

THE CYBER THREAT INTELLIGENCE

EU Conference 2020

“FULL-STACK CYBER-ATTACK”



Francisco Luis de Andrés Pérez
Independent Cybersecurity Researcher
flandres@ciso.es



ORGANISED WITH
THE SUPPORT OF :



Brussels, 30th January 2020

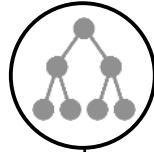
ORGANIZED CYBERCRIME DIGITAL TRANSFORMATION

References to the Jonathan Lusthaus model, Industry of Anonymity: Inside the Business of Cybercrime(Cambridge, Harvard University Press, 2018).

TECHNOLOGIES



PEOPLE



PROCESSES



FINANCES



SUPPLY CHAIN



TACTICS & TECHNIQUES

Malware and packers, steganography, DGA's, anti-debuggers and more powerful and stealth C&C, encrypted beacons over well-known protocols, use of IA and machine learning Gyoithon...

TEAMS

Hierarchical structures, roles and responsibilities with strong disciplines similar to the army, where many of them are coming from.

STRATEGY & PROCEDURES

New and more sophisticated methodologies segmented by attacker profiles, skills ...

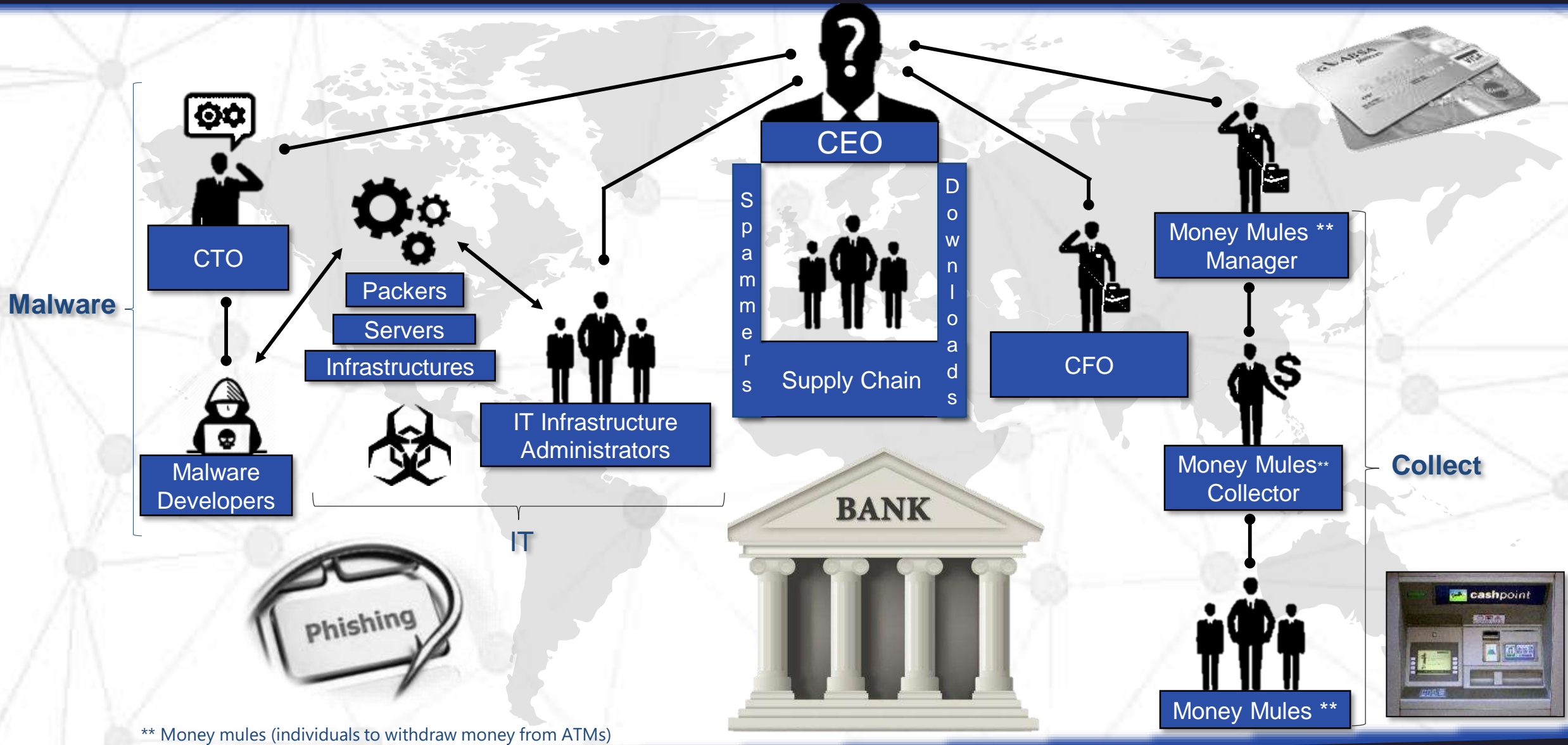
INVESTORS

Financing structures crossed with other criminal organizations and activities, or even sponsored by states: Equation Group, Lazarus, Fancy Bear etc...

SERVICE PROVIDERS

Relations with other criminal organizations services oriented such as money laundry, physical protection, money mules...

ORGANIZED CYBERCRIME HIERARCHICAL STRUCTURES



MONEY MULES IN ACTION "SILENCE APT" 2019 CAMPAIGN



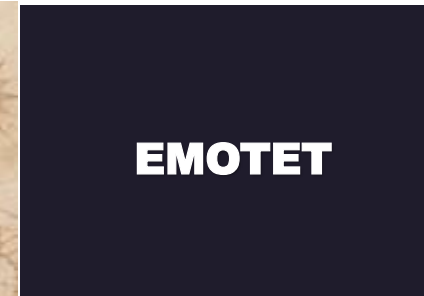
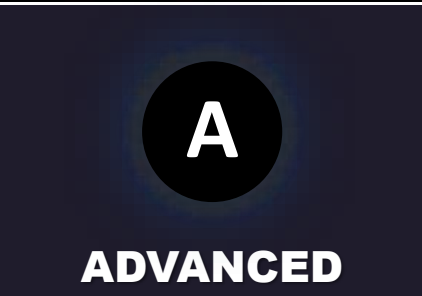
SILENCE APT, a Russian-speaking cybercriminal group, known for targeting financial organizations primarily in former Soviet states and neighboring countries is now aggressively targeting banks in more than 30 countries across America, Europe, Africa, and Asia.

