



صندوق النقد العربي
ARAB MONETARY FUND

Cyber Resilience Oversight Guidelines for the Arab Region, concerning

Financial Market Infrastructures

Arab Regional Fintech Working Group

December 2019, Abu Dhabi

Table of contents

- Cyber Governance: Cyber Resilience Strategy and Framework; Risk Management and Ancillary Components
- Guidance on the Senior Executive or Chief Information Security Officer (CISO)
- Information Assets Identification and Classification
- Protection and Risk Management
- Cyber Incidents Detection
- Incident Response and Recovery
- Information Security Controls Testing
- Situational Awareness and Cyber Threat Intelligence

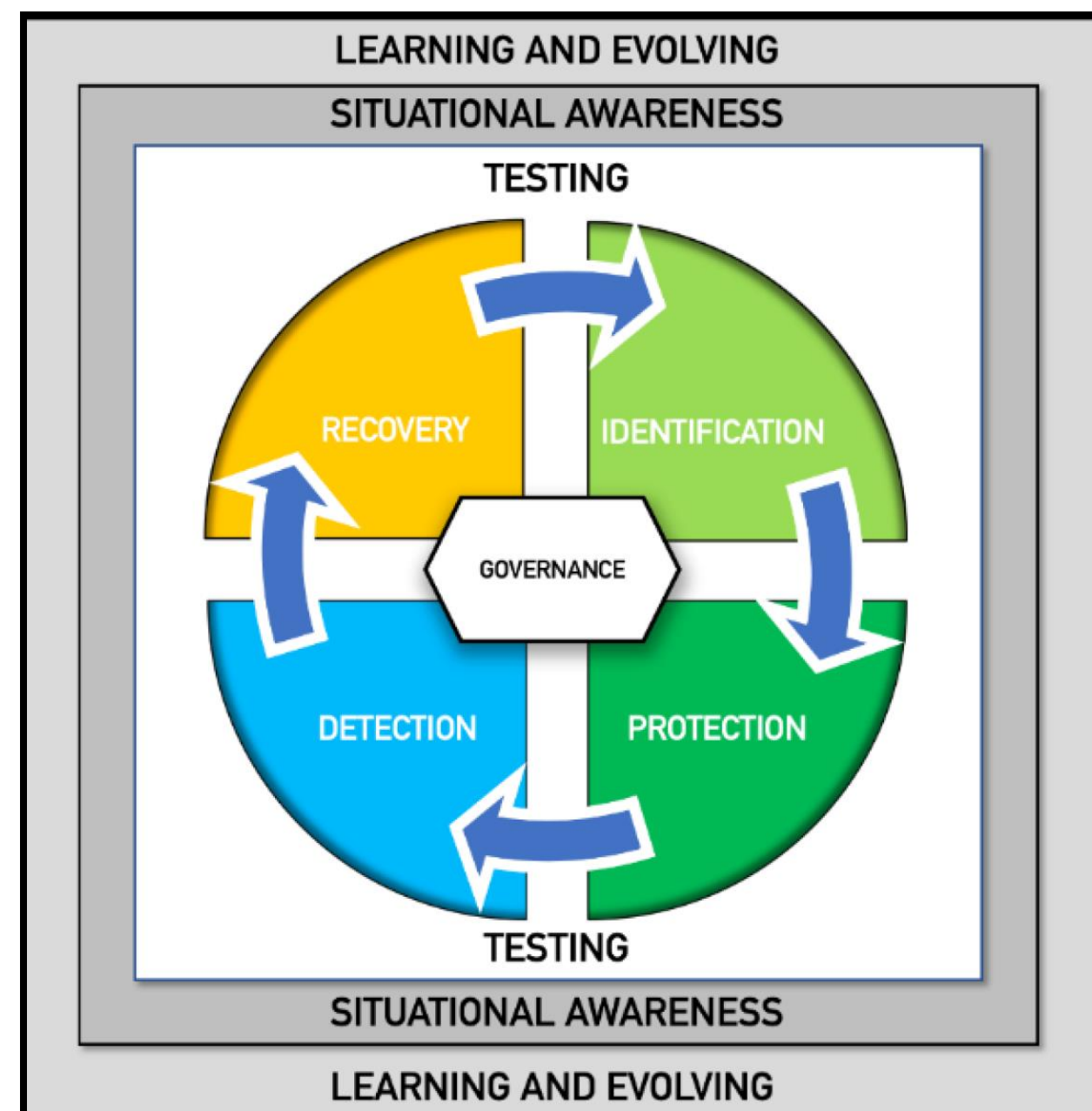


Cyber Governance: Cyber Resilience Strategy and Framework; Risk Management and Ancillary Components

Cyber governance:

- Organisational arrangements for the creation, implementation, examination and review of an Organisation's approach to managing cyber-related risks and cyber-attacks.
- Aims: Mitigating the risk of cyber-attacks, related disruptions, maintain a cyber-resilient environment; financial stability, financial shock resistance, economic growth

Cyber Resilience Strategy and Framework; Risk Management and Ancillary Components



Review and Update of Cyber Resilience Strategy and Framework

7 Factors to consider:

- Ever-evolving threat landscape
- Threat Intelligence on Threat Actors; TTPs
- Risk Assessments Findings and Results
- Incidents
- Lessons Learned
- Performance Metrics
- New Business Developments and Future Strategic Objectives

