Cyber security for Customs in Africa
Dakar, April 25st 2019
Groupe de Travail Régional sur le Développement Informatique
OMD-AOC
Vision
Supporting clients in Sub-Saharan Africa with innovative cyber security services and solutions

• Created in 2015 in Luxembourg, Senegal, Côte d'Ivoire, sister companies in Tunisia
• 3 Sectors: Financial Inclusion & Finance, Government, large corporations
• 5 activities
  ▪ Operational Security (supervision)
  ▪ Governance, Risk Management, Security Assessment
  ▪ Technical Audit, et Penetration Tests, Application Security
  ▪ Security Infrastructure (IBM Business partner)
  ▪ Training
Co-founders
complementary skills with large experience of Africa

Mehdi Azdabbaz
Associate, MD Senegal

BA Industrial Systems
30 years in Financial Systems and Electronic Banking in Africa
Set up and ran ATM/POS/ Electronic banking / Electronic banking security service affiliates in 12 countries
Expert in Electronic Banking Security

Christophe Bianco
CEO

MSc IT Engineering + MBA HEC
20 Years of experience in Cyber Security in marketing, sales, CTO
Co-Founder and MD of Excellium Services (N°1 cyber security in Luxembourg, 130 experts, 15 M€ in 2018), present in Belgium, Morocco, Tunisia, Part of SONAE Group (91 countries, 46.000 employees) cyber security division
Total > 630 experts, one of European leaders in cyber security

Jean-Louis Perrier
Associate, Development

MSc IT Engineering + MBA HEC
30 ans of expérience telecoms, IT, Financial services, distribution
CIO, MD, Fraud and security, Risk Management, Marketing & Business Development EMEA
Management of 50 persons 24x7 in MNO Fraud Operation Centre
Member of GSMA Fraud Forum
West Africa

Financial Institutions Hit by Wave of Attacks

Attackers using commodity malware and living off the land tools against financial targets

Malware used

- NanoCore (Trojan.Nancrat)
- Cobalt Strike (Trojan.Agentemis)
- Mimikatz (Hacktool.Mimikatz)
- Imminent Monitor RAT (Infostealer.Hawket)
- Remote Manipulator System RAT (Backdoor.Gussdoor)

Living off the land tools used

- PowerShell
- PsExec
- RDP
- UltraVNC

- 1st Symantec review of large scale attack in West Africa
- 5 countries affected
- Same basic tools & techniques
- 1 or several groups?
- 4 campaigns in 18 months
- +2 similar attacks we spotted in Benin and Senegal

Cyber crime : things ain't what they used to be
An explosive evolution, a reality in Africa, little assistance from Governments

World

- Losses > € 500 B in 2014 (x9 in 9 years), 1 % of GNP
- 400 M persons affected each year, 20% of Businesses. Yahoo, LinkedIn, Target, JP Morgan, NSA
- 900 000 Malwares in 2015 (x3 in 1 year)
- Professionalization and internationalization of criminal organizations
- In Russia alone, 20 to 30 organizations have the level to attack states. North Korea on the rise.
- Europe : Russians & Ukrainian hacked 100 financial institutions in 10 countries, losses €1Bn in 3 yrs
- Ransomware Petya/NotPetya/Wannacry : Fedex $300M, Maersk $300M, Saint Gobain 220 M€, Reckitt Benckiser £110M
- Central Banks & Banks hacks through Swift network : Ecuador 12 M$, Bangladesh 81 M$, Nepal 4.4 M$, Mexico 15 M$, Taiwan 60 M$, Russia 6 M$, India 2 M$, Chile 10 M$ & 9500 PCs and Servers damaged
- Coincheck : 500 M$ stolen in crypto-currency
- AFI Alliance for Financial Inclusion : “cyber security may become a systemic risk for financial inclusion”

Le ransomware Petya fait un trou dans les comptes de FedEx

Ransomware Petya : un colis à 300 millions de dollars pour Maersk

Coincheck : 500 M$ dans la crypto-euro

Sécurité : La cybercriminalité est de plus en plus agressive. Les cas de rappel apparaissent régulièrement. Les sociétés et les institutions financières sont de plus en plus vulnérables.

Sécurité : Le ransomware Petya a coûté cher à Saint Gobain. L’attaque a coûté à l’entreprise jusqu’à 300 millions de dollars en pertes de revenus.