In 2019 Silence Apt withdrew money from the Bangladeshi bank twice within 2 months

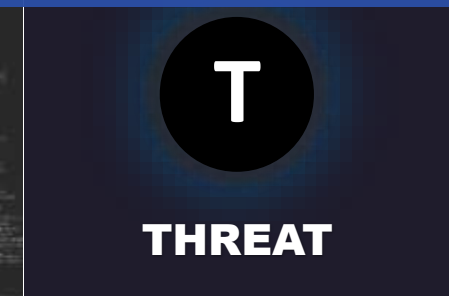
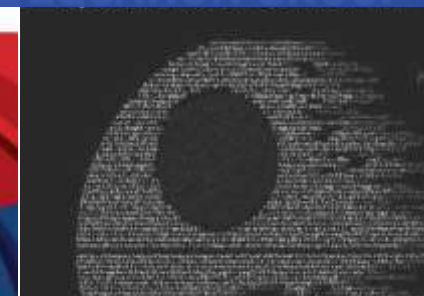
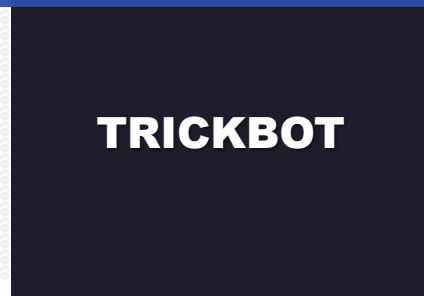
- In the first incident, they used them outside of Bangladesh, according to the media reports.
- In the second incident, money was stolen from a Dutch-Bangla ATM in Dhaka, which was recorded by CCTV cameras. It is interesting to note that the cash withdrawal occurred in the presence of an ATM security guard. The recording shows the faces of the mules wearing medical masks started withdrawing money from the ATMs of Dutch-Bangla Bank.

https://www.group-ib.com/resources/threat-research/silence_2.0.going_global.pdf





CYBERCRIME IS GROWING EXPONENTIALLY



Average to detect an APT 146 days Global, and 469 days at the Eurozone**Ponemon report





ARE WE FOLLOWING THE RIGHT STRATEGIES ?

SOME PEOPLE PREFER TO VOID OR EVEN IGNORE THEIR THREATS



OTHER ONES FEEL SAFE, LIVING A FALSE SENSE OF SECURITY ...



“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”
— Sun Tzu, The Art of War

JUST A FEW ARE MOVING TO ADVANCED ACTIVE DEFENSE SOLUTIONS

RPA, robotic process automation into sandbox

Forensic assessments, before incident occurs

Cyber Threat Intelligence analysis

Orchestration over SIEM, SOAR

Threat hunting analysis IOC's

Deception technologies beyond honeypots



“FULL-STACK CYBER-ATTACK”

Francisco Luis de Andrés



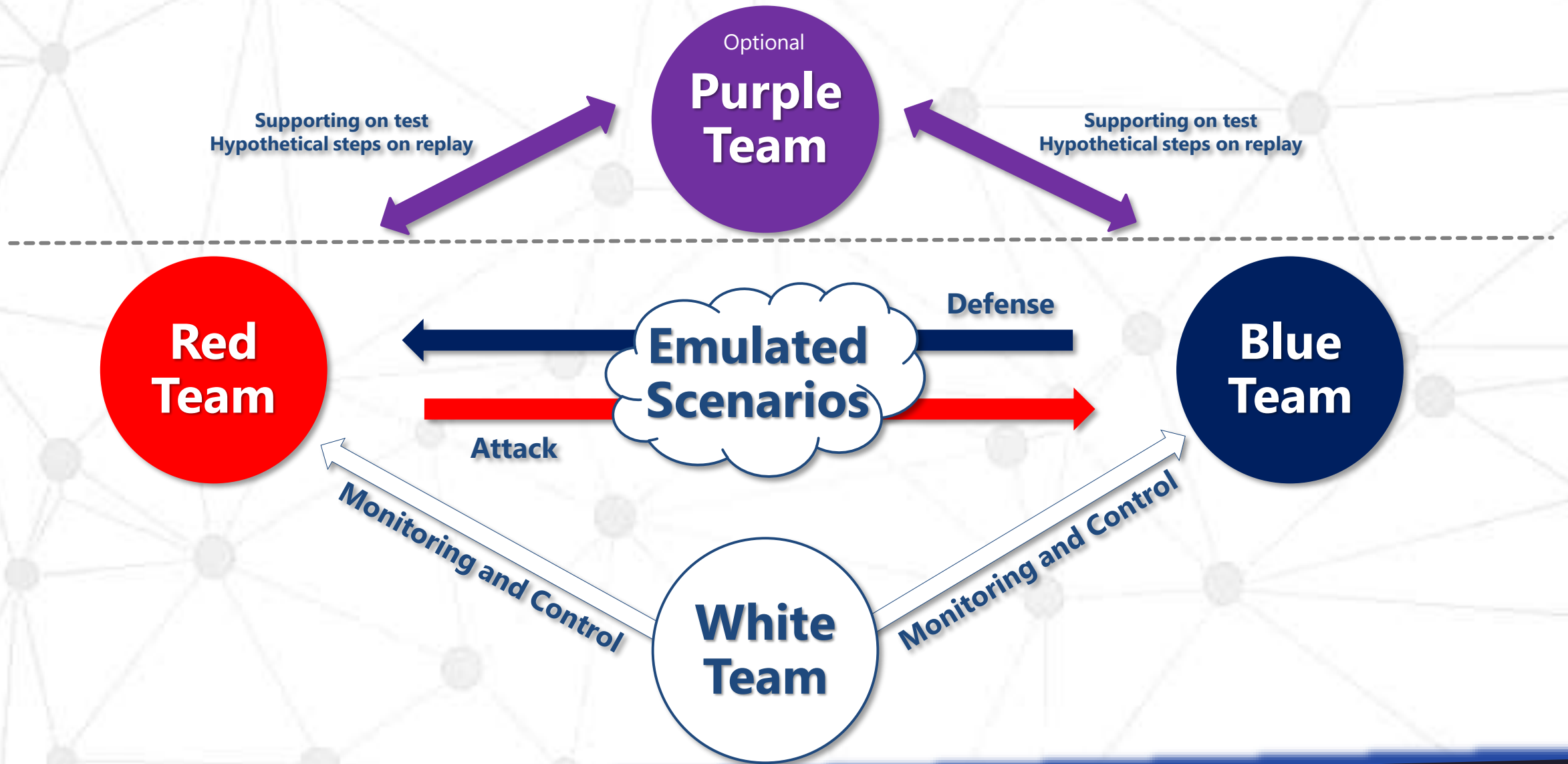
DO WE NEED TO TEST OUR CYBERSECURITY ?

DIFFERENCES BETWEEN PENTESTING AND RED TEAMING



	PENTEST	RED TEAM
SCOPE	Limited to systems and applications	A wider scope in order to cover all different infrastructures, even employees or physical assets
TOOLS	Vulnerabilities detection tools, and exploitation tools or frameworks	The vulnerabilities exploitation is just a step to achieve the final objectives. They need special tools to emulate CC, malware etc.. Moreover different and high skilled engineers, C&C etc...
VULNERABILITIES	Focus: Identification and exploitation of maximum amount of vulnerabilities	Focus: Specific target threats and impacts, for instance being able to transfer money without any authorization. Due to this objective, many vulnerabilities are not detected.