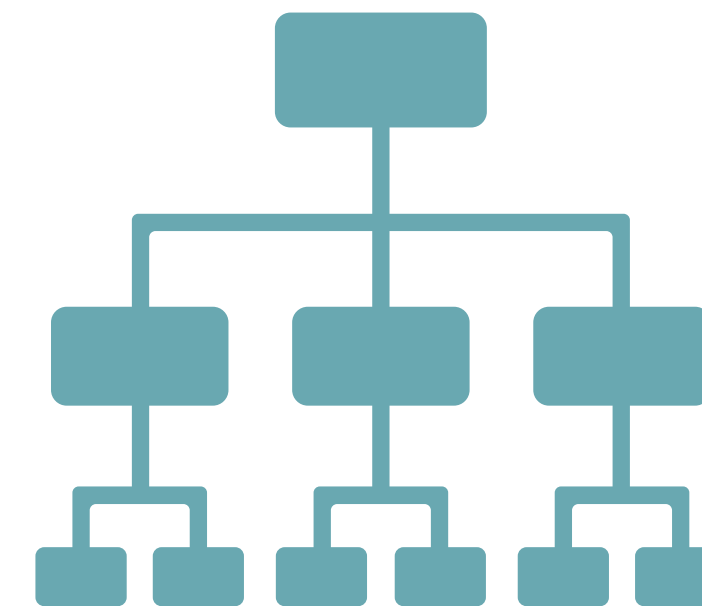
Guidance on the Senior Executive or Chief Information Security Officer (CISO)

- Independent, senior executive, normally a Chief Information Security Officer (CISO), who is responsible for all cyber resilience issues within the organisation, as well as with regard to third parties.
- Responsible to ensure that the cyber resilience objectives and measures defined in the organisation's cyber strategy, cyber resilience policies and guidelines are properly communicated both internally and, when relevant, externally to third parties; and that compliance with the strategy, policies and guidelines is reviewed, monitored and adhered to.
- Primary Tasks: 12 are highlighted
- Independence from IT or operations department
- Not involved in internal audit activities
- Ability to report to Senior Management and the Board directly, at any time



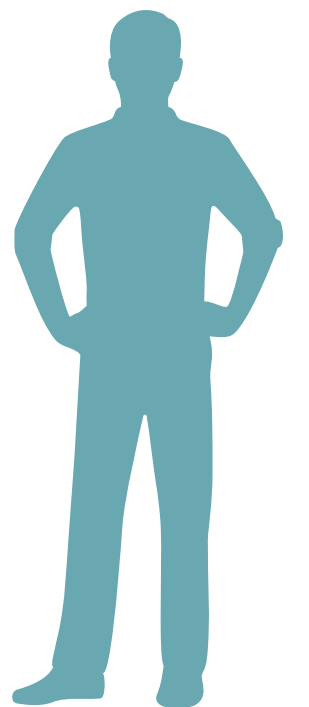
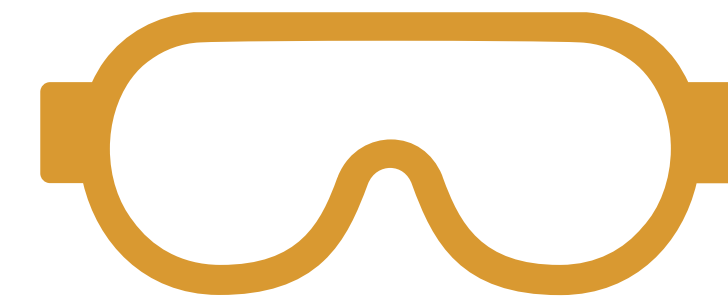
Information Assets Identification and Classification

- Identification: Operations, information assets, internal situation and external dependencies, business functions, current inventory
- Classification of criticality: Prioritisation of protective, detective, response and recovery efforts
- Interconnections with Third Parties
- Impact to and from an Organisation's ecosystem
- Risks from interconnections
- Contracts with service providers/vendors
- Data sharing agreements



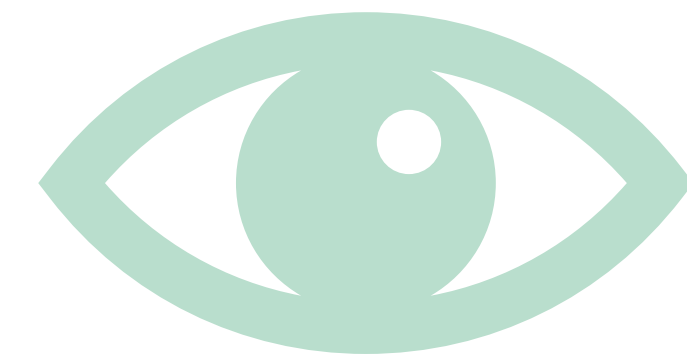
Protection and Risk Management

- Processes and assets
- Security objectives
 - ▶ Continuity and availability of information systems
 - ▶ Integrity of information (in use, at rest, in transit)
 - ▶ Laws, regulations and standards
- Risk based approach; Defence in Depth (Castle approach); Resistance by Design
- Network and Infrastructure management
- Logical and physical security management
- Change and patch management
- People management



Cyber Incidents Detection

- An organisation's ability to recognise signs of a potential cyber incident, or to detect that an actual breach has taken place, is essential to strong cyber resilience.
- Early detection provides an organisation with useful lead time to launch appropriate countermeasures against a potential breach, and allows for the proactive containment of actual breaches.



