ITU

CENTRAL BANK OF EGYPT
Egyptian Banking Institute

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

Keystone

Securing the Critical Infrastructure for Financial Industry

Cairo – Egypt, 14-15 October 2018

Haythem EL MIR & Hosni Tounsi

Haythem.elmir@keystone.tn & hosni.tounsi@keystone.tn

KEYSTONE Consulting

« We help building Cybersecurity as a keystone for Digital Transforamtion »

Workshop agenda

Day 1: Understanding cyber threats and security measures for banks

Part 1: Cyber threats landscape

- Banking information system: Environmental complexity
- Security breaches getting more sophisticated,
- New threats and vulnerabilities
- Threat vectors
- Know your enemy
- Anatomy of an attack: Real cases

Part 2: Cybersecurity needs

- What cybersecurity strategy to secure banks and fight cyberattacks?
- Internal cybersecurity organisation
- Importance of compliance: ISO27k, PCI/DSS, etc.
- Operational security

Workshop agenda

Day 2: Toward a new cybersecurity approach

Part 3: Cybersecurity for the sector

Internal CERTs and SOCs for Banks: why and how?
Information Sharing among the financial sector
Incident response coordination

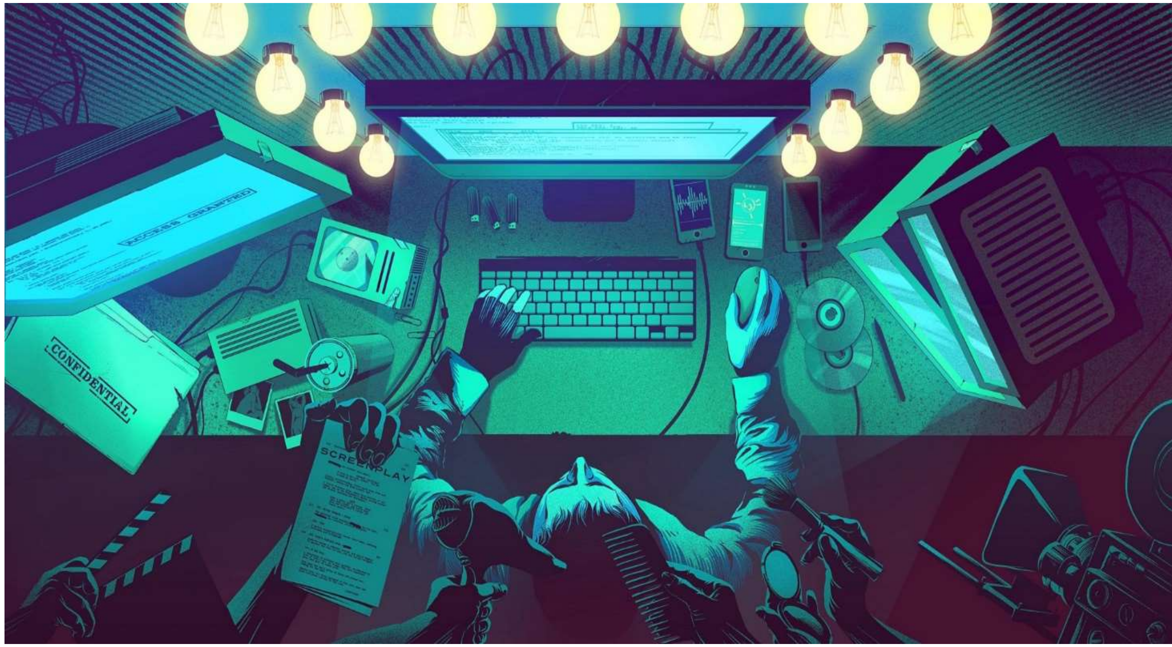
Part 4: Cyber exercise

Live demos - Cases study – Cyber Exercise

INTRODUCTION

Introduction

Criminals are always interested to steal money from banks, they even continue to risk their lives for it.



But …

CYBERCriminals become more interested, more attracted, more efficient, more dangerous and less risky.

Introduction

- In the modern digital economy, criminals are becoming ever more creative in ways to make off with millions without having to leave home.

- Cybercriminals could actually negatively impact a country's economy.

Unchained malware

Multi-stage bank attack

AI bots

Stock exchange attack

Introduction

Banks are a favorite target for cybercriminals and even for hacktivist, script kiddies and state sponsored attacks.

We are no longer in the era of classic virus infection and Trojan horses, hackers are looking to:

- **Steal money,**
- **Steal data,**
- **Damage the bank reputation,**
- **Steal customer information,**
- **Cause service interruption,**
- **Etc.**

Botnet
Jackpotting
Carding
APT
SQLi
Fraud
DDoS
ATM
SWIFT
OLBS
Ransomware
Phishing
SKIMMING

Current situation

- Very fast IT development,
- Open Bank, Online Services, Remote access,
- Digitalization,
- Diversification of means of payment,
- Overlay of multiple perimeters with heterogeneous technologies,
- Difficulties to get a full control over all perimeters,
- Presence of a large number of vulnerable systems,

- **Result➔ systems are exposed to very sophisticated threats = Attacks = Fraud.**

Banking infrastructure

CBS

RBS

Processing

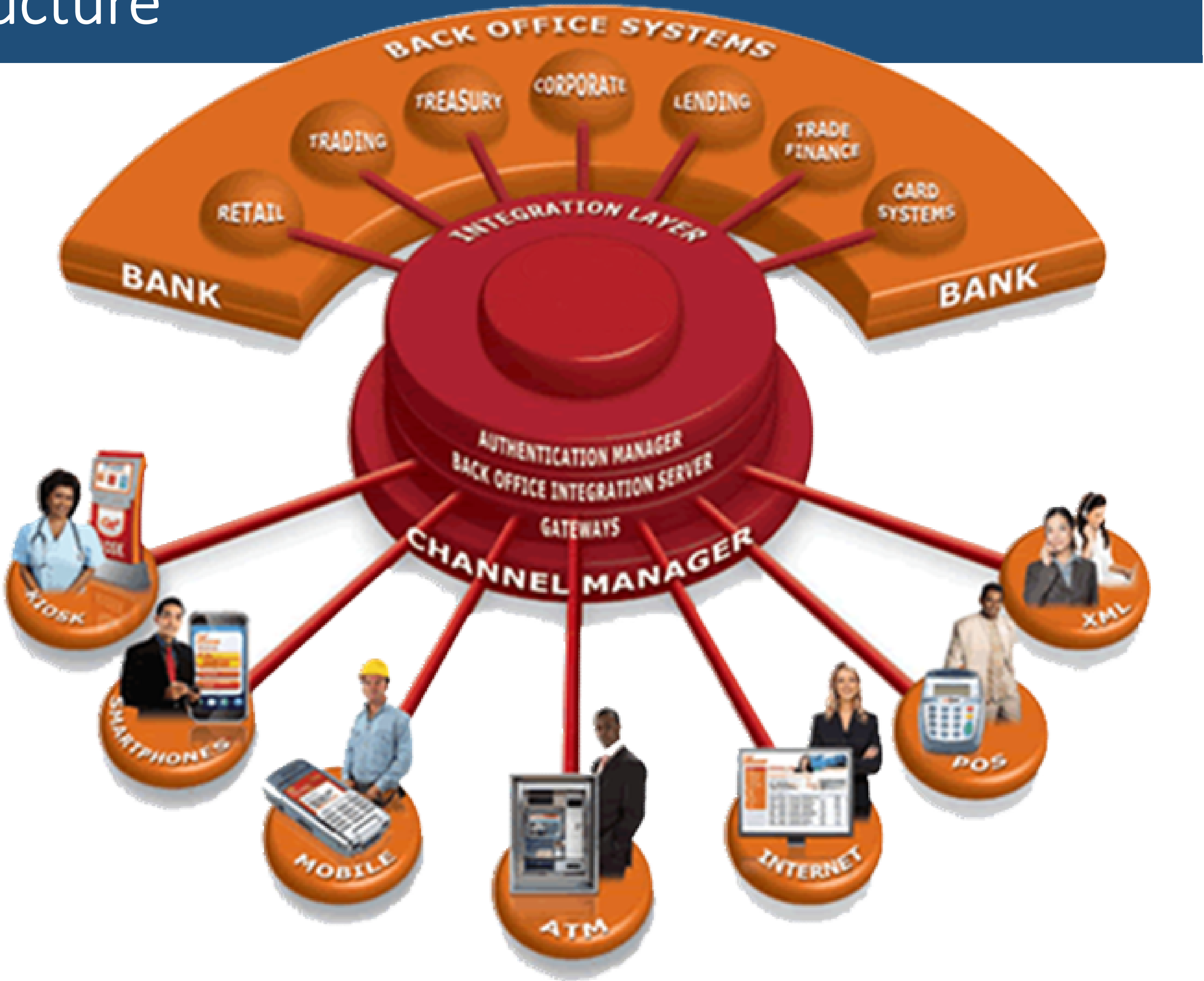
CRM

ERP

HR

DMS

…

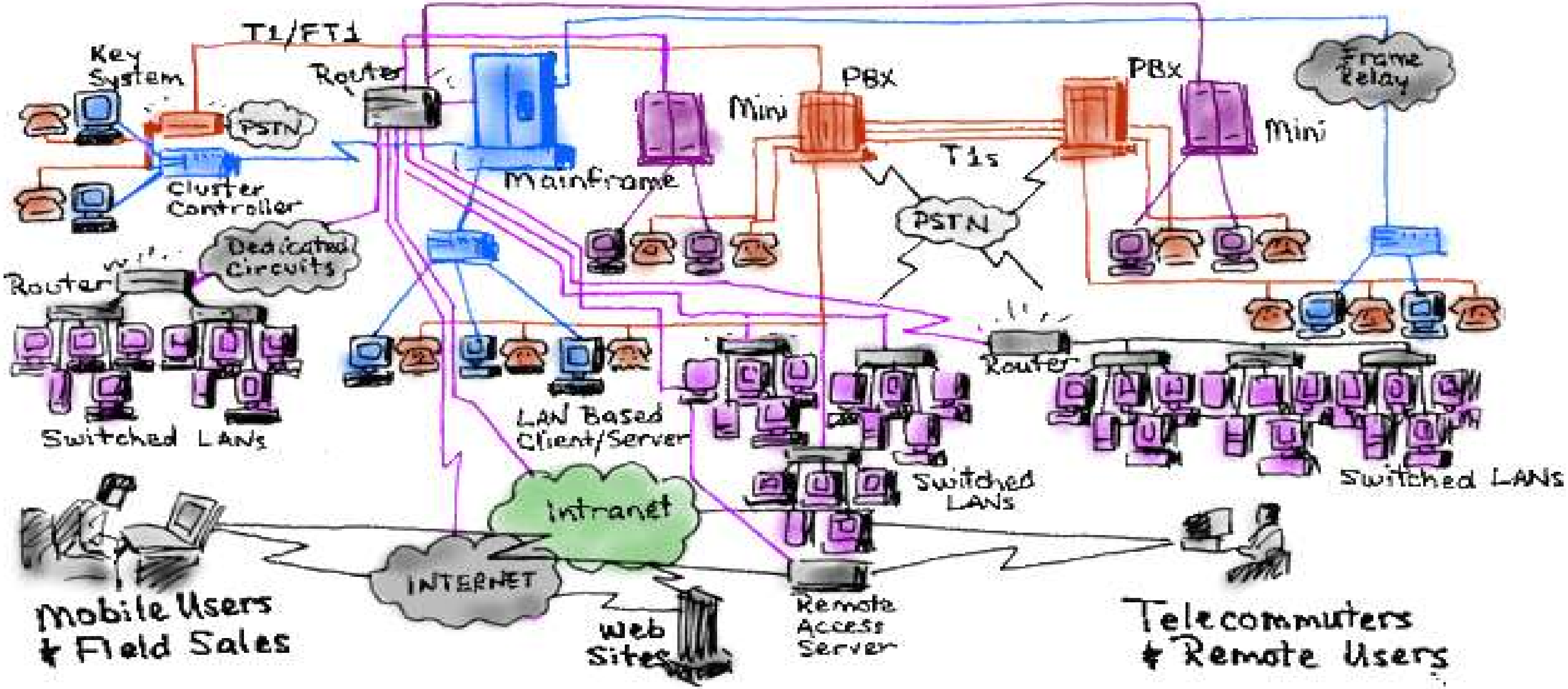


Banking infrastructure

- Thousands of local users:
  - Workstation/smartphones,
  - Multiple accounts for each user,
  - Different access levels and privileges per user,
  - Credit card, Online Banking account,
  - etc.
- Tens/hundreds of thousands of customers,
- Tens/hundreds of applications (local and external),
- Hundreds of remote branches,
- Tens ow WAN connections,
- hundreds of servers,
- Etc.

