Project funded by the European Union

CEPOL EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING

EU/Maroc - Partenariat Contre-Terrorisme

Activité résidentielle

Recueillir les informations dans CT par Internet

DGSN

Hôtel Ibis Agdal Rabat, Maroc

Lundi 10 Juin – Vendredi 14 Juin 2019

Le contenu de ces sessions a été développé dans le respect de la loi et des droits fondamentaux

CEPOL: [redacted]

Experts: [redacted]

Dimanche 9 Juin

Arrivée de la délégation des experts CEPOL, suivant différents itinéraires et horaires.

Lundi 10 juin

9:00 – 9:30	Cérémonie d'ouverture
9:30 – 10:45	Etats des lieux sur la cybercriminalité
10:45 – 11:00	Pause
11:00 – 12:00	Perspective de l'UE sur la collecte d'informations à partir d'Internet
12:00 – 13:00	Déjeuner
13:00 – 14:45	Le renforcement des capacités d'investigation numérique -Définition d'un projet « laboratoire » -objectifs et contraintes -Normes ISO et certification Relations entre acteurs nationaux et internationaux – pyramidage et pilotage Maintien en condition opérationnelle et évolution de domaine de compétence
14:45 - 15:00	Pause
15:00 - 16:00	Présentation et Installation du poste de travail OSINT : Firefox and plugins Tor-Browser Gephi+java Python3 et Twint
16:00	Fin

Mardi – 11 Juin 2019

9:00 – 9:45	Investigations sur Twitter : Utilisation de DMI-TCAT et Gephi Twitter-stream pour le monitoring les tweets en temps réel. Création de clef d'API et paramétrage de l'app
9:45 – 10:45	Exercice cas 1 pratique sur Twitter : Collecte automatisée Extraction et analyse grâce à DMI-TCAT et Gephi, sous forme de graphe Notion de Social network Analysis, intérêt des algorithmes pour l'analyse.
10:45 – 11:00	Pause
11:00 – 12:00	Exercice cas 2 (CT) pratique sur Twitter : Collecte automatisée grâce à Twint. Visualisation et Analyse des données
12:00 – 13:00	Déjeuner
13:00 – 14:45	Formation Télécommunication - Intérêt de la téléphonie dans le CT (appels mais aussi financement) - Généralités sur la téléphonie - Architecture physique d'un réseau GSM
14:45 - 15:00	Pause
15:00 - 16:00	Formation Télécommunication - Les données de l'opérateur (Fadet, bornages, extinction, reboot, portables non communicants) - Le réseau SS7 et le Spoof Id - La navigation internet et les ports de communications - La carte SIM et ses informations - Le telephone portable (IMEI, android Id, Mac address…) - Recherches opensource - Les comptes utilisateurs (android Gmail, Apple id…)
16:00	Fin

Mercredi 12 Juin

9:00 – 9:45	Investigations sur Facebook – Présentation et utilisation avancée du FB-Graph
10:00 – 10:45	Cas pratique Facebook : extraction automatique des liens d'amitié sur un profil. Construction d'une matrice relationnelle sous Libreoffice. Injection des données dans Gephi.
10:45 – 11:00	Pause
11:00 – 11:45	Cas pratique Facebook (part 2) : extraction automatique des liens d'amitié sur un profil. Construction d'une matrice relationnelle sous Libreoffice. Injection des données dans Gephi.
11:45 – 13:00	Déjeuner
13:00 – 13:45	Aller plus loin sur Facebook :

	Reverse imaging Analyse de profil Identification mail et téléphones.
13:45 – 14:45	Formation Télécommunication (4) L'analyse des données opérateurs (excel , ANB, Mercure)
14:45 - 15:00	Pause
15:00 - 16:00	Formation Télécommunication (5) - Précautions à prendre lors d'une saisie de téléphone - L'exploitation des données du telephone - Xry/Ufed
16:00	Fin