TEAM COLORS INVOLVED IN THE TIBER-EU EMULATED ATTACKS





STANDARIZING RED TEAM SCENARIOS



TIBER-EU: Threat Intelligence-Based Ethical Red Teaming

What about TIBER-EU?

TIBER-EU is the framework to developed by the European Central Bank in order to execute Red Team tests based on previous cyber threat intelligence analysis. It defines how all parties involved (Organizations, Providers, Authorities or Leas) should work together in order to test and improve the organizations cyber resilience by testing their infrastructures with controlled emulated attacks.

In the next slide ...



PRODUCTION ENVIRONMENT

"TIBER-EU is a common framework that delivers a controlled, bespoke, intelligence led red team **test of entities' critical live production systems.**"



REAL ACTORS TTPS EMULATION

"Intelligence-led red team tests mimic the tactics, techniques and procedures (TTPs) of real-life threat actors."



NO PRIOR KNOLEGDE (SOC)

"... It is equally critical that **the test is conducted without the prior knowledge of the entity** in order to gain a true picture of the entity's protection, detection and response capabilities."



TESTS AGREED IN THE SCOPE

"The Red Team provider plans and **executes a TIBER-EU test of the target systems and services, which are agreed in the scope.**"



"FULL-STACK CYBER-ATTACK"

DIFFERENCES BETWEEN SIMULATION AND EMULATION (MIMIC)

SIMULATION



"A good simulation could become emulation"

BIG ROOM FOR INTERPRETATION

EMULATION



MIMIC TO MATCH AN EXISTING TARGET



TIBER-EU: Threat Intelligence-Based Ethical Red Teaming



COMPARE DIFFERENT PROVIDERS: *"The market for threat intelligence and red team testing varies widely, with many providers providing an array of services. It is important that entities take due care during their procurement process. It is therefore recommended that entities and the TIBER Cyber Teams (TCTs) work in close collaboration with TI/RT providers, to ensure that a standardized and consistent approach is followed in using the services of TI/RT providers, and that there is a common understanding of the standards required to perform such tests."*

EFFECTIVE ANALYSIS OF THEIR CAPABILITIES: *"...Due to the sensitive nature of TIBER-EU tests, entities need to carefully select TI and RT providers which can provide an appropriate level of professional expertise and support for conducting the test."*

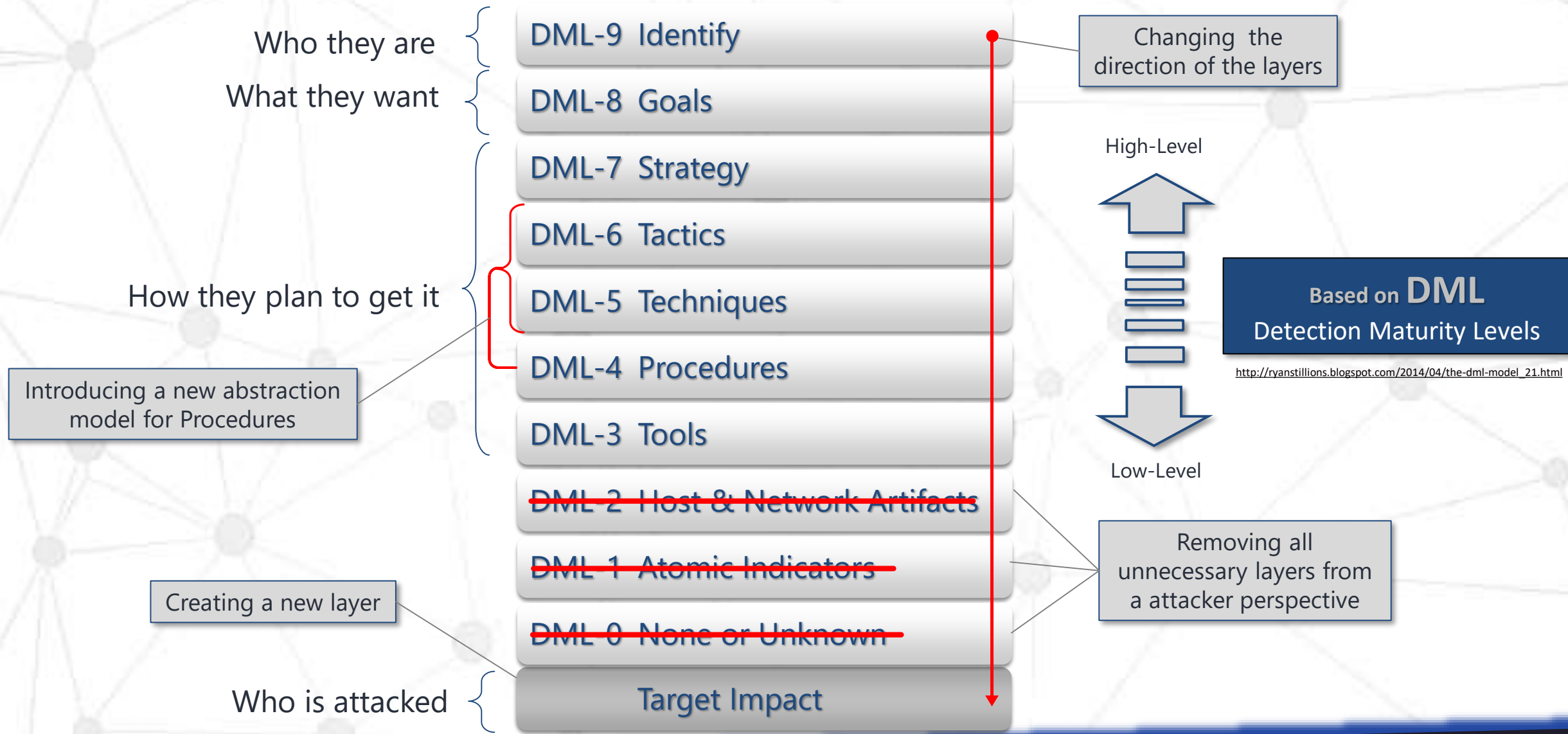
https://www.ecb.europa.eu/pub/pdf/other/ecb.1808tiber_eu_framework.en.pdf