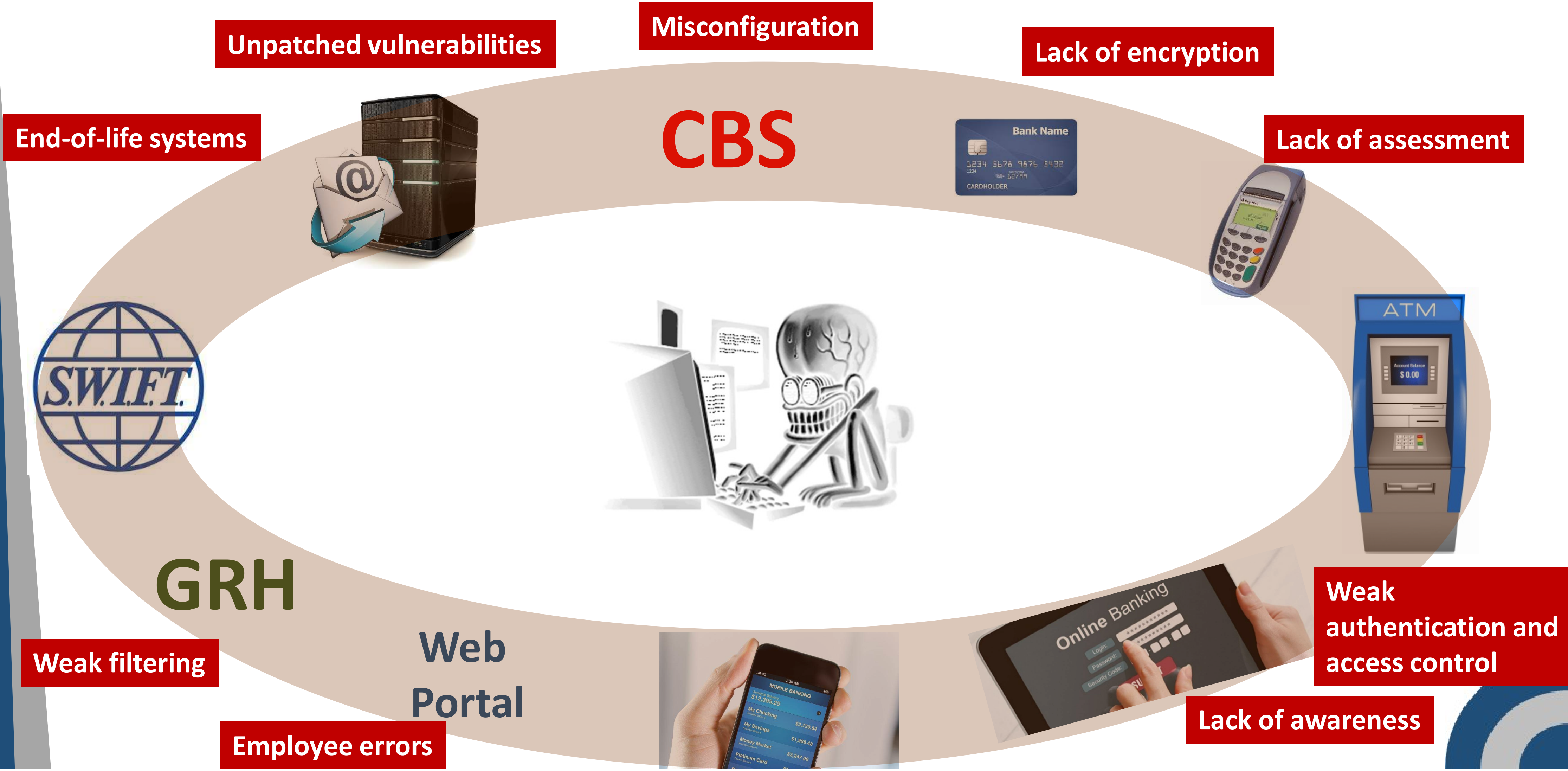
➔ Securing a bank is very challenging

Banking infrastructure



MAIN THREATS AND ATTACK VECTORS

Attack vectors



Unpatched vulnerabilities

Misconfiguration

Lack of encryption

End-of-life systems

CBS

Lack of assessment

GRH

Web Portal

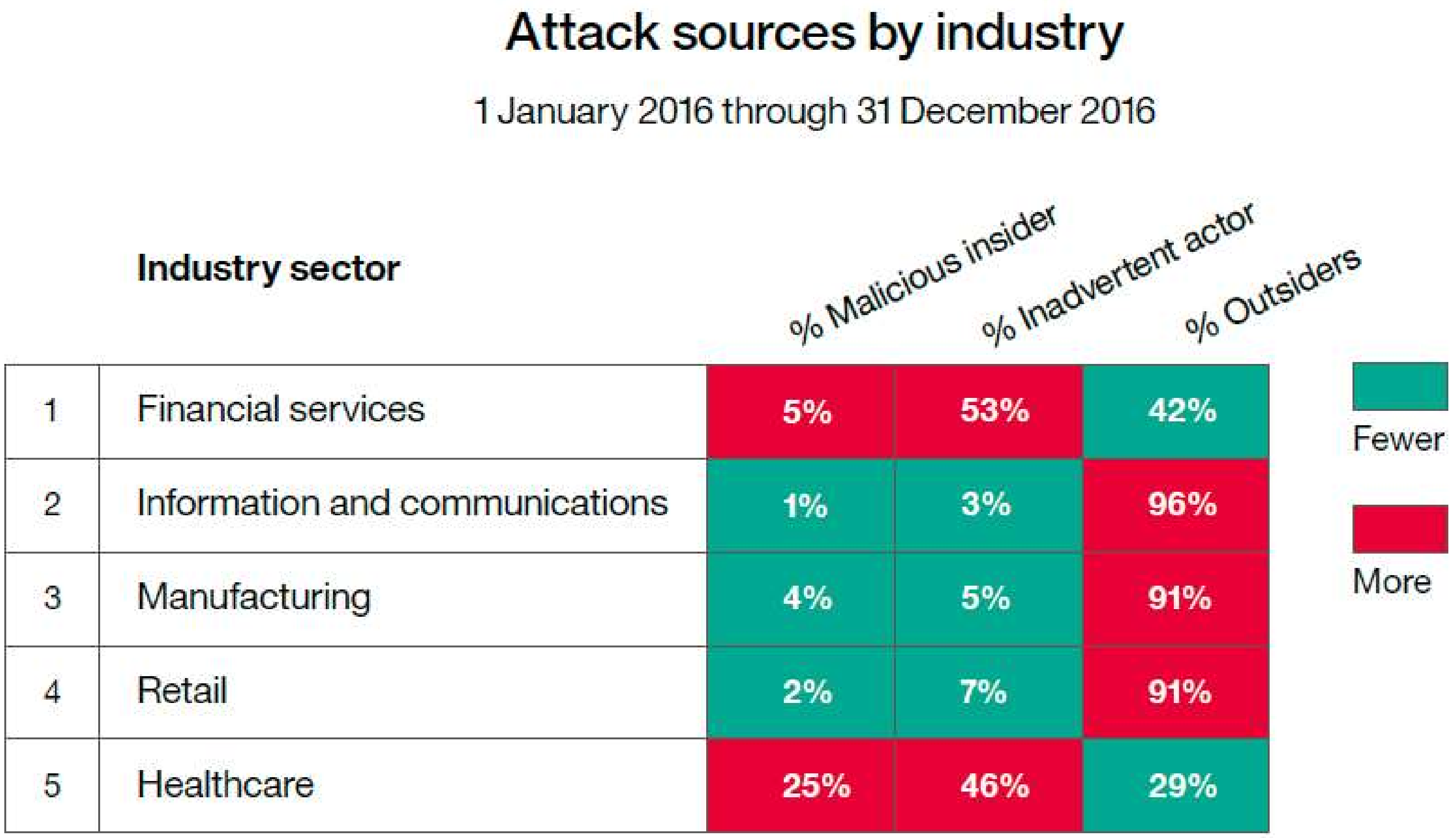
Weak filtering

Employee errors

Weak authentication and access control

Lack of awareness

Attack vectors



Attack sources by industry

1 January 2016 through 31 December 2016

	Industry sector	% Malicious insider	% Inadvertent actor	% Outsiders
1	Financial services	🟥 5%	🟥 53%	🟩 42%
2	Information and communications	🟩 1%	🟩 3%	🟥 96%
3	Manufacturing	🟩 4%	🟩 5%	🟥 91%
4	Retail	🟩 2%	🟩 7%	🟥 91%
5	Healthcare	🟥 25%	🟥 46%	🟩 29%

🟩 Fewer

🟥 More

Figure 9: Attack sources by industry – 1 January 2016 through 31 December 2016.

IBM X-Force Threat Intelligence Index 2017

83 millions of new fraudulent account between 2015 and 2017

Fraudulent payment increased by 100% during last years.

Full control of remote systems attack increased by 170%, and now every 10 sec.

Attack statistics

2017 Incident Highlights

❑159,700 total cyber incidents in 2017 (OTA)

❑93% of breaches could have been prevented (OTA)

❑18.2% increase in reported breach incidents (RBS)

❑7 billion records exposed in first 3 quarters (RBS)

❑$5 billion financial impact of ransomware (CV)

❑90% rise in business targeted ransomware (Symantec)

❑$5.3 billion in global BEC losses (FBI)

Worldwide estimates. Sources: (OTA) Online Trust Alliance, (RBS) Risk Based Security, Cybersecurity Ventures (CV)

Cyber Incident & Breach Trends Report

Vulnerabilities

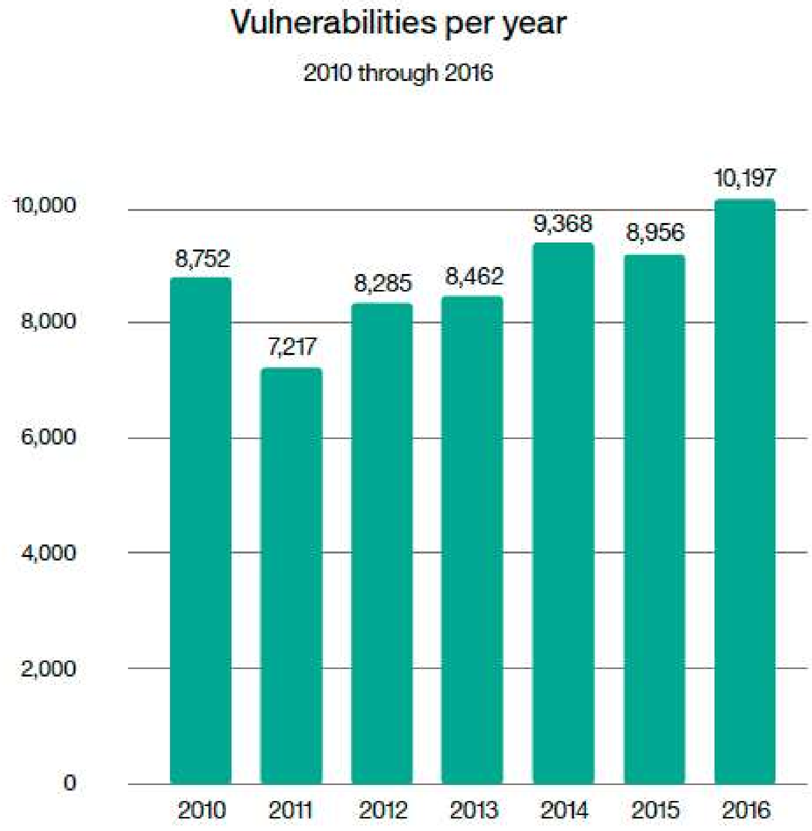


Figure 5: Vulnerabilities per year – 2010 through 2016.

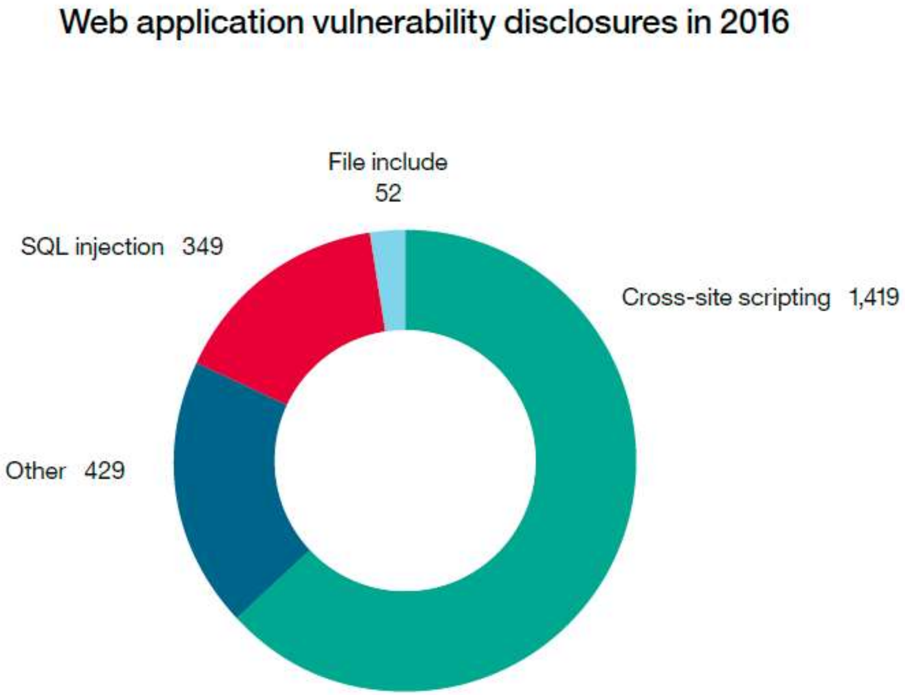


Figure 6: Web application vulnerability disclosures in 2016.

IBM X-Force Threat Intelligence Index 2017

SQLi

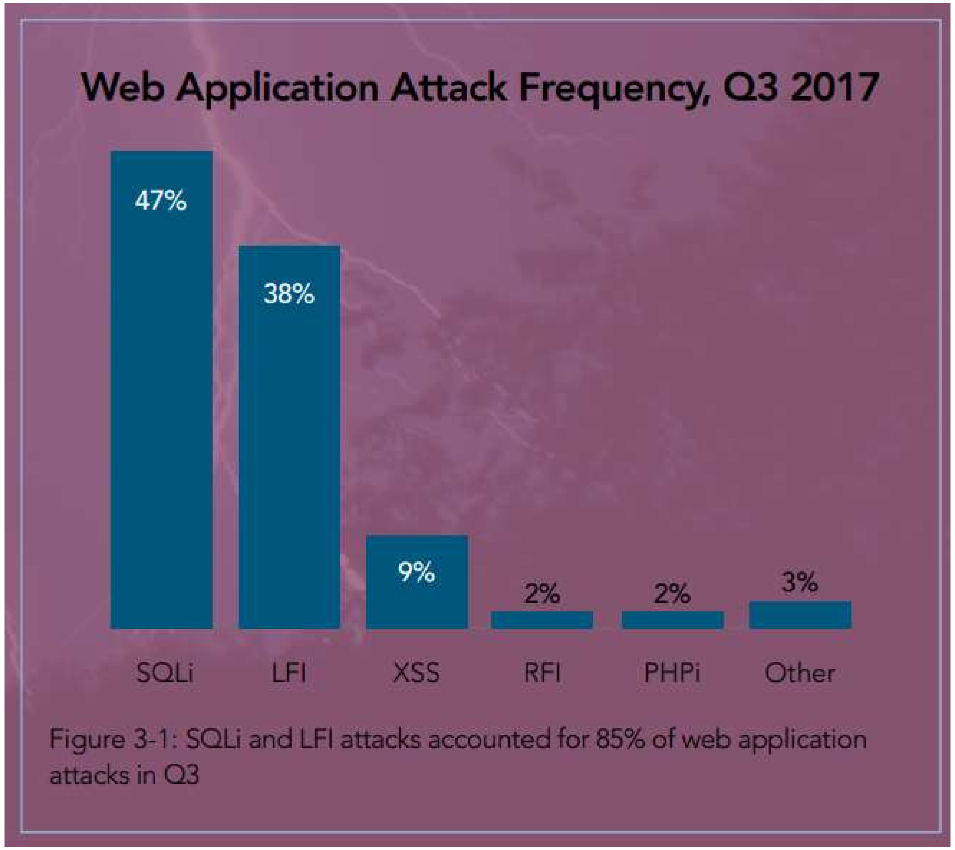


Figure 3-1: SQLi and LFI attacks accounted for 85% of web application attacks in Q3

https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3-2017-state-of-the-internet-security-report.pdf

SWIFT attack case (2016)

US$81 million

Lazarus group could have made off with $1 billion

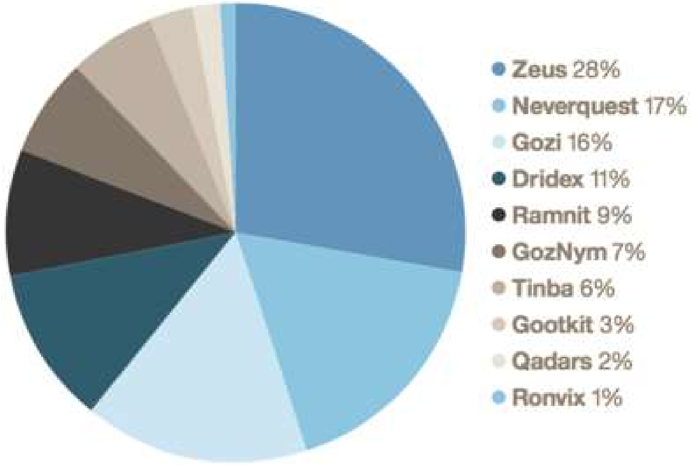
APT: Carbanack case

- Spear phishing → Old vulnerabilities exploitation,
- Remote command execution (screenshot capture while accessing sensitive web application, cookies theft, etc.)
- Install a RAT (Ammyy Admin) for lateral attacks to access the banking accounts processing systems,
- On the target, the attacker record the screen activities to get familiar with procedures and banking workflow via the stolen data.
- These information is used to steal money via SWIFT network.