Jeudi 13 Juin

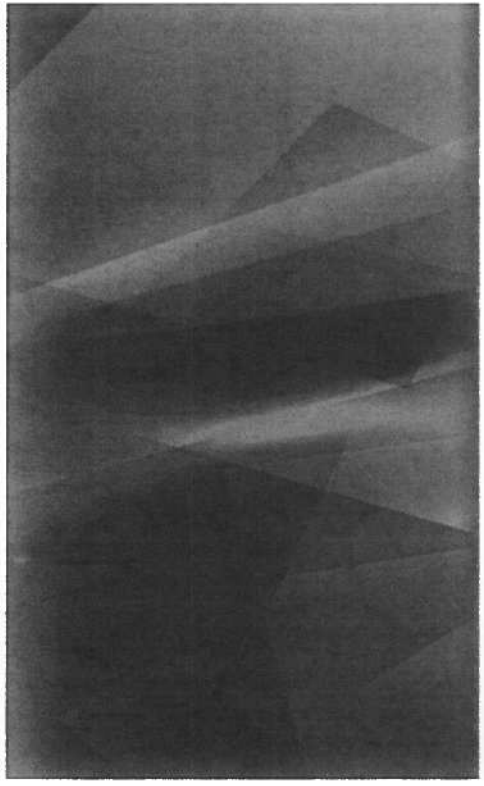
9:00 – 9:45	Techniques d'identification de comptes et pseudo sur Internet. Social Hacking.
10:00-10:45	De l'information à la preuve - Les fondamentaux de la preuve numérique - Les acteurs (experts, spécialistes police,…) - La communication de preuve numérique au niveau international (accès, format, transport, projet EU EVIDENCE
10:45 – 11:00	Pause
11:00 – 12:00	De l'information à la preuve - Les données stockées à distance - la collecte (données publiques, données accessibles via réquisition, techniques spéciales d'enquête) - le traitement (croisement de données, données à caractère personnel)
12:00 – 13:00	Déjeuner
13:00 – 13:45	De l'information à la prevue – données continues dans un support numérique - la collecte (perquisitions, saisies, copies, blocage en écriture) - le traitement (problématiques de volume, de chiffrement, de stockage, de croisement de données) - méthodologies de discrimination et analyses par étapes
14:00 – 14:45	De l'information à la preuve – le live forensics - objectifs (capture de RAM, lutte contre le chiffrement, stockage à distance,…) - outils (First, OSTriage, Darwin,..) - méthodologie (discrimination et préservation de l'intégrité de la preuve)
14:45 - 15:00	Pause
15:00 - 16:00	De l'information à la preuve – Le compte rendu d'analyse - Du compte rendu oral au rapport d'expertise - Caractéristiques fondamentales d'un rapport d'exploitation
16:00	Fin

Vendredi 14 Juin

9:00 – 10:30	De l'information à la preuve – Le témoignage du spécialiste numérique au procès pénal -contexte et acteurs du procès - se présenter - défendre une expertise -les attaques courantes
10:30 – 10:45	Pause
10:45 – 11:00	Evaluation
11:00 – 12:00	Remise des certificats
12:30	Fin

Liste des participants

N	Nom et Prénom	Grade	Service/ville
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			



Recueillir les informations par Internet dans le contre terrorisme

État des lieux sur la cybercriminalité

CEPOL

[redacted] – CEPOL - Maroc - 2019

État des lieux sur la cybercriminalité

1)La complexité du périmètre

2)La fiabilité de l'information

3)L'évolution des usages

4)Les phénomènes marquants de 2018

5)La perception de la menace

6)Les réponses actuelles en France

"Il y a trois sortes de mensonges : les mensonges, les sacrés mensonges et les statistiques."

Mark Twain, autobiographie

La complexité du périmètre

La cybercriminalité : quel périmètre ?

.Cyber et criminalité ?

- Contraction de cyber et criminalité
- Cyber : du grec « gouvernail » ou « gouverner »
- De nombreuses définitions liées à Internet, au virtuel, aux multimédia, à l'informatique et au numérique

.Cybercriminalité et législation française?

- Le mot n'est pas utilisé dans le code pénal français
- Atteintes aux systèmes de traitement automatisés de données, 323-1 et suivants (loi Godfrain de 1988)
- Rapport du Procureur Marc Robert sur la cybercriminalité (2014) : *« La cybercriminalité regroupe toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet. »*

Cybercriminalité : quel périmètre ?

.***Cybercriminalité et législation européenne***

- *La convention sur la cybercriminalité dite convention de Budapest du 22/11/2001*
- *Le préambule introduit les notions de criminalité dans le cyber-espace, numérisation, réseaux informatiques, information électronique, réseaux, etc.*
- *Le préambule évoque la cybercriminalité sans la définir*
- *Les seules définitions visées à l'article 1 : système informatique, données informatiques, fournisseur de service*

Cybercriminalité : quel périmètre ?

.*La convention de Budapest, vise*

- *Titre 1 : infractions visant la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques*
- *Titre 2 : infractions informatiques*
- *Titre 3 : infractions se rapportant au contenu*
- *Titre 4 : infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes*

Cybercriminalité et cybermenaces ?

.La cybercriminalité, un angle trop restrictif ?

- *Les cybermenaces recouvrent la cybercriminalité, la cyberdéfense et la sécurité des systèmes d'information*
- *En France, une approche globale prend forme avec le DMISC : délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces, créé en janvier 2017, dépendant du Ministère de l'Intérieur*

.Les dangers d'une approche globale ?

- *La confusion des genre*
- *La confusion des outils*
- *La confusion entre les modes opératoires et les outils*

La fiabilité de l'information

L'état de la cybercriminalité, quels chiffres ?

.Des sources variées mais non exhaustives

- *Les forces de l'ordre, la Justice, les sociétés d'anti-virus, les associations de cyber sécurité, les sites internet spécialisés, ...*
- *Le chiffre noir de la cybercriminalité :*
  - *Les victimes ne veulent pas s'exposer : mauvais publicité pour les sociétés, honte pour les particuliers, …*
  - *Quel sera l'impact du RGPD ?*
  - *Les victimes ne savent pas toujours qu'elles sont victimes*

.La valeur des indicateurs

- *En fonction de qui produit l'indicateur, du panel observé, de la méthode d'exploitation ?*

L'état de la cybercriminalité, quels chiffres ?