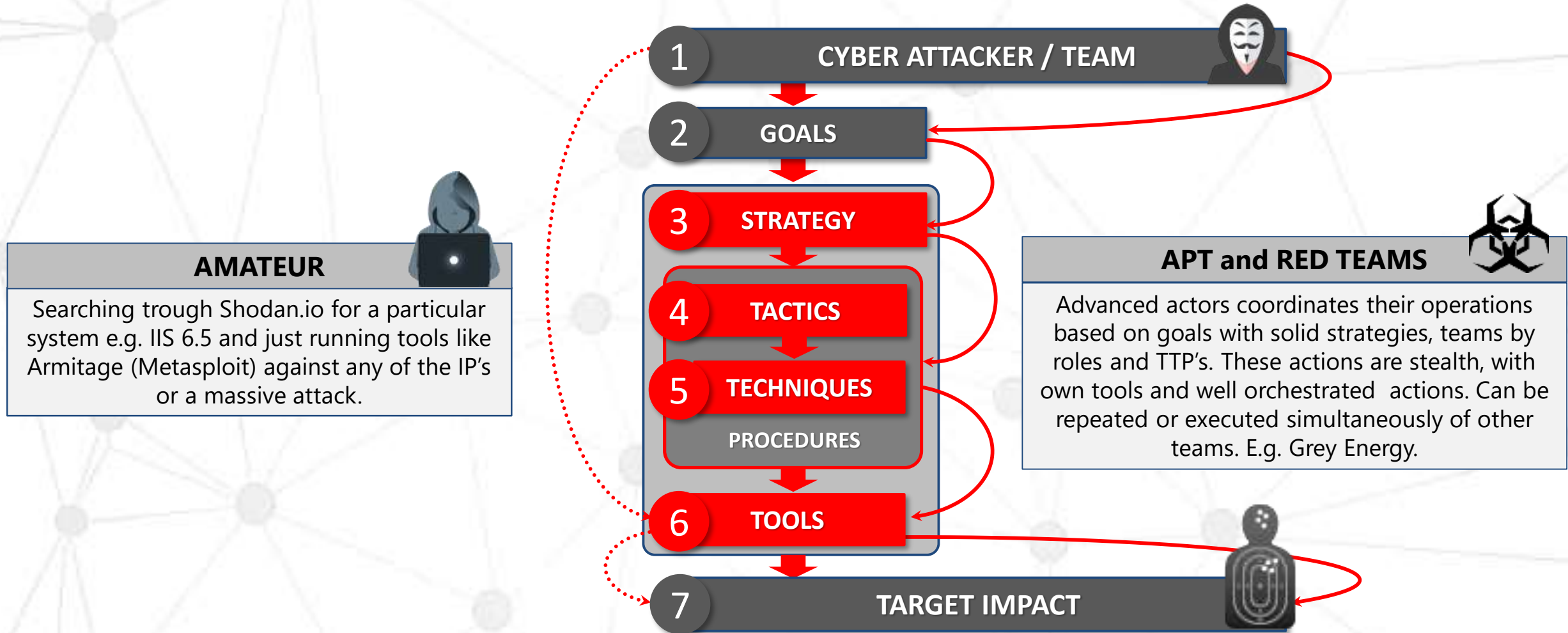
IT IS IMPORTANT TO COMPARE WITH THE SAME CRITERIA