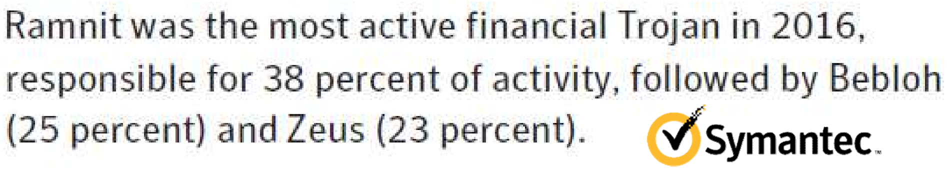
A billion-dollar APT

Malware and malicious apps

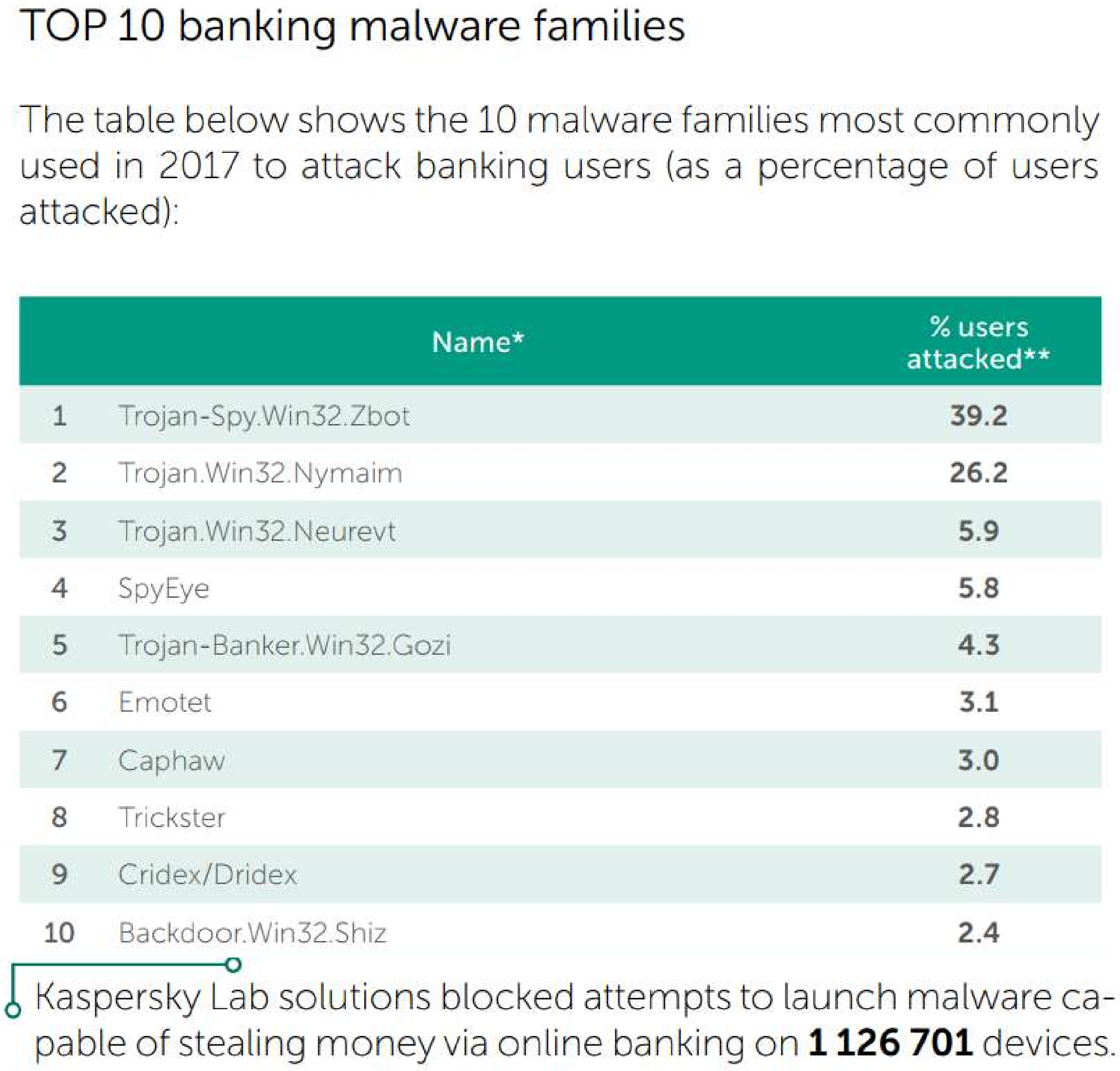
The Top 10 Banking Trojans for 2017



https://blog.barkly.com/top-banking-trojans-2017



Ramnit was the most active financial Trojan in 2016, responsible for 38 percent of activity, followed by Bebloh (25 percent) and Zeus (23 percent). Symantec.



TOP 10 banking malware families

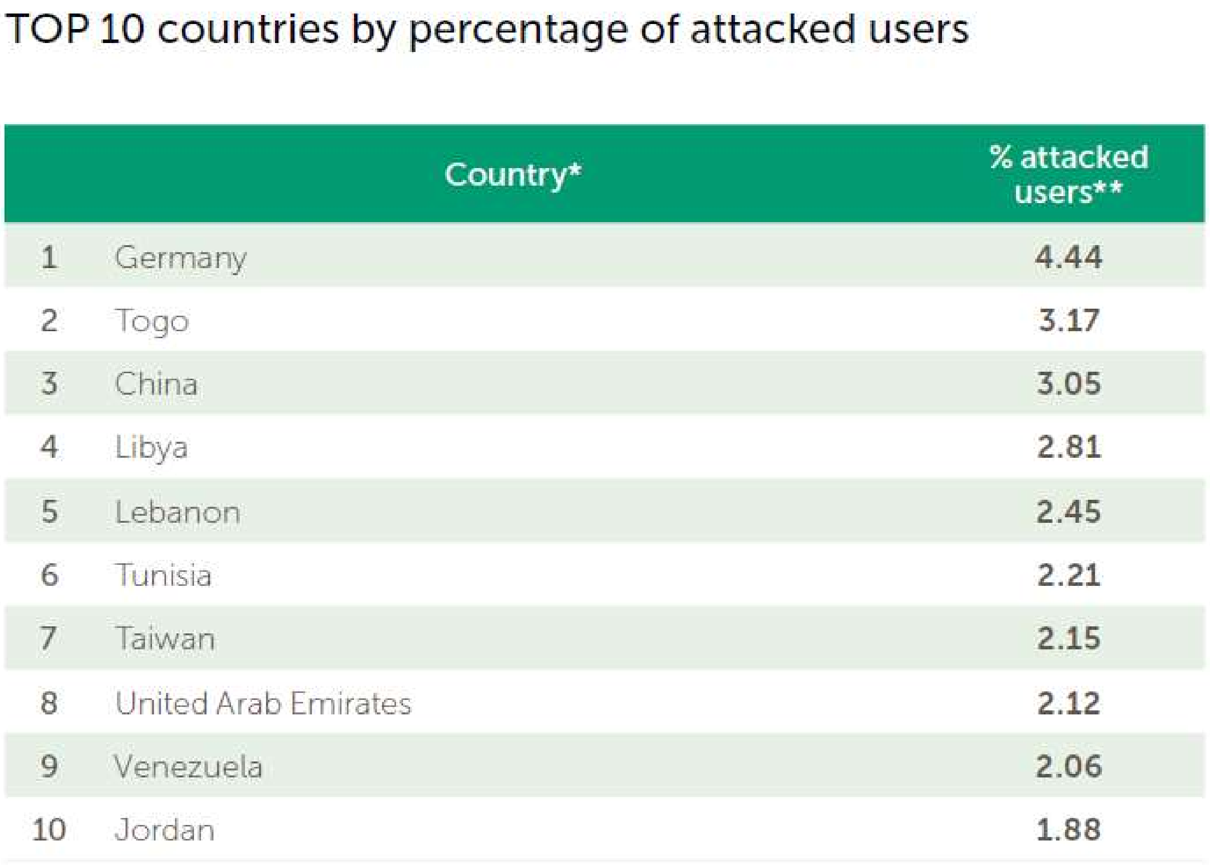
The table below shows the 10 malware families most commonly used in 2017 to attack banking users (as a percentage of users attacked):

	Name*	% users attacked**
1	Trojan-Spy.Win32.Zbot	39.2
2	Trojan.Win32.Nymaim	26.2
3	Trojan.Win32.Neurevt	5.9
4	SpyEye	5.8
5	Trojan-Banker.Win32.Gozi	4.3
6	Emotet	3.1
7	Caphaw	3.0
8	Trickster	2.8
9	Cridex/Dridex	2.7
10	Backdoor.Win32.Shiz	2.4

Kaspersky Lab solutions blocked attempts to launch malware capable of stealing money via online banking on **1 126 701** devices.

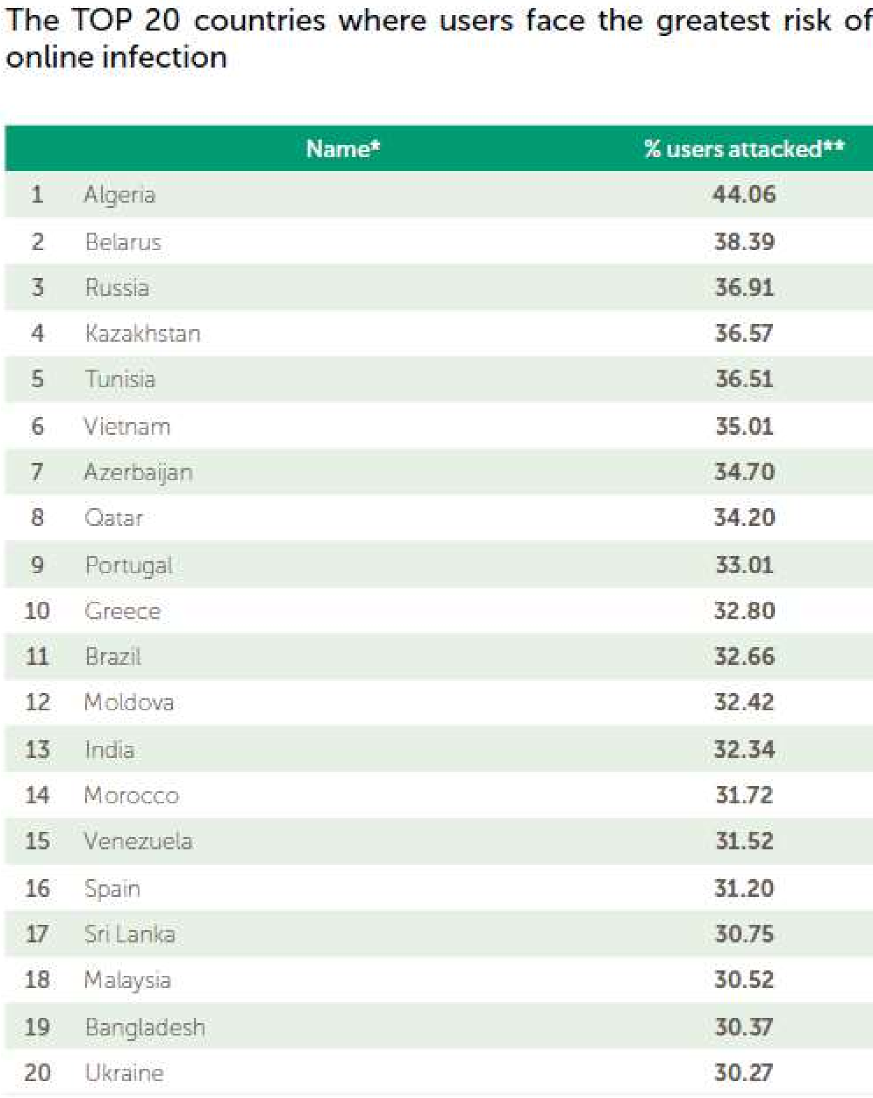
Malware

Kaspersky 2017: ONLINE THREATS IN THE FINANCIAL SECTOR



TOP 10 countries by percentage of attacked users

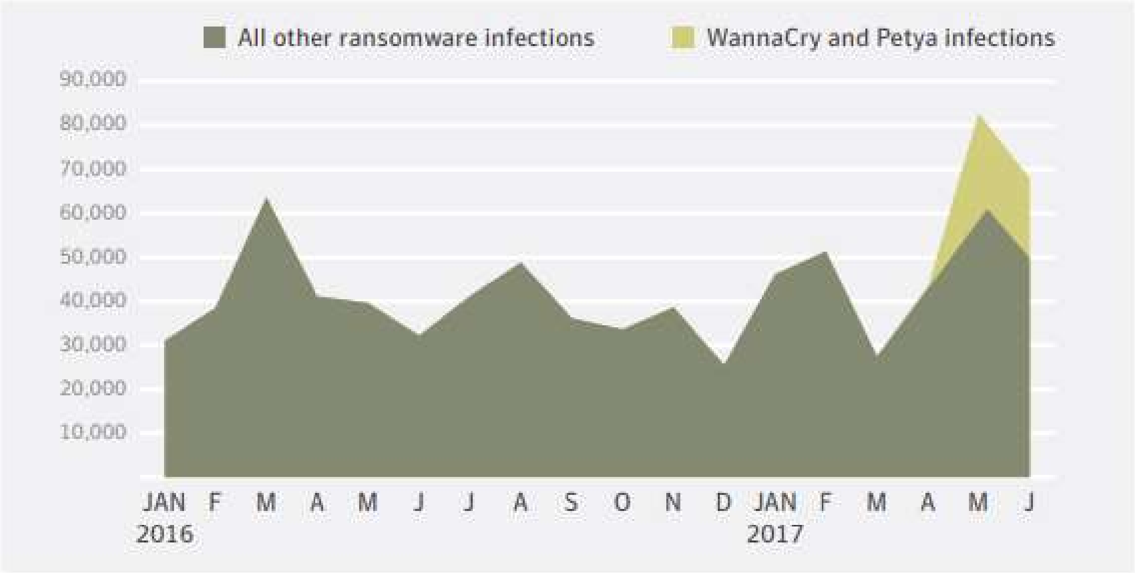
	Country*	% attacked users**
1	Germany	4.44
2	Togo	3.17
3	China	3.05
4	Libya	2.81
5	Lebanon	2.45
6	Tunisia	2.21
7	Taiwan	2.15
8	United Arab Emirates	2.12
9	Venezuela	2.06
10	Jordan	1.88

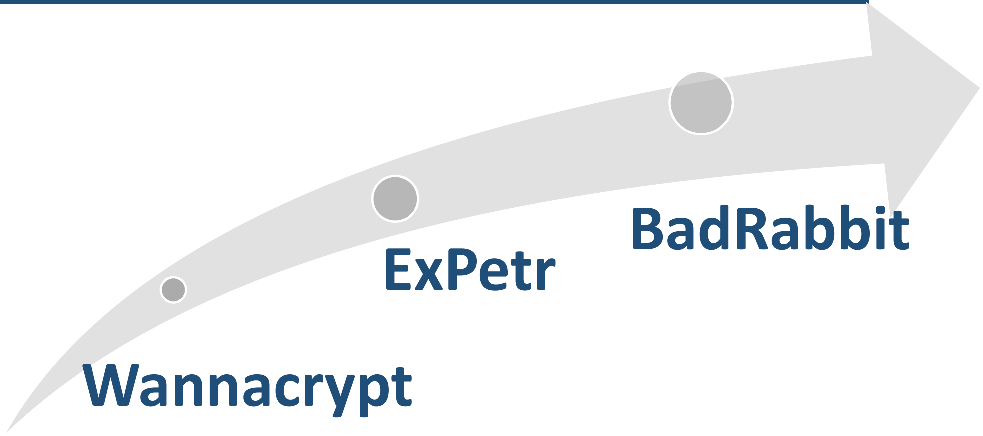


The TOP 20 countries where users face the greatest risk of online infection

	Name*	% users attacked**
1	Algeria	44.06
2	Belarus	38.39
3	Russia	36.91
4	Kazakhstan	36.57
5	Tunisia	36.51
6	Vietnam	35.01
7	Azerbaijan	34.70
8	Qatar	34.20
9	Portugal	33.01
10	Greece	32.80
11	Brazil	32.66
12	Moldova	32.42
13	India	32.34
14	Morocco	31.72
15	Venezuela	31.52
16	Spain	31.20
17	Sri Lanka	30.75
18	Malaysia	30.52
19	Bangladesh	30.37
20	Ukraine	30.27