.La cible des chiffres

- *Attaques enregistrées par un système de détection ?*
- *Infractions constatées par la police ?*
- *Autres ?*

.La définition du préjudice

- *Arrêt de l'activité ? (9 semaines en moyenne pour réparer les dégâts causés par une cyberattaque)*
- *Facture indue à honorer ?*
- *Le temps « homme » ?*
- *Préjudice d'image ?*
- *Etc.*

La fiabilité des chiffres ?

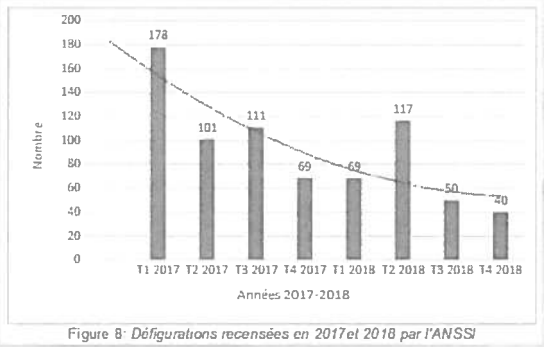
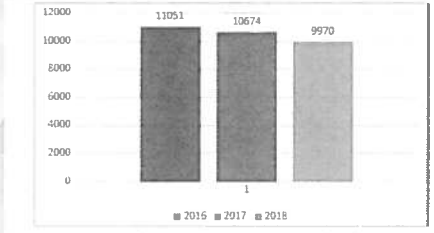


Figure 8: *Défigurations recensées en 2017et 2018 par l'ANSSI*



Atteintes aux STAD – Évolution du nombre d'infraction déclarées

La fiabilité des chiffres ?

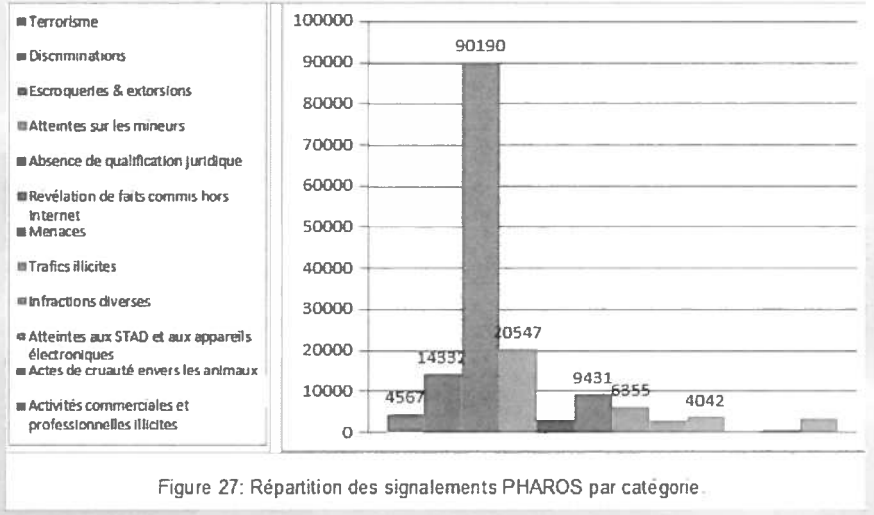
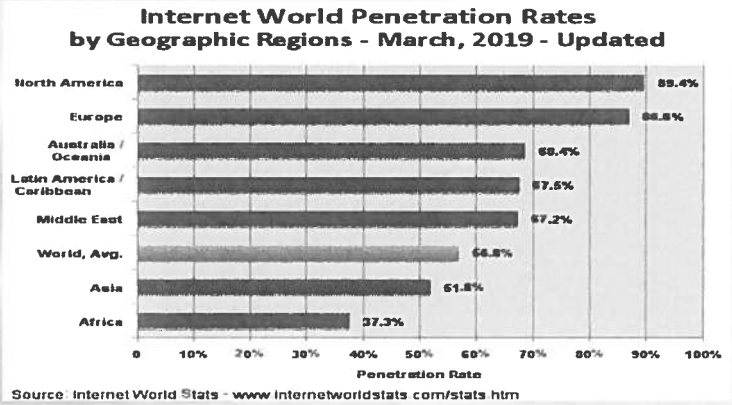


Figure 27: Répartition des signalements PHAROS par catégorie

La fiabilité des chiffres ?