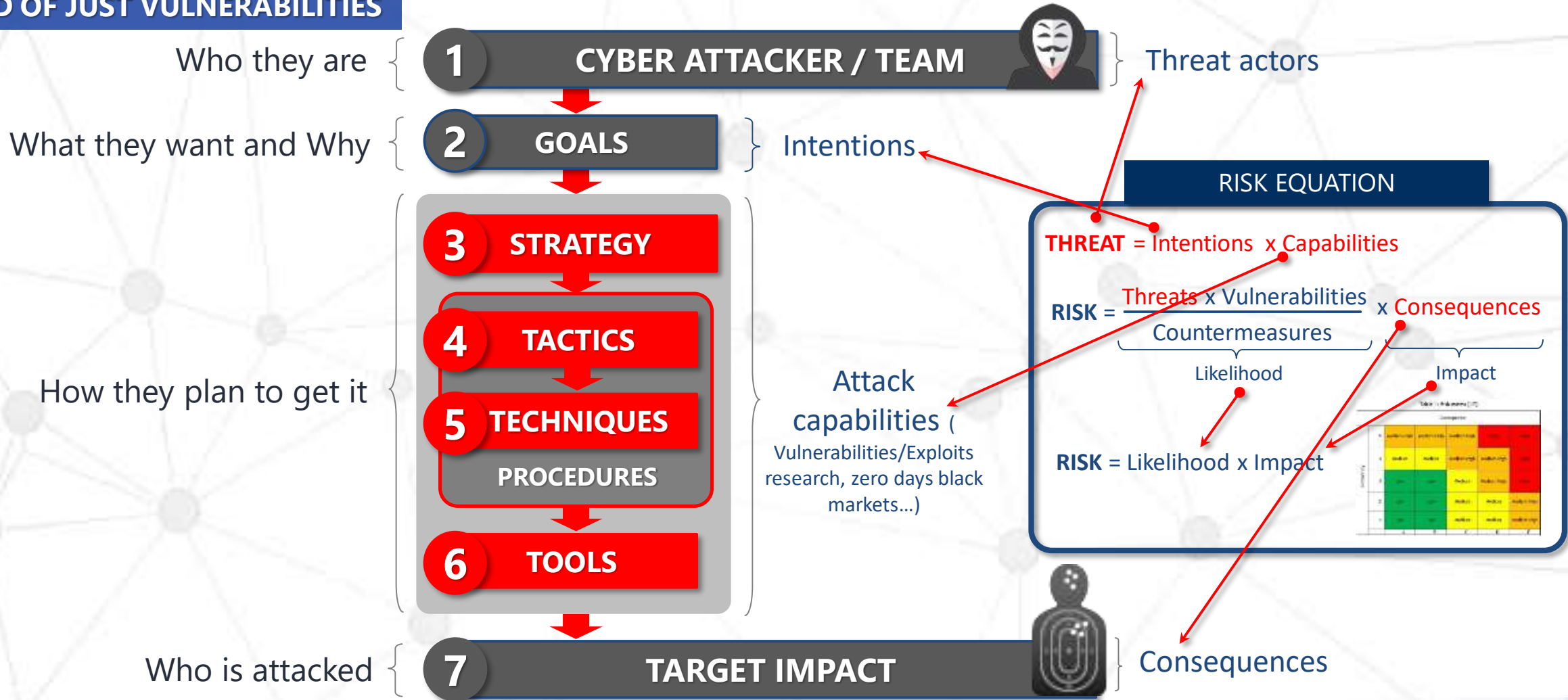


FULL-STACK CYBER-ATTACK MODEL





KEEPING AN EYE ON THREATS INSTEAD OF JUST VULNERABILITIES



Esta foto de Autor desconocido esta bajo licencia CC BY

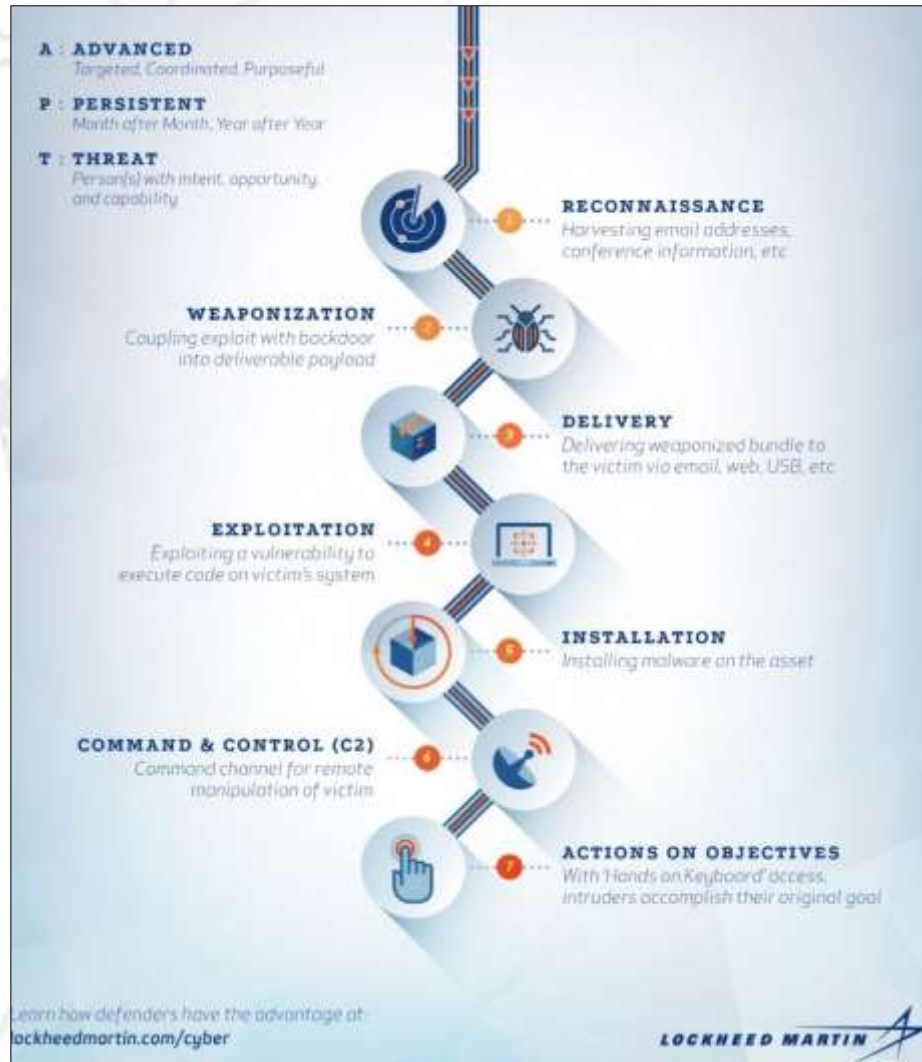
“FULL-STACK CYBER-ATTACK”

Francisco Luis de Andrés



STATE OF THE ART

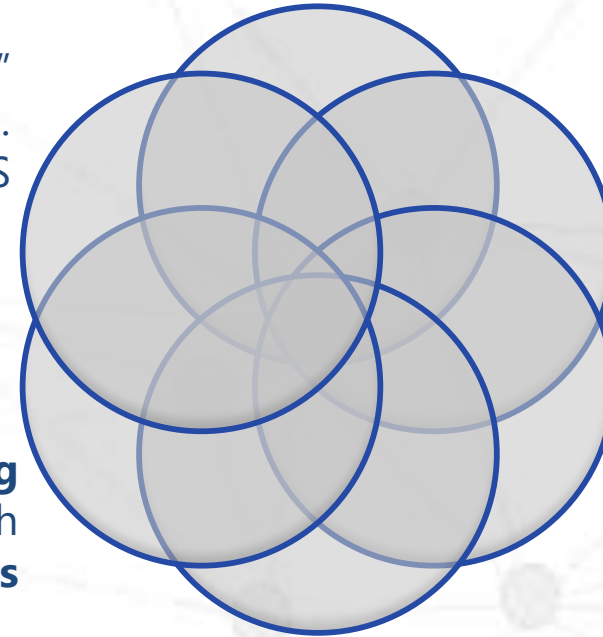
LOCKHEED MARTIN PROPRIETARY CYBER KILL CHAIN MODEL



SOME OF THE PUBLISHED SHORTCOMINGS ABOUT KILL CHAIN:

"Weaponization phase"
Unnecessary phase, impossible to control

"Chain"
A wrong concept. E.g. DDOS



Lateral Movements
Used very often on actual on attacks however was not included

Not representing complex attacks with concurrent teams

Only Malware or perimeter-oriented
leaving apart important threats like insider, etc.

Not considering jumps between different phases

THERE ARE MANY KILL CHAIN ALTERNATIVE MODELS



Laliberte's Kill Chain



Nachreiner's Kill Chain



Bryant's Kill Chain



Malone's Internal Kill Chain

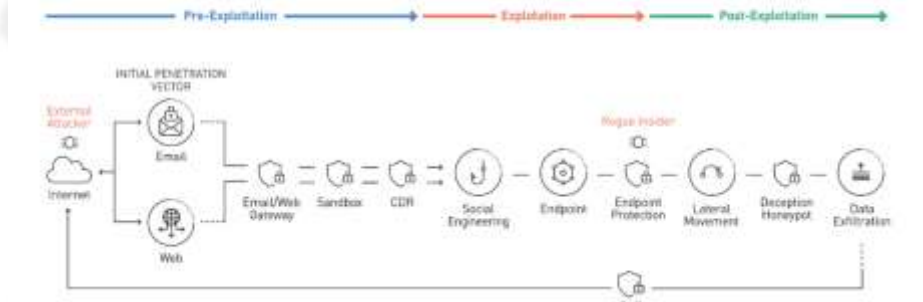


Malone's Target Manipulation Kill Chain



Unified Cyber Kill Chain

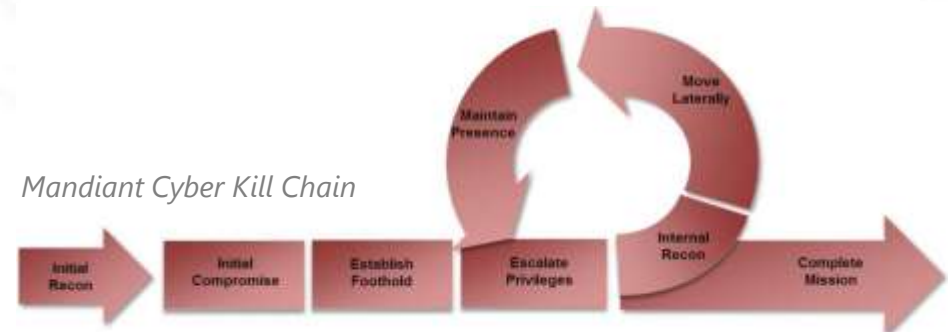
Cymulate Breach & Attack Simulation
Infographic
Full Kill-Chain APT Diagram



Red Team Operations Attack Lifecycle



Mandiant Cyber Kill Chain




“FULL-STACK CYBER-ATTACK”

Francisco Luis de Andrés

**CYBER KILL CHAIN,
A LEGACY MODEL**

Smoking Kills



... even if all we know about that, we continue using it irrationally ...

CAT, Intelligence-Led Cyber Attack Taxonomy



Attacker / Teams

With or without strong motivations they use any exposure and vulnerabilities in order to materialize any risk to be converted on a cybersecurity incident.

