

Partie I:

- I.1 De la sécurité des biens et personnes à la sécurité informatique
- **I.2 Enjeux de la sécurité Informatique**
- I.3 Propriétés de la sécurité
- I.4 Vulnérabilités, Failles, Menaces, Attaques

Définition

Enjeux: C'est ce qu'on risque de **gagner** ou de **perdre** en adoptant ou en omettant la sécurité

Les enjeux s'appliquent à la fois à la cible et à l'attaquant



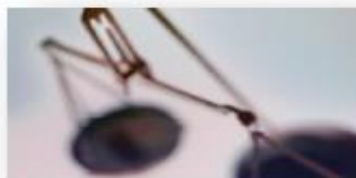
Impacts financiers



Impacts sur l'image et la réputation

Sécurité
des S.I.

Impacts juridiques
et réglementaires



Impacts
organisationnels



Enjeux: Impact Financiers

- Supposant qu'une entreprise innovant ne sécurise pas sans SI

Risque de vol des inventions en cours de réalisation et qui ne sont pas encore breveté → Une perte financière pour l'entreprise, car elle ne pourras pas prouver son antériorité, surtout si l'attaquant brevette/rend publique l'invention

- Que se passera t-il si les inventions, projets en cours de Apple, Samsung, Microsoft, etcc. Sont volés dévoilés avant leur aboutissement finale?

Enjeux: Impact sur l'image et la réputation

- Supposons que le système de passeport biométrique Algérien n'est pas sécurisé

Risque de délivrer un passeport falsifié → L'image du pays et sa réputation au niveau internationale sera fortement affectée

- Supposons que le SI d'une banque est attaqué, et que les informations des clients divulgués (numéro de compte, soldes, ...)

Risque de ne plus attirer de nouveaux clients et de voir ses propre clients actuel partir → La banque risque de fermer ses portes!

Enjeux: Impact Juridique/réglementaire

- Supposons que mon PC n'est pas sécurisé (ex; pas d'antivirus), et qu'un virus a infecté mon PC et par la suite une attaque a été lancée de mon PC à mon insu!

Je suis juridiquement responsable de l'attaque malgré moi! → C'est comme si tu prends en STOP quelqu'un en voiture, et lors d'un contrôle de police on trouve sur lui de la drogue!

C'est pas le même cas pour une voiture de location!

Enjeux: Impacts Organisationnel

- Si jamais une attaque ce produit, les personnes ayant été la cause de façon direct/indirect devront être sanctionnés (dégradés, radiés, etc.), ce qui pourra perturber l'organisation existante de l'entreprise
- Risque de licenciement des employés, dû aux pertes financières

Enjeux: Impact Temps/Argent

- Le temps nécessaire pour un rétablissement suite à une attaque, signifie:
 - Pertes financières, suite à un arrêt totale/partiel d'activité
 - Coût pour le rétablissement: faire appel à des experts, achats de nouveaux équipements/logiciels
 - Coûts pour faire un back-up de données -données perdues et/ou modifiés
 - Possibilité de ne pouvoir jamais récupérer ses données

Impact financiers: Mesurer les coûts des attaques Informatiques *

Putting Malicious Cyber Activity in Context			
CRIMINAL ACTION	ESTIMATED COST	PERCENT OF GDP	SOURCE
GLOBAL			
Piracy	\$1 billion to \$16 billion	0.008% to 0.02%	IMB
Drug Trafficking	\$600 billion	5%	UNODC
Global cyber activity	\$300 billion to \$1 trillion	0.4% to 1.4%	Various
US ONLY			
Car Crashes	\$99 billion to \$168 billion	0.7% to 1.2%	CDC, AAA
Pilferage	\$70 billion to \$280 billion	0.5% to 2%	NRF
US- cyber activity	\$24 billion to \$120 billion	0.2% to 0.8%	Various

- En 2013, le coût –direct & indirect- dû aux attaques informatiques, était estimé entre **300-1000 Milliard \$**, le trafic de drogue/stupéfiant à **600 Milliard \$**
- À l'Horizon **2019** le coût estimé prédit avoisine les **2000 Milliard de \$**

* <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf>

Les cibles des Attaquants: Qui est concerné/victime?