L'évolution des usages

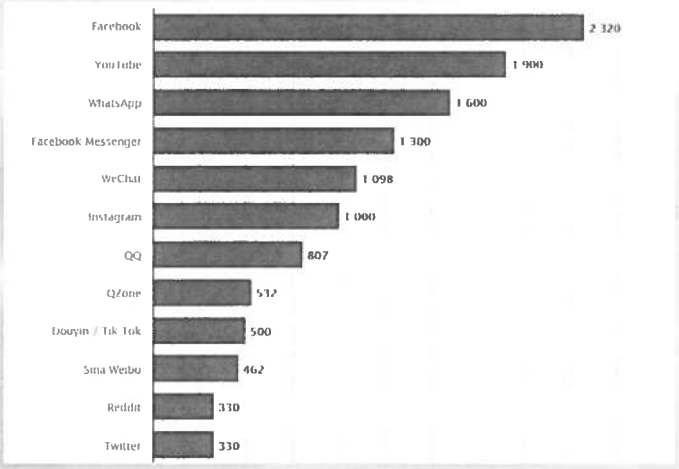
Le taux de pénétration d'internet en hausse



Source: Internet World Stats - www.internetworldstats.com/stats.htm

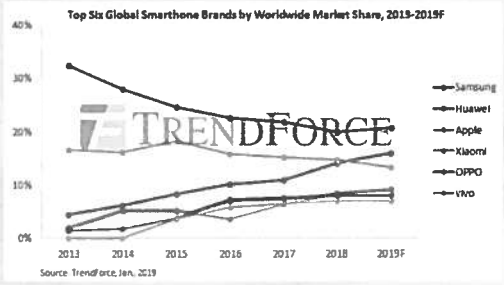
MOROCCO
MA - 36,635,156 population (2019) - Country Area: 458,730 sq km
Capital city: Rabat - population 1,967,917 (2015)
GNI (per capita): $8,062 PPP (2017) per World Bank.
22,667,184 Internet users in Dec/2018, 61.8% penetration, per IWS.
15,000,000 Facebook users in Dec/2017, 40.9% penetration rate
Local Time and Weather in Rabat, Morocco

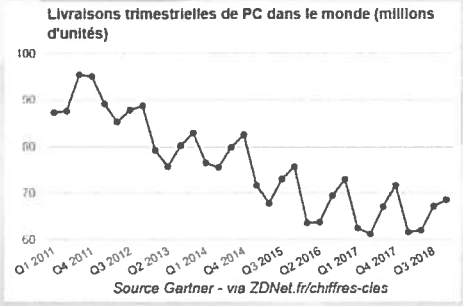
La croissance de l'usage des réseaux sociaux



Popularité des réseaux sociaux par nombre d'utilisateurs
https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Vers un marché de renouvellement

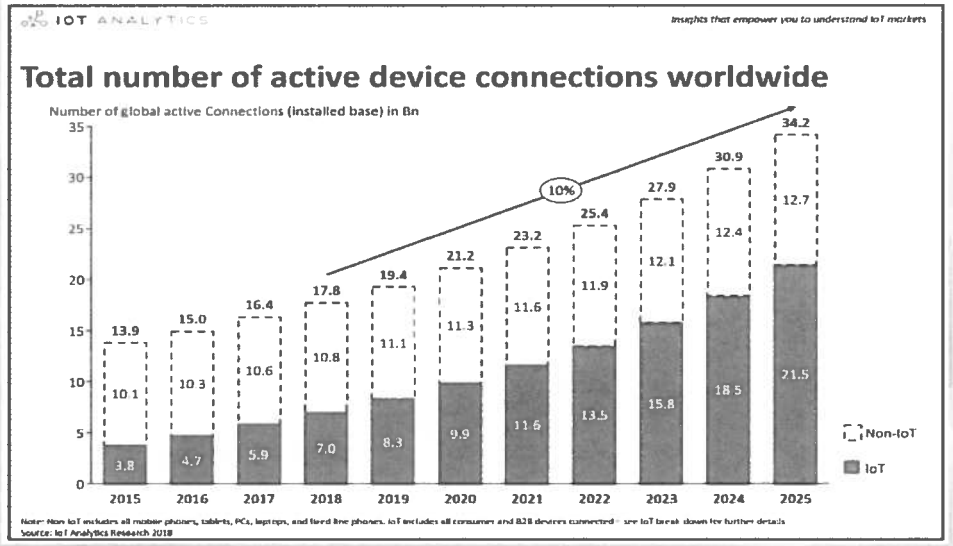




Les cryptomonnaies

- *2100 crypto monnaies différentes en 2019*
- *Le Bitcoin représente 53% des crypto monnaies en valeur*
- *Les échanges entre monnaies se développent : une vingtaine d'acteurs depuis 3 ans*
- *Quid de la réglemantation ?*
  - *En France, les cartes non rechargeables sont plafonnées à 250€ et à 250€ par mois pour les cartes rechargeables (R.561-16-1 du Code monétaire et financier).*
  - *Proposition d'amendement de la loi PACTE pour une bancarisation des acteurs et permettre un contrôle de l'AMF*

L'internet des objets



L'internet des objets

.Problématiques : croissance rapide, diversité, traçabilité, dérives d'utilisation...

INTERNATIONAL

Des drones paralysent l'aéroport londonien de Gatwick, l'armée appelée à la rescousse

Le deuxième aéroport le plus important outre-Manche était à l'arrêt jeudi après avoir été survolé par plusieurs drones. La police britannique soupçonne « un acte délibéré ».

