M2 CyberSecurity
Threat and Risk Analysis, IT Security Audit and Norms

Security Assessment of Information System
Standards, Methods and Tools

Florent Autréau - florent.autreau@imag.fr

2016 /2017

Exercice 2 : Security Mindset

- Objective : Steal information stored on a laptop belonging to the CEO of competitor

List / categorize the attacks for the scenario “Steal information from CEO laptop”

Use mindmap to present/synthetize your work (http://freemind.sourceforge.net)

- Find a 0-day exploit in pdf/word/graphic processing and mail infected doc to target
- Idem with known bug
- “water-hole” attack
- Insert boobytrapped USB key in laptop (yourself, or target, or target's admin, ...)
- Bribe the admin, the sysadmin, the janitor
- Inspect the laptop during immigration control
- Attack the home or the hotel's network
- ...

Outline

- *Introduction*
- Concepts
- Risks and Threats
- Methods and standards
  - ISO2700x, OCTAVE, Ebios, Mehari,
- Tools
  - Nessus, nmap, wireshark, ntop, ...
- Hand-on Labs

Risk Analysis - Terminology

- **Threat** :
  - what from you want protect valuable assets
  - anything (man made or act of nature) that has the potential to cause harm (a.k.a Menace)
- **Vulnerability** :
  - Failure or Deviation of the Information System
  - weakness that could be used to endanger or cause harm to an informational asset
- **Risk** :
  - when Threat exploits Vulnerability against Valuable Asset
  - Probability that event will happen with a negative impact to an informational asset

The good questions

- What are the assets ?
- What are the threats ?
- What are the vulnerabilities ?
- What could be the impact/cost ?
- What are the strategies to handle the risk ?

Security as a process

While true repeat

- Identify the assets at risk
- Ascertain enemies interested in it and assess capabilities
- Select application technologies
- Evaluate vulnerabilities for each component
- Identify defensive solutions
- Estimate cost including damage

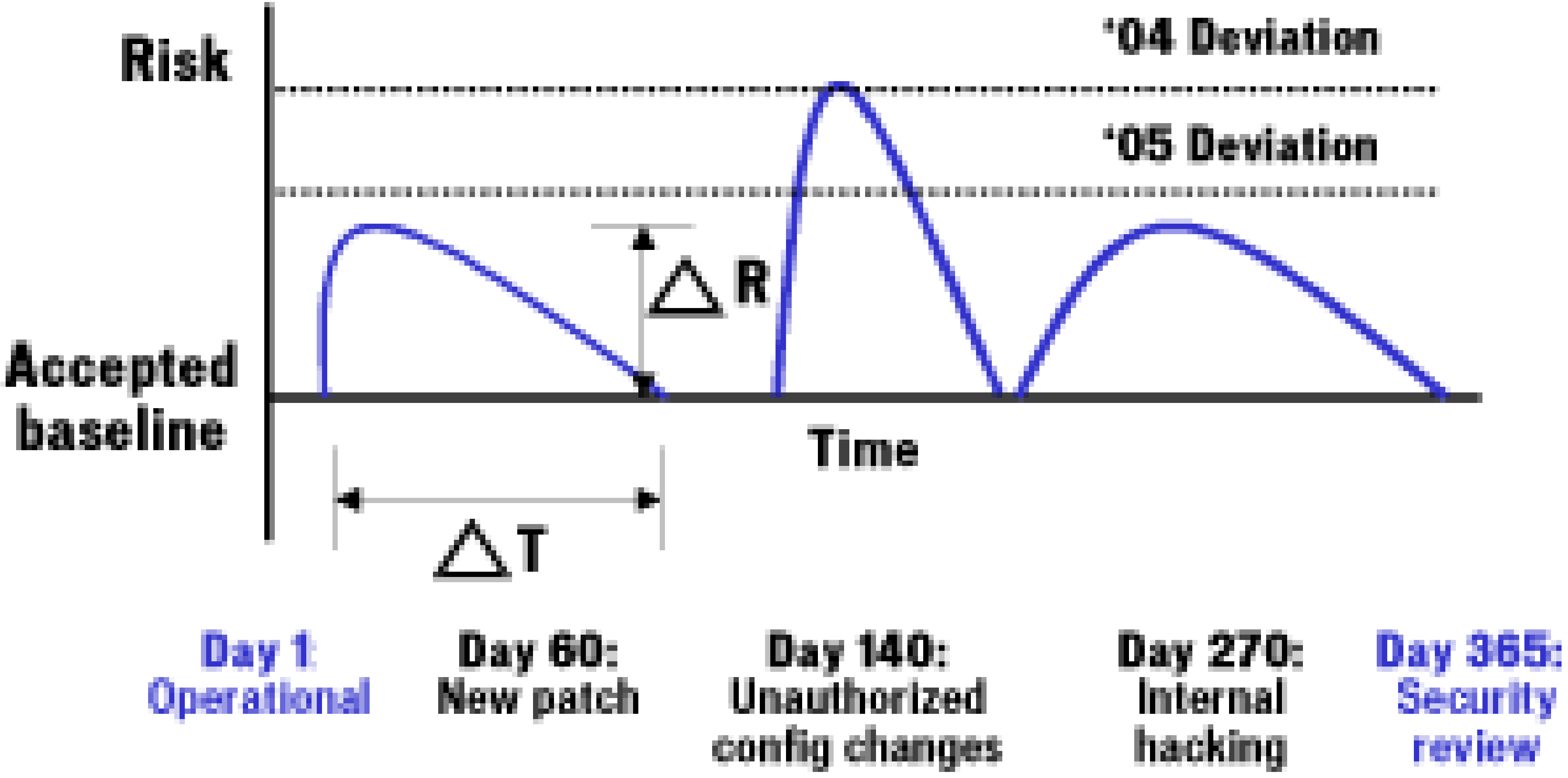
ALE – Annual Losses Expectancies

- Estimate the cost of replacing or restoring that asset (its Single Loss Expectancy)
- Estimate the vulnerability's expected Annual Rate of Occurrence
- Multiply these to obtain the vulnerability's Annualized Loss Expectancy

Single Loss x expected Annual = Annualized
Loss

Expectency (cost) Rate of Occurrences Expectancy
(cost/year)

Measuring Security (1)