Ransomware

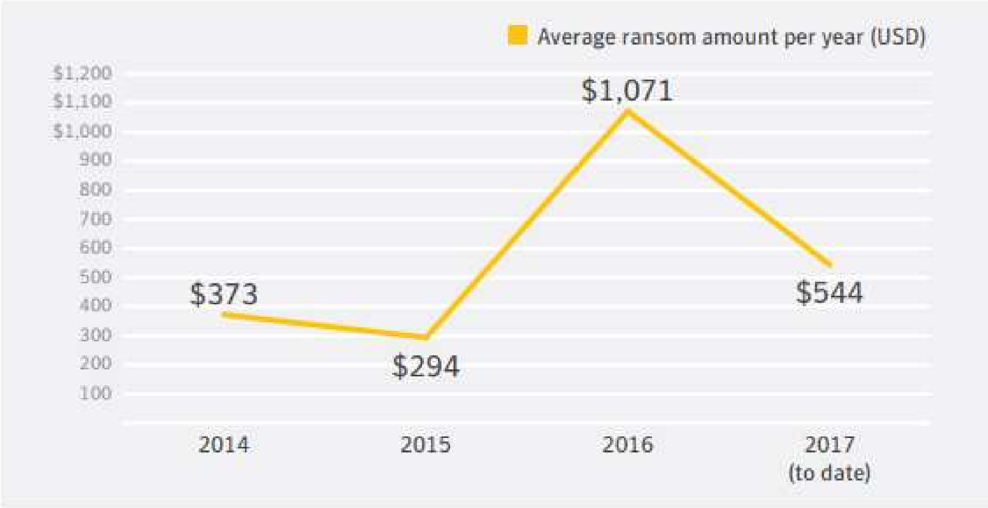




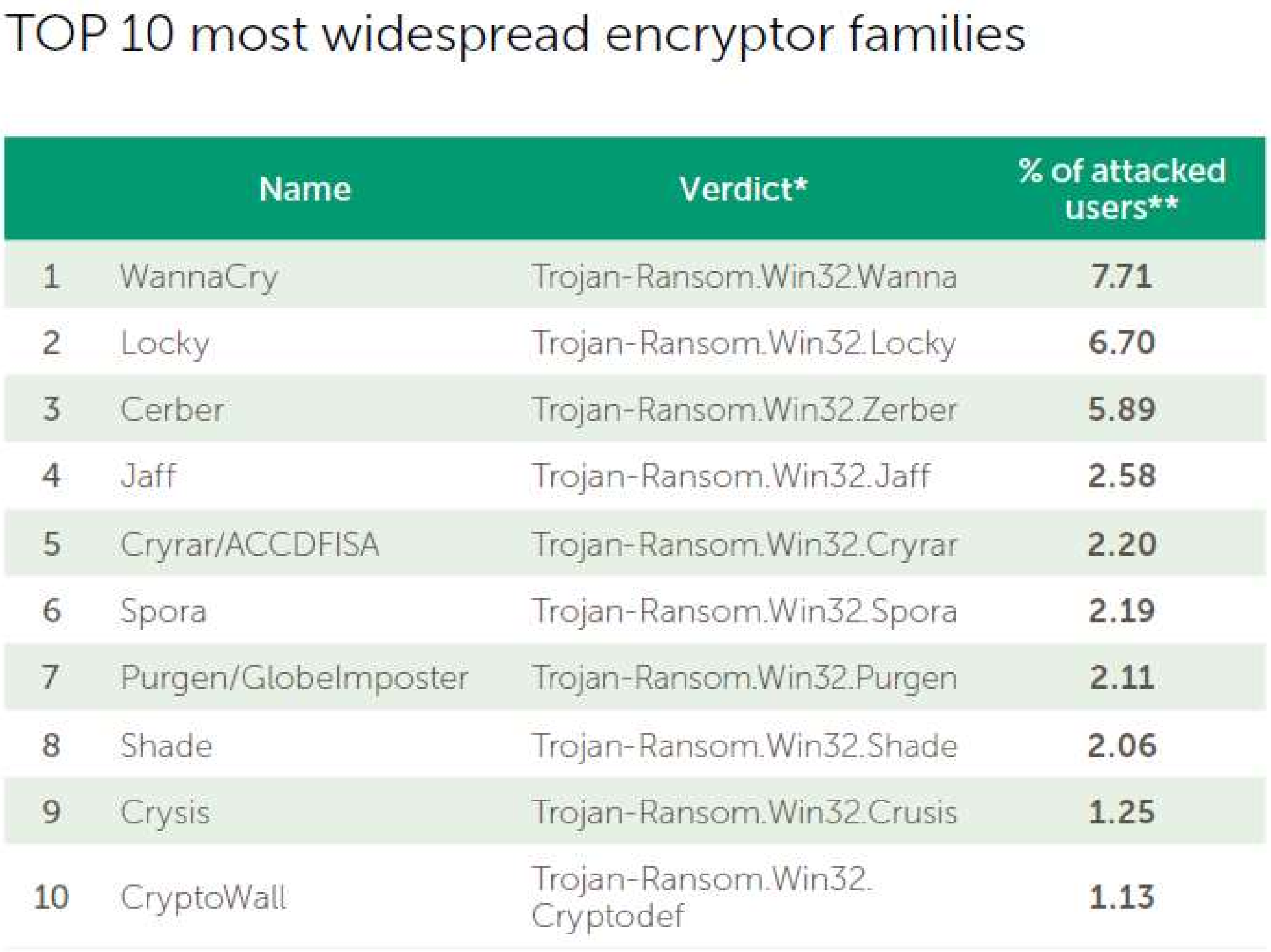
According to Cybersecurity Ventures, ransomware damages reached $5 billion in 2017

Cybersecurity Ventures predicts ransomware will cost $6 trillion annually by 2021.

Average ransom amount in US dollars, by year



Ransomware



TOP 10 most widespread encryptor families

	Name	Verdict*	% of attacked users**
1	WannaCry	Trojan-Ransom.Win32.Wanna	7.71
2	Locky	Trojan-Ransom.Win32.Locky	6.70
3	Cerber	Trojan-Ransom.Win32.Zerber	5.89
4	Jaff	Trojan-Ransom.Win32.Jaff	2.58
5	Cryrar/ACCDFISA	Trojan-Ransom.Win32.Cryrar	2.20
6	Spora	Trojan-Ransom.Win32.Spora	2.19
7	Purgen/GlobeImposter	Trojan-Ransom.Win32.Purgen	2.11
8	Shade	Trojan-Ransom.Win32.Shade	2.06
9	Crysis	Trojan-Ransom.Win32.Crusis	1.25
10	CryptoWall	Trojan-Ransom.Win32.Cryptodef	1.13

SPAM

The volume of spam emails increased 4x in 2016.

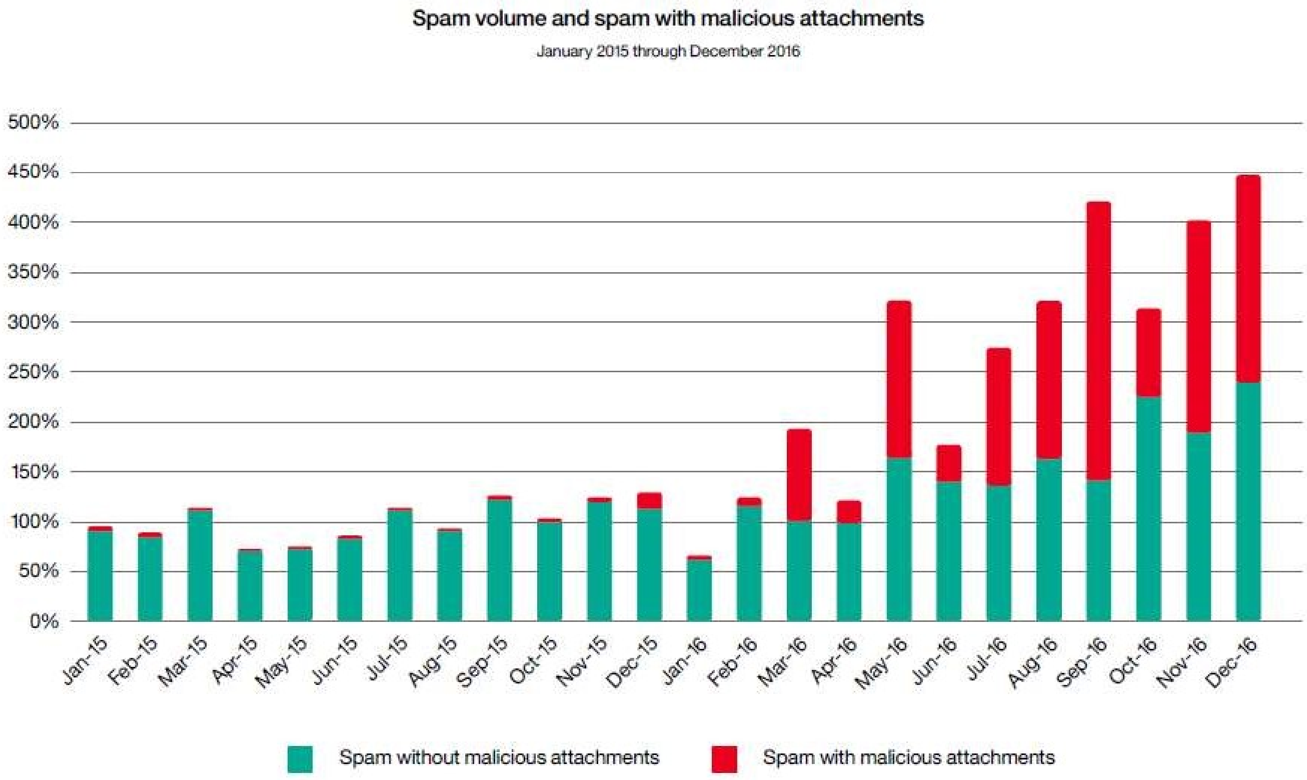


Figure 4: Spam volume and spam with malicious attachments – January 2015 through December 2016.

IBM X-Force Threat Intelligence Index 2017

Email is still the #1 delivery vehicle for most malware (just not ransomware)

Fake invoice messages are the #1 type of phishing lure.

Reports of W-2 phishing emails increased 870% in 2017.

Social engineering: Human Factor

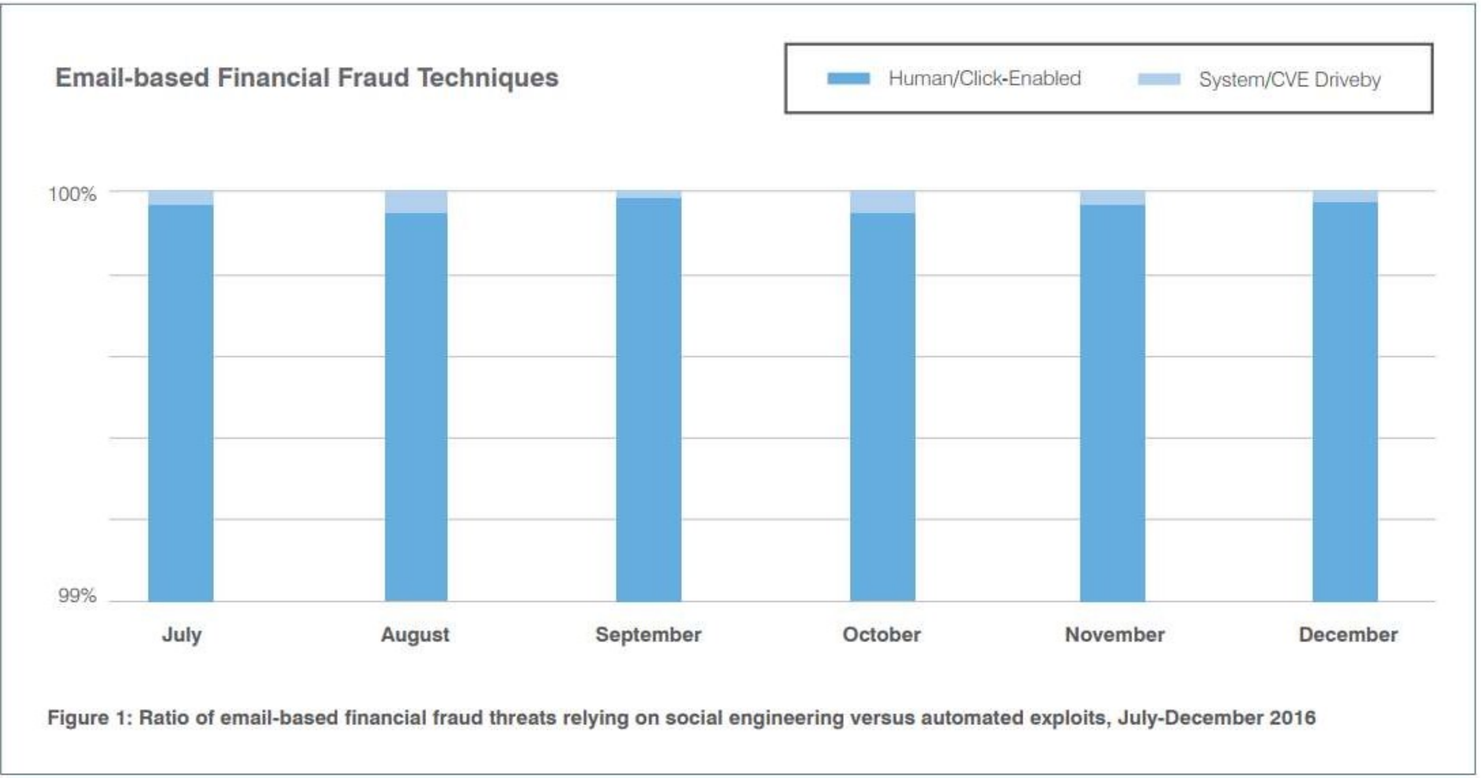


Figure 1: Ratio of email-based financial fraud threats relying on social engineering versus automated exploits, July-December 2016

Most cyberattacks on banking infrastructure rely on social engineering

Employees: the weak link in security.

One of the most effective tools for a hacker is the telephone.