Incident Response and Recovery

- Financial stability may depend on an organisation's ability to settle obligations when they are due.
- Therefore, an organisation's arrangements should be designed to enable it to resume critical operations rapidly, safely and with accurate data in order to mitigate the potentially systemic risks of failure to meet such obligations, when participants are expecting it to meet them.
- Business continuity planning is essential for meeting the organisation's objectives
- Effective and Efficient Incident Management requires:
 - ▶ Preparation
 - ▶ Detection
 - ▶ Analysis
 - ▶ Containment
 - ▶ Eradication
 - ▶ Recovery
 - ▶ Lessons learned
- Data Confidentiality, Integrity & Availability
- Crisis Communication, Communicability (Contagion), Collaboration & Responsible Disclosure
- Forensic Readiness



Information Security Controls Testing

- Vulnerability Assessments
- Scenario-based Testing
- Penetration Testing
- Red Team Testing
- Taxonomy (Classification) of Cyber Risk Controls

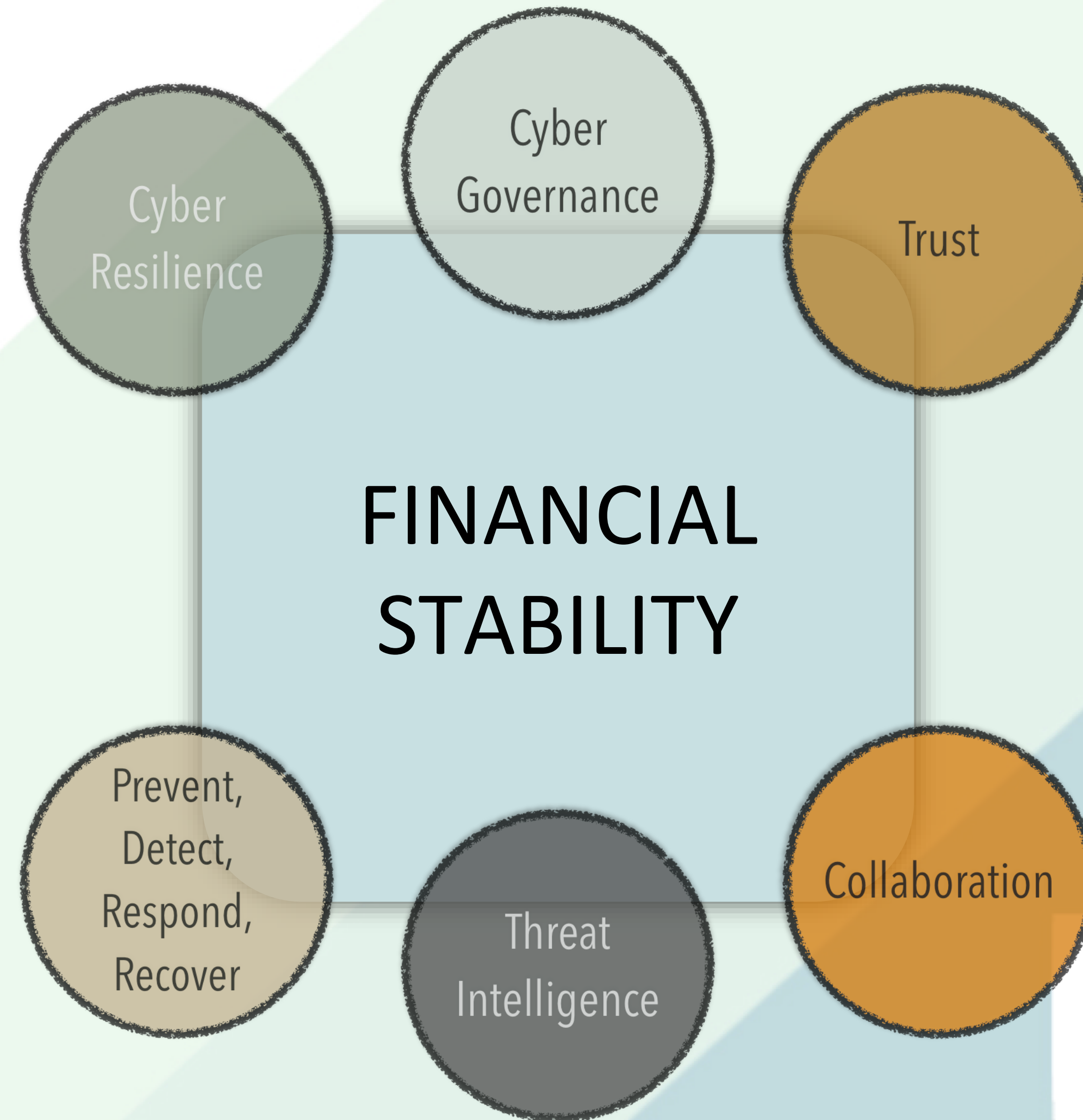




صندوق النقد العربي
ARAB MONETARY FUND

Situational Awareness and Cyber Threat Intelligence

Threat Intelligence and Situational Awareness



TOTAL **ACTIVE MALICIOUS OBSERVABLES** LINKED TO AMF MEMBER COUNTRIES

873,962



Threat Intelligence and Situational Awareness

Malware C2 (Command and Control)

- Communication channel between malicious actor and malicious software or tools
- This infrastructure is used by cyber criminals to control and update/change their malware as needed

APT (Advanced Persistent Threat)

- An actor/group that has a high level of sophistication and skill, they are usually well funded and or supported by nation states

Botnet

- A network of systems used for various types of attacks like DDoS or act as C2 for malware

