou autres identifiants / données sensibles

Escroquerie au commerce électronique

Attaquants isolés

Parfois très « local »

Accès frauduleux

Crime organisé

Escroqueries à l'avance de frais

Botnets

Déni de service

Scareware, ransomware...

Escrocs isolés

Script-kiddies

Logiciels malveillants

Développeurs

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

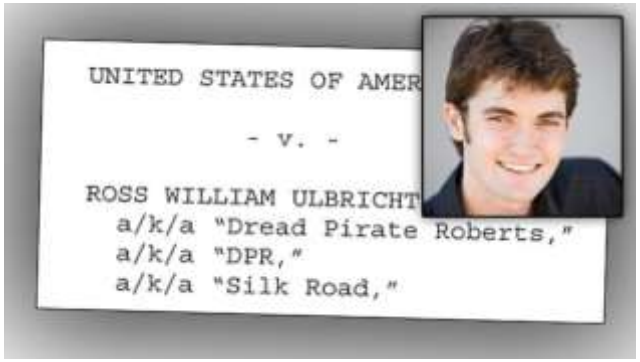
AUTOUR DES CARTES BANCAIRES

- **Virus contre terminaux de point de vente (TARGET)**
  - Kit BlackPos serait développé par un jeune russe de 17 ans (ree4 / Sergey Taraspov) selon IntelCrawler

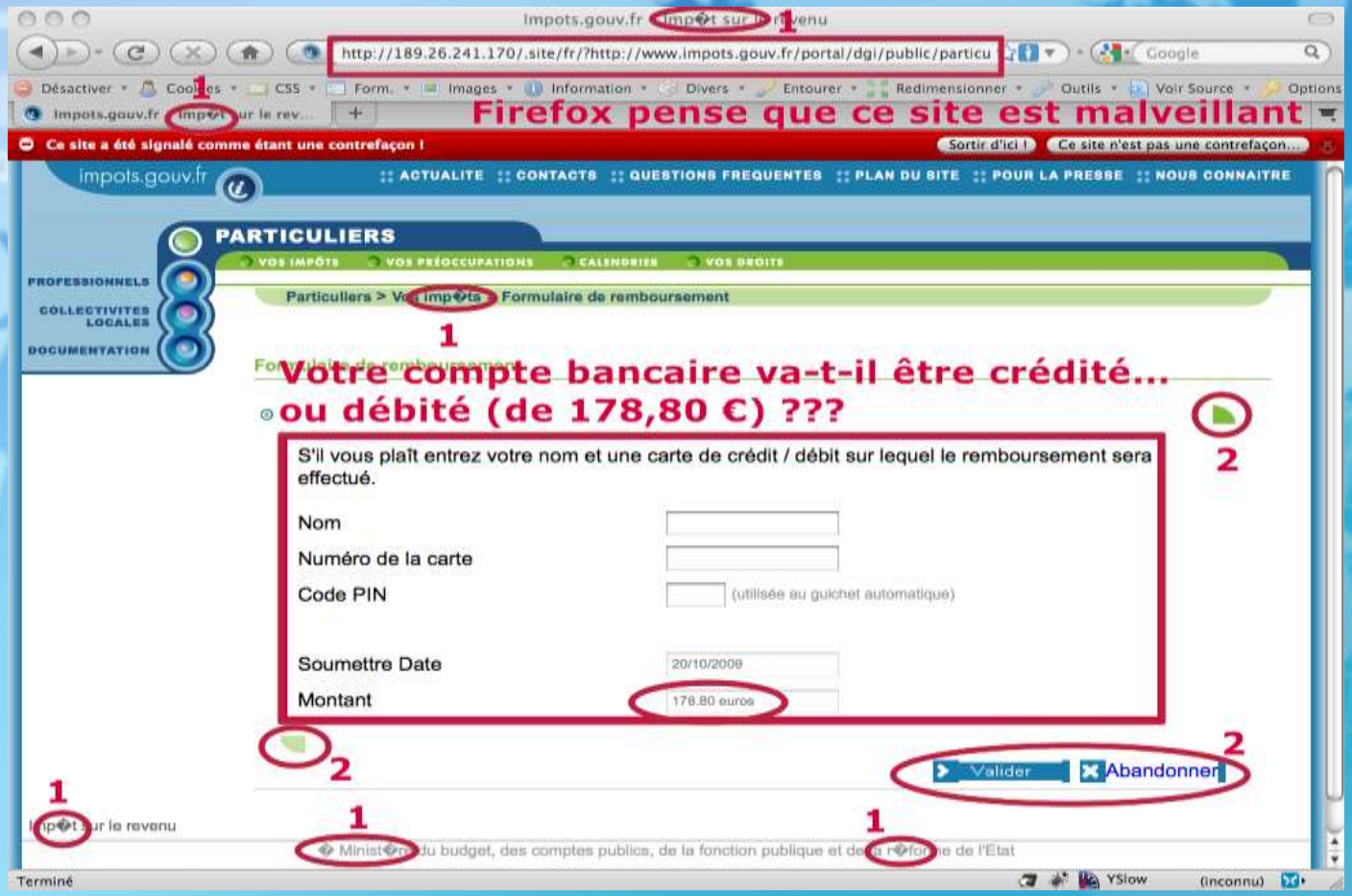
- **Virus installés dans des DAB pour les vider (Cf. CCC)**