Statistical Approach

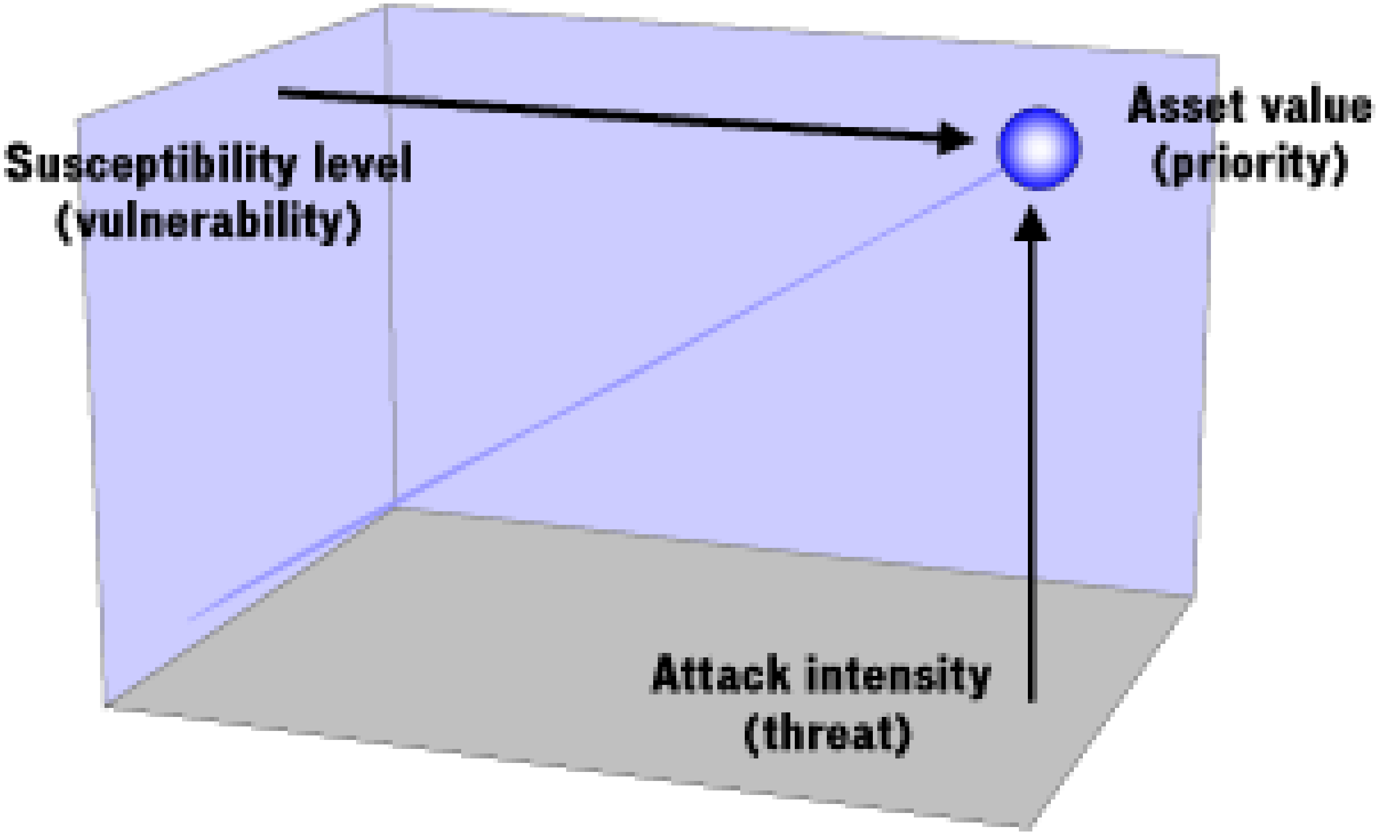
Risk = Pm * (1-Pc) * C

Pm = proba(menace)

Pc = proba(efficiency of countermeasures)

C = cost of incident

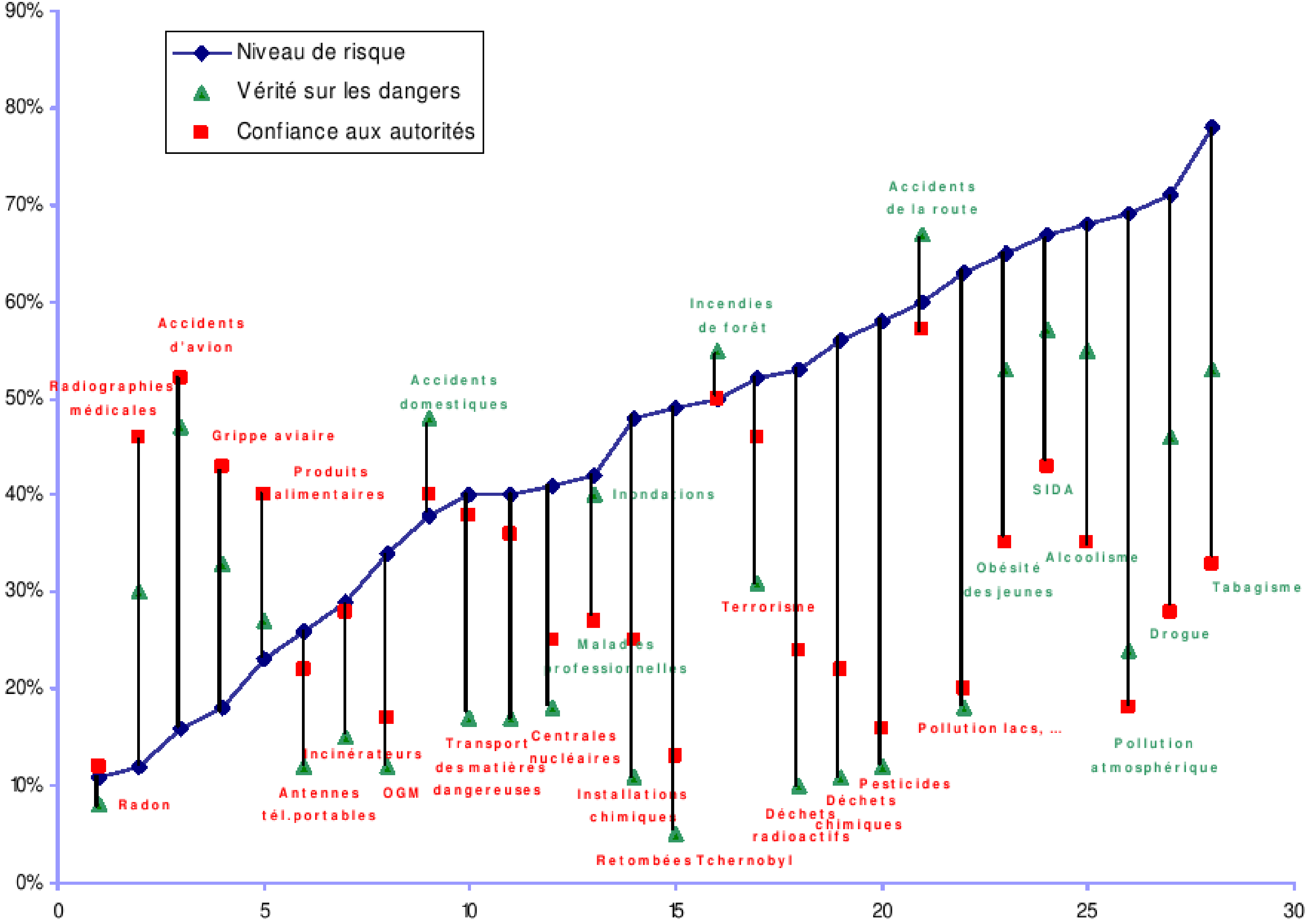
Measuring Security (2)



Threat + Vulnerability + Priority = △ Risk

Risk Management :
A Matter of Perception ?

- Source “Barometer 2006 – IRSN”
- French Institute for Radiological Protection and Nuclear Safety / Institut de radioprotection et de sûreté nucléaire
- http://www.irsn.org



Graphique n°1 : comparaison des 28 situations à risques selon les trois aspects étudiés

Taxonomy of Risks

- Accidents
  - Disaster
  - Malfunction or Misfunction
- Errors
  - Operation, Exploitation
  - Bug
- Malicious
  - Intruders, Hackers, Organized Criminals
  - Competition, Economic Intelligence

Taxonomy of Risks (cont.)

- Infrastructure
  - Unavailability, Faults, Defects
  - Illegal Use of Unlicensed Software
- Data
  - Unauthorized use or access
  - Storage of illegal material/information
  - Loss of data

Taxonomy of Risks (cont.)

- Trading or Operating Losses
  - Impact on Manufacturing Plant
  - Loss of configuration
  - Loss of data
- Data Leakage
  - Financial Information
  - Pricing or Sales Information
  - Customer Database
  - Contract, Answers to RFP (Request For Proposal)

Taxonomy of Risks (cont.)

- Identity Theft
- Fraud
- Employee's abuse
- Corporate's abuse
- Blackmail
- ...