Brute Force

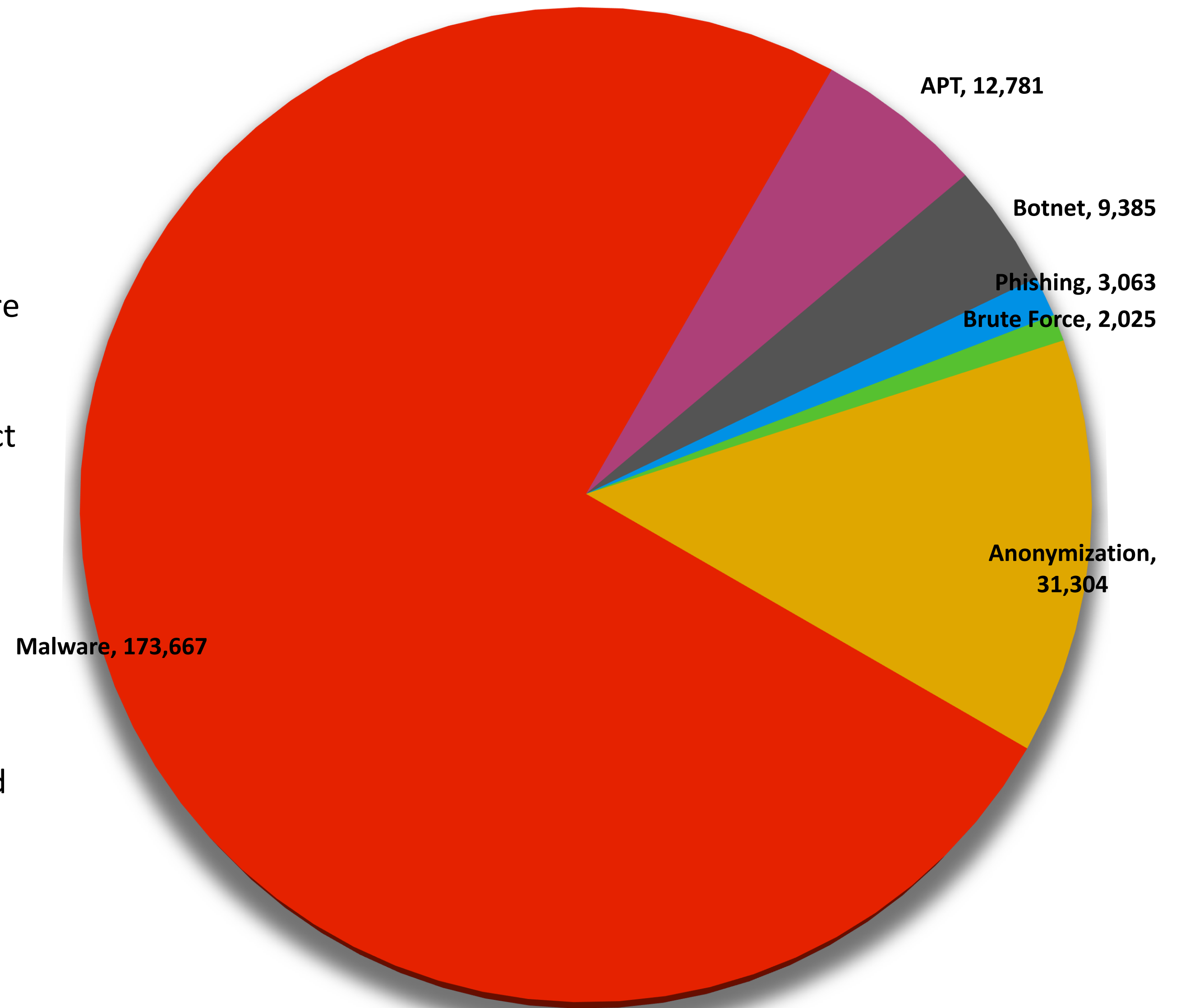
- Systems that carry out scans and brute force attacks on systems, to crack passwords

Anonymization

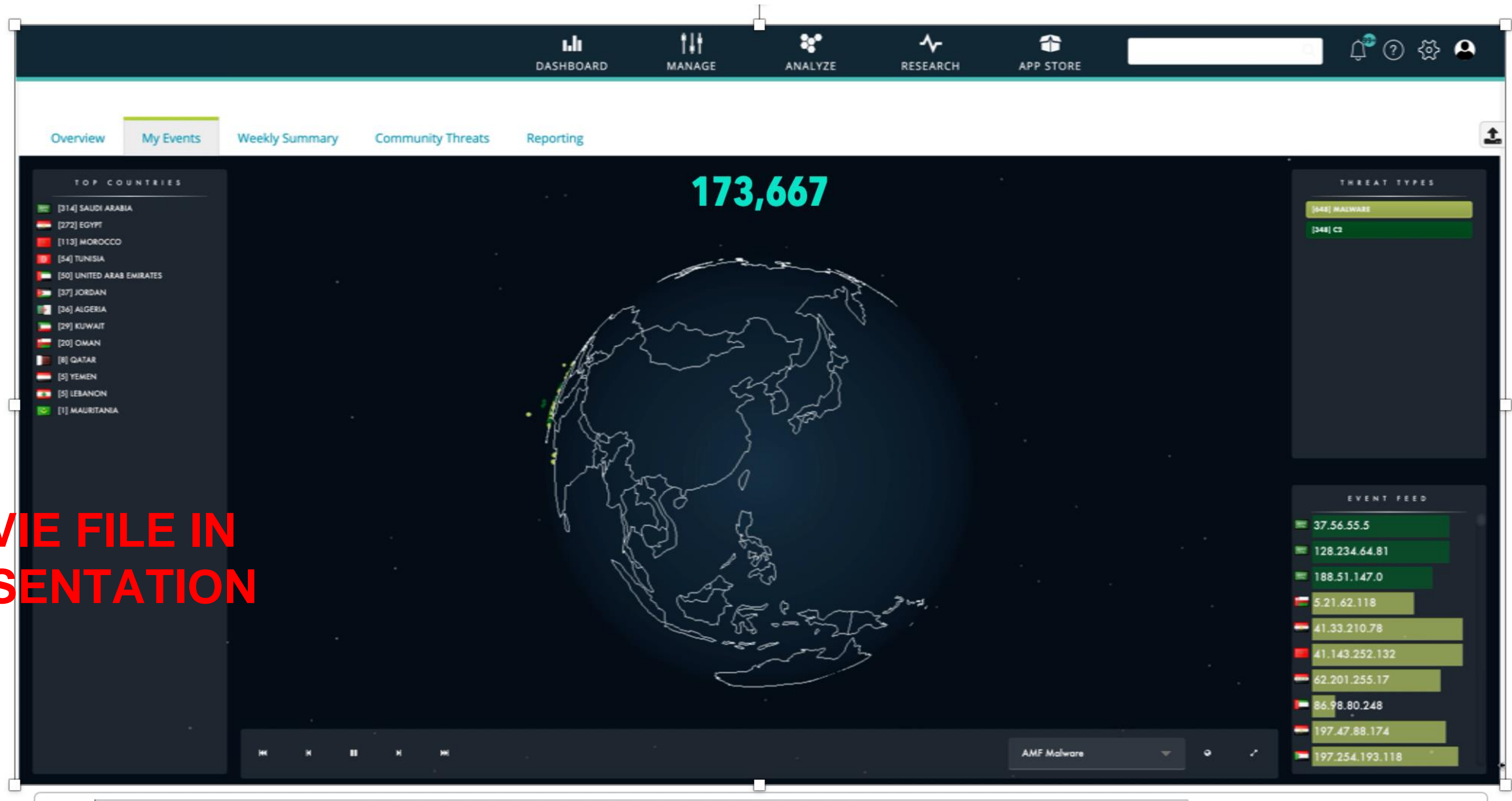
- Systems on the internet that obfuscates the origin of an attack