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…

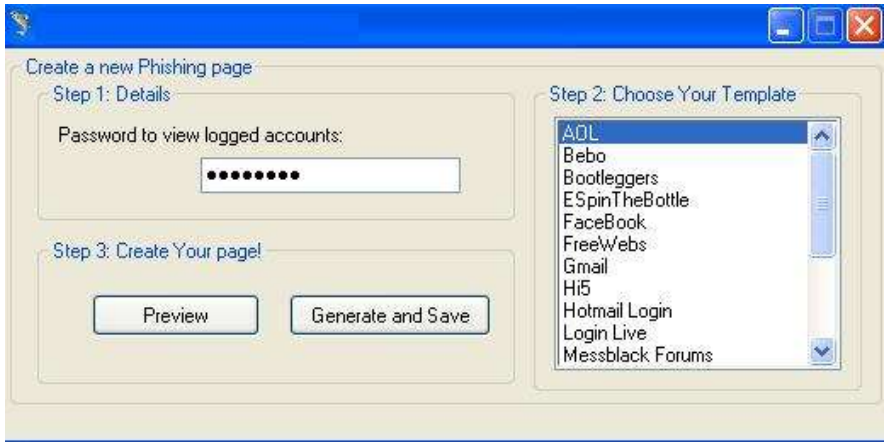


HAMEÇONNAGE PROVENANT DES IMPÔTS



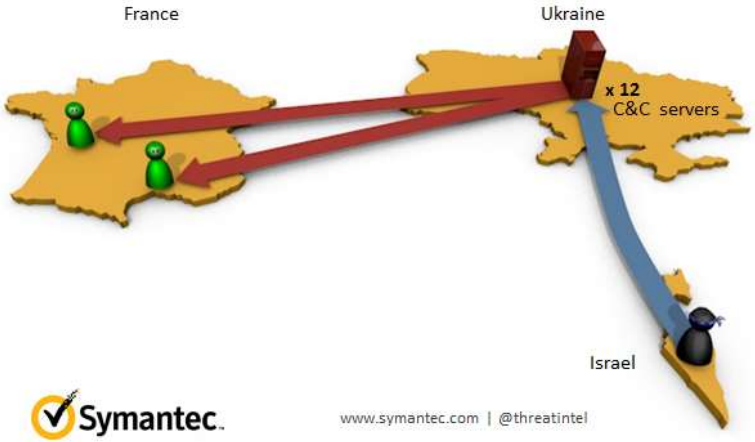
HAMEÇONNAGE

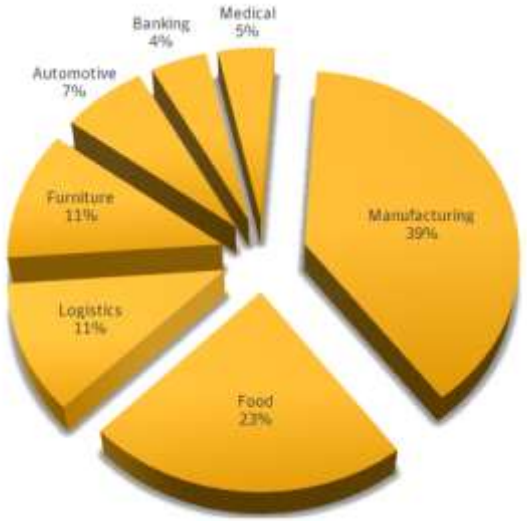
- Kits (achat, gratuit…)
- Hébergement des pages
- Diffusion des messages
- Revente des données