Bank employees using social networks at work: danger or distraction?

https://www.proofpoint.com/sites/default/files/pfpt-en-us-human-factor-report-2017.pdf

Social engineering: Human Factor

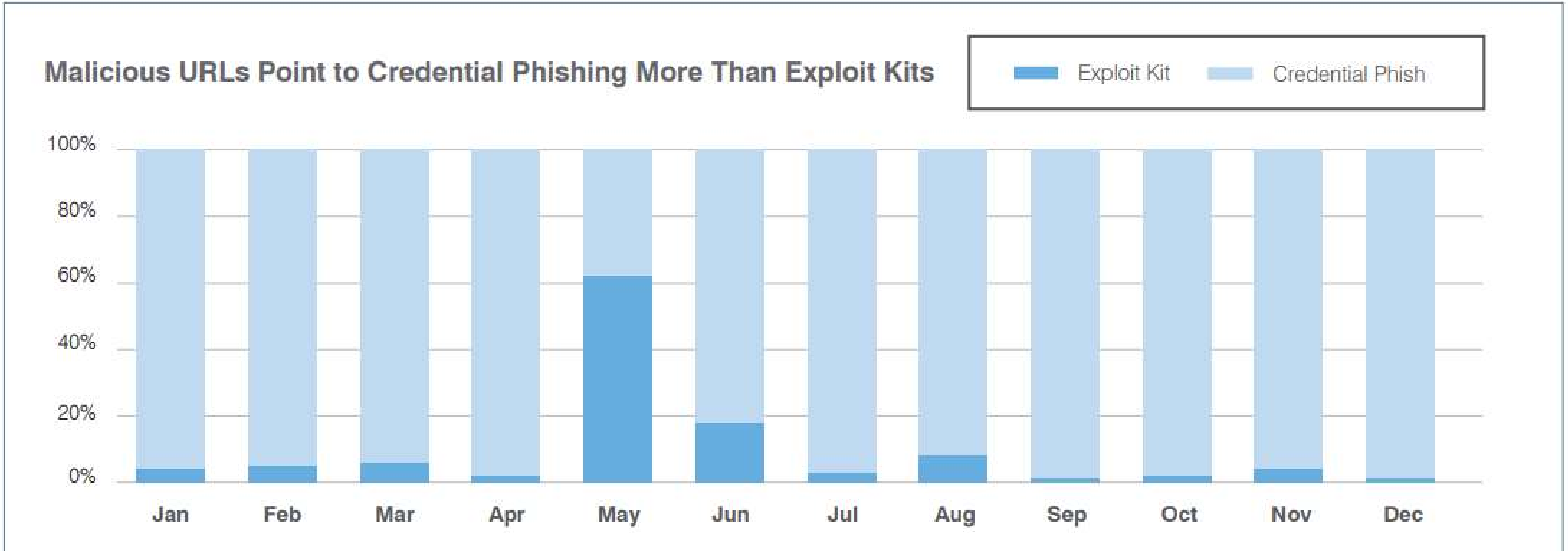


Figure 2: URLs in malicious messages linking to credential phish versus exploit kits

https://www.proofpoint.com/sites/default/files/pfpt-en-us-human-factor-report-2017.pdf

Phishing – Spear Phishing

76% of organizations reported being victim of a phishing attack in 2016.

Reports of W-2 phishing emails increased 870% in 2017.

One specific form of BEC scam that attackers have been having particular success with is impersonating high-level company executives and requesting employee W-2 forms from personnel in payroll or HR departments. The goal is to use the captured W-2 information to file fraudulent tax returns and claim refunds.

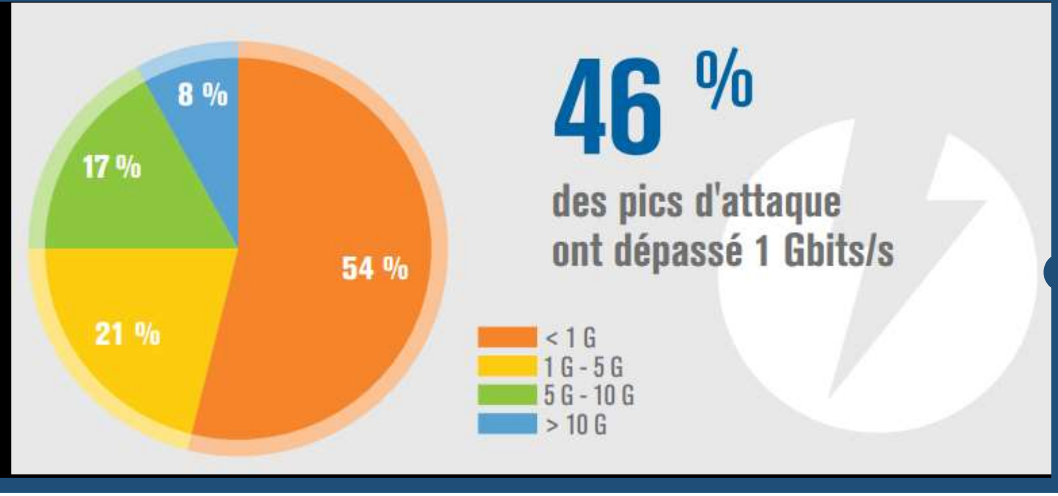
More than 400 businesses are targeted by BEC scams every day.

The past year has also seen significant growth in the number of business email compromise (BEC) scams. Also referred to as CEO fraud or "whaling," a BEC scam is a form of spear phishing attack where an attacker impersonates a company executive (often the CEO), and attempts to get an employee, customer, or vendor to transfer funds or sensitive information.

According to the FBI, BEC scams have accounted for more than $5 billion in losses between October 2013 and December 2016, with more than 24,000 victims reporting incidents worldwide.

https://www.shrm.org/resourcesandtools/hr-topics/compensation/pages/beware--form-w-2-phishing-scheme.aspx

DDoS



46 %

des pics d'attaque ont dépassé 1 Gbits/s

VERISIGN

1. 52 % SERVICES INFORMATIQUES/ CLOUD/SAAS
2. 31 % SERVICES FINANCIERS
3. 13 % COMMERCE ÉLECTRONIQUE ET PUBLICITÉ EN LIGNE

www.akamai.com/stateoftheinternet-security

DDoS Attack Frequency By Industry Q3 2017–Q2 2017

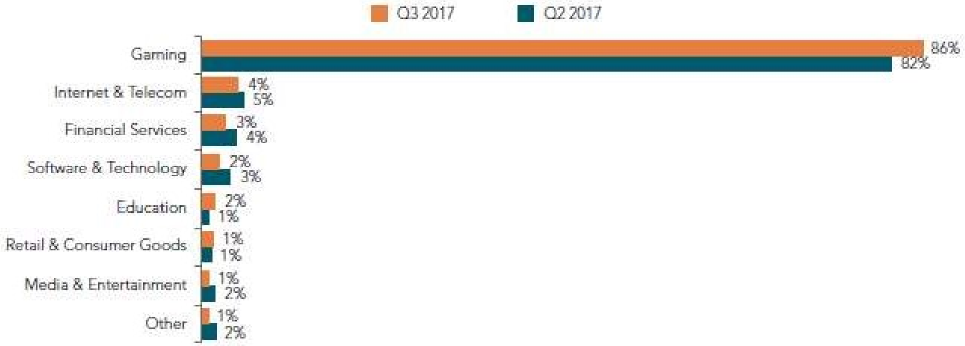


Figure 2-4: Gaming continues to be the most attractive target to attackers

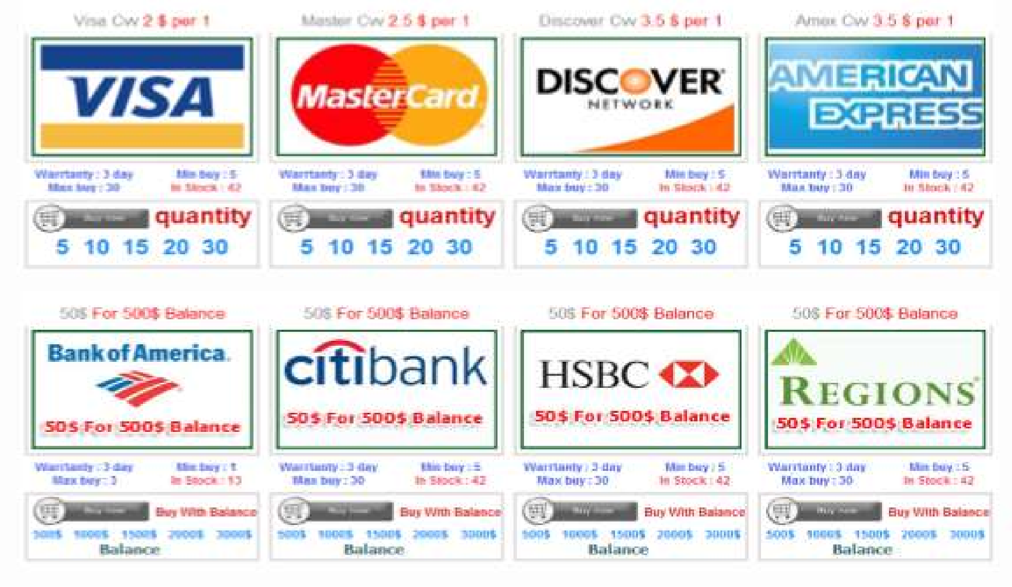
Black Market – Underground Economy

- DDOS attack $5 USD per hour,
- Bank account for 1% to 5% of the balance,
- 300,000 of miles for $90 USD
- American Express Card for $30 USD
- ATM Skimming Kit for $400 USD
- RATs for $5 USD
- Crypters starting from $80 USD
- Exploit Kits starting from $100 USD
- « how-to » guides for $20 USD.

2016 Underground Hacker Marketplace Report

Carding

- Theft can be done by attacking merchant sites, call centers, online payment sites, gaming sites, payment servers, etc.
- The cards are either used or sold on the black market,
- Cards are used for online shopping (easy to trace) or by manual numbering on POS.



Visa Cvv 2 $ per 1
Warrtanty : 3 day Min buy : 5
Max buy : 30 In Stock : 42
quantity
5 10 15 20 30

Master Cvv 2.5 $ per 1
Warrtanty : 3 day Min buy : 5
Max buy : 30 In Stock : 42
quantity
5 10 15 20 30

Discover Cvv 3.5 $ per 1
Warrtanty : 3 day Min buy : 5
Max buy : 30 In Stock : 42
quantity
5 10 15 20 30

Amex Cvv 3.5 $ per 1
Warrtanty : 3 day Min buy : 5
Max buy : 30 In Stock : 42
quantity
5 10 15 20 30

50$ For 500$ Balance
Bank of America
50$ For 500$ Balance
Warrtanty : 3 day Min buy : 1
Max buy : 3 In Stock : 13
Buy With Balance
500$ 1000$ 1500$ 2000$ 3000$
Balance

50$ For 500$ Balance
citibank
50$ For 500$ Balance
Warrtanty : 3 day Min buy : 5
Max buy : 30 In Stock : 42
Buy With Balance
500$ 1000$ 1500$ 2000$ 3000$
Balance

50$ For 500$ Balance
HSBC
50$ For 500$ Balance
Warrtanty : 3 day Min buy : 5
Max buy : 30 In Stock : 42
Buy With Balance
500$ 1000$ 1500$ 2000$ 3000$
Balance

50$ For 500$ Balance
REGIONS
50$ For 500$ Balance
Warrtanty : 3 day Min buy : 5
Max buy : 30 In Stock : 42
Buy With Balance
500$ 1000$ 1500$ 2000$ 3000$
Balance

CRITICAL VULNERABILITIES AND SECURITY WEAKNESSES

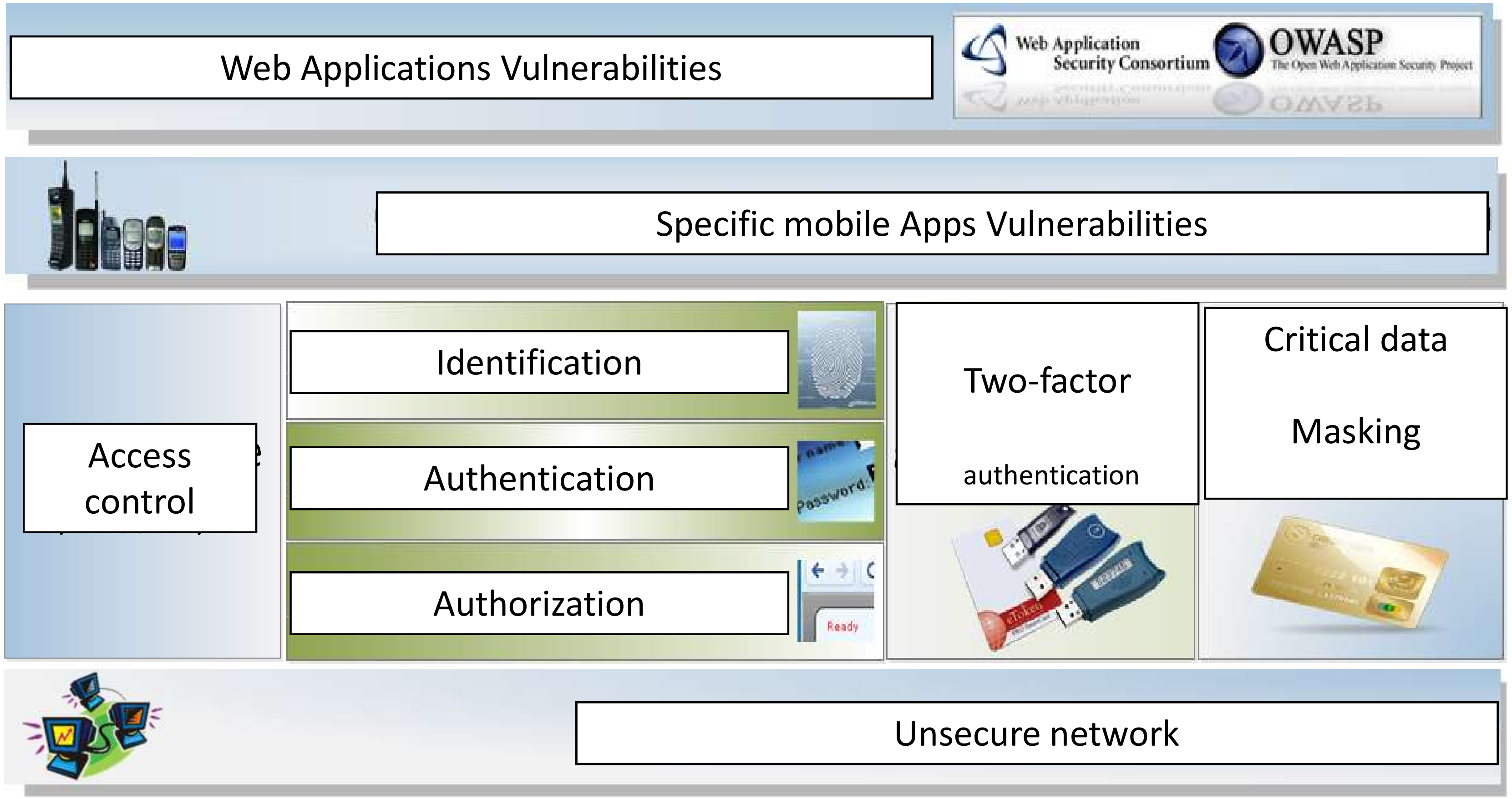
Remote Banking Systems: features

- Centralized or distributed architecture
- Different user groups
- Up to 1000000 accounts and more
- Lots of configurations and modules
- Additional secure configurations are required for the Web servers, OS, DBMS, Network and connectors to other systems
- …

Core banking system, weak points?