Cibles			
États	Institutions Économiques, Industriels, Financières, etc.	Individus	Infrastructures Critiques
Ministères, Armée, Services de souveraineté	Banques, compagnies, sociétés, entreprises, Bourses, universités, centres de recherches, hôpitaux, etc.	Nos PCs, Smart Phones nos données, nos emails, comptes sociaux, nos smart devices (E-car, TV, etc.)	Système de transport, système d'énergie, système d'épuration d'eaux, Télécommunications, etc.

Les motivations des Attaquants: Ce qui les pousse!

- Gain Financier
 - Vol, utilisation/revente d'information de cartes bancaire où autres information sensibles, ...
- Espionnage
 - Étatique, Industriel, Concurrentiel, ...
- Chantage
 - Manipulation des opposants, recrutement des agents, ...
- Utilisation des ressources
 - Mobiliser les ressources d'autrui (BP, CPU, stockage), ...
 - Botnet: lancer une attaque à partir d'autres machines victime

Les motivations des Attaquants: Ce qui les pousse!

- Défis/Challenge
 - Démontrer les limites des systèmes existants
- Sabotage/Vandalisme
 - Destruction, tout simplement
 - Faire le maximum de dégâts (données/matériel/humains)
- Vengeance
 - Un employé licencié qui se venge de son entreprise, ...

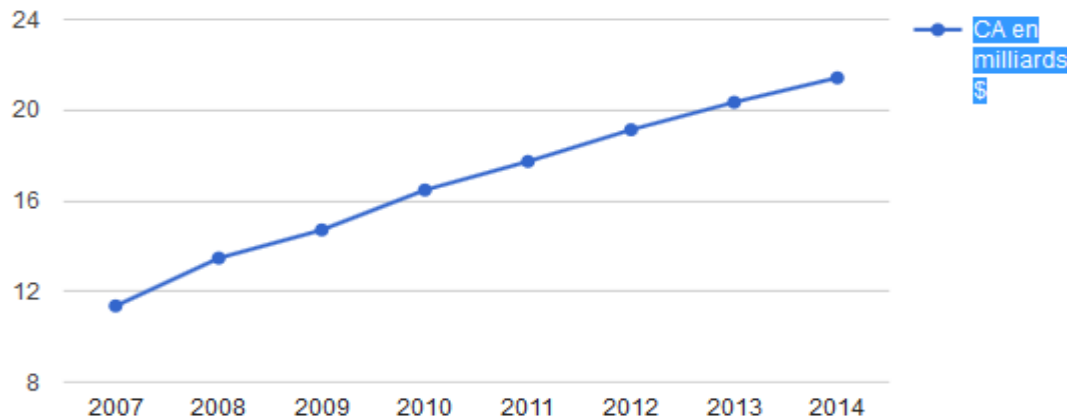
Les Attaquants, Qui sont-ils?

- En majorité, des professionnels, bien organisé
 - Des organisations criminelles ou pas (ANONYMOUS, DAESH, etc.)
 - Des états, des services de renseignement (CIA, MOSSAD, etc.)
 - Des concurrents industriels
 - Des mercenaires
 - Etc.
- Dans certains cas, des actes isolés
 - Des employés licenciés ou en désagrément avec leur employeurs
 - Des individus passionnés par la sécurité informatique, désirant relever le challenge!

La sécurité Informatique: une vraie économie!

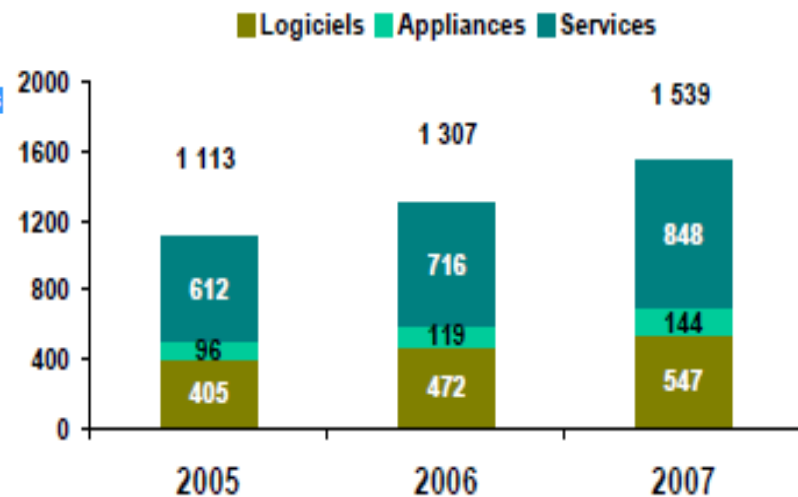
- Statistiques pour certains **éditeurs de logiciel de sécurité**: Norton, Symantec, Kaspersky, etc.