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

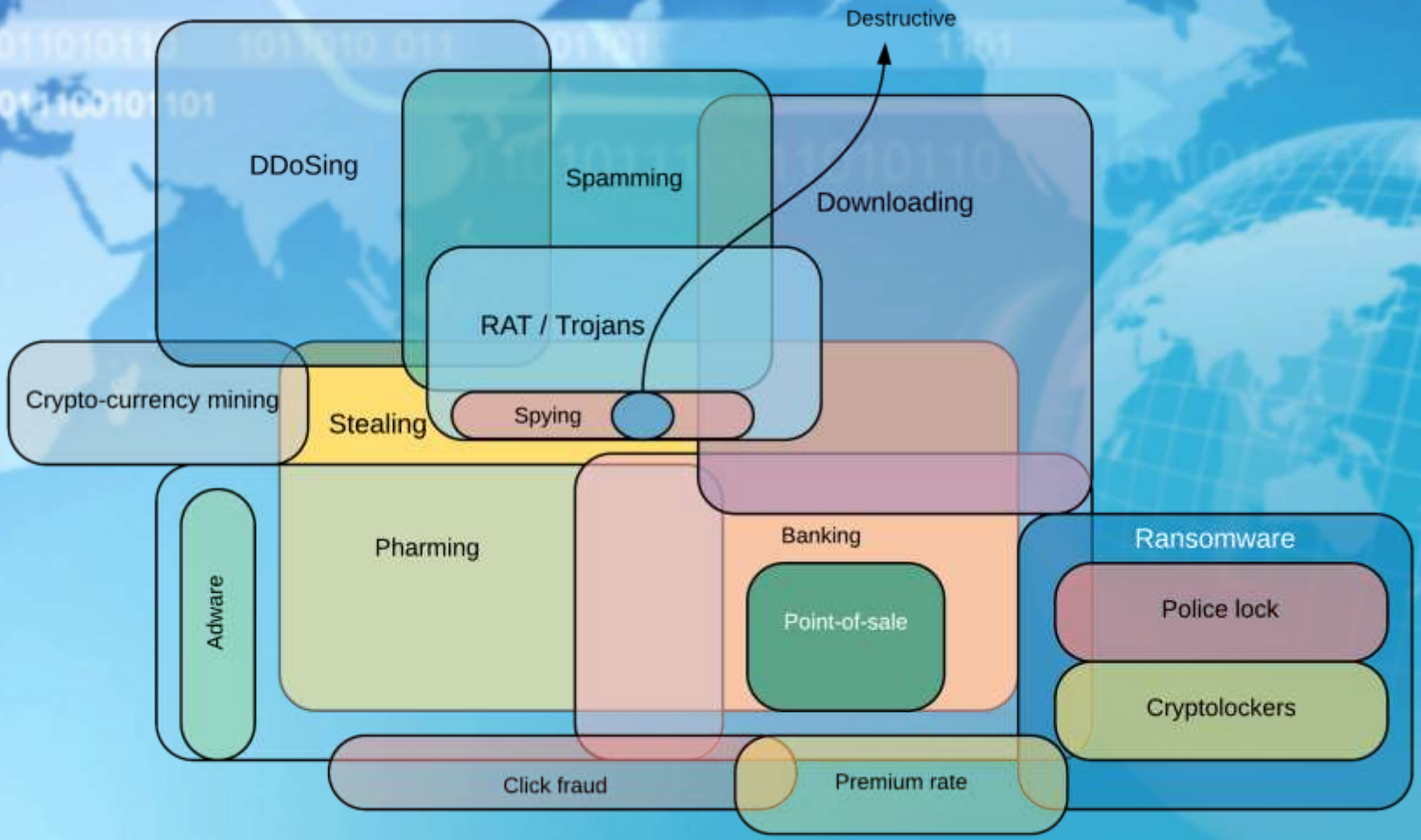
- **Phénomène des faux ordres de virement – FOVI**
  - Facilités par des virus
  - Facilités par des attaques contre des systèmes téléphoniques





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

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

21 Banks: Card Breach at Goodwill Industries

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

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

According to industry
locations of Goo been ide
likely point of co number o

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

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.