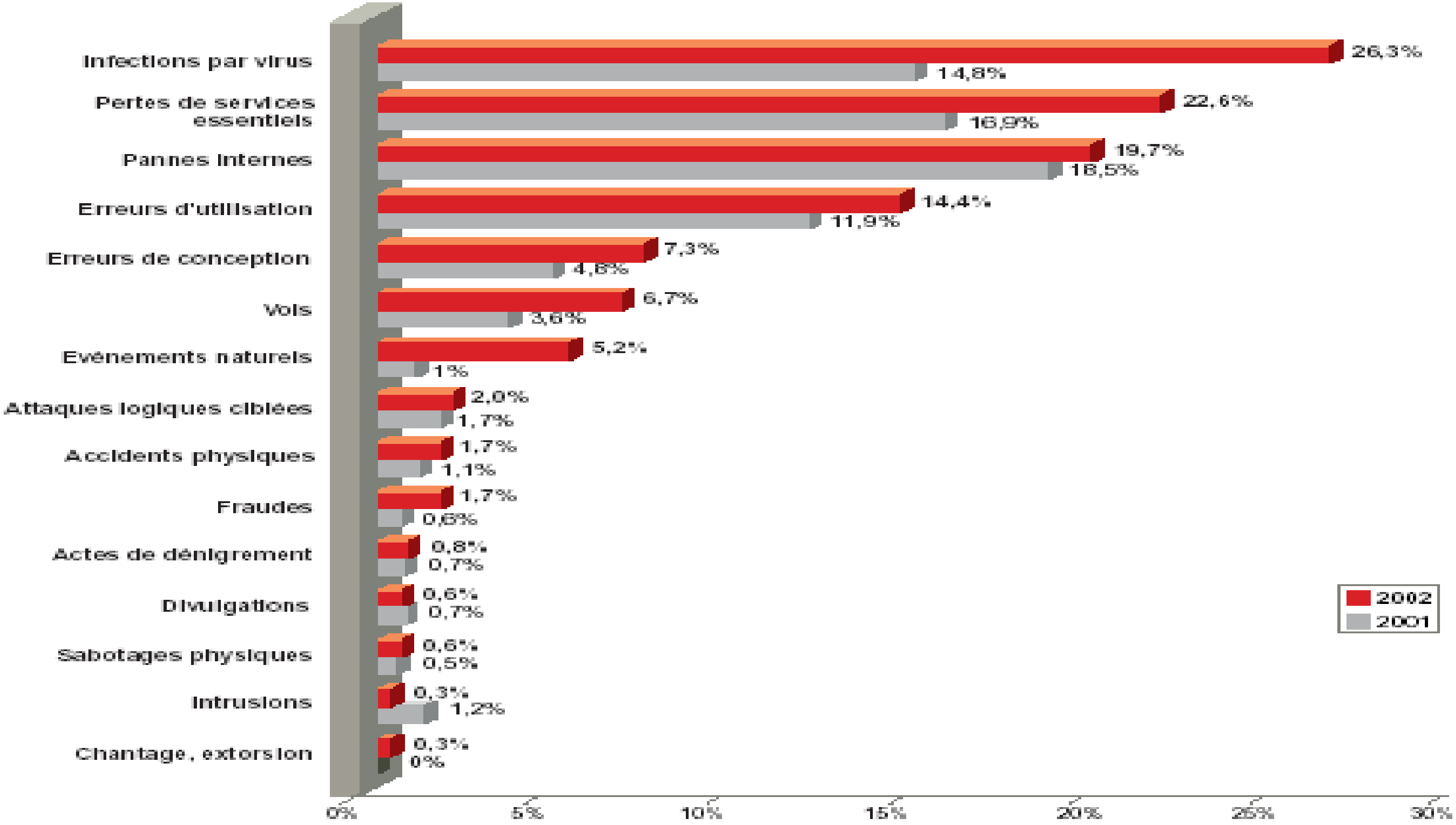
Classification

	Incident	**Security Incident**	**Disaster**
Class 4 : Critical	Major Failure of Server	DNS redirection	Tornado, fire
Class 3 : Severe	Application Error	DdoS, Root Compromis	Spying, theft
Class 2: Serious	Bug, Incomplete Backups	Scans, Probes	
Class 1 : Low Impact	User's Mistake	Virus , Abuse	

Outline

- *Introduction*
- Concepts
- Risks and Threats
- Methods and standards
    - ISO2700x, OCTAVE, Ebios, Mehari,
- Tools
    - Nessus, nmap, wireshark, ntop, ...
- Hand-on Labs

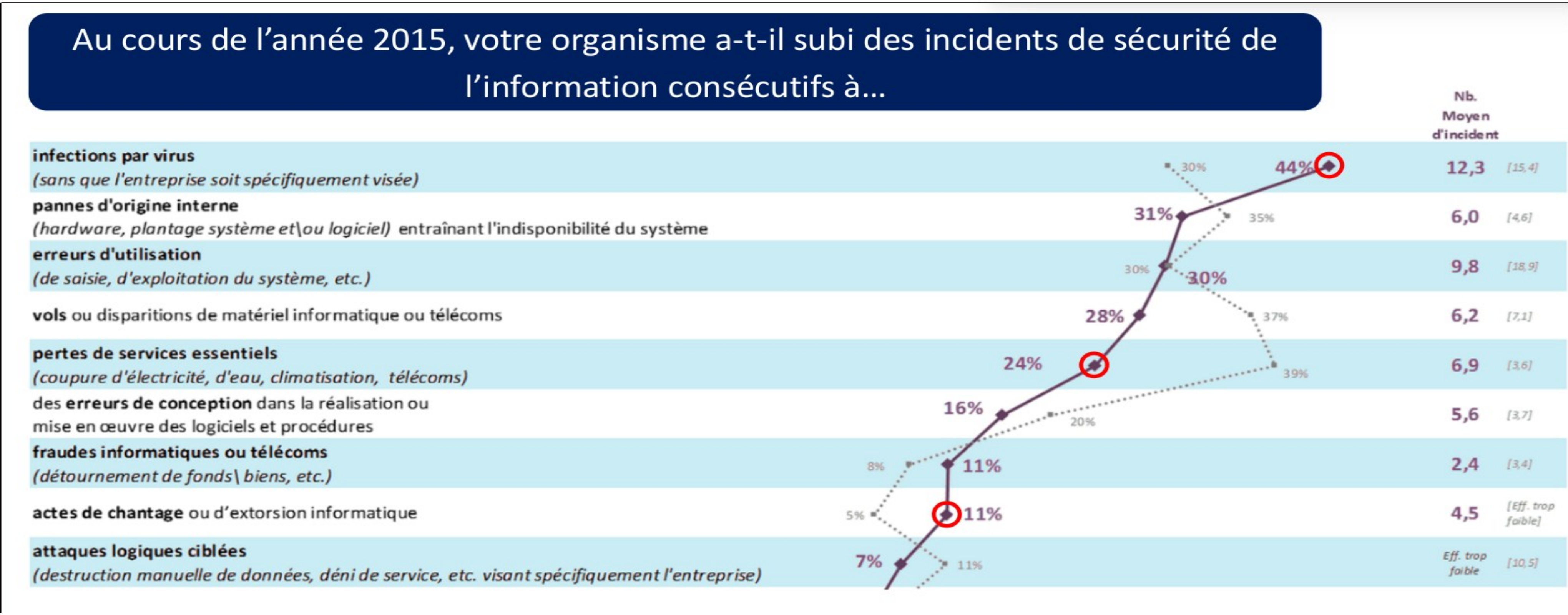
Threats by Clusif - Ages ago ...