Le marché des logiciels de sécurité de 2007 à 2014 (milliards de \$)



Source Gartner - via ZDNet.fr/chiffres-cles

- Dépense en matière de sécurité Informatique en France



La cyber criminalité: une vraie économie bien organisée!

Une majorité des actes de délinquance réalisés sur Internet (**Cyber-criminalité**) sont commis par des groupes criminels organisés, professionnels et impliquant de nombreux acteurs, se partageant tous de gros bénéfices (à l'instar des acteurs du réseau de trafic de drogue)

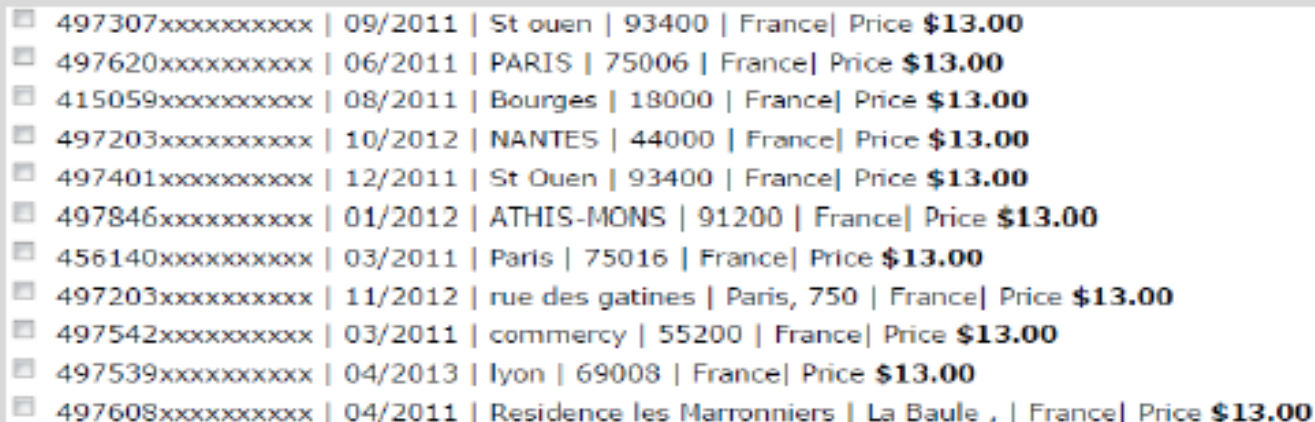
- des groupes spécialisés dans le **développement de programmes malveillants** et virus informatiques
- des groupes en charge de l'**exploitation et de la commercialisation** de services permettant de réaliser des attaques informatiques
- un ou plusieurs **hébergeurs** qui stockent les contenus malveillants, soit des hébergeurs malhonnêtes soit des hébergeurs victimes eux-mêmes d'une attaque et dont les serveurs sont contrôlés par des pirates
- des groupes en charge de la **vente des données volées**, et principalement des données de carte bancaire
- des **intermédiaires financiers** pour collecter l'argent qui s'appuient généralement sur des réseaux de **mules**

Economie de La Cybercriminalité (1)

Vol d'information sensible (ex, numéro carte bancaires)

2 - 15 \$

Prix moyen de vente de numéro de carte bancaire



A screenshot of a list of stolen French bank cards for sale. Each entry includes a card number (partially redacted with 'x'), an expiration date, a location, a postal code, the country (France), and a price of \$13.00. The locations include St ouen, PARIS, Bourges, NANTES, St Ouen, ATHIS-MONS, Paris, rue des gatinés, commercy, Lyon, and Residence les Marronniers. The list is presented in a table-like format with a light gray background.