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

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 →*

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-lasted-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.

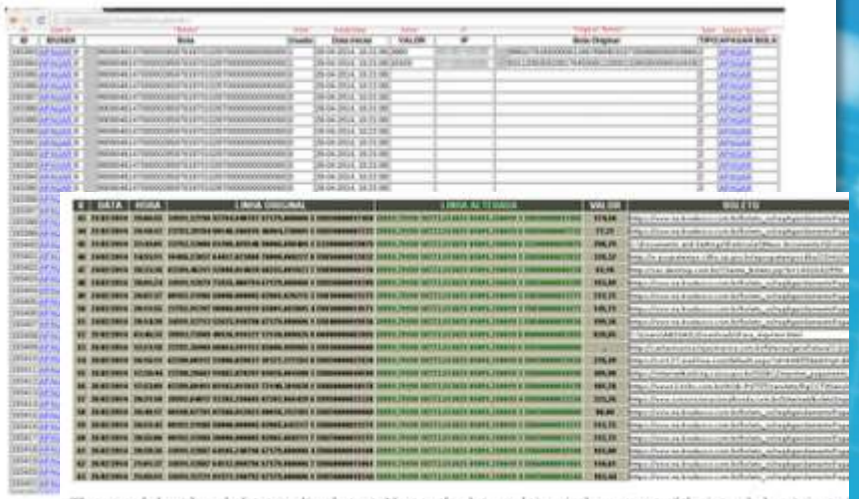
Many of the hijacked boleto transactions are low-dollar amounts, but in the aggregate these purloined payments can generate an impressive income stream for even a small malware gang. On Tuesday, for example, a source forwarded me a link to a Web-based control panel for a boleto-thieving botnet (see screenshot 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.



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 "Conta 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 ur… harsh reality that for nearly every legi… 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… advertisers try to attack competitors by ra… early in the day.

Enter "GoodGoogle," the nickname chos… fraudsters operating on the Russian-langua… software and hands-on customer service, … 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."

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 block between three to ten ad units for 24 hours to $80 for 15 to 30 ad units. For a flat fee of $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.

"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."

…ary 2012, …n $100 to …flat fee of …handful of …currencies (**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 botted computers so that it appears to be done organically from search results.

…ch as …sts of …k of …using …said. …rk in …vice, …but he also lists several Gmail accounts as points of contact. My guess is it will not be difficult for Google to shutter this operation, and possibly to identity 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

Piégées 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

Voici 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.

```
Hi,

I am the author of the Locker ransomware and I'm very sorry about that has happened. It was never my
intention to release this.

I uploaded the database to mega.co.nz containing "bitcoin address, public key, private key" as CSV.
This is a dump of the complete database and most of the keys weren't even used.
All distribution of new keys has been stopped.
```

BUGAT / DRIDEX


THE UNITED STATES DEPARTMENT of JUSTICE

EN ESPAÑOL

HOME ABOUT AGENCIES BUSINESS RESOURCES

Home » Office of Public Affairs » Briefing Room » Justice News

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Tuesday, October 13, 2015

Bugat Botnet Administrator Arrested and Malware Disabled

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.

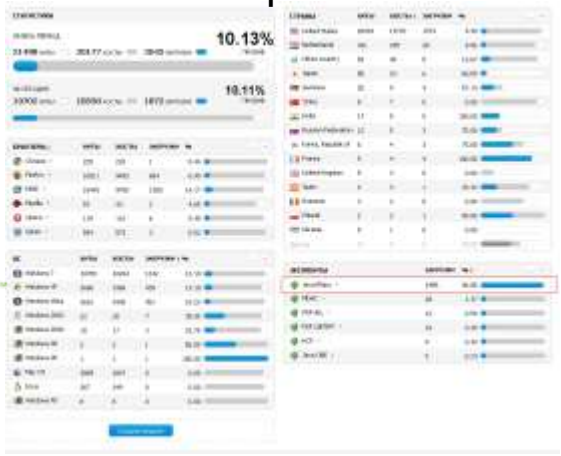
DRIDEX also performs form grabbing, screenshots and clickshots in order to steal more personal information from the affected system.