Threats – Evolution

- Data Theft (*CLUSIF - Panorama 2004)*
- Malware (spyware, bots, keyloggers)
- Extortion / Ransomware (ex: crypted file)
- Identity Theft (*CLUSIF - Panorama 2006)*
- SCADA and critical infrastructures (*2007*)
- Auction Scam, illicit purchases

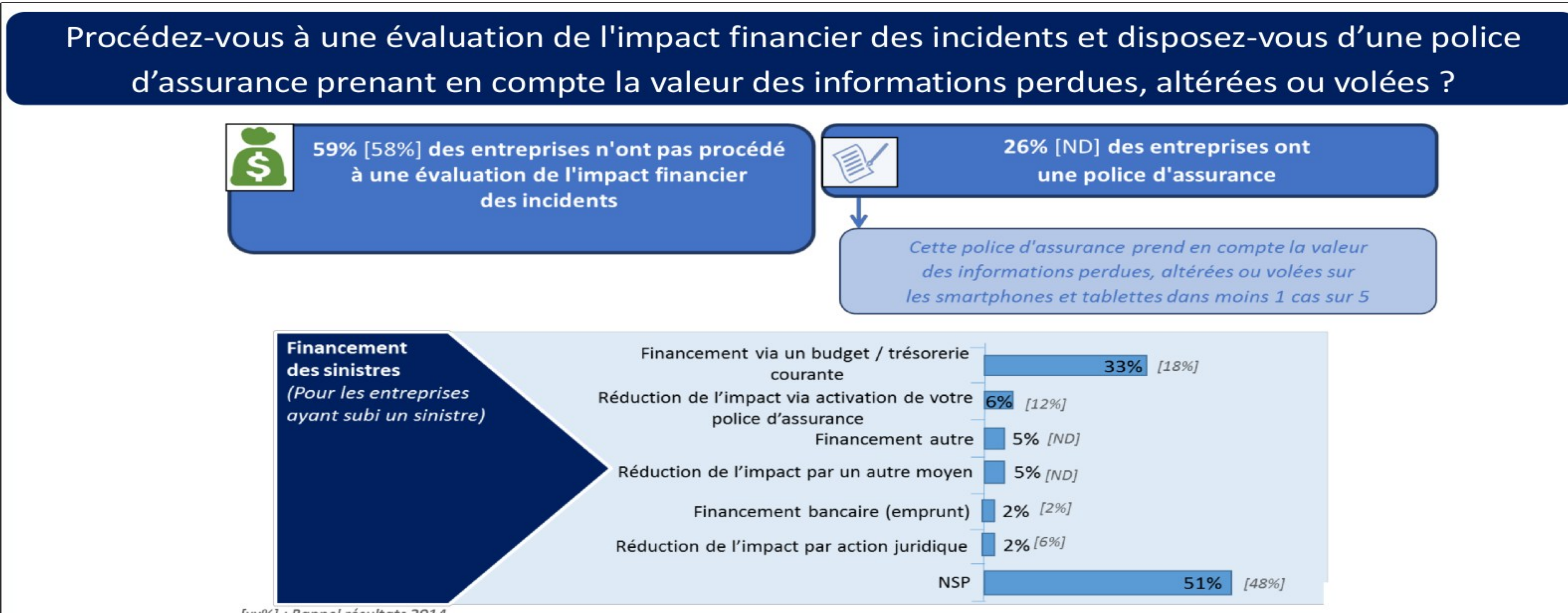
CLUSIF – Panorama 2016



Au cours de l'année 2015, votre organisme a-t-il subi des incidents de sécurité de l'information consécutifs à…

			Nb. Moyen d'incident	
infections par virus *(sans que l'entreprise soit spécifiquement visée)*	44%	30%	12,3	[15,4]
pannes d'origine interne *(hardware, plantage système et\ou logiciel)* entraînant l'indisponibilité du système	31%	35%	6,0	[4,6]
erreurs d'utilisation *(de saisie, d'exploitation du système, etc.)*	30%	30%	9,8	[18,9]
vols ou disparitions de matériel informatique ou télécoms	28%	37%	6,2	[7,1]
pertes de services essentiels *(coupure d'électricité, d'eau, climatisation, télécoms)*	24%	39%	6,9	[3,6]
des **erreurs de conception** dans la réalisation ou mise en œuvre des logiciels et procédures	16%	20%	5,6	[3,7]
fraudes informatiques ou télécoms *(détournement de fonds\ biens, etc.)*	11%	8%	2,4	[3,4]
actes de chantage ou d'extorsion informatique	11%	5%	4,5	[Eff. trop faible]
attaques logiques ciblées *(destruction manuelle de données, déni de service, etc. visant spécifiquement l'entreprise)*	7%	11%	Eff. trop faible	[10,5]

CLUSIF – Panorama 2016 (2)



Procédez-vous à une évaluation de l'impact financier des incidents et disposez-vous d'une police d'assurance prenant en compte la valeur des informations perdues, altérées ou volées ?

59% [58%] **des entreprises n'ont pas procédé à une évaluation de l'impact financier des incidents**

26% [ND] **des entreprises ont une police d'assurance**

Cette police d'assurance prend en compte la valeur des informations perdues, altérées ou volées sur les smartphones et tablettes dans moins 1 cas sur 5

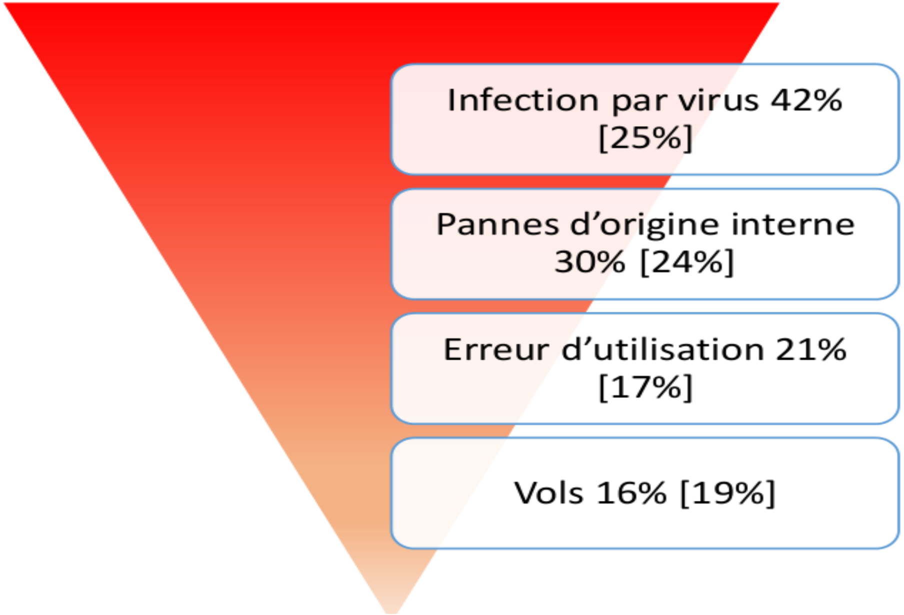
Financement des sinistres
(Pour les entreprises ayant subi un sinistre)

Financement via un budget / trésorerie courante	33%	[18%]
Réduction de l'impact via activation de votre police d'assurance	6%	[12%]
Financement autre	5%	[ND]
Réduction de l'impact par un autre moyen	5%	[ND]
Financement bancaire (emprunt)	2%	[2%]
Réduction de l'impact par action juridique	2%	[6%]
NSP	51%	[48%]

[xx%] : Rappel résultats 2014

CLUSIF – Panorama 2016 (3)

- Les pertes de services essentiels sont en recul constant depuis 2008, passant de 44% à 18% en 2016



Infection par virus 42% [25%]

Pannes d’origine interne 30% [24%]

Erreur d’utilisation 21% [17%]

Vols 16% [19%]

« New » Threats ?

Historical Motivations

- Extortion
- Unfair Competition
- Spying, Economic Intelligence
- Money
- Theft of data
- Identity theft

« New » Threats ?

New Targets

- Intellectual Property
- Market Share
- MindShare / Fame
- I.S. Availability / Operation
- *Executive's Liability*
- *Finance*
- *Profiles or Virtual Goods (Paypal, Online game),*
- *...*

New Vectors

- Sophisticated Malware
- Sophisticated Attack Strategies
- Active or Executable Contents everywhere
- Pervasive networking and computing
- USB, ZigBee, X10, ...
- IoT
- ...