497307xxxxxxxxxx	09/2011	St ouen	93400	France	Price \$13.00
497620xxxxxxxxxx	06/2011	PARIS	75006	France	Price \$13.00
415059xxxxxxxxxx	08/2011	Bourges	18000	France	Price \$13.00
497203xxxxxxxxxx	10/2012	NANTES	44000	France	Price \$13.00
497401xxxxxxxxxx	12/2011	St Ouen	93400	France	Price \$13.00
497846xxxxxxxxxx	01/2012	ATHIS-MONS	91200	France	Price \$13.00
456140xxxxxxxxxx	03/2011	Paris	75016	France	Price \$13.00
497203xxxxxxxxxx	11/2012	rue des gatinés	Paris, 750	France	Price \$13.00
497542xxxxxxxxxx	03/2011	commerc	55200	France	Price \$13.00
497539xxxxxxxxxx	04/2013	Lyon	69008	France	Price \$13.00
497608xxxxxxxxxx	04/2011	Residence les Marronniers	La Baule ,	France	Price \$13.00

Figure 12 : shop proposant des cartes bancaires françaises

Économie de la Cybercriminalité (2)

- Prix commercialisation logiciels/ malveillant (malware, rançomware)

2.399 \$	le prix de commercialisation du malware « Citadel » permettant d'intercepter des numéros de carte bancaire (+ un abonnement mensuel de 125 \$)
250 - 1500 \$	prix commercialisation rançomware



-325 M\$: c'est la somme extorqué aux USA en 2015 par les créateurs du rançomware CryptoWall

Économie de la Cybercriminalité (3)

200 - 300 \$

Serveur Buletproof: Hébergement de données illicites (données volés, virus, contenu à droits d'auteurs, contenu interdit, etc.)



The image is a screenshot of a web page advertisement for "Bullet Proof Web Site Hosting". At the top, the title "Bullet Proof Web Site Hosting" is centered. Below it, a list of features is displayed: "Unlimited Disk Space & Bandwidth", "FTP Access", "Supports PHP", "99% Uptime Guarantee", "Never Get Shut Down Due to Complaints", and "Reliable and 100% Bulk Email Friendly!". To the right of the list, the price "\$299" is shown in large red font, with "p/ month" in smaller text below it. Below the price list, there is an orange button with the text "Click Here". Underneath the main advertisement box, there is a separate grey button labeled "Bullet Proof Hosting". Below this button, the text "Highly Stable Bullet Proof & Bulk Email Friendly Web Site Hosting" is centered. At the bottom, a paragraph of text explains that many web hosting companies have Terms of Service (TOS) or Acceptable Use Policies (AUP) against the delivery of emails advertising or promoting your web site, and that if your web site host receives complaints or discovers that your web site has been advertised in email broadcasts, they may disconnect your account and shut down your web site.

Bullet Proof Web Site Hosting

- Unlimited Disk Space & Bandwidth
- FTP Access
- Supports PHP
- 99% Uptime Guarantee
- Never Get Shut Down Due to Complaints
- Reliable and 100% Bulk Email Friendly!

\$299
p/ month

[Click Here](#)

Bullet Proof Hosting

Highly Stable Bullet Proof & Bulk Email Friendly Web Site Hosting

As you may already know, many web hosting companies have **Terms of Service (TOS)** or **Acceptable Use Policies (AUP)** against the delivery of emails advertising or promoting your web site. If your web site host receives complaints or discovers that your web site has been advertised in email broadcasts, they may disconnect your account and shut down your web site.

Figure 25 : Promotion d'un serveur bulletproof

Economie de La Cybercriminalité (4)

5 \$	le tarif moyen de location pour 1 heure d'un botnet, système permettant de saturer un site internet
------	---

CHEAP PROFESSIONAL DDOS SERVICE

Cheap Professional **DDOS** Service
Trusted
Strong/Fast Service
Takes down Large Website/Forum/Game Servers etc.
No time limit

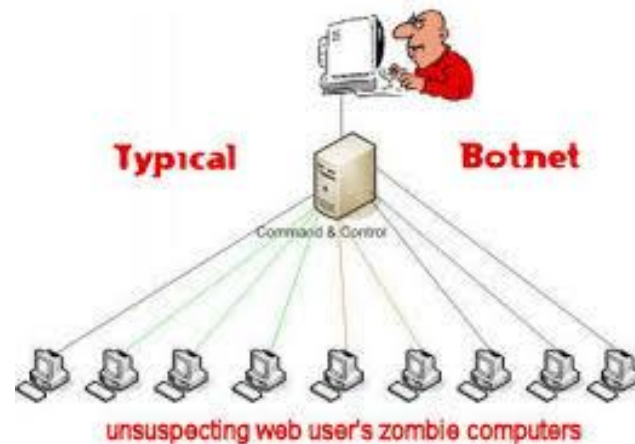
PRICE

1 - 4 hours / 2\$ per hour
12 - 24 hours / 4\$ per hour
24 - 72 hours / 5\$ per hour
1 month / 1000\$ fix price