PRENONS UN PEU DE RECUL

Javascript malveillant
- Sur des sites piratés
- Dans des bannières publicitaires

CLICKSOR

Exploit kits

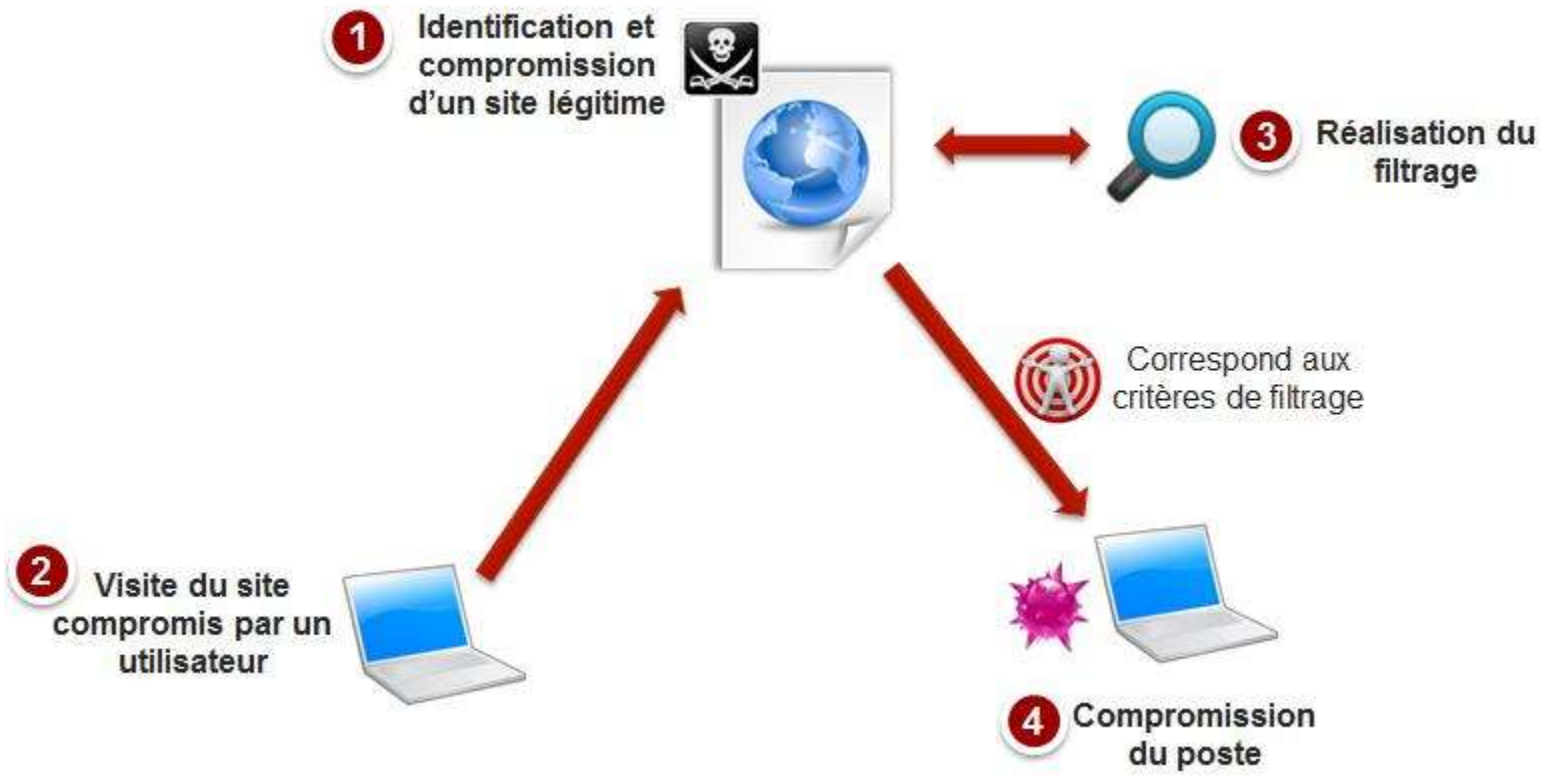


Drive-by download

- 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] Poste[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] "

J'ai un[redacted]Star Addict, je ne sais pas si c'est un virus. Quand j'ai vérifier l'url du téléchargement sa venait d'un serveur mail, et le whois me disais que sa venait d'arabie.