Phishing

- Websites that trick victims to enter their credentials which is captured by an attacker



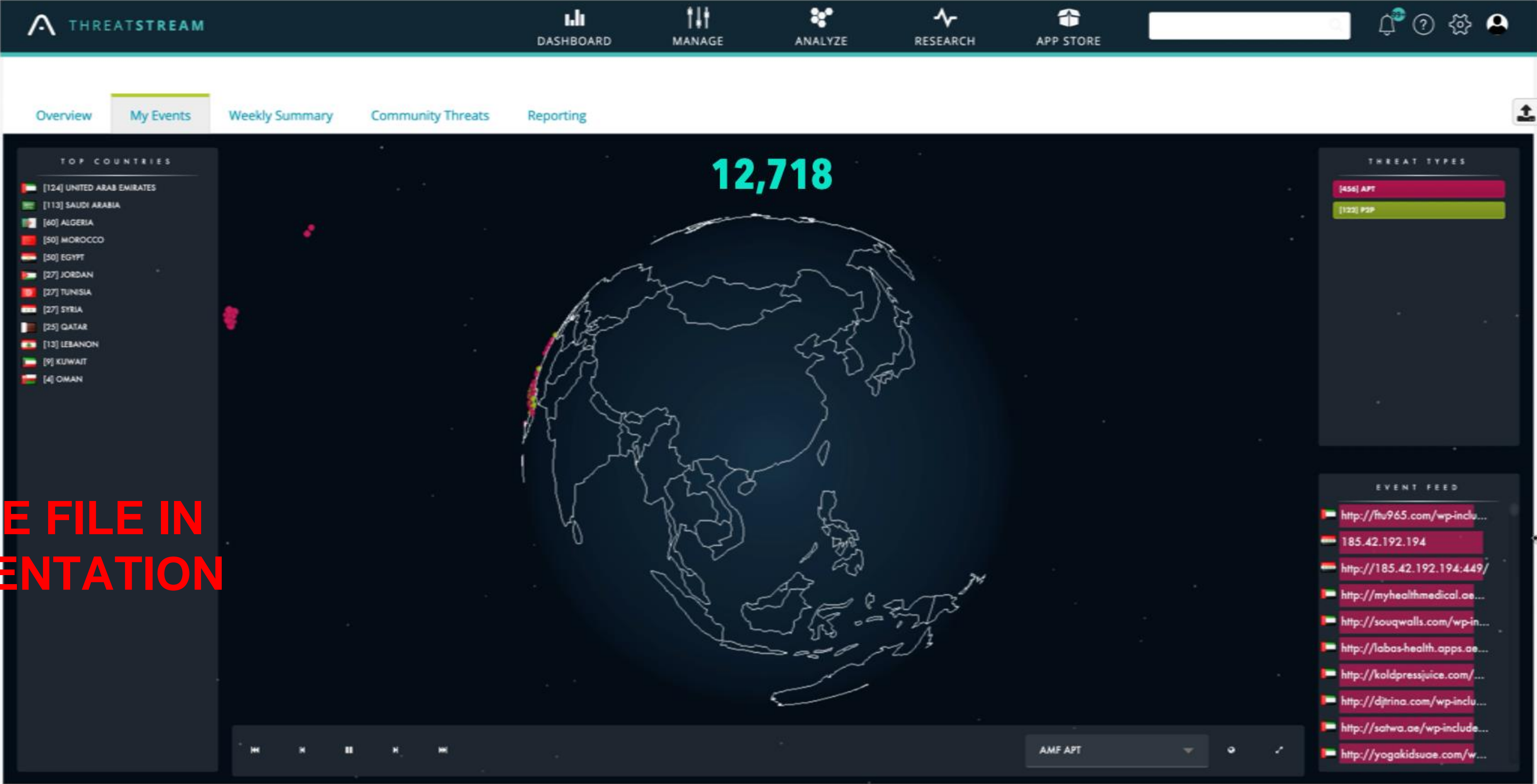
MALWARE INFRASTRUCTURE LOCATIONS



MOVIE FILE IN PRESENTATION



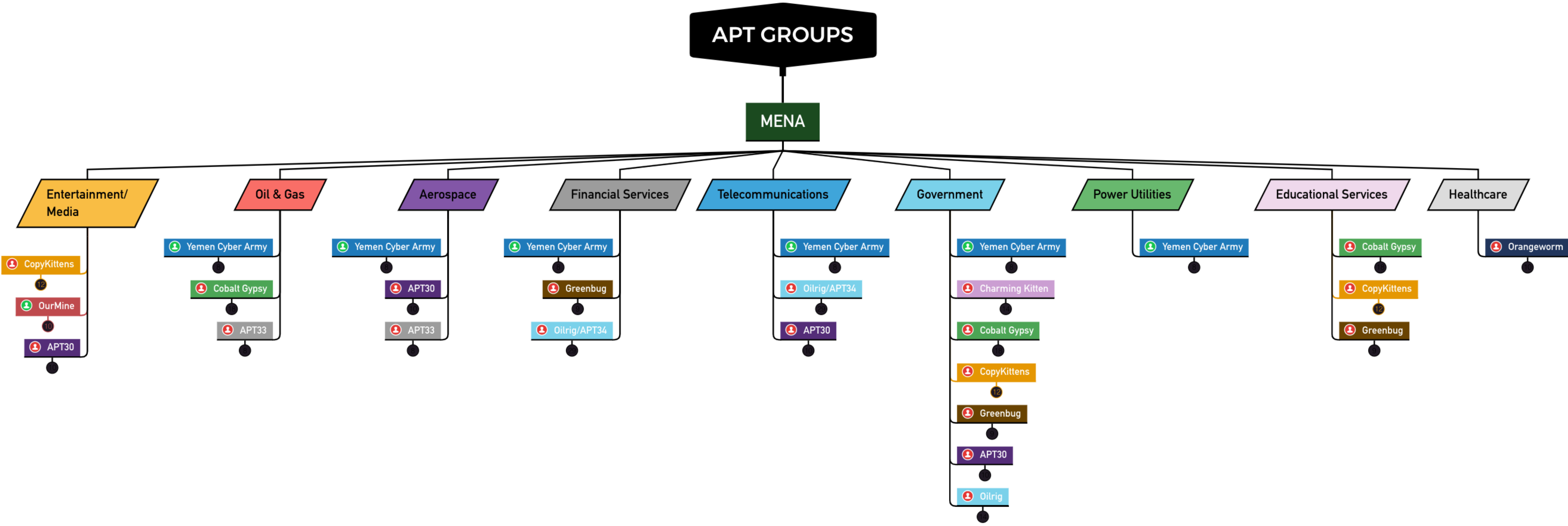
APT INFRASTRUCTURE LOCATIONS



MOVIE FILE IN PRESENTATION



Threat Intelligence and Situational Awareness





صندوق النقد العربي
ARAB MONETARY FUND

FINANCIAL INDUSTRY SPECIFIC THREAT INTELLIGENCE

FINANCIAL MALWARE/BANKING TROJANS

- **Zeus** (The father of Active and Notable Trojan Banking Malware Families)
- **Gozi** (Also known as Ursnif)
- **GozNym** (A Hybrid of Gozi and Nymaim)
- **Carberp** (Used by the Russian Carbanak group)
- **SpyEye** (Competitor for Zeus)
- **Shylock**
- **Citadel** (Zeus Variant)
- **Tinba** (Also known as Tiny Banking Trojan)
- **VawTrak** (Also known as Neverquest or Snifula)
- **Emotet** (Very active and connected to Dridex)
- **Kronos** (Spinoff of Carberp)
- **Dyre/Dyreza** (Variant of Zeus)
- **Trickbot** (Successor to Dyre, Very active)
- **Dridex** (Connected to Emotet and Gozi)
- **Danabot** (Possible link between Gozi and Tinba)
- **Ramnit** (Zeus variant)
- **Panda** (Zeus variant)
- **Backswap** (Tinba Variant)