Vulnerability

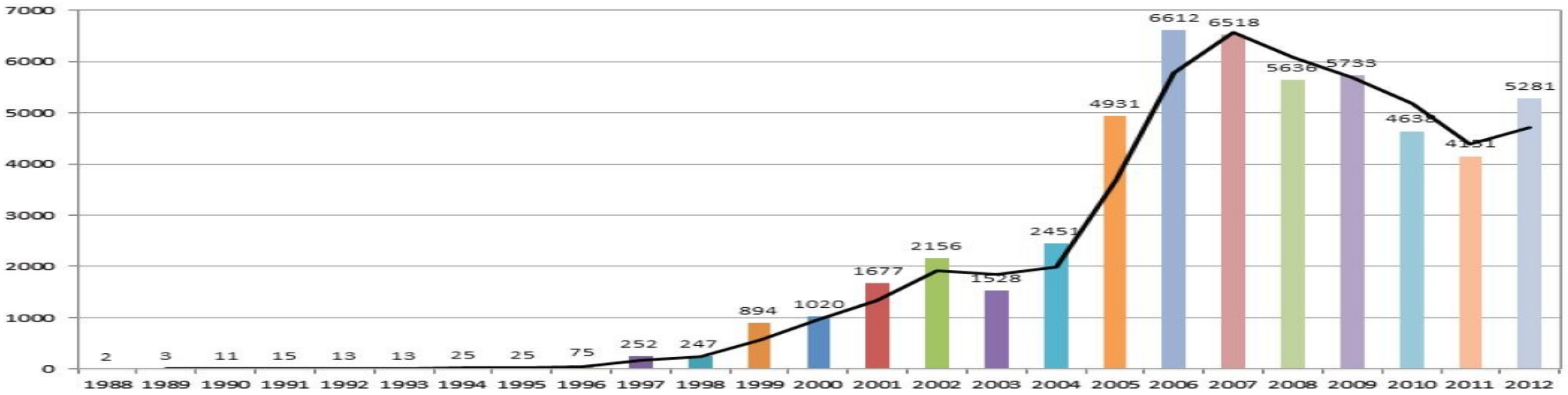
Failure or operational weakness of IS

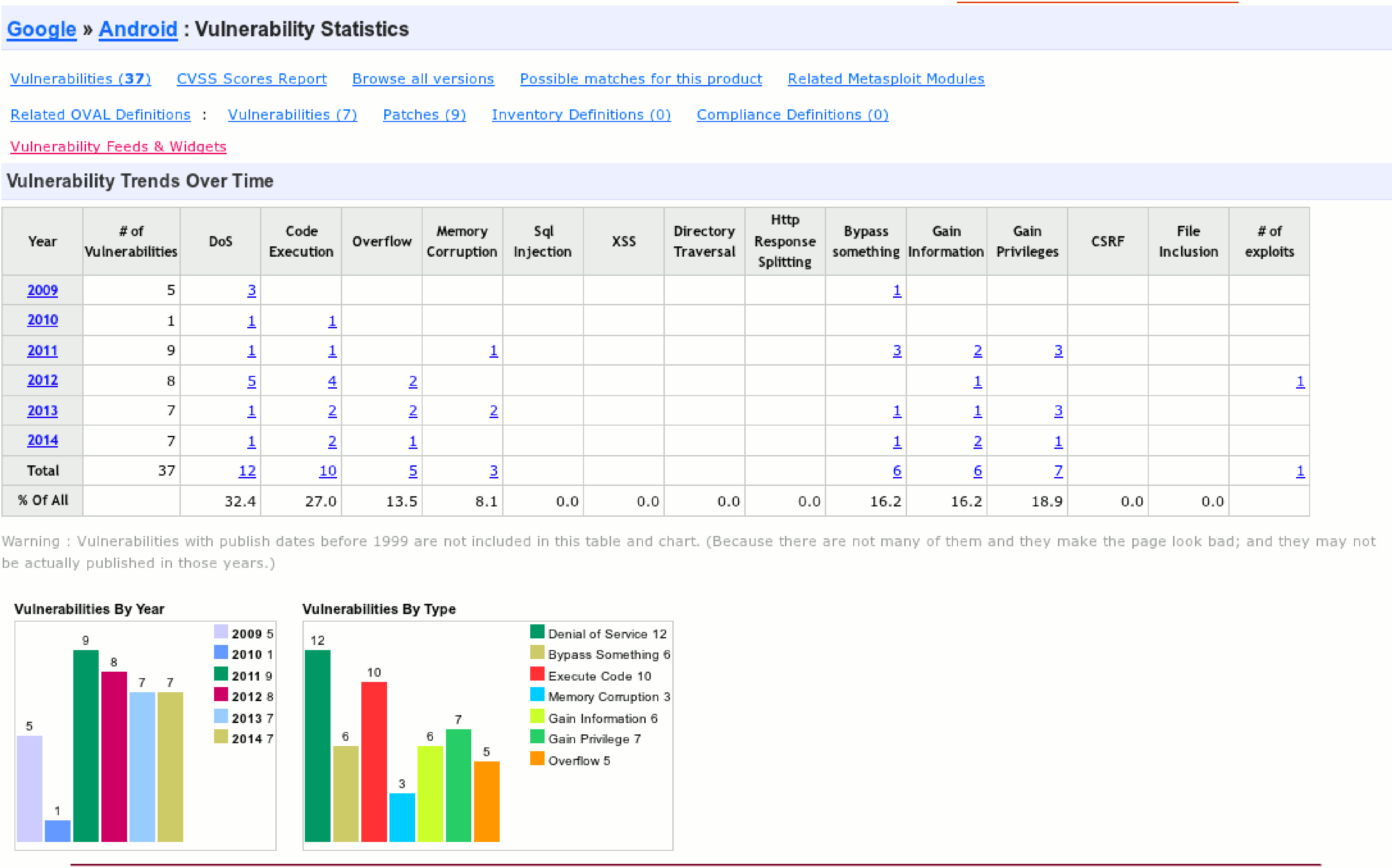
- Eventually known and documented;
- Can eventually be exploited.

Main reasons :

- Design/inception;
- Implementation;
- Operation.

0Day vuln


7000
6000
5000
4000
3000
2000
1000
0
2
3
11
15
13
13
25
25
75
252
247
894
1020
1677
2156
1528
2451
4931
6612
6518
5636
5733
4638
4151
5281
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012



Google » Android : Vulnerability Statistics

Vulnerabilities (37)   CVSS Scores Report   Browse all versions   Possible matches for this product   Related Metasploit Modules

Related OVAL Definitions : Vulnerabilities (7)   Patches (9)   Inventory Definitions (0)   Compliance Definitions (0)