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, prennait le réseau envoyez des sms etc...

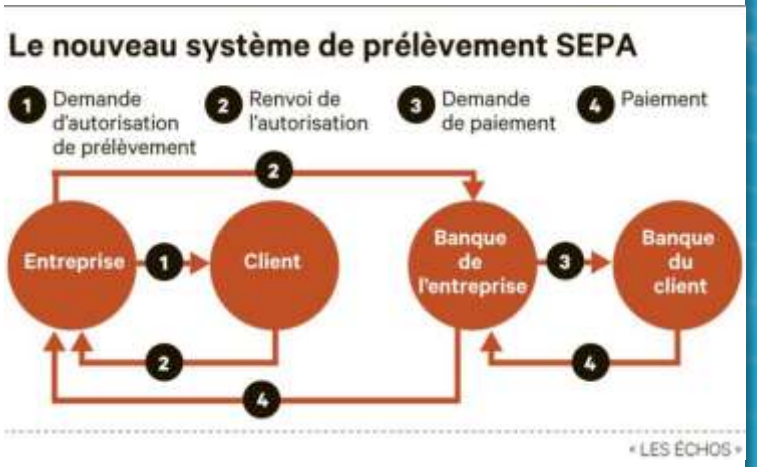
Merci beaucoup!

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

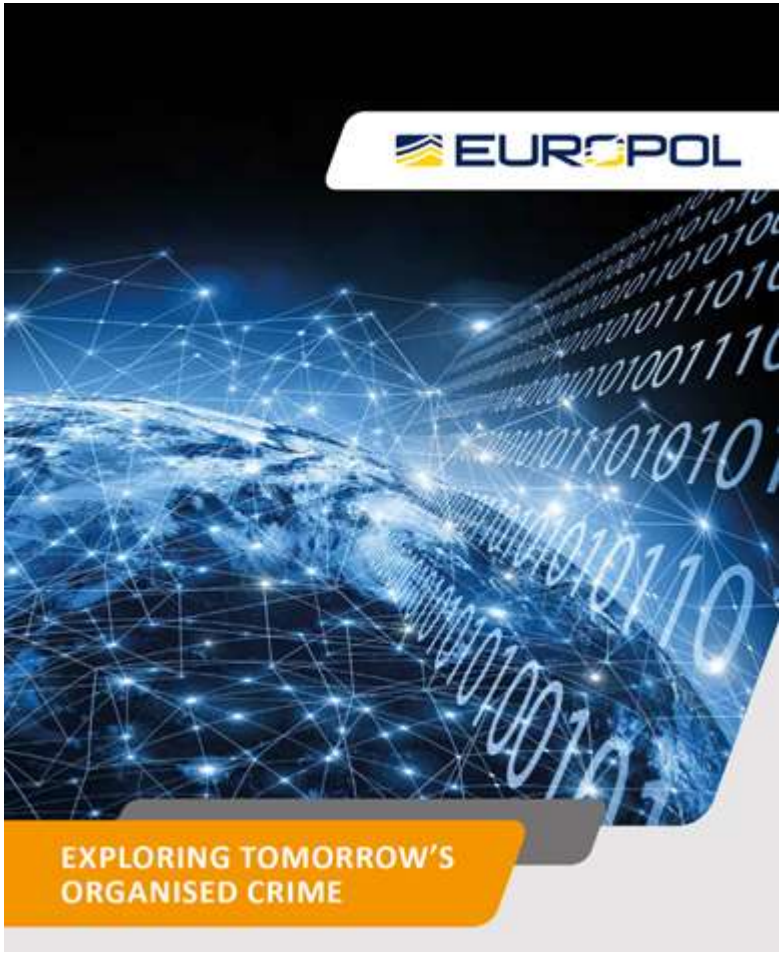


  - Poursuite de la professionnalisation
  - Meilleure prise en compte des techniques d'évasion ou de camouflage

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

- **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 cyberespace, 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