PAYMENT ACCEPTED

Paypal (Verified users only)
Liberty Reserve
Western Union

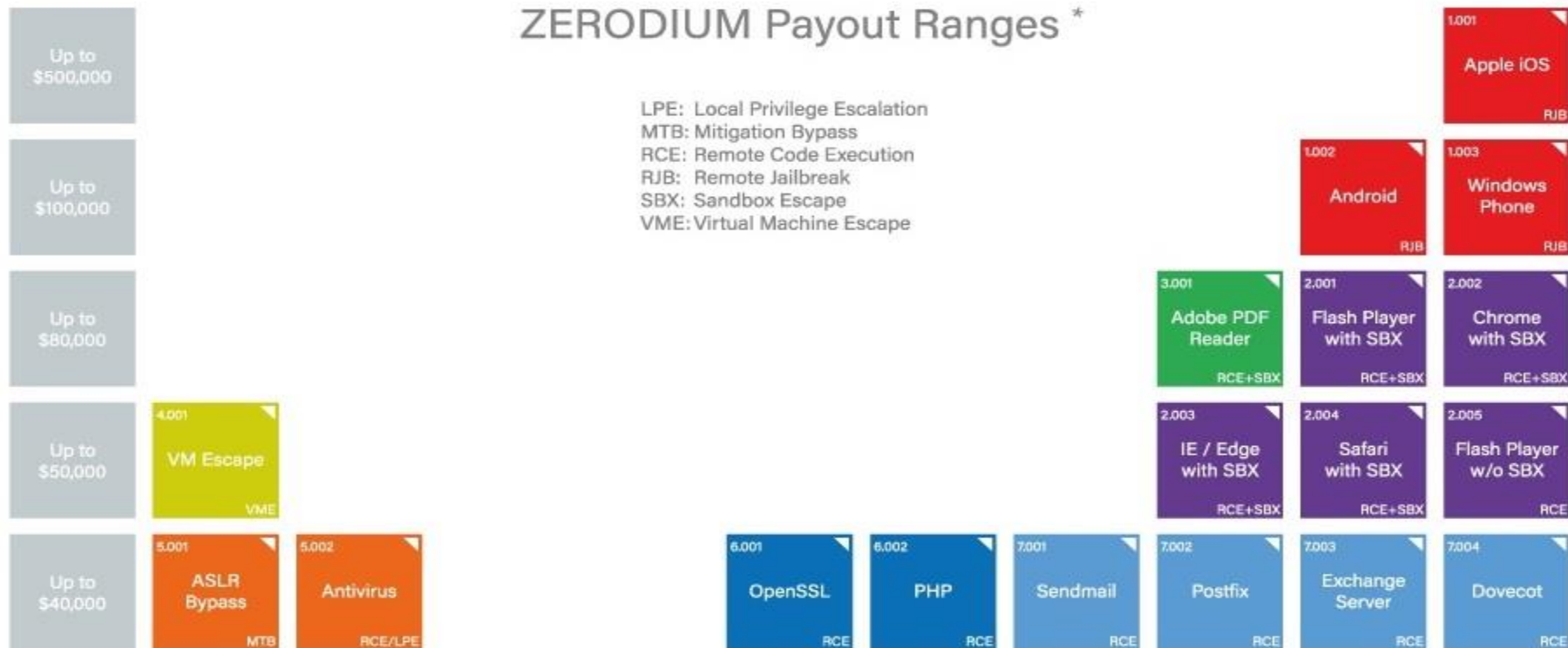
b



Économie de la Cybercriminalité (5)

- **Des compétitions/challenges rémunérés**: certaines sociétés de développement logiciels proposent des primes à tous ceux prouvant l'existence de failles/faiblesses dans leurs produits

ZERODIUM Payout Ranges *



Des Exemples de Cyberattaque (1)

- L'algérien Hamza Bendellaj, Co-créateur du virus **SpyEye**
 - Pirater les comptes bancaires de clients de **217** banques à travers le monde → **Centaines millions de \$** détournés!
 - Soupçonner d'avoir pirater plusieurs sites de **MAE** de plusieurs pays étrangers.
 - Soupçonner d'avoir pirater le site du **gouvernement israélien**, et la délivrance à la résistance palestinienne des informations classé "**secret**"