Le Monde avec AFP · Publié le 20 décembre 2018 à 13h58 - Mis à jour le 21 décembre 2018 à 03h42

Greenpeace lance un drone contre la centrale nucléaire du Bugey

Depuis plusieurs mois, l'ONG défie EDF, qui assure que ses centrales nucléaires sont « sûres, bien surveillées et bien protégées ».

Le Monde avec AFP · Publié le 03 juillet 2018 à 12h28 · Mis à jour le 04 juillet 2018 à 06h40

L'internet des objets

- *La Direction générale de l'aviation civile (DGAC) a mis à la disposition des usagers une carte interactive, ainsi qu'une notice d'avertissement rédigée conjointement avec la Commission nationale Informatique et Libertés - CNIL.*
- *Loi relative au renforcement de la sécurité de l'usage des drones civils entrée en vigueur le 1er juillet 2018.*
- *Adoption d'une réglementation par le Conseil de l'Europe le 26 juin 2°18*
- *Au niveau international, l'Organisation de l'aviation civile internationale (OACI) a lancé en 2017 une consultation entre les différents États...*

Smart cities ?

City	Region	Capital City	World city ranking*
London	Europe	x	Alpha++
Singapore	Asia	x	Alpha+
Barcelona	Europe		Alpha-
Amsterdam	Europe	x	Alpha-
Boston	North America		Beta+
New York City	North America		Alpha++
Hong Kong	Asia		Alpha+
Chicago	North America		Alpha
Delhi	Asia	x	Alpha-
Paris	Europe	x	Alpha+
Berlin	Europe	x	Beta
Mumbai	Asia		Alpha
Toronto	North America		Alpha
Dubai	Asia		Alpha+
Los Angeles	North America		Alpha
Stockholm	Europe	x	Alpha-
Melbourne	Oceania		Alpha
Tokyo	Asia	x	Alpha+
Vancouver	North America		Beta+
Vienna	Europe	x	Alpha-
Shanghai	Asia		Alpha+
Seoul	Asia	x	Alpha
Copenhagen	Europe	x	Beta+
Beijing	Asia	x	Alpha+
San Jose	North America		Gamma
Portland	North America		Sufficiency
Brussels	Europe	x	Alpha

*GaWC ranking 2018

En 2017, plus de 2,3 milliards d'objets connect

2015, la Préfecture de Police a édité à l'attenti

https://phys.org/news/2019-02-smart-cities-global-reveals.html

Les phénomènes marquants de 2018

Les phénomènes constatées en 2018 : méthodes, social engineering

.*Phishing, smishing (sms phishing), vishing (phone call phishing), spear phishing (target phishing)*

.*+7 à 9% (State of the phish report, Proofpoint Inc.)*

.*Ou X2 (Kaspersky Lab)*

KASPERSKY

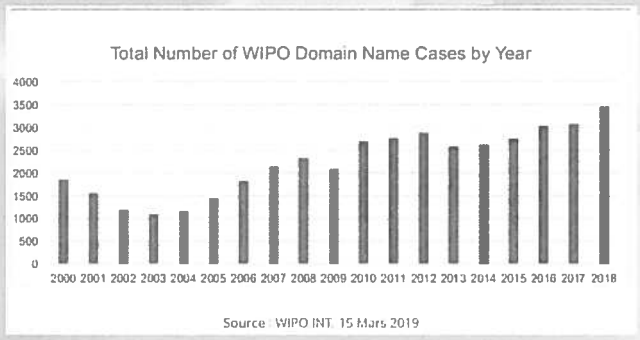
Phishing attacks more than doubled in 2018 to reach almost 500 million

.*En France, montée en puissance du spear phishing (rapport sur l'Etat des cybermenaces, DMISC)*

Les phénomènes constatées en 2018 : méthodes, social engineering

Cybersquatting : +12%

Cibles : sites officiels ou commerciaux



Les phénomènes constatées en 2018 : méthodes, malwares

Ransomware, rançongiciels, quelques chiffres clés

.Préjudice 2018 : 8 milliards en $ dans le monde

.Préjudice estimé en 2019 : 25 milliards en $

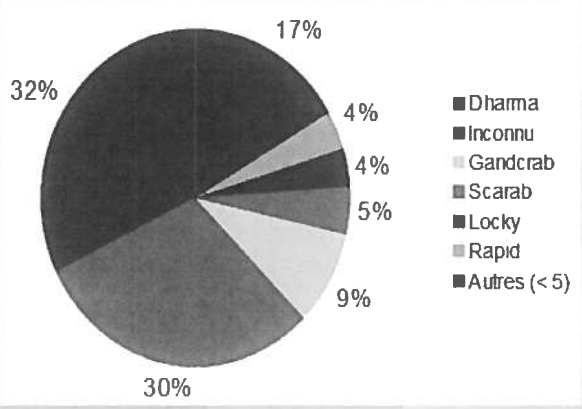
.Coût moyen d'une attaque : 133 000$

.Les ransomware représentent 56% logiciels malveillants

.95% des ransomware utilisent les bitcoins

.