Attributs

Auteurs
Motifs
Buts
Compétences

Entité

Origine

Destination

Victimes
Cibles
Impacts
Compétences

Haut niveau

Hiérarchie

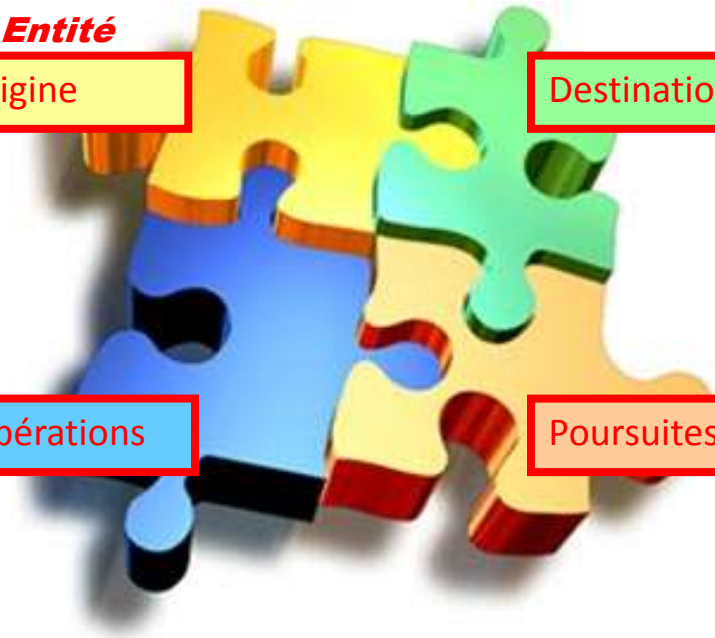
Intentions
Objectifs
Méthodes
Techniques
Outils
Vecteurs

Opérations

Poursuites

Plaintes
Qualifications
Enquête
Instruction
Expertise
Jugement

Bas niveau



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

DYNAMIQUE D'UNE CYBERATTAQUE

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 **privilèges, 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

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**

Serveur C2 : ... *quelque part*

Renseignement 1

Conception 2

Données

Infiltration : *Ouverture de pièces jointes injectées , et leur communication, pour compromettre des machines servant de têtes de pont, afin d'obtenir des privilèges plus élevés*

Action : *Capture et exfiltration des données à l'insu des utilisateurs légitimes, puis effacement des traces*

Machines compromises en "bonnet" et servant de relais pour l'anonymat : acteurs-lieu

Internet

Données sensibles exfiltrées
...01000110111100010...

Passage du pare-feu

Personnes ciblées et plusieurs courriels avec pièce jointe injectée par un cheval de Troie élaboré "0-day" ou modifié pour ne pas être détecté par le dispositif "anti-virus" en place