- **Lots of user groups**
- **Distributed architecture. A lot of remote users**
- **Interconnected with other banking systems**
- **High privileged users**
- **Different systems in one network**
- **Complicated business logic**

Typical RBS security issues


Web Application Security Consortium
OWASP
The Open Web Application Security Project
Password:
Ready

Web Applications Vulnerabilities

Specific mobile Apps Vulnerabilities

Access control

Identification

Authentication

Authorization

Two-factor

authentication

Critical data

Masking

Unsecure network

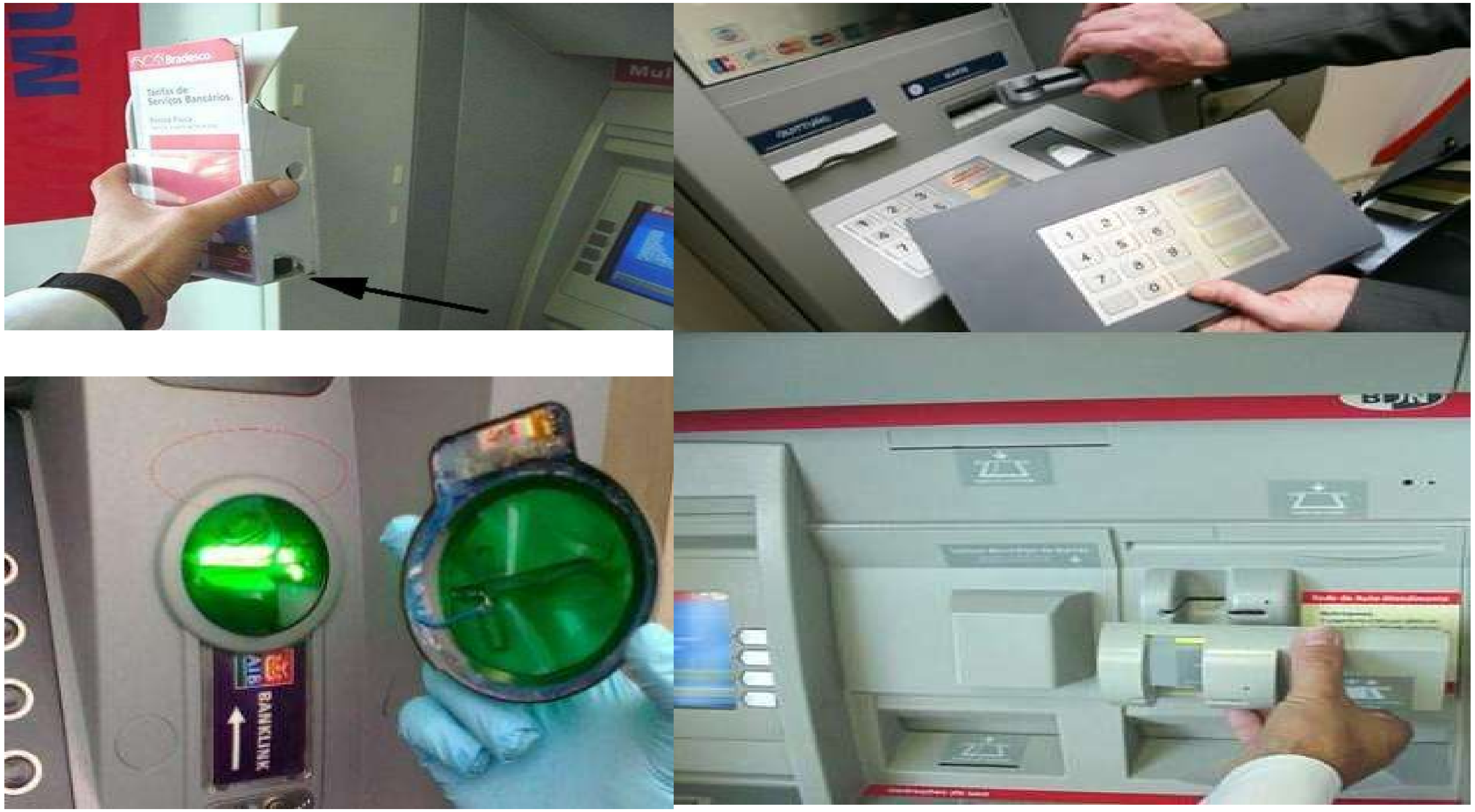
Live demo:
Attack against an Online Banking System

Attacks against ATM

Windows XP still alive!

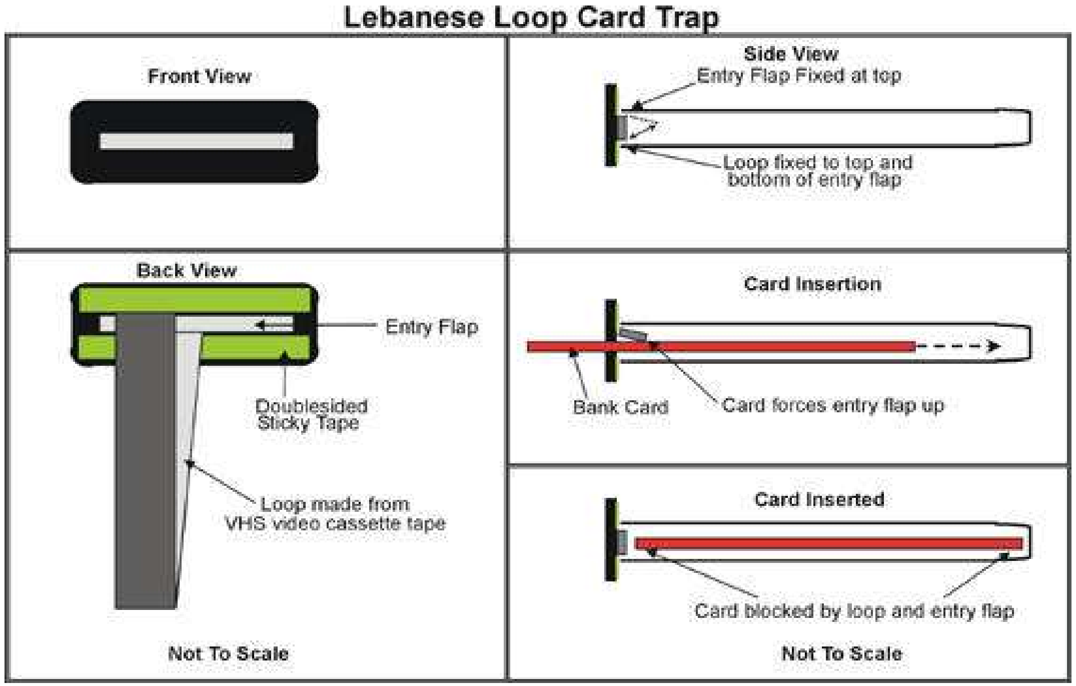
- En 2014 – 95% of ATMs under Windows XP
- End of support Avril 2014
- >9000 vulnerabilities >> patches