Les phénomènes constatées en 2018 : méthodes, malwares



Souches constatées en France,

Gendarmerie Nationale, C3N

Les phénomènes constatées en 2018 : méthodes, malwares

Nov 15, 2018 17:53 GMT · By Sergiu Gatlan

macOS and iOS users are not as safe as they think they are when it comes to ransomware given that during the first six months of 2018 the number of attacks on macOS/iOS systems reported by managed service providers (MSPs) surged by 500%.

LILY HAY NEWMAN SECURITY 04.23.18 08:55 PM

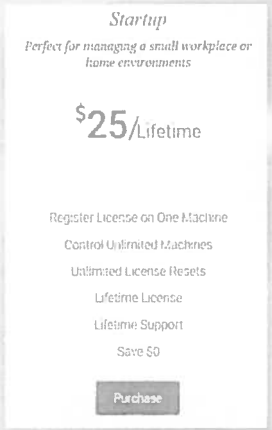
ATLANTA SPENT $2.6M TO RECOVER FROM A $52,000 RANSOMWARE SCARE

C'est une leçon qui coûte cher : la cyberattaque de juin dernier, « NotPetya », aura fait perdre au groupe Saint-Gobain quelque 220 millions de chiffre d'affaires et 80 millions de résultat.

https://business.lesechos.fr/

Les phénomènes constatées en 2018 : méthodes, malwares

Les malwares prennent la 1ère place d'infection devant les exploits. Ex : Remote Access Tools, Imminent Monitor. Plusieurs dossiers en cours à l'OCLCTIC



SECTION 3 - USAGE RULES; PROHIBITED CONDUCT & USES

YOU UNDERSTAND AND HEREBY ACKNOWLEDGE AND AGREE THAT YOU MAY NOT AND WARRANT THAT YOU WILL NOT:

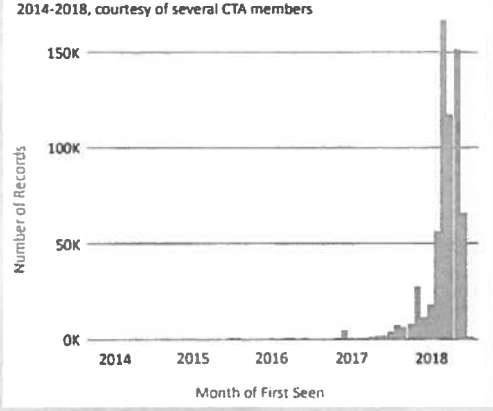
1. Use the Imminent Monitor Software for any illegal purpose, or in violation of any laws, including, without limitation, laws governing intellectual property, data protection and privacy, and import or export control;

2. Remove, circumvent, disable, damage or otherwise interfere with security-related features of the Imminent Monitor Software, features that prevent or restrict use or copying of any content accessible through the Imminent Monitor Software, or features that enforce limitations on use of the Imminent Monitor Software;

3. Install and/or use Imminent Monitor Software on any computer which you do not have explicit permission to do so on;

Les phénomènes constatées en 2018 : méthodes, malwares

Figure 1. Cryptocurrency Mining Malware Detections from 2014-2018, courtesy of several CTA members

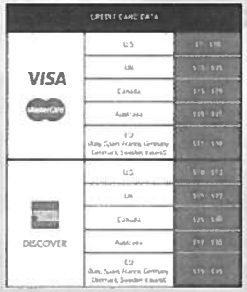


Cryptojacking
Cryptojacking

+450%
Monero : 85%
Bitcoin : 8%

https://www.cyberthreatalliance.org/resources/cta-illicit-cryptomining-whitepaper/

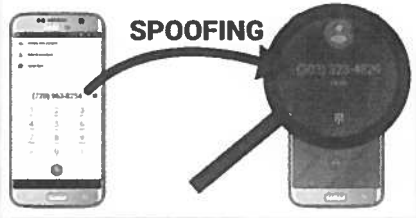
Les phénomènes constatées en 2018 : méthodes, Crime as Service