***Personnes** traitant de points recherchés*
Postes/serveurs relevant de données ciblées

Exploration : *Portes d'entrée*

Collecte : *Pour + de privilèges*

Eléments et données ciblés

Périmètre dit *"de confiance"*

Crise

Gestion appropriée pour le retour définitif à la normale

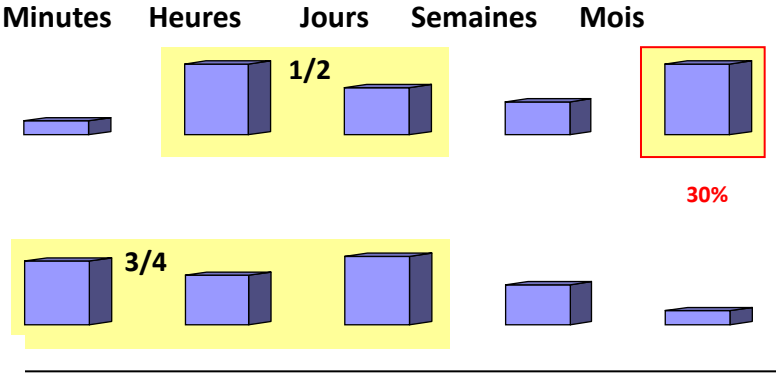
DELAIS USUELS D'UNE CYBERATTAQUE

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

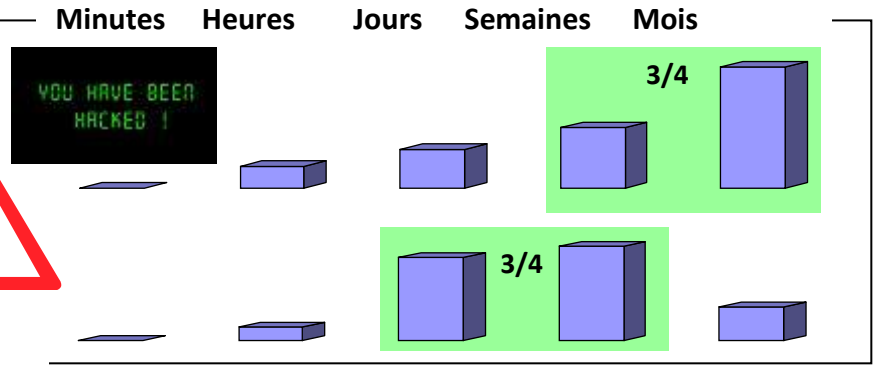
Poursuites

Etat de crise

Délai de maîtrise

Fin de crise lors du retour à la normale

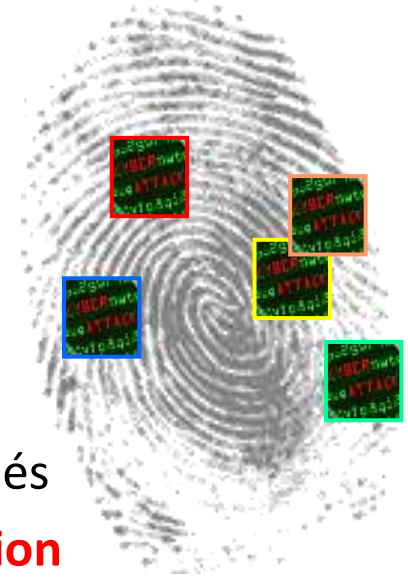
Etat de post-crise **Poursuites** **Année(s)**



CONCLUSION

- **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
- …

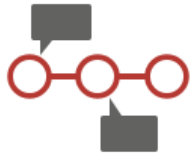
INCIDENT HANDLING (IH) : OBJECTIFS

❑ 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)

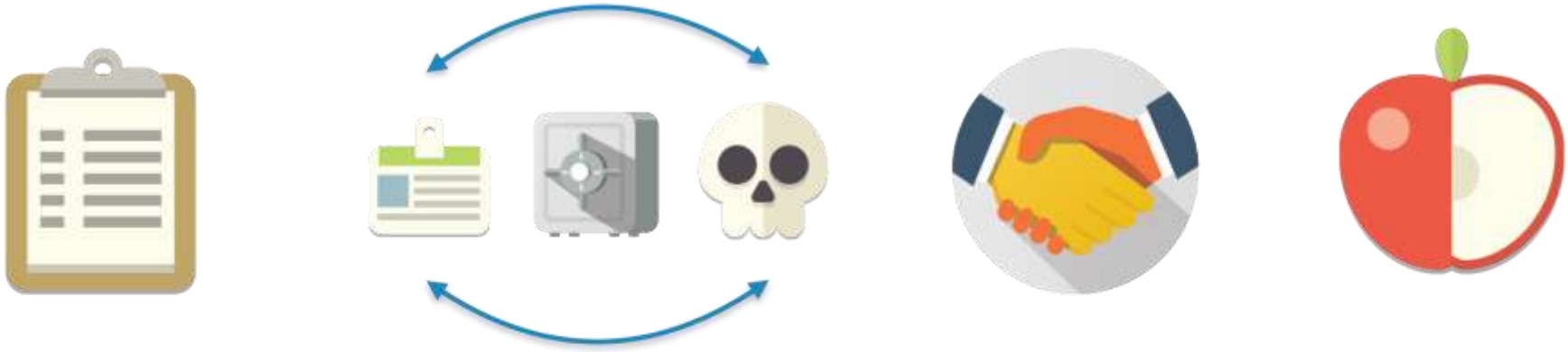
- Chaîne de commande unique
- Terminologie commune
- Objectifs -> Stratégies -> Tactiques
- Flexible et modulaire
- Etendue du contrôle (« span of control »)

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



The SANS Incident Response Process visualized by @markнca

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 !

GESTION D'UNE CYBERATTAQUE

Comment éviter une cyberattaque ?

Eric WIES

Se protéger
des menaces connues