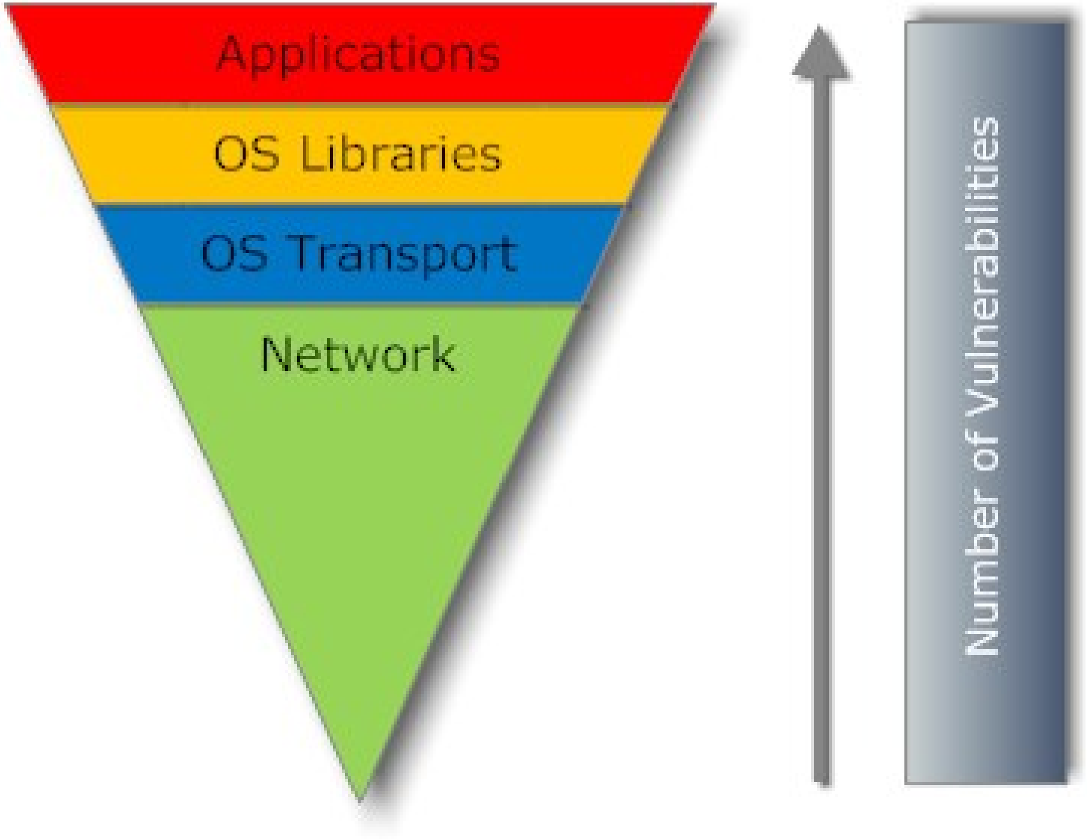
Vulnerability Feeds & Widgets

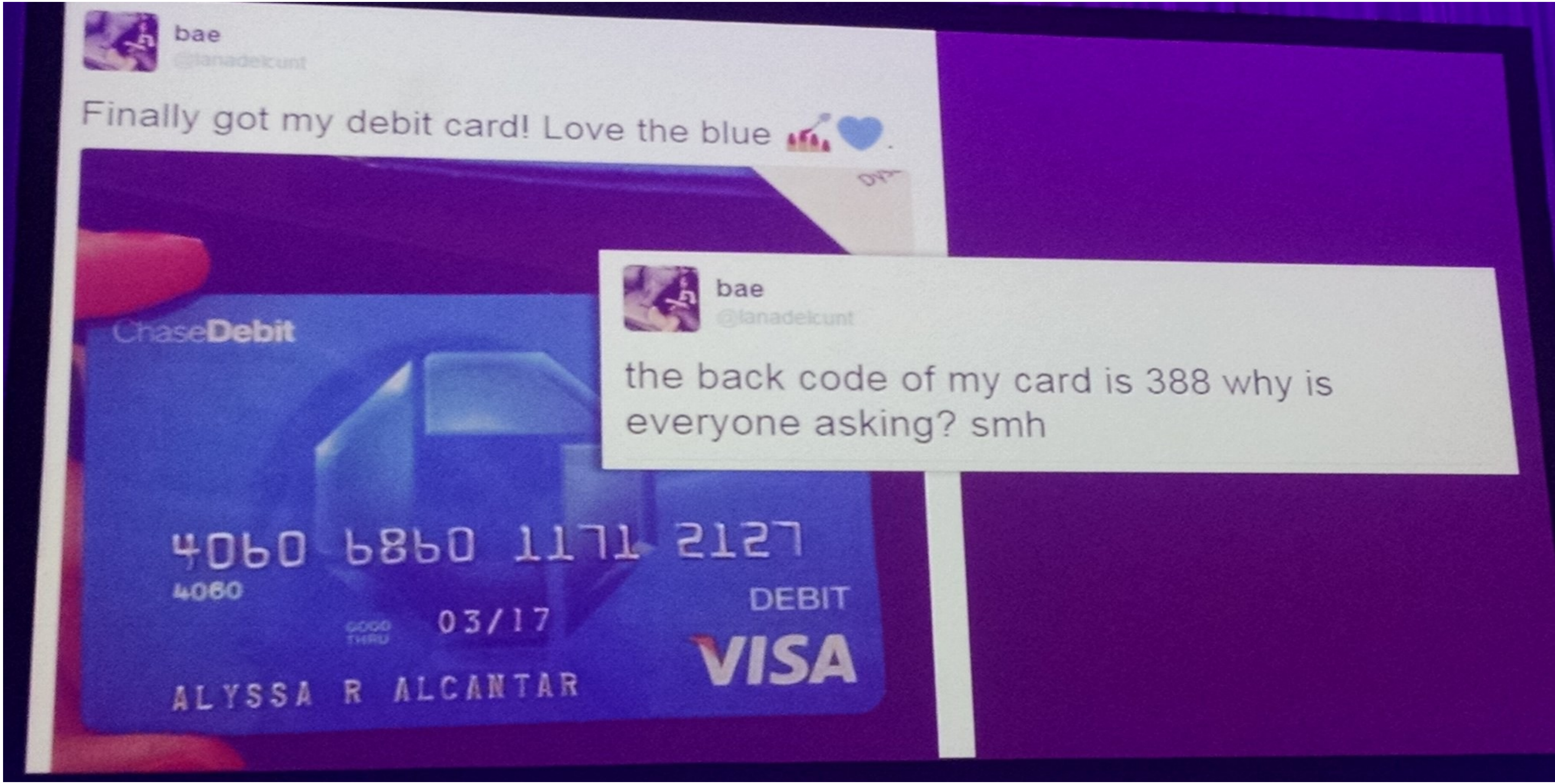
Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2009	5	3								1					
2010	1	1	1												
2011	9	1	1		1					3	2	3			
2012	8	5	4	2							1				1
2013	7	1	2	2	2					1	1	3			
2014	7	1	2	1						1	2	1			
Total	37	12	10	5	3					6	6	7			1
% Of All		32.4	27.0	13.5	8.1	0.0	0.0	0.0	0.0	16.2	16.2	18.9	0.0	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

Vulnerability - trends





bae
@lanadelcunt

Finally got my debit card! Love the blue 💅💙.