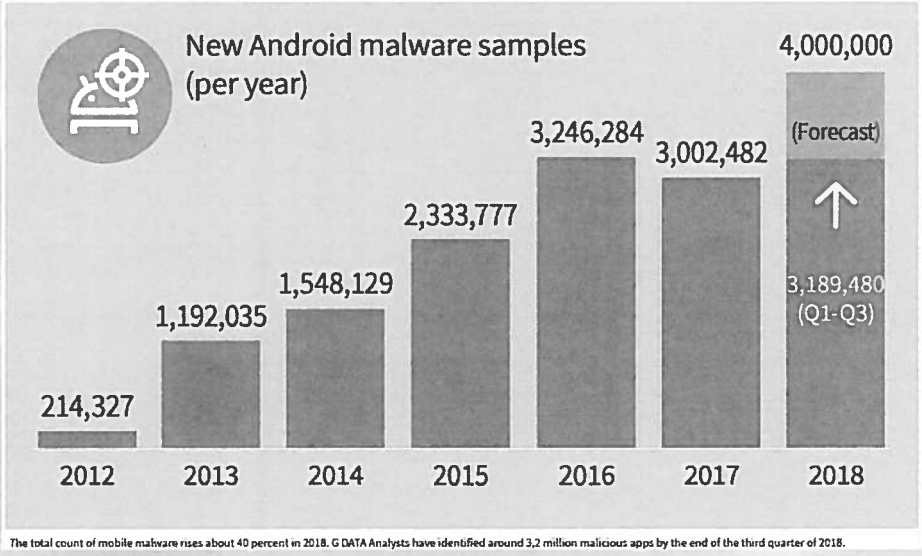
Primo délinquants

Faible niveau technique

Les phénomènes constatées en 2018 : méthodes, attaques téléphoniques



Les phénomènes constatées en 2018 : cibles, les supports mobiles



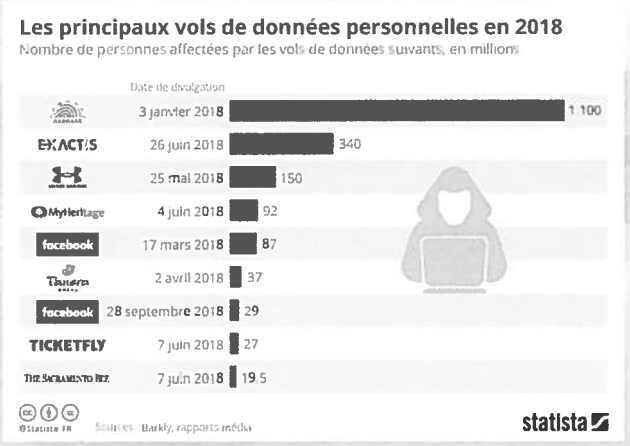
The total count of mobile malware rises about 40 percent in 2018. G DATA Analysts have identified around 3,2 million malicious apps by the end of the third quarter of 2018.

Les phénomènes constatées en 2018 : cibles, systèmes bancaires

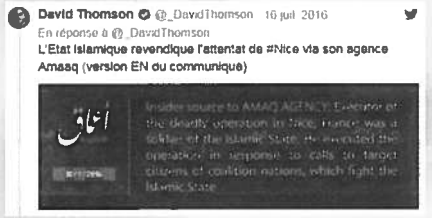
Barnaby Jack, BlackHat 2010, Las Vegas

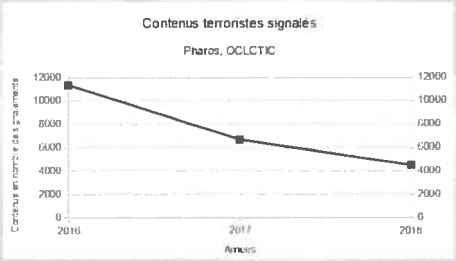
Plusieurs dossiers traités par l'OCLCTIC depuis 2016, dont « ATM Deep » en 2018

Les phénomènes constatées en 2018 : cibles, les données



Les phénomènes constatées en 2018 : motivations, terrorisme, Etat Islamique et Al Qaïda





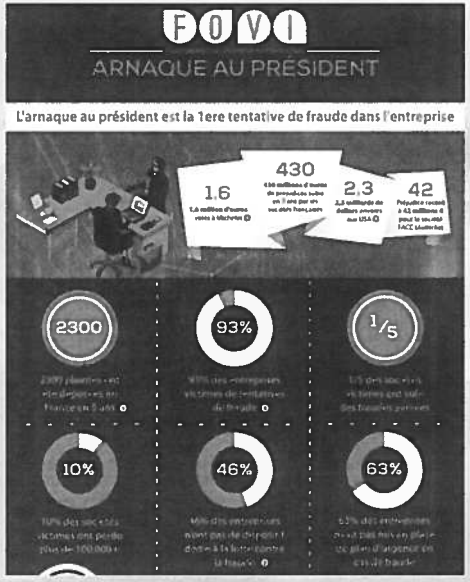
Les phénomènes constatées en 2018 : motivations, terrorisme, Etat Islamique et Al Qaïda

.2018 : 12.100 demandes de retrait pour des contenus à caractère terroriste (

.Sur saisine de la personnalité qualifiée (en charge du contrôle du blocage ac

.Relais européen : plateforme IRMa, Internet Referral Management applicatic

Les phénomènes constatées en 2018 : motivations, l'argent



Les phénomènes constatées en 2018 : motivations, l'argent

Les phénomènes constatées en 2018 : motivations, l'atteinte aux personnes

Austin Jones, un Youtubeur américain vient d'être condamné à dix ans de prison pour avoir réclamé à ses fans mineures, des vidéos sexuellement explicites, comme le rapporte le site *BuzzFeed News*

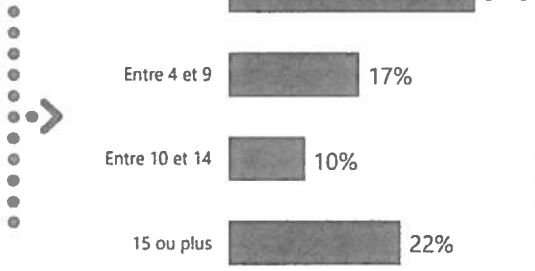
Les phénomènes constatées en 2018 : motivations, astroturfing et déstabilisation politique

La perception de la menace

Perception de la menace : pour les entreprises française ?