Skimming



Trapping

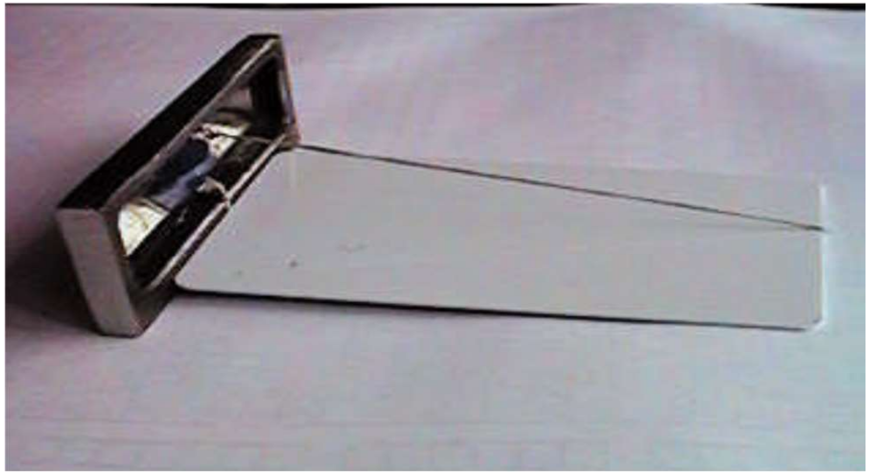
- Lebanese Loop
  - Using VHS X-Ray

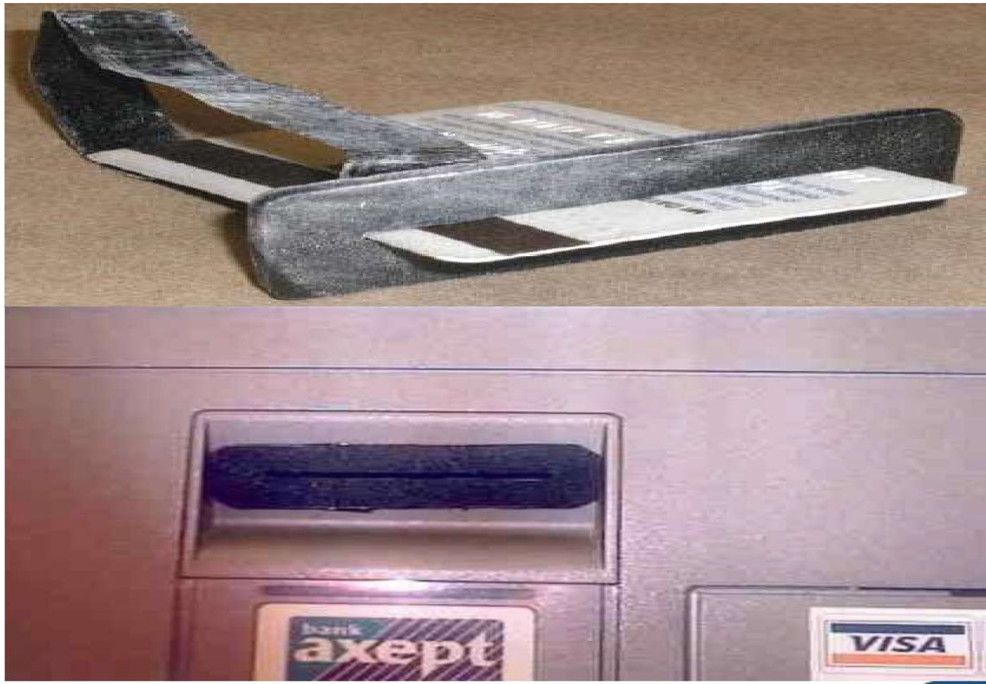


Trapping

- Romanian

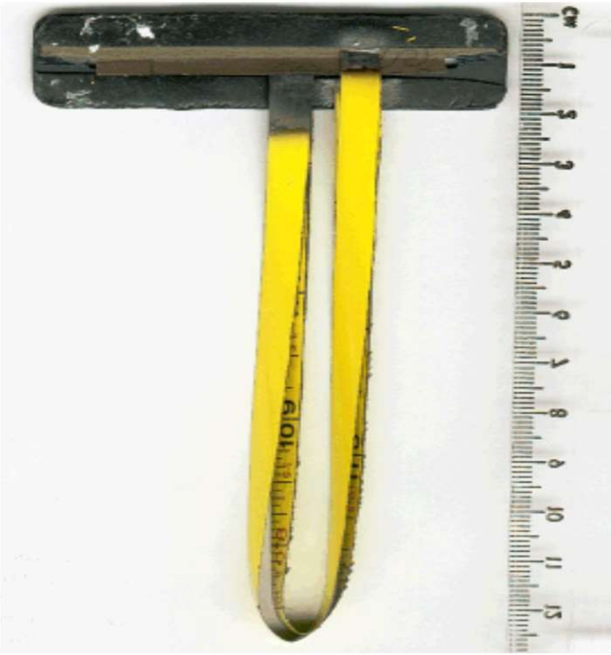
- Dental floss loop



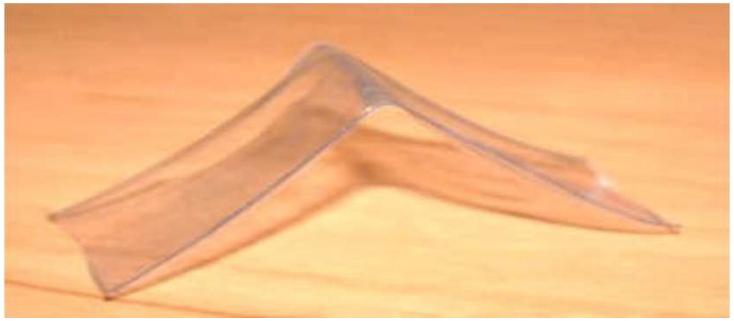


Trapping

- Mason loop

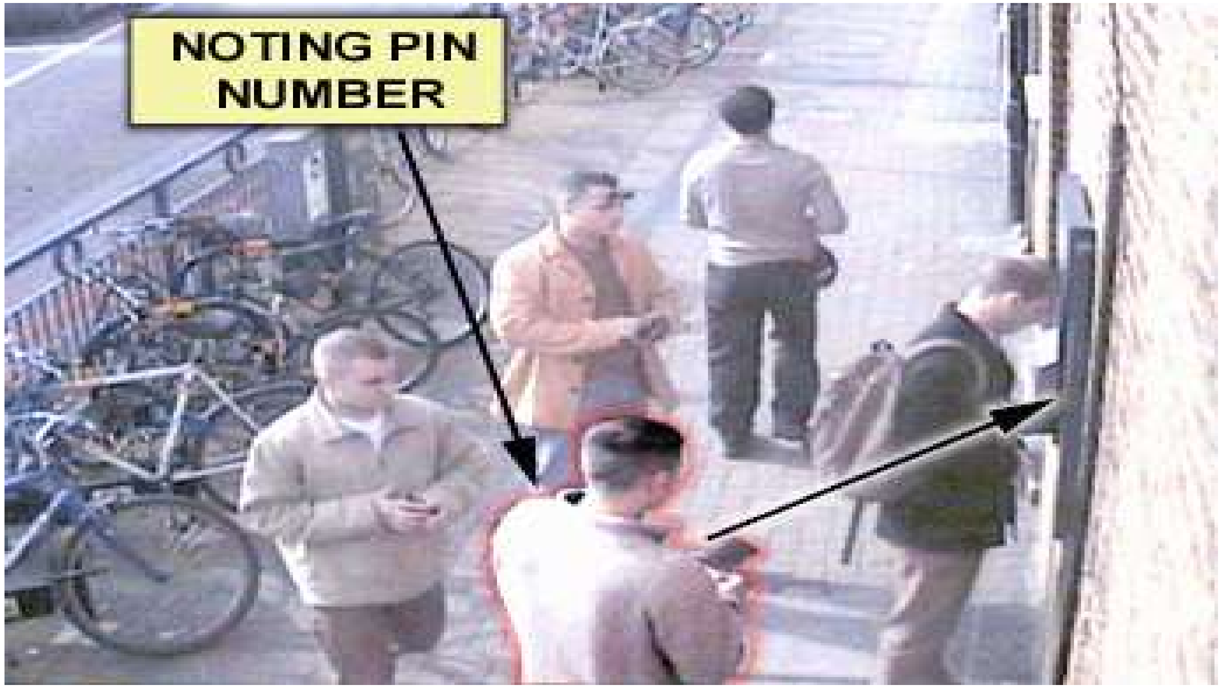


- Algerian V

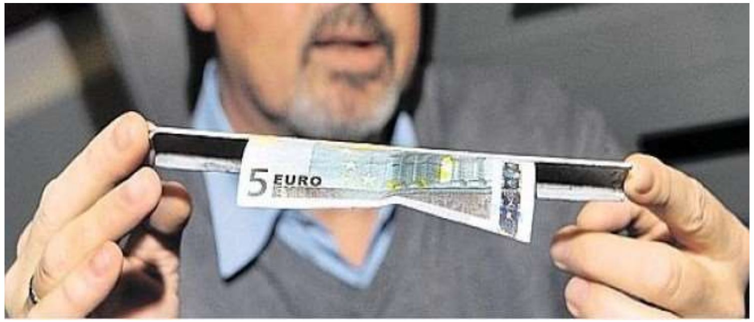


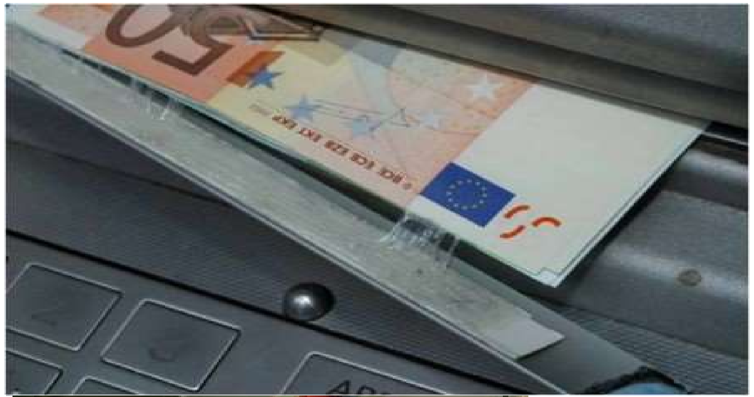
Fake ATM

Shoulder surfing



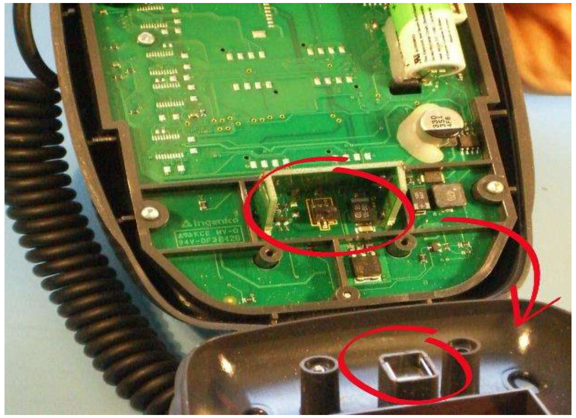
Cash trapping





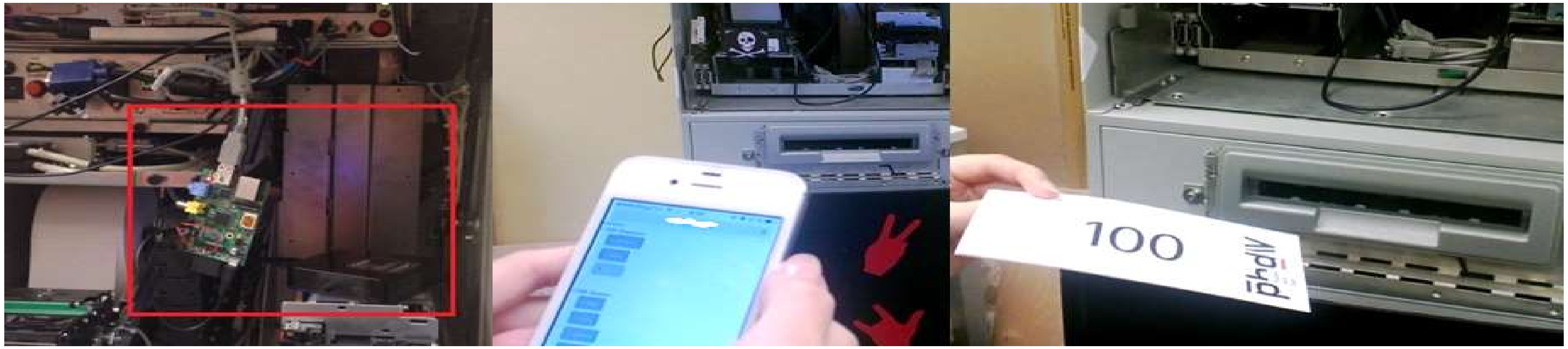
Point of Sale

Point of Sale

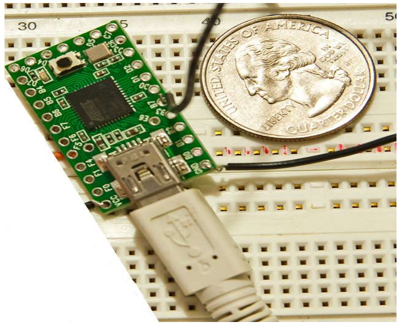


→ **Anti-tampering**

Blackbox, jackpotting

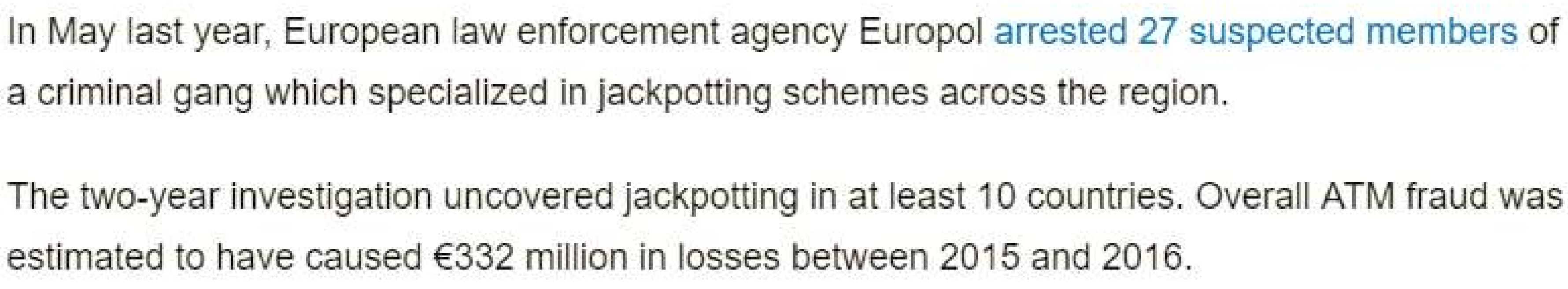


“Black box attack”: unauthorized cash withdrawal is possible with a cheap and popular computer. The credit-card sized and fast programmable device can be easily hidden inside an ATM. Sometimes it can be plugged even outside an ATM.



USB-based microcontroller – the most HIDden jackpotting device

Blackbox, jackpotting



In May last year, European law enforcement agency Europol arrested 27 suspected members of a criminal gang which specialized in jackpotting schemes across the region.

The two-year investigation uncovered jackpotting in at least 10 countries. Overall ATM fraud was estimated to have caused €332 million in losses between 2015 and 2016.

There are many active ATM and POS threat families, such as Ploutus (Backdoor.Ploutus), Flokibot, Trojan.Skimer, FastPOS (Infostealer.Fastpos), Infostealer.Poslit, Infostealer.Donpos, Infostealer.Jackpos, Infostealer.Scanpos, and Backdoor.Pralice

Symantec

018-04/0005 –Potential Jackpotting US (Update on 017-34/0002)

20180126/BR/01

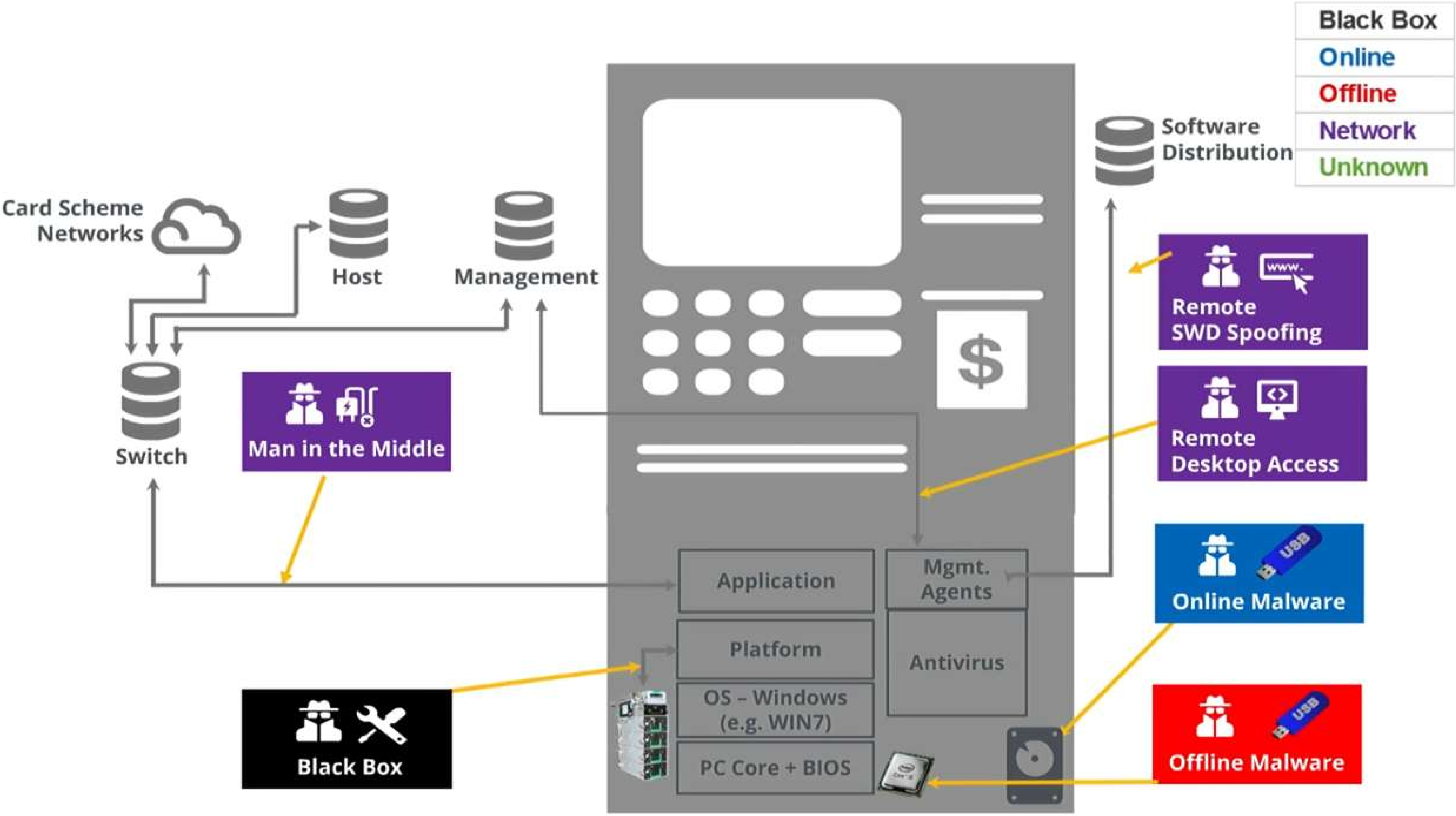
January 25, 2018

Jackpotting

The criminal takes access to ATM dispenser

The criminal bypasses the ATM processor and connects an electronic device to the ATM

The criminal sends unauthorized commands to drill the dispenser.


Black Box
Online
Offline
Network
Unknown
Software Distribution
Card Scheme Networks
Host
Management
Switch
Man in the Middle
Remote SWD Spoofing
Remote Desktop Access
Online Malware
Offline Malware
Black Box
$
Application
Mgmt. Agents
Platform
Antivirus
OS – Windows (e.g. WIN7)
PC Core + BIOS
USB
www.

Anatomy of an attack
Real case : Cobalt

KNOW YOUR ENEMY

Types of attackers

- Cybercriminal
- Criminals
- Hacktivist
- Script Kiddies
- Customers
- Internal (employees)
- Service provider employees
- Partner employees
- Compromised partner
- State sponsored
- Competitor

- Targeted attack vs Inadvertent attack
- Foreign vs local
- Local vs internal accomplice

It’s fundamental to know who wants to attack you and who is able to do it.

HOW TO SECURE?
CYBERSECURITY NEEDS

Implement a defense strategy.

How to deal with all these threats?

❑ Have a strategy and a plan.

❑ Deploy your Process-People-Technology and ensure a continuous improvement.

❑ Enforce security control and monitoring.

❑ Be proactive and prepare a response plan.

❑ Be informed about new threats and share information with relevant stakeholders.

❑ Collaborate with other actors.

What security do we need?

- Basic/usual approach:
  - Network protection: Segmentation, filtering, intrusion detection, access control, VPN,
  - Endpoint protection,
  - Security Organization: Security Policy, Procedures, etc.
  - Business continuity plan, IT backup plan,
  - Audit of the security of the IS,
  - Training, awareness,
  - Compliance: ISO27001, PCI / DSS
  - Monitoring
  - Strong authentication
  - Etc.

Facing today's threats, the conventional approach may not be effective enough.

Developping cybersecurity strategy

- Today we are talking about a cyber defence strategy for banks:
  - Have a better perception and visibility on all operations and perimeters,
  - Involve all stakeholders within the bank for the development of the strategy,
  - Be more proactive: intelligence, continuous monitoring, rapid response to threats, information sharing,
  - Develop the bank's capabilities to deal with complex attacks,
  - Develop the means of detection: behavioural analysis, honeypot, zero-day analysis, combination of protection technologies,
  - Awareness of employees and customers,
  - Defence in depth.

What security do we need?

- A defense in depth,
- A proactive approach,
- Intelligence based on continuous data collection and analysis,
- Rapid reactivity,
- Effective communication,
- Internal and external collaboration involving all stakeholders
- A defense that is based on careful behavior.

What security do we need?

- Study the ecosystem:
  - Who are these hackers,
  - What are their motivations,
  - What is their level of expertise,
  - What are their tools,
  - How they coordinate and plan,
- Stealing card data does not motivate hackers in countries with non-convertible currency,
- In some countries hacktivists pose a greater risk than criminals,
- Sometimes bank transfer order falscification is a bigger threat than attacks on e-banking.

What security do we need?

Develop a strategy and define a cybersecurity vision as an integral part of the overall vision and especially digital development.

Study the internal and especially external threats: identify who are really these crimonals and if they are really present.

Strategy should be adopted by the top management and inclusive by including all perimeters and all stakeholders (internal and external).

OPERATIONAL SECURITY CHALLENGES

Incident Detection and response

- It is impossible to know if the bank has been subject to attacks or has experienced an incident if it has no visibility that is usually provided by the monitoring technologies,
- Incident processing requires trained human resources, procedures and tools.
- It is a question of preparing a team to treat different types of attacks and to make use of specialists in the event of major incidents: detection, Analysis, Containment, Eradication, Restoration.
- The establishment of SOC is one of the most effective ways to ensure cyber-defense.

Vulnerability management

- The number of systems and the technological variety means that the number of vulnerabilities is generally quite high,
- All systems are affected by vulnerabilities: Server, DB, Workstation, Network Equipment, Desktop Application, etc.
- Identifying and fixing the flaws remains a difficult but indispensable task because as long as there are vulnerabilities as long as there are incidents and attacks,
- The implementation of continuous vulnerability management process is essential.

Web application security

- The applications are the origin of 80% of the vulnerabilities,
- Secure applications require:
  - Integration of security at the development lifecycle,
  - The audit of the application and its source code before the exploitation and during the development cycle,
  - Applying good secure development practices and good security management practices (authentication, session management, storage, encryption, traceability, etc.),
  - Have application filtering resources, especially for sensitive applications and for applications exposed on the Internet.