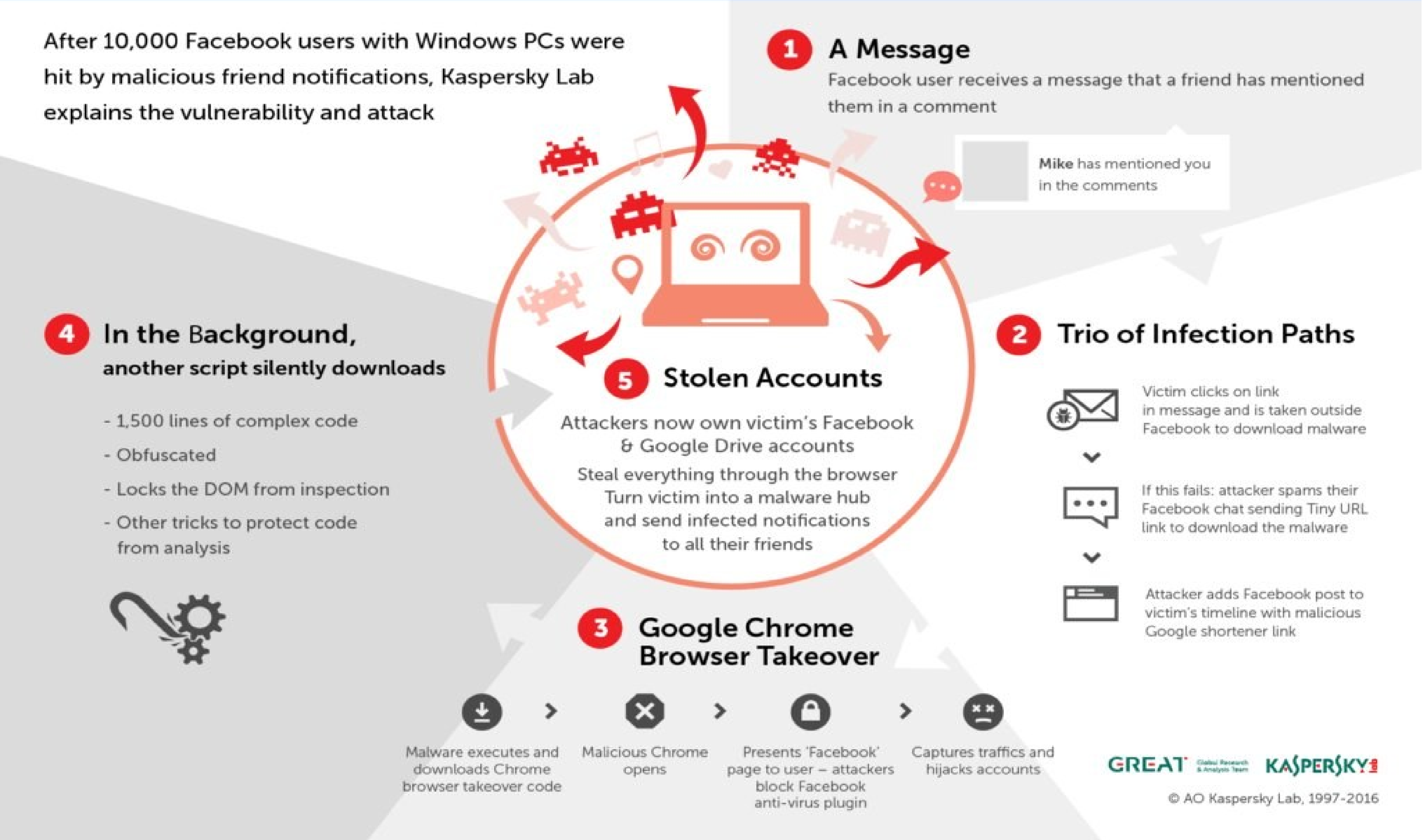
bae
@lanadelcunt

the back code of my card is 388 why is everyone asking? smh

There's no patch for stupidity ...

FACEBOOK MALWARE: COMPLEX CODE TRAPS VICTIMS INTO TARGETING FRIENDS

After 10,000 Facebook users with Windows PCs were hit by malicious friend notifications, Kaspersky Lab explains the vulnerability and attack



1 A Message

Facebook user receives a message that a friend has mentioned them in a comment

Mike has mentioned you in the comments

2 Trio of Infection Paths

Victim clicks on link in message and is taken outside Facebook to download malware

If this fails: attacker spams their Facebook chat sending Tiny URL link to download the malware

Attacker adds Facebook post to victim's timeline with malicious Google shortener link

3 Google Chrome Browser Takeover

Malware executes and downloads Chrome browser takeover code

Malicious Chrome opens

Presents 'Facebook' page to user – attackers block Facebook anti-virus plugin

Captures traffics and hijacks accounts

4 In the Background,

another script silently downloads

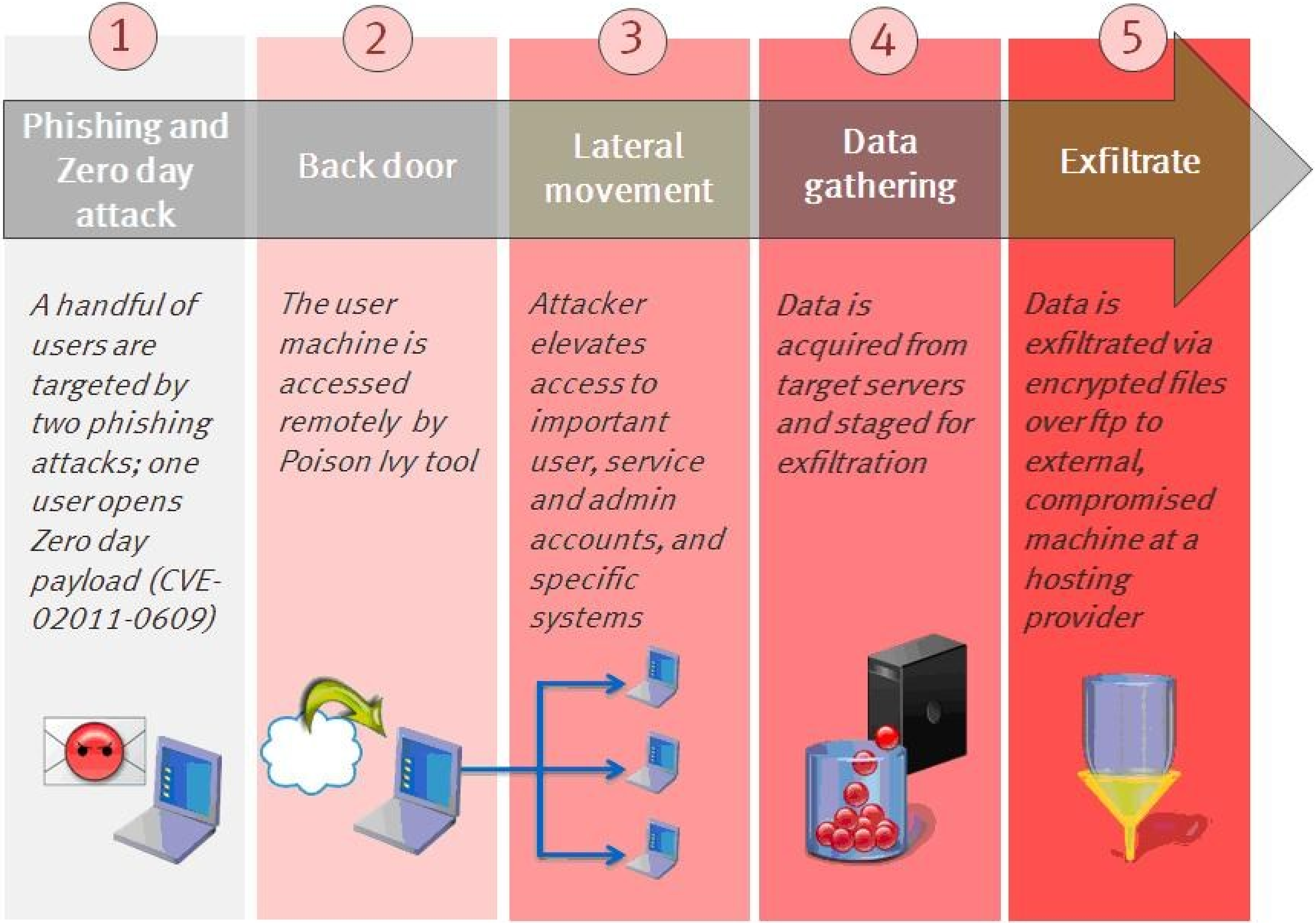
- 1,500 lines of complex code
- Obfuscated
- Locks the DOM from inspection
- Other tricks to protect code from analysis

5 Stolen Accounts

Attackers now own victim's Facebook & Google Drive accounts

Steal everything through the browser
Turn victim into a malware hub
and send infected notifications
to all their friends

GREAT Global Research & Analysis Team KASPERSKY lab



1

Phishing and Zero day attack

A handful of users are targeted by two phishing attacks; one user opens Zero day payload (CVE-02011-0609)

2

Back door

The user machine is accessed remotely by Poison Ivy tool

3

Lateral movement

Attacker elevates access to important user, service and admin accounts, and specific systems