Target Profiling

Target Selection, investigation, and identification of key vulnerabilities

Lateral Movements

Jumping from one system to others in order to compromise new or more qualified objectives.

Internal Reconnaissance

Once the attacker are inside the network, it is necessary to analyse internal infrastructures in order to draw and find more precious targets or cybersecurity measures to neutralize them.



HOWEVER ... WHERE ARE THE TTP'S?



execute the necessary techniques in order to exploit different vulnerabilities into the target infrastructures.

Infiltration

After compromise phase is accomplished, payloads and other infiltration methods will complement the tactics in order to built a control channel to the attacker side, opening the highway to new attack phases.

Persistence

This phase purpose is to ensure attacker continuity, so stealth, delete any attack tracks, or develop attacker resiliency by beaoning the C&C communications. To do so important question, special tactics and technics are applied by the attackers



CC creative commons



“FULL-STACK CYBER-ATTACK”

Francisco Luis de Andrés

TACTICS & TECHNIQUES REPOSITORY CLASSIFIED BY MITRE ATT@CK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript CMSTP	.bash_profile bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Command-Line Interface		Binary Padding	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Compiled HTML File	Account Manipulation	AppInit DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted for Impact	Data Encrypted
Hardware Additions	Component Object Model and Distributed COM	AppCert DLLs AppInit DLLs	Application Shimmin	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Defacement	Defacement
Replication Through	Control Panel	Application Shimmin	Bypass User Account	CMSTP	Credentials from Web Browsers	File and Directory Discovery	Network Service	Data from Local System	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe

TACTICS

HOWEVER ... WHERE IS THE STRATEGY?

Spearphishing Link	Execution through API	Bootkit	Dynld Hijacking	Component Firmware	Credential Access	Password Policy Discovery	Pass the Ticket	Removable Media	Domain Fronting	Control Channel	Recovery
Spearphishing via Service	Execution through Module Load	Browser Extensions	Elevated Execution with Prompt	Component Object Model Hijacking	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Domain Generation Algorithms	Exfiltration Over Other Network Medium	Network Denial of Service
Supply Chain Compromise	Exploitation for Client Execution	Change Default File Association	Emond	Connection Proxy	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Fallback Channels	Exfiltration Over Physical Medium	Resource Hijacking
Trusted Relationship	Graphical User Interface	Component Firmware	Exploitation for Privilege Escalation	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture	Multi-hop Proxy	Scheduled Transfer	Service Stop
Valid Accounts	InstallUtil	Component Object Model Hijacking	Extra Window Memory Injection	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser	Multi-Stage Channels	Stored Data Manipulation	Stored Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Disabling Security Tools	Kerberoasting	Remote System Discovery	Security Software Discovery	Screen Capture	Shared Webroot	Video Capture	
	Local Job Scheduling	Create Account	DLL Search Order Hijacking	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	SSH Hijacking	Video Capture			

TECHNIQUES

“FULL-STACK CYBER-ATTACK”

The background features a dark blue gradient with a central graphic of a glowing padlock icon. Surrounding the padlock are various circular and linear patterns resembling circuit boards or data flow diagrams, all rendered in lighter shades of blue and white.

CAT METHODOLOGY BASED ON FULL-STACK CYBER-ATTACK

INTELLIGENCE-LED CYBER ATTACK METHODOLOGY (CAT)

FULL-STACK CYBER-ATTACK



CYBER CRIMINALS / TEAMS

1

2 OBJECTIVES

3 STRATEGY

4 TACTICS

5 TECHNIQUES

PROCEDURES

6 TOOLS

7

PESTLE Analysis

CAT Taxonomy

MITRE ATT@CK & OTHER TTP'S ...

CAMN & CATO

SCRIPS, ZERO DAYS...

POLITICAL	ECONOMICAL	SOCIAL	TECHNOLOGICAL	LEGAL	ENVIRONMENTAL
...



MITRE ATT@CK
...

TARGET'S IMPACT



ABSTRACTION

High-Level



Low-Level

PESTLE ANALYSIS IN ORDER TO DEFINE TARGET & OBJECTIVES

POLITICAL

- Trading policies
- Funding, grants and initiatives
- Home market lobbying
- Pressure groups
- International pressure groups
- Wars and conflict
- Government policies
- Government term and change
- Elections

ECONOMICAL

- Home economy situation
- Home economy trends
- Overseas economies and trends
- General taxation issues
- Tax changes specific to products
- Seasonality/weather issues
- Market and trade cycles
- Specific industry factors
- Market routes & trends

SOCIAL

- Consumer attitudes and opinions
- Media views
- Law changes & social factors
- Brand, company, technology
- Consumer buying patterns
- Events and influences
- Buying access and trends
- Ethnic/religious factors

TECHNOLOGICAL

- Competing technology development
- Research funding
- Associated/dependent technology
- Replacement solutions
- Maturity of technology
- Manufacturing maturity/capacity
- Information and

LEGAL

- Current legislation
- home market
- Future legislation
- European/international legislation
- Regulatory bodies and processes
- Environmental regulations
- Employment law
- Consumer protection

ENVIRONMENTAL

- Ecological
- Environmental issues
- International
- National
- Local regulations
- Customer values
- Market values
- Stakeholders
- Investor values

“If I had 5 minutes to chop down a tree, I’d spend the first 3 sharpening my axe”, Abraham Lincoln

- Shareholder needs/demands

- Consumer confidence index
- Import/export ratios
- Production level
- Internal finance
- Cash flow

- Living standards
- Fashion & role models
- Attitudes: work, people
- Leisure activities
- Occupations
- Earning capacity
- Management style
- Organizational culture
- Changes to education system

- Global communications
- Inventions & Innovations
- New discoveries & Research
- Energy uses/sources/fuels
- Communications
- Rate of obsolescence
- Manufacturing advances
- Information technology
- Internet
- Transportation
- Waste removal/recycling
- Software changes

Environment: “Macro - CTI”

Cyber Threat Intelligence Landscape Analysis



PESTEL: Political, Economical, Socio, Technical, Environmental (Geographical), Legal