Business continuity

- The bank must be able to handle major incidents that may affect the bank's business,
- Ensure business continuity even when critical resources are not available or even if Internet service is not available.
- The development of BCP must provide continuity for all critical operations.
- Setting up a back-up center has become an obligation.
- Test the BCP.

Security assessment

- Have a continuous assessment plan for all applications, systems and network,
- Real hacking and fraud simulation: internal and external,
- All perimeters:
  - ATM
  - OBS
  - CBS
  - Web portals
  - SWIFT
  - Information System
  - Branches
  - Mobile payment
  - Etc.
- Blackbox, GreyBox, WHiteBox – RED TEAM

+ Physical Intrusion – Social Engineering

Threat intelligence

- Be informed:
  - New attack trends,
  - Vulnerabilities,
  - New malware,
  - New trends,
- Identify all threats related to your company,
- Be connected with the dark web and anticipate attacks,
- Have the capacity to analyze events and information inside your IS and from the outside world.
- Alert and respond rapidly.

COMPUTER EMERGENCY RESPONSE TEAM

What is a CSIRT?

- The acronym CSIRT, which stands for Computer Security Incident Response Team, is primarily used as a synonym for the protected term CERT, filed in the United States by the CERT Coordination Center (CERT / CC).
- Several abbreviations designate centers of this type:
  - CERT or CERT / CC (Computer Emergency Response Team / Coordination Center)
  - Computer Security Incident Response Team (CSIRT)
  - IRT (Incident Response Team)
  - CIRT (Computer Incident Response Team)
  - SERT (Security Emergency Response Team)

CSIRT Definition

- A CSIRT is a team of computer security experts whose main mission is to respond to incidents by providing the necessary services to deal with attacks and by helping their stakeholders to restore the systems that have been attacked.
- Most CSIRTs also offer their stakeholders, with the aim of mitigating the risks and minimizing the number of interventions required, preventive and educational services.
- They publish bulletins and notices of vulnerabilities concerning the software and hardware in use, and inform the users of exploits and viruses taking advantage of the faults found

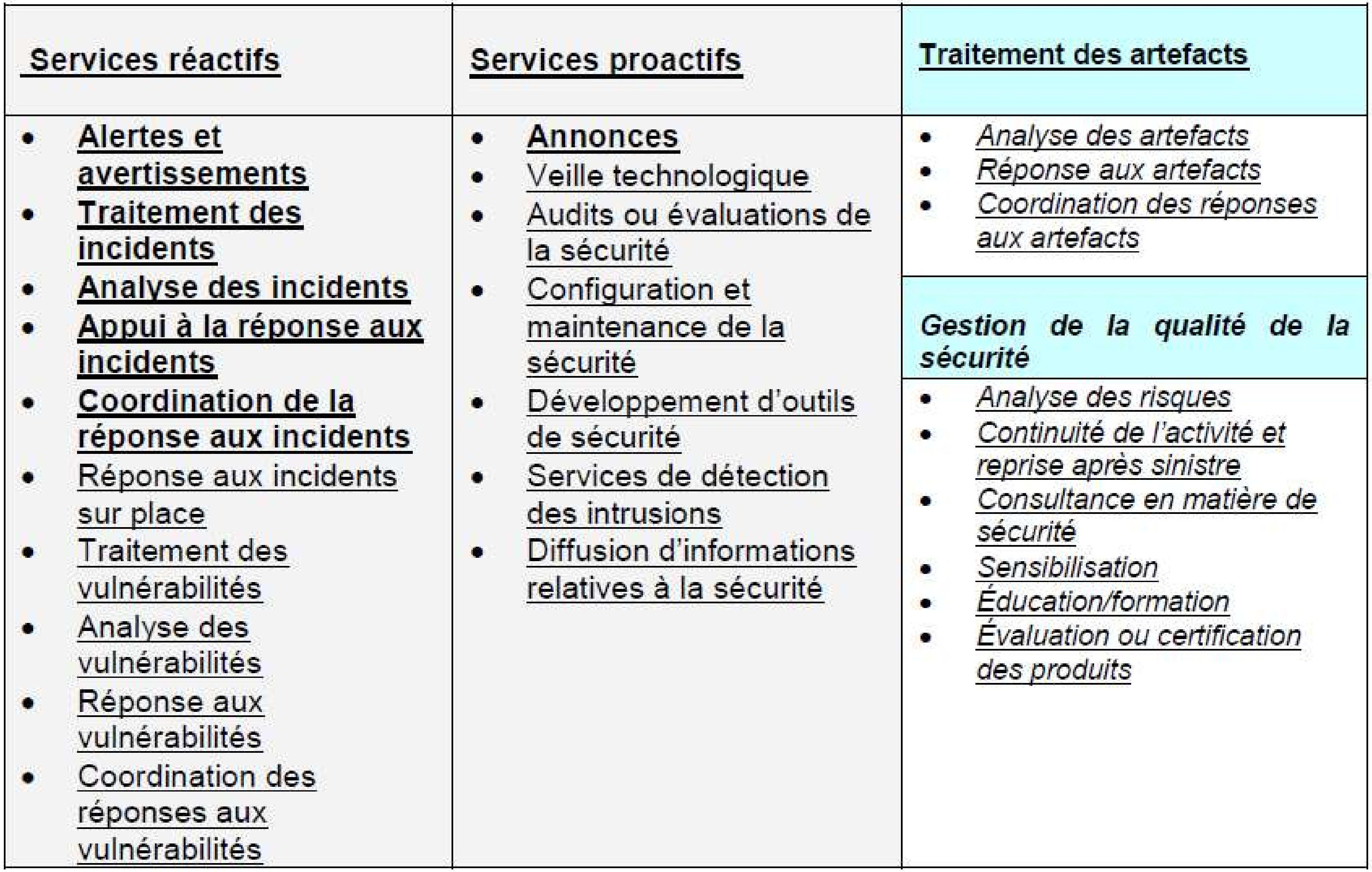
CSIRT advantages

- Having a dedicated IT security team helps any organization reduce, prevent or prevent major incidents and protect valuable assets.
- The CSIRT can also offer the following advantages:
  - centralization of IT security coordination within the organization (point of contact);
  - centralization and specialization of computer incident handling and response;
  - the availability of expertise to support users and help them restore their system after a security incident;
  - the management of legal aspects and the protection of evidence in case of legal action;
  - monitoring developments in the field of security;
  - the encouragement of stakeholders to cooperate on computer security (awareness raising).

CSIRT types

- Commercial
- Vendor
- governmental
- Internal
- Military
- National
- CIP / CIIP
- SMEs (small and medium-sized enterprises)
- University

CSIRT services



Services réactifs	**Services proactifs**	**Traitement des artefacts**
- **Alertes et avertissements** - **Traitement des incidents** - **Analyse des incidents** - **Appui à la réponse aux incidents** - **Coordination de la réponse aux incidents** - Réponse aux incidents sur place - Traitement des vulnérabilités - Analyse des vulnérabilités - Réponse aux vulnérabilités - Coordination des réponses aux vulnérabilités	- **Annonces** - Veille technologique - Audits ou évaluations de la sécurité - Configuration et maintenance de la sécurité - Développement d'outils de sécurité - Services de détection des intrusions - Diffusion d'informations relatives à la sécurité	- *Analyse des artefacts* - *Réponse aux artefacts* - *Coordination des réponses aux artefacts* ***Gestion de la qualité de la sécurité*** - *Analyse des risques* - *Continuité de l'activité et reprise après sinistre* - *Consultance en matière de sécurité* - *Sensibilisation* - *Éducation/formation* - *Évaluation ou certification des produits*

SECURITY OPERATION CENTRE

Why do we build operational security controls & capabilities?

Reduce enterprise risk. Protect the business.

Move from reactive response to proactive mitigation.

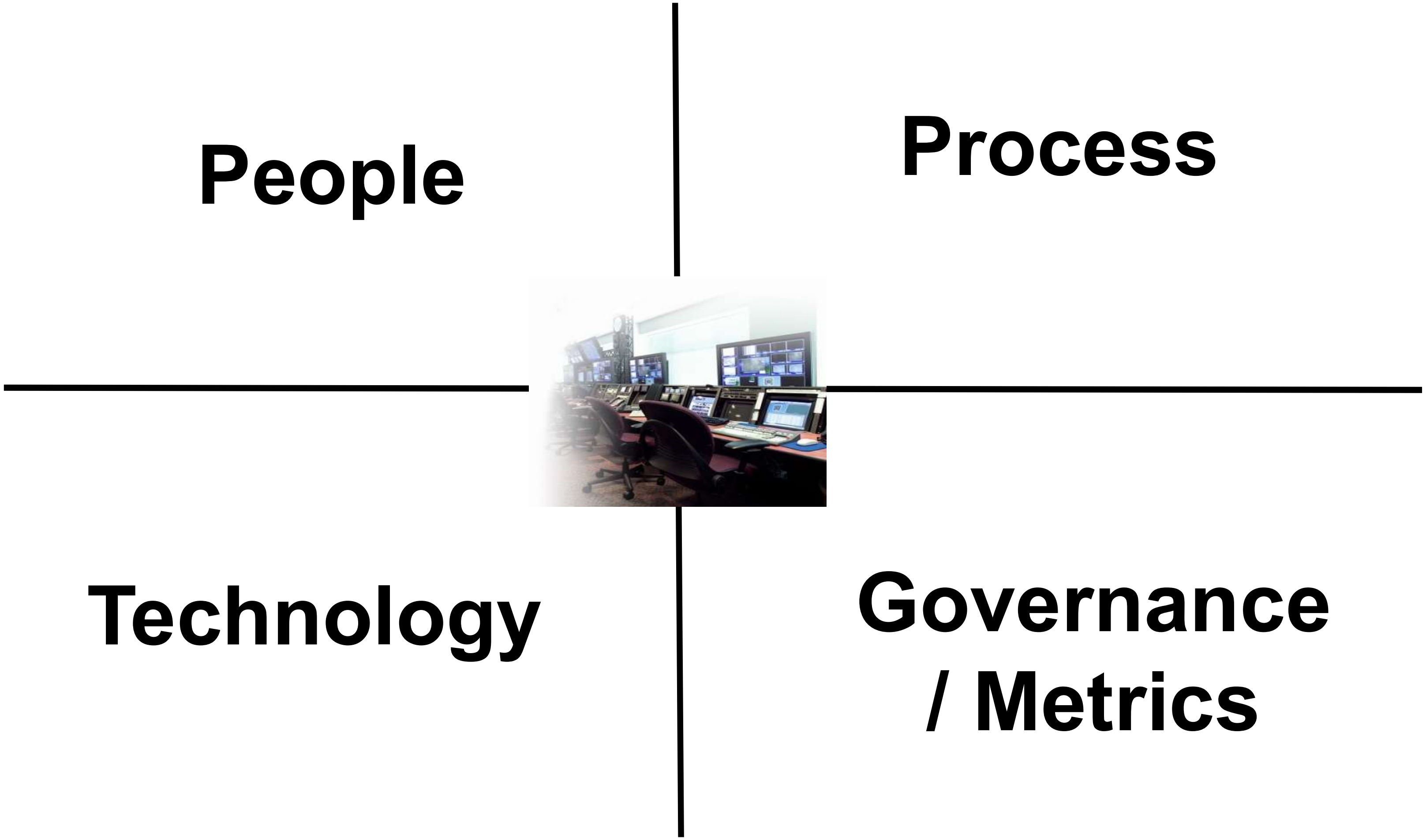
Increase visibility over the environment.

Meet compliance/regulatory requirements.

What is a Security Operations Center, or SOC?

- **A Security Operations Center is a highly skilled team following defined definitions and processes to manage threats and reduce security risk**
- Security Operations Centers (SOC) are designed to:
  - protect mission-critical data and assets
  - prepare for and respond to cyber emergencies
  - help provide continuity and efficient recovery
  - fortify the business infrastructure
- The SOC's major responsibilities are:
  - Monitor, Analyze, Correlate & Escalate Intrusion Events
  - Develop Appropriate Responses; Protect, Detect, Respond
  - Conduct Incident Management and Forensic Investigation
  - Maintain Security Community Relationships
  - Assist in Crisis Operations

Building a Security Operations Center involves multiple domains



People

Process

Technology

Governance / Metrics

What you can expect as a result from a SOC implementation

- Better understanding of how your security program reduces risk in operations and therefore business risk
- Measurement of the real-time compliance of particular security controls in the organization
- Insight into the current state of your security posture
- Visibility of issues, hacks, infections and misuse that otherwise would require human discovery and correlation.
- Easier measurements of compliance and audit effort reduction

INTERNAL ORGANISATION

Inclusive approach

- IT Security vs IS Management
- CISO (IT Department vs Risk s Compliance vs General Manager)
- IT Division
- Security Comity
- SOC: Internal vs Outsourced SOC
- CERT/CSIRT
- Red Team
- Security Compliance
- Security Governance
- Business continuity

Need to define a clear organization and governance model.

Inclusive approach

- All stakeholders should be involved:
  - Top management
  - Risk
  - Business Units
  - Compliance
  - Fraud
  - Legal Departement
  - Physical security
  - HR
  - PR

Everybody needs to be trained.

COMPLIANCE

Compliance requirements

- ISO27001
- PCI/DSS
- GDPR
- TIA942
- Internal IT control
- Internal Security Policy
- Technical compliance (CIS)
- Legal compliance

How to reach compliance?

- Real engagement (Top Management, Risk, IS, IT Department),
- Process,
- Tools,
- Continuous control,
- Continuous improvement.

CYBERSECURITY FOR THE SECTOR

Current situation

- **Stakeholders:**
  - **Public and private banks**
  - **Central Bank**
  - **Bank Federation/Association**
  - **National CERT**
- **Threats & Attacks:**
  - **Fraud**
  - **E-banking**
  - **PoS**
  - **ATM**
  - **Card Fraud,**
  - **Physical risk,**
  - **Etc.**

- Coordination:
  - No data exchange,
  - No coordination,
  - Loss of time for response,
  - Declaration to the legal authorities?
- Incident handling:
  - No specialized teams at banks,
  - No coordination between banks.
- Interdependencies not well understdood.

We need to coordinate and consolidate the efforts of all stakeholders in the financial sector ... Information sharing and coordination will be more effective in fighting cyberattacks and fraud.

Collaborative approach

- Being informed: Gathering and sharing information can help to:
  - Anticipate attacks,
  - Handle threats,
  - Respond effectively to attacks / frauds,
- A sectoral protection approach involving all stakeholders and ensuring better coordination with external entities.
- Tunisian Example: The Financial Cert:
  - Threat intelligence,
  - Coordination to the response them incident,
  - Collection and sharing of data.

Collaborative approach

The concept of the Financial CERT is based on the following objective:

coordinate and consolidate the efforts of all stakeholders in the financial sector ... information sharing and coordination will be more effective in combating attacks and fraud.

Mission:

Strengthen the capacity of the financial sector to fight cyber attacks by coordinating and sharing information on new threats and incidents.

Financial sector CERT

- Specialized unit to ensure the coordination between banks to face cyber-threats by ensuring the preventive and proactive activities.
- Mission: strengthen the capacity of the financial sector to respond to cyber-threats, vulnerabilities and incidents, and serve as the main communication channel for the sector.

Cyber Exercise
Attack scenario simulation
Crisis Management

Keystone

Securing the Critical Infrastructure for Financial Industry

Haythem EL MIR

Haythem.elmir@keystone.tn

&

Hosni Tounsi

hosni.tounsi@keystone.tn