Sécurité : L’entreprise française estime que la campagne de ransomware dont elle a été victime a coûté 1% de ses revenus, soit plus de 200 millions d’euros.
Cyber crime: things ain't what they used to be
An explosive evolution, a reality in Africa, little assistance from Governments

**Africa**
- 330 M internet users, +30% pa
- 200 M cyber attacks pa (+38%)
- **Losses > € 1B**: € 573 M South Af., € 500M Nigeria, € 39M Ivory Coast, € 36M Kenya, € 23M Senegal
- 15 countries / 54 have a national security centre (West Africa: Ivory Coast, Burkina, Nigeria)
- 2015 Ivory Coast: Money transfers hijack (+207%), mobile payment frauds (+74%)
- 2016 Liberia: no internet for a week
- 2017 West Africa MFI: € 60 k in 2 months on fraudulent money transfers
- 2018 National Bank of Kenya: 0.25 to 0.6 M€ in 2 hours
- 2017-2018 Banks in 5 West African countries

No mechanism to gather, analyze and report security incidents in the region: => Very few incidents are publicized

Various sources, Suricate summary
Cyber crime: things ain't what they used to be
An explosive evolution, a reality in Africa, little assistance from Governments

Senegal

• 2014 5 ministries: foreign affairs, interior, Official Journal, Sports, Social Protection and National Solidarity
• 2015 Agence de l’Informatique de l’Etat (ADIE), Ministry of Livestock and Animal Productions (MEPA)
• 2015 Money transfer operator Jonijoni, Money express business continuity in question
• 2015 Most big MFI and major money transfer operators,
• 2016 No operations for 2 major banks for a day
• 2017 CBAO €1.5 M, La Poste €1.5 M: ISO27001 & PCI DSS certification did not avoid intrusions, costly post hack security investments on inappropriate technologies
• 2017 Largest money transfer operator: no operations for 3 days for “maintenance” ... in Dec
• 2018 05 Most of Government internet services
• 2019-01 BCEAO eludes €1,25 M cyber attack in 6 countries
Serianu Africa Cyber security report 2017
Survey 700 institutions from 12 sectors across West and East Africa, 5th Edition

- Cost of Cyber Crime $3.5 B in 2017, +20%
- $1 B for Nigeria, Kenya, Ghana, Tanzania, Uganda

Financial institutions, Saccos and organisations that deal with transaction processing are the primary targets for the Cyber-attacks.

90% of the respondents have had an impact of Cyber crime

Money Lost: 40%
System Downtime: 32%
All of the above: 18%
Reputation damage: 10%

72% did not report cybercrime to the authorities

- 5% reported cyber crime to the police and followed it through to successful prosecution
- 72% did not report to the police

Reported to the police with no further action: 14%
Reported to the police, who contacted me /organisation but no further action: 6%
Reported to the police, who followed it up to successful prosecution: 5%
Reported to the police, who followed it up but no successful prosecution: 4%

40% of the respondents were actually not texting to the police.

Breakdown of Direct Cost of cyber attacks

- Compensation to Victims of Breaches: 43% ($185M)
- Money withdrawn from victim accounts: 43% ($185M)
- Investigation and Remediation Costs: 14% ($61M)

Total Direct Cost: $431 Million

60% of the respondents were actually not texting to the police.

Breakdown of Indirect Cost of cyber attacks

- Technical Controls: 46% ($304M)
- Security Consulting Services: 22% ($142M)
- Loss of trust in e-services: 16% ($103M)
- Training: 11% ($71M)
- Reputational Damage: 3% ($19M)
- Insurance and Compliance Costs: 1% ($6M)

Total Indirect Cost: $647 Million

Source: http://www.serianu.com/resources.htm
Cyber crime insights

- **Consequences worsen**
  - Customer data losses (in a context of stronger regulation)
  - Financial losses: 80% money related
  - Denial of Service (34% of attacks)

- **A huge and evolving variety of modus operandi**
  - 85% of attacks use 10 vulnerabilities within >900 listed
  - >110,000 vulnerabilities (CVE) listed in 10 years
  - Tenth of attack models, of which 9 are related to 95% of cases.
  - Fast pace: 2017: Ransomware, 2018: Crypto Currency Mining
  - 80% external intrusions, but FI should not forget internal intrusions

- **Poor detection: you can find only what you know**
  - Reduced intrusion and data leakage time: few minutes for >80% of cases
  - Long detection time: several weeks for >80% of cases

- **INTRUSIONS DO HAPPEN**: Ethical Hackers get administration rights in 95% of cases in about 10 days