EXAMPLE HOW CAT PHASE SEVEN IS INTEGRATED WITH MITRE TTP'S

STRATEGY



CAT phase 7: TARGET EXECUTION

Strategy

TACTICS

TA0009 –
Collection

Tactic

MITRE

TA0010 –
Exfiltration

Tactic

MITRE

TECHNIQUES

T1123 - Audio
Capture

Technique

T1119 -
Automated
Collection

Technique

T1115 - Clipboard
Data

Technique

T1020 -
Automated
Exfiltration

Technique

T1002 - Data
Compressed

Technique

T1022 - Data
Encrypted

Technique





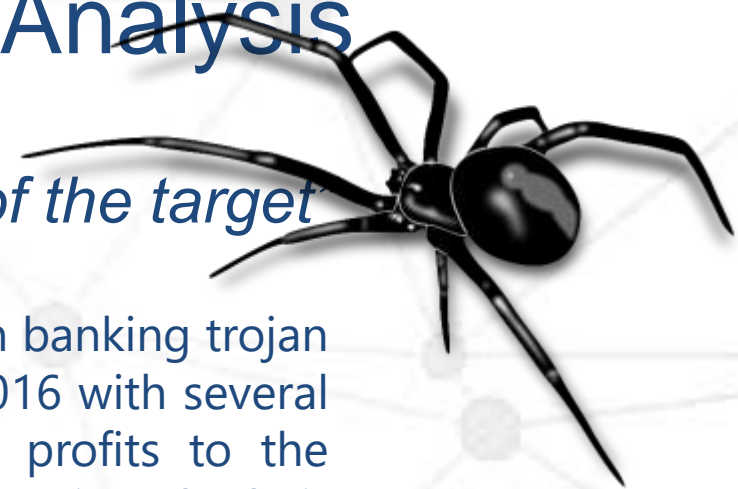
INDRIK SPIDER CYBER ATTACK, CAT ANALYSIS

INDRIK SPIDER Campaign Analysis

“Attack objectives are encryption and extortion of the target”

INDRIK SPIDER criminal organization operates the well-known banking trojan Dridex from year 2014. His mayor activity was from 2015 to 2016 with several attacks over the financial sector that it brought important profits to the organization quantified by millions of dollars. Dridex continued their development with new functionalities like the improvement of the defence evasion. The next slides will present their attack “modus operandi” by combining Dridex and Bitpayment, a powerful release of their own ransomware. Their most recent attack to the NHS (UK National Health Service) implied an important rescue of more tan \$200.000,00 USD.