4

Data gathering

Data is acquired from target servers and staged for exfiltration

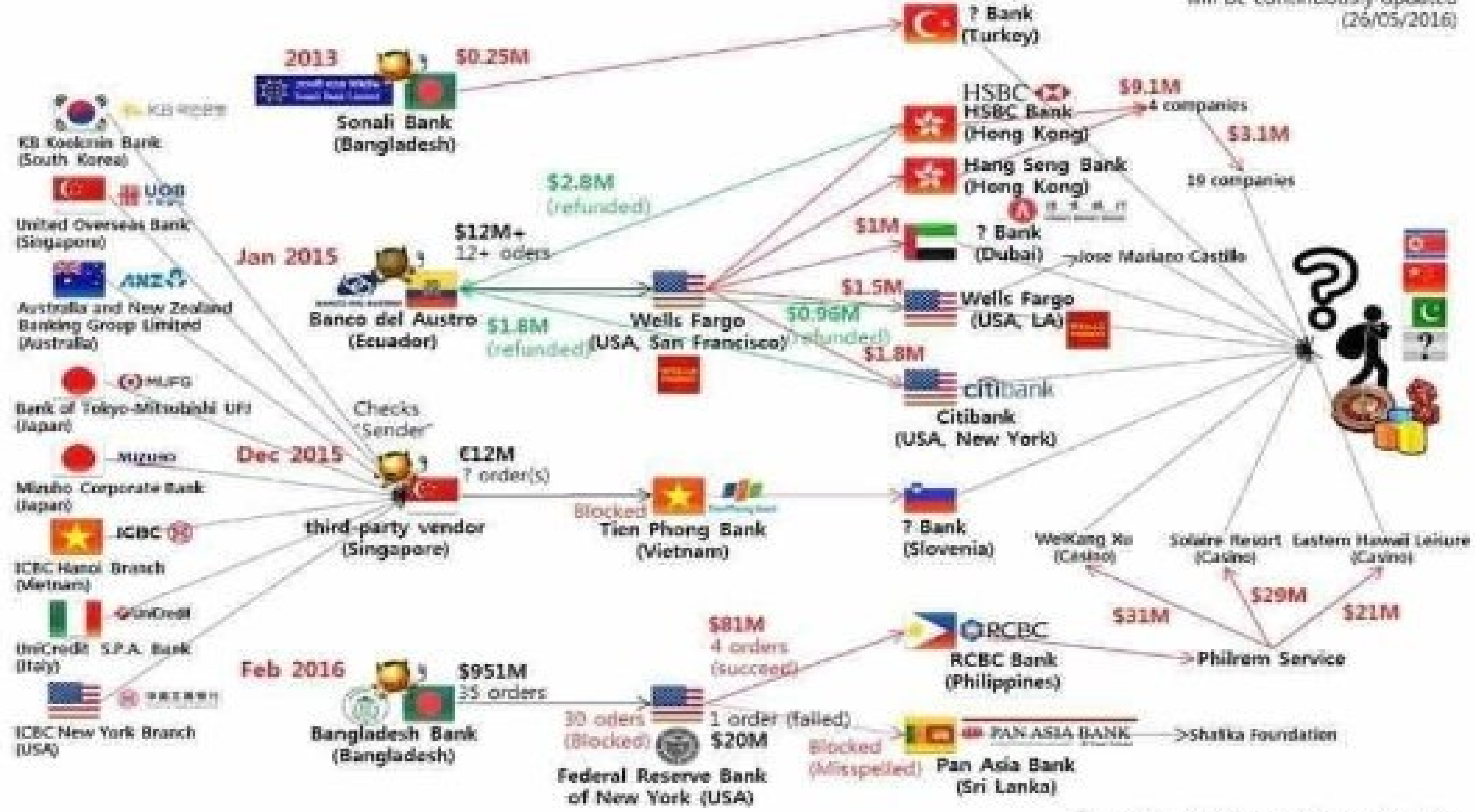
5

Exfiltrate

Data is exfiltrated via encrypted files over ftp to external, compromised machine at a hosting provider

Hacking the Worldwide Banking System (Using fraudulent SWIFT messages)

will be continuously updated
(26/05/2016)



2013
Sonali Bank
(Bangladesh)
$0.25M
? Bank
(Turkey)

KB Kookmin Bank
(South Korea)

United Overseas Bank
(Singapore)

Australia and New Zealand
Banking Group Limited
(Australia)

Bank of Tokyo-Mitsubishi UFJ
(Japan)

Mizuho Corporate Bank
(Japan)

ICBC Hanoi Branch
(Vietnam)

UniCredit S.P.A. Bank
(Italy)

ICBC New York Branch
(USA)

Jan 2015
Banco del Austro
(Ecuador)
$12M+
12+ oders
$2.8M
(refunded)
$1.8M
(refunded)
Wells Fargo
(USA, San Francisco)
HSBC
HSBC Bank
(Hong Kong)
Hang Seng Bank
(Hong Kong)
$1M
? Bank
(Dubai)
$1.5M
Wells Fargo
(USA, LA)
$0.96M
(refunded)
$1.8M
citibank
Citibank
(USA, New York)
$9.1M
4 companies
$3.1M
19 companies
Jose Mariano Castillo

Checks
"Sender"

Dec 2015
third-party vendor
(Singapore)
€12M
7 order(s)
Blocked
Tien Phong Bank
(Vietnam)
? Bank
(Slovenia)

WeiKang Xu
(Casino)
Solaire Resort
(Casino)
Eastern Hawaii Leisure
(Casino)
$31M
$29M
$21M

Feb 2016
Bangladesh Bank
(Bangladesh)
$951M
35 orders
30 oders
(Blocked)
Federal Reserve Bank
of New York (USA)
$81M
4 orders
(succeed)
RCBC
RCBC Bank
(Philippines)
Philrem Service
1 order (failed)
$20M
Blocked
(Misspelled)
PAN ASIA BANK
Pan Asia Bank
(Sri Lanka)
Shalika Foundation

From https://twitter.com/issuemakerslab

Top 10 – owasp.org (1)

- **A1 – Injections Flaws Injection flaws, such as SQL, OS, and LDAP** injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.
- **A2 - Cross Site Scripting (XSS)** XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.
- **A3 - Broken Authentication and Session Management**

  Application functions related to authentication and session management are often notimplemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users’ identities.

Top 10 – owasp.org (2)

- **A4 - Insecure Direct Object Reference** A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.
- **A5 - Cross Site Request Forgery (CSRF)** A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the web application that it attacks.
- **A6 – Security Misconfiguration**

  Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform.

Top 10 – owasp.org (3)

- **A7: Insecure Cryptographic Storage** Many web applications do not properly protect sensitive data, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing.
- **A8: Failure to Restrict URL** Access Many web applications check URL access rights before rendering protected links and buttons.
- **A9: Insufficient Transport Layer Protection** Applications frequently fail to authenticate, encrypt, and protect the confidentiality and integrity of sensitive network traffic.
- **A10: Unvalidated Redirects and Forwards** Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination page

References – More readings

- 'Secret and Lies', Bruce Schneier
- Clusif - https://clusif.fr
- RISKS DIGEST
  - Forum on Risks to the Public in Computers and Related Systems
  - http://catless.ncl.ac.uk/Risks

Tutoring

Exercise 3

- Investigate and present an existing attack or incident from the vulnerability to exploitation amongst the following categories
    - Virus/Worm (ex: stuxnet, flame)
    - Priviledge escalation
    - Use of weak cryptography
    - Social Engineering
    - Heartbleed, ShellShock
    - 0-Day / Xploit toolkit (Shadow Broker)

Exercise 4

- Identify, quantify and classify the risks for the following scenario:
  - As a system administrator of an SMB, you are requested to deploy laptops with nomadic access to corporate network. You will present the company management with a risk analysis as well as way to mitigate the threats.
  - A similar assesment will be conducted for the deployment and use of hosted services (aka “cloud”) such as Gmail, google doc, salesforce.com, ...