- **CUSTOMS may be a key target and are amongst major financial players in the region**

- **Very limited resources**: 10,000 security engineers in Africa, 780,000 in USA. 3.5M engineers missing WorldWide

- **International police and legal cooperation limited**

- **$1.5 Billion has been lost in Africa (of whom at US banks)**
<table>
<thead>
<tr>
<th>Summary of findings</th>
<th>VERIZON 2018 Data Breach Investigations Report</th>
</tr>
</thead>
</table>

**Who's behind the breaches?**
- 73% perpetrated by outsiders
- 28% involved internal actors
- 2% involved partners
- 2% featured multiple parties
- 50% of breaches were carried out by organized criminal groups
- 12% of breaches involved actors identified as nation-state or state-affiliated

**What tactics are utilized?**
- 48% of breaches featured hacking
- 30% included malware
- 17% of breaches had errors as causal events
- 17% were social attacks
- 12% involved privilege misuse
- 11% of breaches involved physical actions

<table>
<thead>
<tr>
<th>Top internal actor varieties in breaches</th>
</tr>
</thead>
<tbody>
<tr>
<td>System admin</td>
</tr>
<tr>
<td>End-user</td>
</tr>
<tr>
<td>Other</td>
</tr>
<tr>
<td>Doctor or nurse</td>
</tr>
<tr>
<td>Developer</td>
</tr>
<tr>
<td>Manager</td>
</tr>
<tr>
<td>Executive</td>
</tr>
<tr>
<td>Cashier</td>
</tr>
<tr>
<td>Finance</td>
</tr>
<tr>
<td>Human resources</td>
</tr>
</tbody>
</table>

**What are other commonalities?**
- 49% of non-POS malware was installed via malicious email
- 76% of breaches were financially motivated
- 13% of breaches were motivated by the gain of strategic advantage (espionage)
- 68% of breaches took months or longer to discover

Every dept. is involved

>100% in Luxembourg, neutral country!

[https://enterprise.verizon.com/resources/reports/dbir](https://enterprise.verizon.com/resources/reports/dbir)
Cyber crime - A complex landscape

Business Process

Weakness led to fraud

Fraud Case

Business Process Assault Plan/Scenario

Implemented by

Modus Operandi

Pre-attack phase

Cyber Attack Vector (Campaign)

Post-attack phase

Uses techniques

Tactics, Techniques and Procedures

E.g. recon based on human engineering

TTP 1

TTP n

Based on cyber threats

Cyber Threats

Cyber threat 1

Cyber threat 2

Cyber threat 3

Cyber threat 4

Threats eventually used in KC phases

Kill Chain

Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command & Control

Actions on Objectives

Targeting assets

Affected Assets

Figure 2: Big picture CTI elements from Modus Operandi to affected assets

Source EM
Crisis Management and Cyber Resilience: procedures, detection and response systems, collaborations, communication, must have been thought out and tested upstream ... even if the reality will not (probably) match as expected

=> Need to promote and build a collaborative environment

Cyber attack Crisis simulation room from C3.LU Luxembourg Cyber security Competence Centre
Houston, we have a problem

- You cannot rely on norms, standards and certifications only
- You cannot rely on technology
- You cannot rely on networks operators’ security (*)
- You cannot trust devices security & App security (*)
- You cannot rely on your staff (*), and they are not enough
- You should not wait for governments, police, justice, for an international issue

(*) CGAP Webinar Cybersecurity for mobile financial services, October 2018
PERSPECTIVES
See: IBM X-Force *Threat Intelligence Index 2018*
Investissements réalisés

Axes d’engagement

Source Thalès 2017, analyse Suricate Solutions
Cyber Hygiene – A Baseline Set of Practices

Cybersecurity hygiene is a set of practices for managing the most common and pervasive cybersecurity risks faced by organizations today.

1. Identify and prioritize key organizational services, products and their supporting assets
2. Identify, prioritize, and respond to risks to the organization’s key services and products
3. Establish an incident response plan.
4. Conduct cybersecurity education and awareness activities.
5. Establish network security and monitoring.
6. Control access based on least privilege and maintain the user access accounts.
7. Manage technology changes and use standardized secure configurations.
8. Implement controls to protect and recover data.
10. Manage cyber risks associated with suppliers and external dependencies.
11. Perform cyber threat and vulnerability monitoring and remediation.