TOTAL **ACTIVE FINANCIAL MALWARE OBSERVABLES** LINKED TO AMF MEMBER COUNTRIES

11,379



Threat Intelligence and Situational Awareness



Malicious
Financial
Indicators
Observed



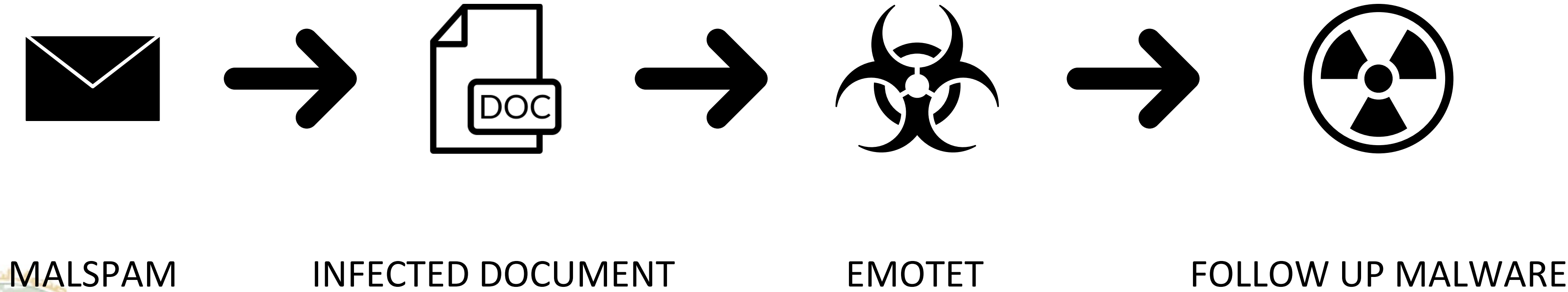
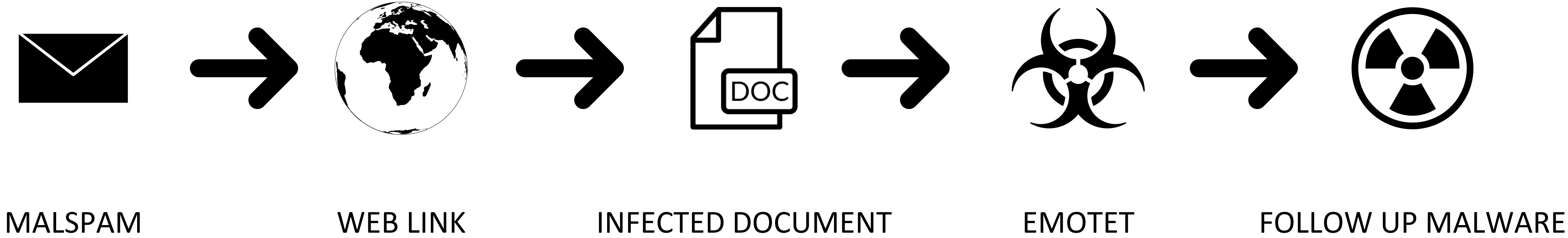
DRIDEX and EMOTET

Capabilities:

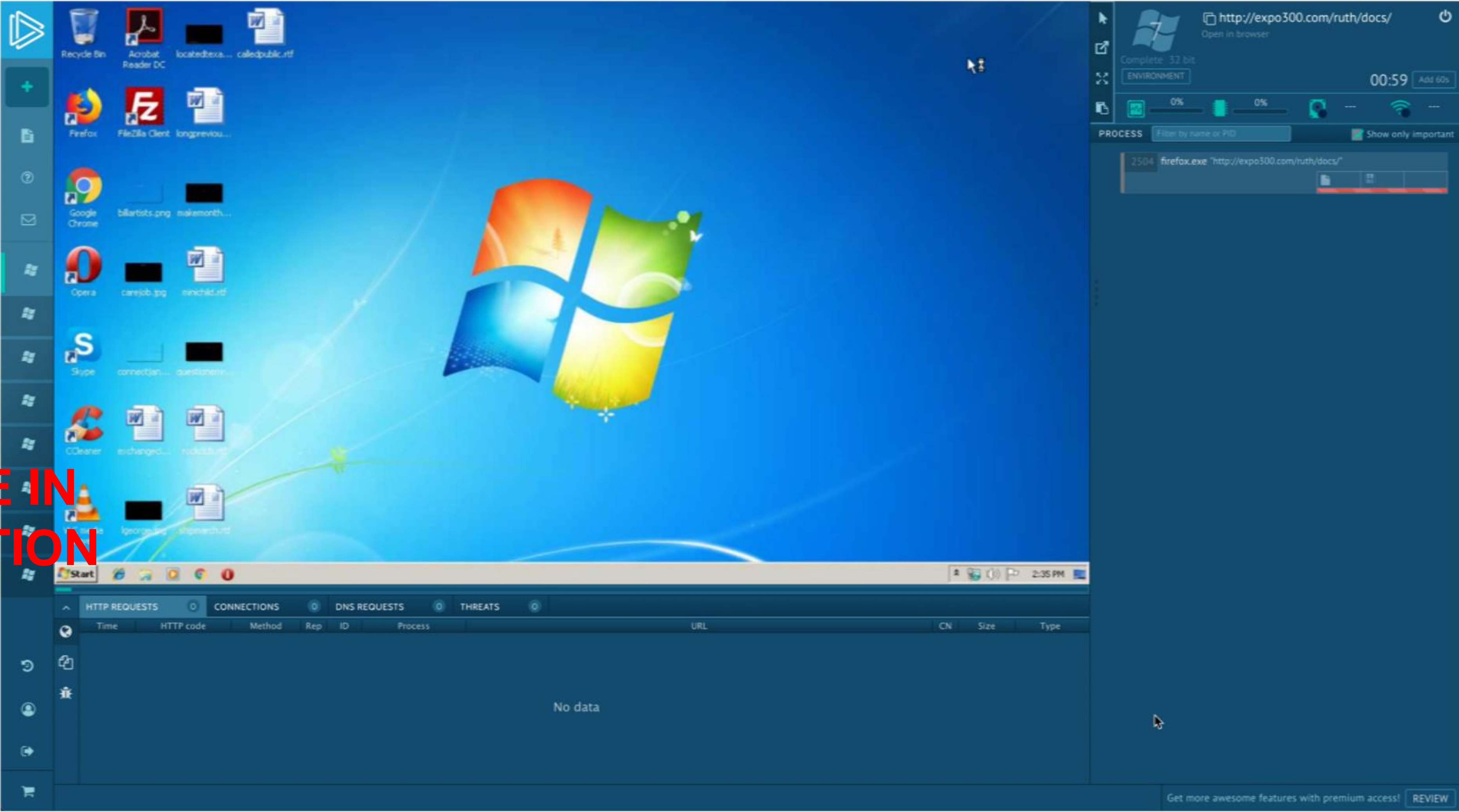
- Primary Objective - Steal banking information
- Steals Sensitive Data/Files
- Steals victim keystrokes (Usernames, Passwords etc)
- Installs other types of malware ie: Ransomware
- Turns victim system into a bot for **Botnet Attacks**



EMOTET infection chains



Threat Intelligence and Situational Awareness



MOVIE FILE IN PRESENTATION




Real World Incident

#DECEMBER STRIKES FRANCE EUROPE INTERNATIONAL SCIENCE & TECHNOLOGY CULTURE

Focus on Africa: Kenya: Home-grown hackers have looted millions from banks

f WhatsApp Twitter Share

Issued on: 03/05/2019 - 09:45



Threat Intelligence and Situational Awareness

Real World Incident

Threat Intelligence is a team sport.