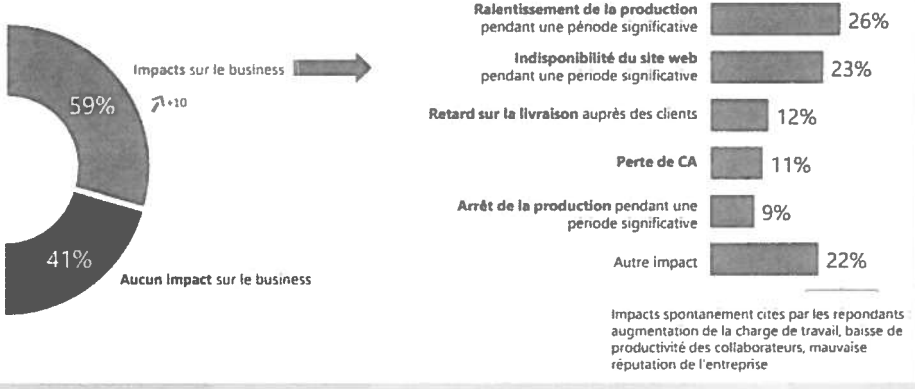
80%

des entreprises ont constaté au moins une cyber-attaque



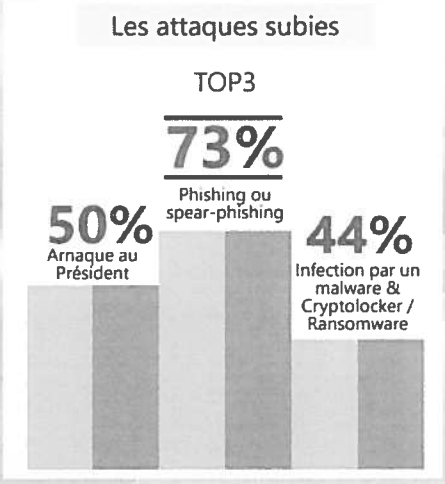
https://www.cesin.fr/fonds-documentaire-4eme-edition-du-barometre-annuel-du-cesin.html

Perception de la menace : pour les entreprises française ?



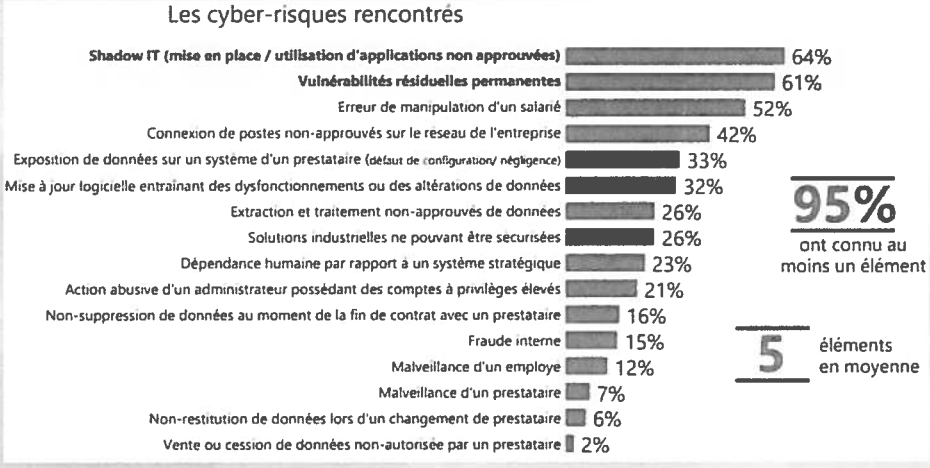
https://www.cesin.fr/fonds-documentaire-4eme-edition-du-barometre-annuel-du-cesin.html

Perception de la menace : pour les entreprises française ?



https://www.cesin.fr/fonds-documentaire-4eme-edition-du-barometre-annuel-du-cesin.html

Perception de la menace : pour les entreprises française ?



https://www.cesin.fr/fonds-documentaire-4eme-edition-du-barometre-annuel-du-cesin.html

Perception de la menace : pour l'Europe ?

.Ransomware

.Cryptomining

.Contenus liées à l'exploitation sexuelle des enfants

.Fraudes aux moyens de paiement et visant les automates de distrib

.Marchés criminels sur le darknet

.Utilisation du cyber par le terrorisme

https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-a

Les réponses actuelles en France

Réponses et perspectives ?

Répression, détection, prévention, information

.PHAROS (contenu illicite)

.Info escroquerie (aide aux victimes de cyber escroqueries)

.PERCEVAL (usage frauduleux de cartes bancaires)

.Cybermalveillance.gouv.fr (assistance aux victimes de cybermalveillance)

.THESEE (plainte en ligne pour les cyber escroqueries)

.Réseau cyber menaces

.DMISC

.Etc.

Des questions ?