Des Exemples de Cyberattaque (2)

- Attaque contre la compagnie **Sony** en 11/2014
 - Vol et diffusion en ligne de films non encore sorti en salle Cinema/DVD
 - Paralyser du réseau informatique de Sony durant plusieurs jours
 - Vol de données confidentiels, et suppression d'autres



Des Exemples de Cyberattaque (3)

- Attaque Déni de Service, Groupe **Anonymous**
 - 2/1/2011: Mise hors services de plusieurs sites (serveurs) ministériels en Tunisie, en soutien au printemps arabe
 - 11/06/2012 Mise hors service du site de la police nationale espagnole
 - 05/2012: Mise hors service de plusieurs sites gouvernementaux au Québec
- 12/2015 Cyberattaque à Hollywood, plus de **40 films non encore sortie en cinéma/DVD** circulent déjà sur Internet et les réseaux P2P

Des Exemples de Cyberattaque (4)

- Attaque Red October, **Cyber Espionage** (ambassade, sites étatique, universités, centre de recherche, etc.)



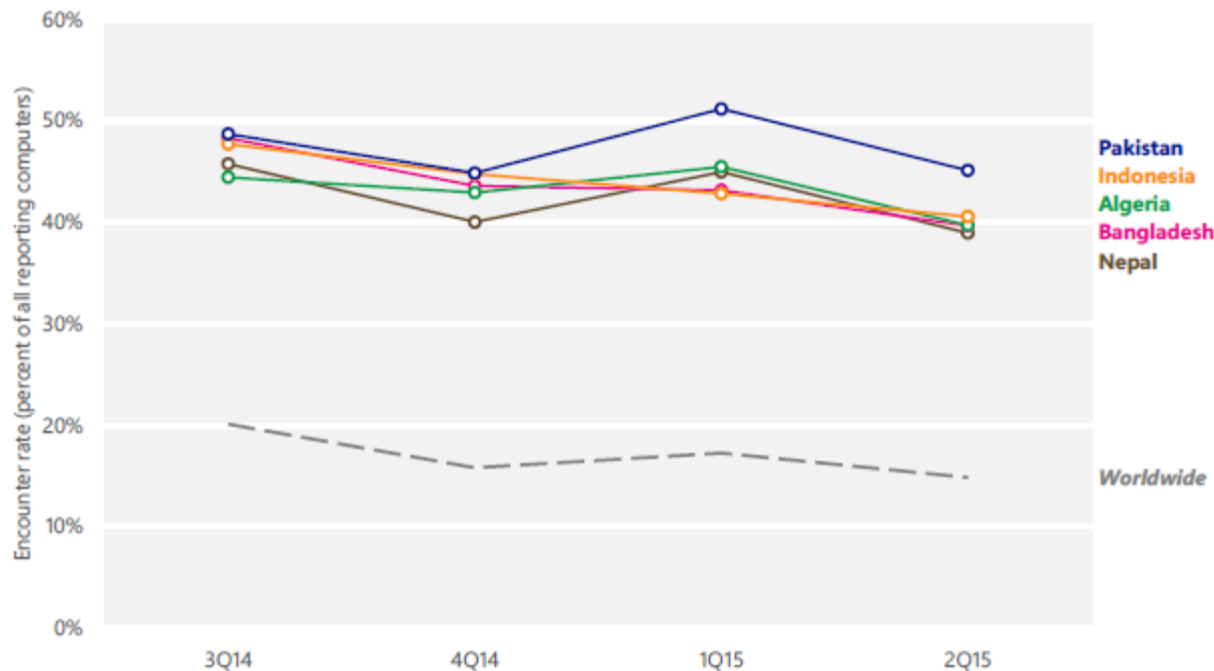
Constat en Algérie

- Malheureusement peu de statistiques, mais plusieurs antécédents
 - Plusieurs sites d'institution de souveraineté (présidence, premier ministre, Défense, etc.) ainsi que plusieurs médias ont été attaqués
- L'Algérie est classé parmi les TOP15 des pays les plus attaqués

Constat en Algérie

- Taux d'attaques/Infection en Algérie (3° mondiale! selon Microsoft, 2015)

Figure 44. Trends for the five locations with the highest encounter rates in 1H15 (100,000 reporting computers minimum)



Constat en Algérie

- Nombre d'attaques perpétré contre des institution financières