MALICIOUS Sandbox Report for explorer.EXE

Watch 0 Star 0 [Dropdown] 0 [Dropdown] Share

Sandbox Report ID: 253270
Platform: Windows 7
Classification: My Organization

Sample reads its own file content

Uses code obfuscation techniques (call, push, ret)

Drops files with a non-matching file extension (content does not match file extension)

Found API chain indicative of debugger detection

Injects code into the Windows Explorer (explorer.exe)

Installs a global keyboard hook

Behavior Analysis

FILES REGISTRY KEYS MUTEXES

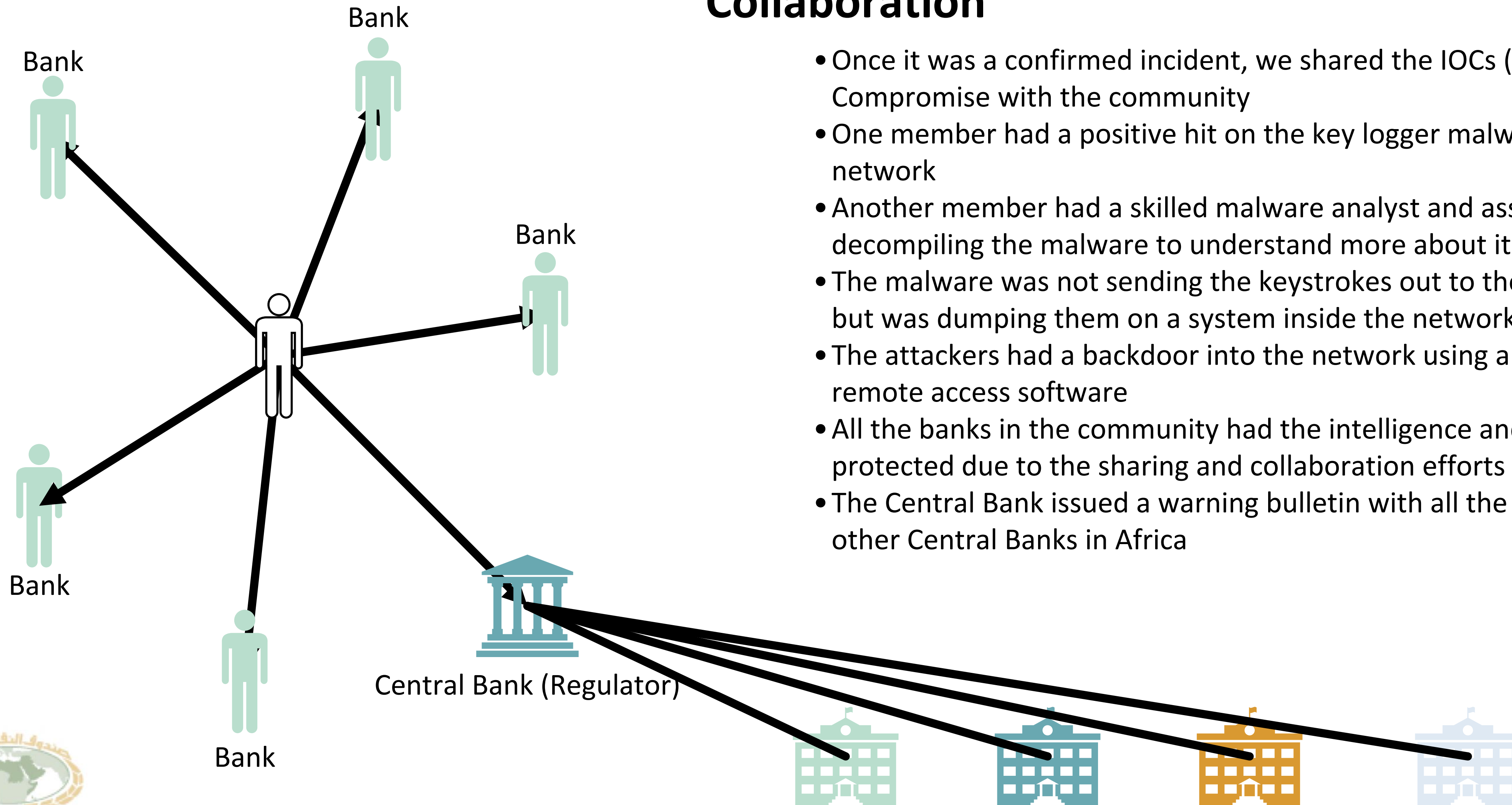
Screenshot: #4 of 7



Threat Intelligence and Situational Awareness

Collaboration

- Once it was a confirmed incident, we shared the IOCs (Indicators of Compromise) with the community
- One member had a positive hit on the key logger malware file in their network
- Another member had a skilled malware analyst and assisted us in decompiling the malware to understand more about it
- The malware was not sending the keystrokes out to the internet to a C2 but was dumping them on a system inside the network
- The attackers had a backdoor into the network using a commercial remote access software
- All the banks in the community had the intelligence and was now protected due to the sharing and collaboration efforts
- The Central Bank issued a warning bulletin with all the intelligence to other Central Banks in Africa



Closing Remarks