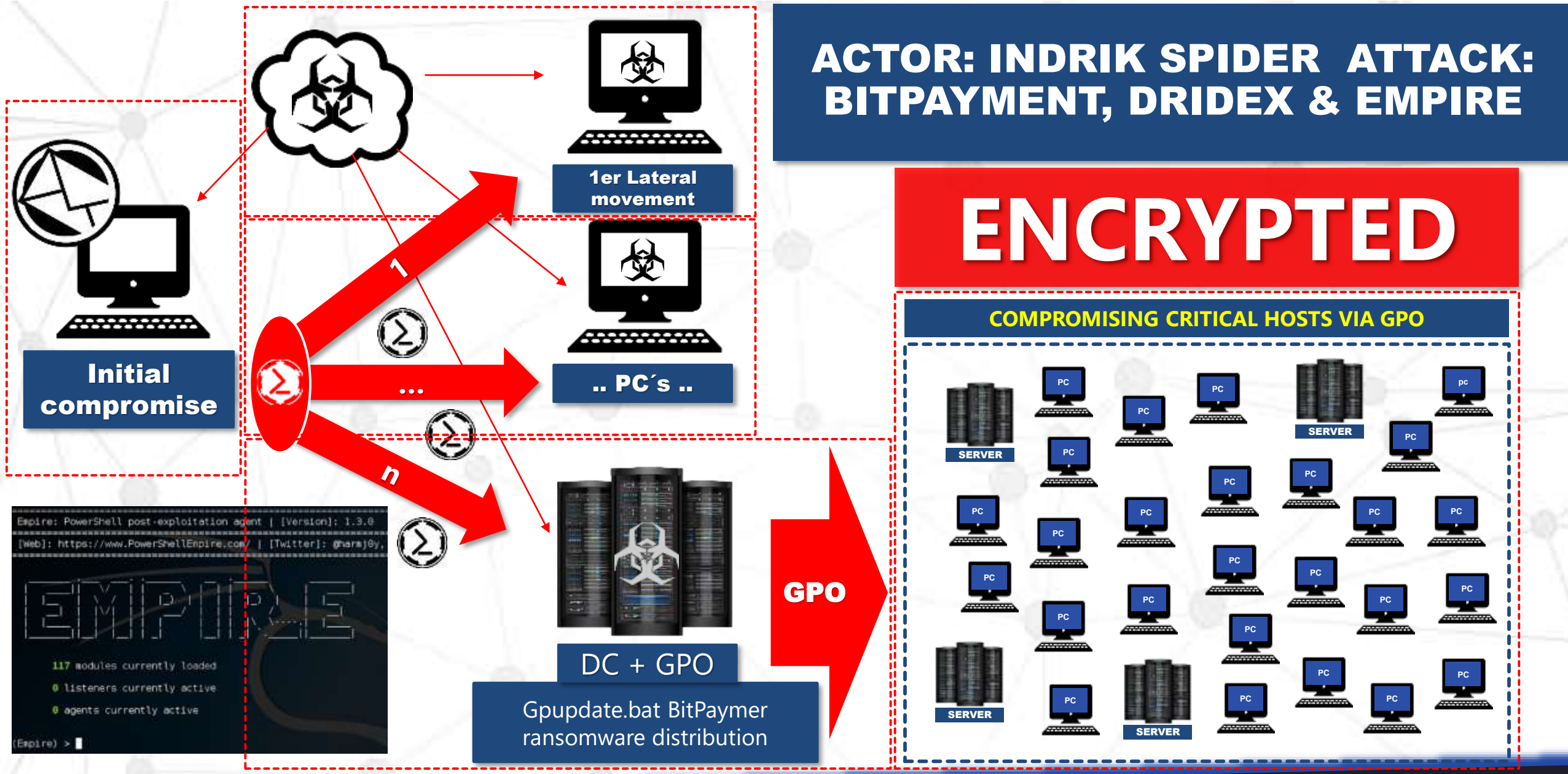
Fuente: <https://www.crowdstrike.com>



ACTOR: INDRIK SPIDER ATTACK: BITPAYMENT, DRIDEX & EMPIRE

ENCRYPTED

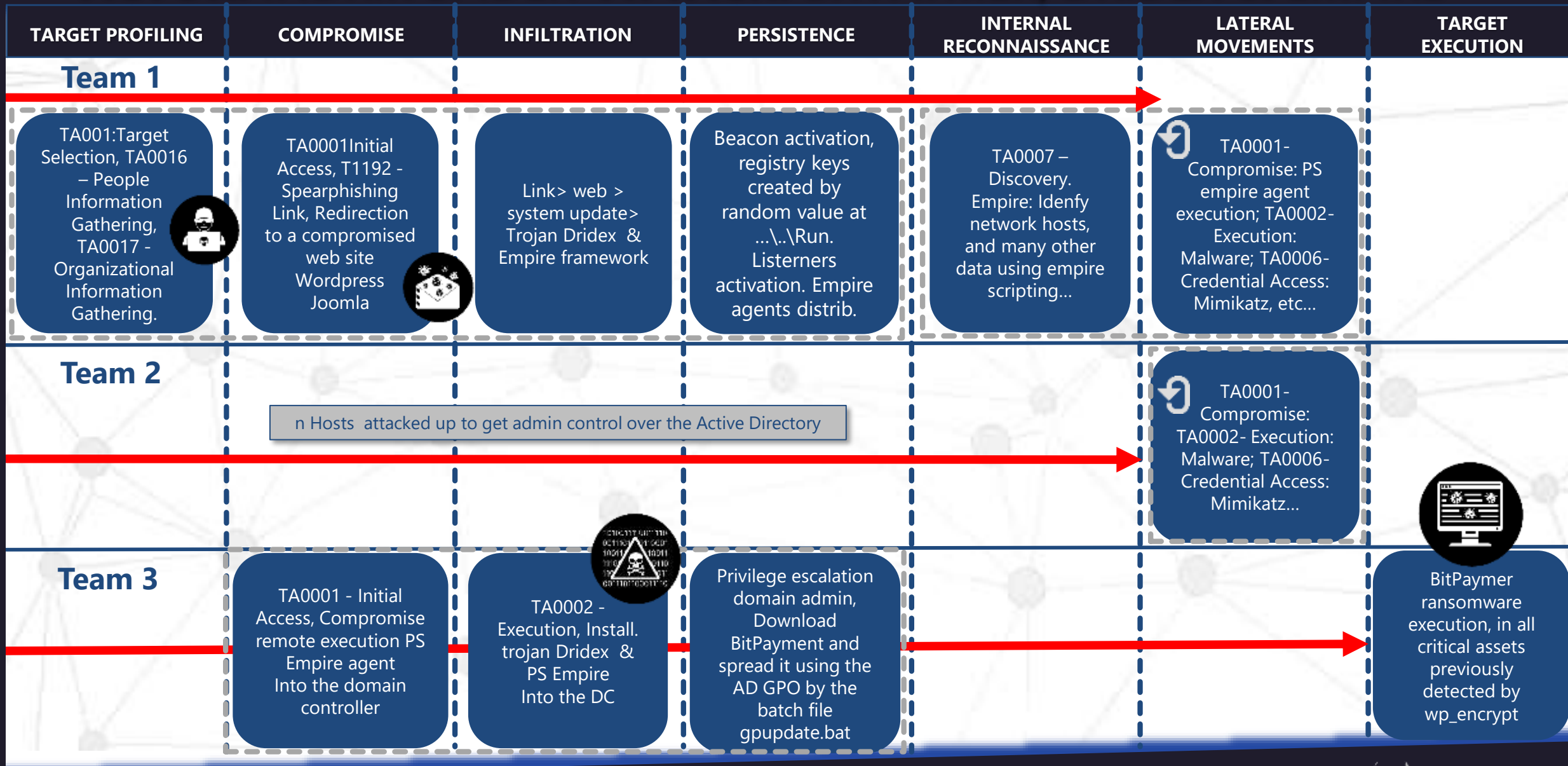
COMPROMISING CRITICAL HOSTS VIA GPO



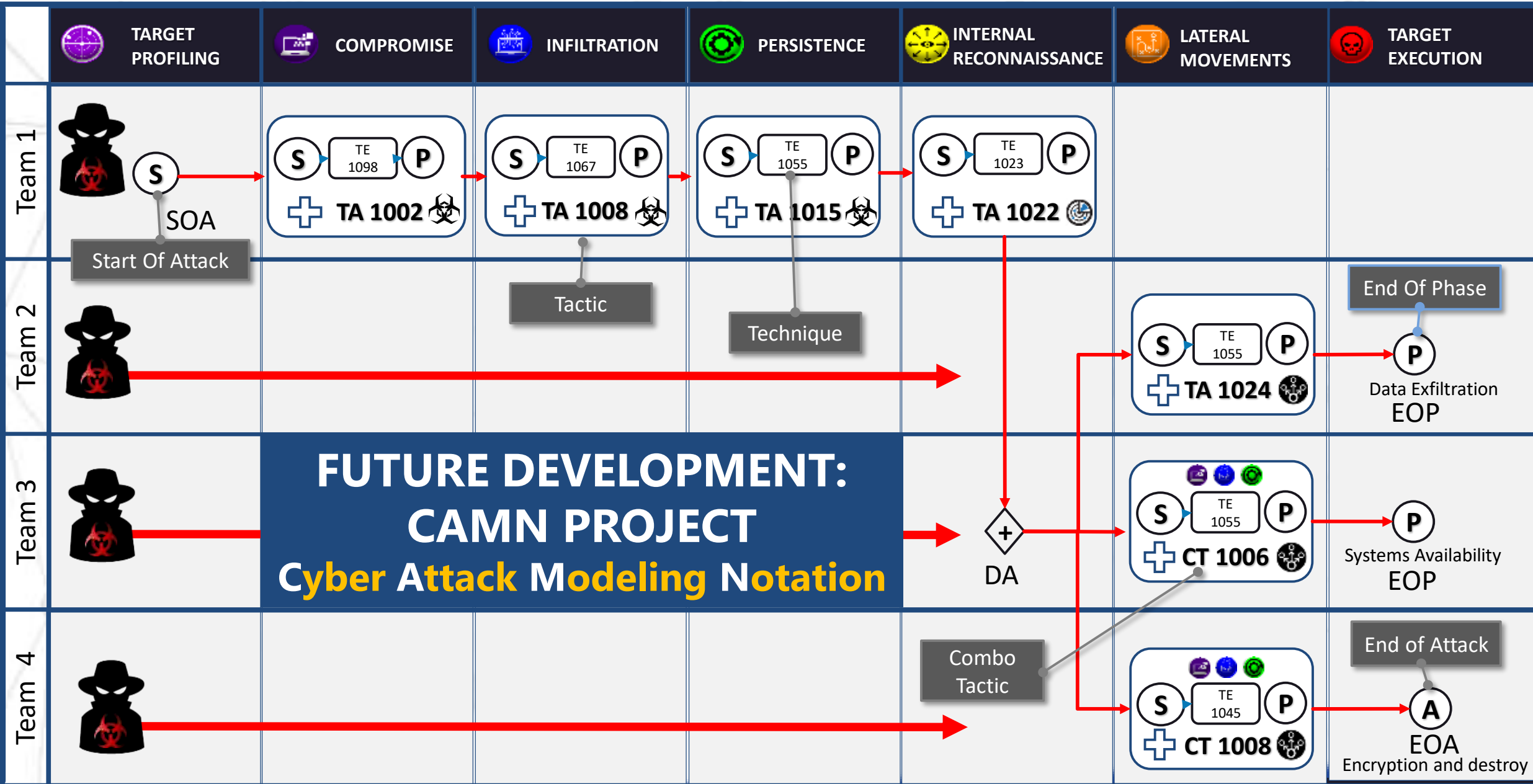
“FULL-STACK CYBER-ATTACK”

ACTOR: INDRIK SPIDER ATTACK: BITPAYMER, DRIDEX & EMPIRE

TACTICS & TECHNIQUES



“FULL-STACK CYBER-ATTACK”



“FULL-STACK CYBER-ATTACK”

THANK YOU !!!

Francisco Luis de Andrés Pérez
e-mail: flandres@ciso.es