Sources:
- 10 Steps to Cybersecurity, UK Government Communications Headquarters (GCHQ)
- 20 Critical Security Controls, Center for Internet Security (CIS) aka SANS 20
- Cybersecurity Framework, National Institute of Standards and Technology (NIST)
- Resilience Management Model, Carnegie Mellon University, Software Engineering Institute CERT Division
- Strategies to Mitigate Cyber Security Incidents, Australian Signals Directorate (ASD)
OUR APPROACH
Prevention & remediation need a global expertise.
CERTs are organized in an international network.

CERT COMPUTER EMERGENCY RESPONSE TEAM

Business Process

Weakness led to fraud

Fraud Case

Business Process Assault Plan/Scenario

Implemented by

Modus Operandi

Pre-attack phase

Cyber Attack Vector (Campaign)

Post-attack phase

Uses techniques

Tactics, Techniques and Procedures

E.g. recon based on human engineering

TTP 1

Based on cyber threats

TTP n

E.g. monetization based on money mules

Cyber-Threats

Cyber threat 1

Cyber threat 2

Cyber threat 3

Cyber threat 4

Threats eventually used in KC phases

Kill Chain

Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command & Control

Actions on Objectives

Targeting assets

Affected Assets

Legend:
IT/Cyber-related content

Source: ENISA
Detection needs a real time 24x7 operational organisation.
Accredited CERT is at the heart

- Phishing monitoring
- Malware analysis
- Vulnerability Monitoring
- Reputation Monitoring
- Log Mining
- Forensic Investigations
- Malicious document analysis
- Incident Response
- Server take down
- Persistance Malware detection
- MISP: Malware Information Sharing Platform
- IP Reputation Protection
- Vulnerability Notification

CERT-XLM
Excellium Services
Computer Security
Incident Response Team

TF-CSIRT
Trusted Introducer

cert.lu
CSOC: 4 key components for efficient response

- **Security Intelligence**
  - MISP (Malware Information Sharing Platform)
  - CERT LU / CERT national Luxembourg
  - CERT XLM / CERT Excellence
  - CERT BIF
  - AFRICACERT (en développement)
  - CERT Monde CERT

- **Organisational Component**
  - Equipe Pentest
  - Equipe Infrastructure
  - Equipe SOC
  - Equipes CERT Niveau 3
    - #25 experts
  - Equipes SOC Niveau 2
    - 8h-22h + astreinte
  - Equipes SOC Niveau 1
    - 8h-22h puis 24x7

- **Operational security team**
  - 7 to 8 Security Analysts in Senegal
  - #45 SOC - CERT experts in Luxembourg
  - Availability up to 24 x 7
  - Initial and life long training
  - Coaching and skills development

- **Technical Infrastructure**
  - Virtual Datacenter Luxembourg
  - Suricate Solutions Datacenter Sénégal
  - Suricate Solutions (Luxembourg)
  - Excellium Services (Luxembourg)
  - Suricate Solutions (Sénégal)

- **State of the Art performance**
- Proximity and local costs
Cyber Security Operation Centre

Based in Dakar - Senegal
Regional & Continental reach

Protection of customers & Private and public institutions

Mutualized services to prevent, detect & mitigate attacks, improve compliance

World Class technology, processes & security intelligence
A comprehensive set of continuous improvement security services to accompany institutions

- **Security Supervision & Incidents Response:** This core service is a 24x7 real time detection capability

- **Capacity building:** Coaching, and technical support, Part time CISO, Awareness and cyber security training programs for management, technical teams, local offices and employees,

- **Information Security Risk Management:** “Flash Diagnostic” Maturity assessment, MONARC Risk Management framework, Business Continuity, Penetration testing, Security Policies ...

- **Intelligence sharing network** to report and research incidents, identify attack models, share information, recommendations and best practices within the sector and with external parties, R&D on new tools and methods

- At the start, we rely on 2 public and private Luxembourg CERTs, then

- Develop Panafrican Financial Inclusion CERT
Conclusions

- Let’s be pragmatic: the threats and attacks are there even if we do not measure well.
- Don’t translate 100% locally overly sophisticated frameworks. Our top 4:
  - Awareness at MD level
  - Security Supervision KISS Keep It Simple Stupid, but based on strong cyber threat intelligence
  - Prepare recovery
  - Information Sharing
- Security should be embedded in every structure in the organization.
- You are not alone: Contribute to local or regional or continental sharing network.
- Discussions with several government in the region for SOC operations and CERT build up assistance.
- GTR may have a leading role in that perspective to promote cooperation.
- We are there to help the customs community in the region.