EU Conference 2020

“FULL-STACK CYBER-ATTACK”

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

Brussels, 30th January 2020
KEVIN MITNICK

- Alone or small teams
- Simple tools
- The spirit of Robin Hood, popular
- From Year 1979 (16 years old)

CARBANAK

- Objective Banks, money
- Sophisticated tools
  - Carbanak Backdoor
- Organized cybercrime
- Year 2018

CYBERCRIME EVOLUTION IN JUST 40 YEARS

"FULL-STACK CYBER-ATTACK"

Francisco Luis de Andrés
SOME OF THE FBI MOST WANTED CRIMINALS ARE “CYBER”

IRANIAN DDoS ATTACKS
CONSPIRACY TO COMMIT COMPUTER INTRUSION

IRANIAN MABNA HACKERS
CONSPIRACY TO COMMIT COMPUTER INTRUSIONS; CONSPIRACY TO COMMIT WIRE FRAUD; COMPUTER FRAUD; WIRE FRAUD; AGGRAVATED IDENTITY THEFT

CYBERCRIME HIGH PRIORITY

IRGC-AFFILIATED CYBER ACTORS
Conspiracy to Commit Computer Intrusion; Computer Intrusion; Aggravated Identity Theft; Aiding and Abetting

RUSSIAN INTERFERENCE IN 2016 U.S. ELECTIONS
CONSPIRACY TO COMMIT AN OFFENSE AGAINST THE UNITED STATES; FALSE REGISTRATION OF A DOMAIN NAME; AGGRAVATED IDENTITY THEFT; COMMIT MONEY LAUNDERING
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...

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

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

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

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

ORGANIZED CYBERCRIME HIERARCHICAL STRUCTURES

** Money mules (individuals to withdraw money from ATMs)
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

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.
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

“FULL-STACK CYBER-ATTACK”

Francisco Luis de Andrés
“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

Orchestration over SIEM, SOAR

Threat hunting analysis IOC´s

Deception technologies beyond honeypots

Forensic assessments, before incident occurs

Cyber Threat Intelligence analysis
DO WE NEED TO TEST OUR CYBERSECURITY?
### Differences Between Pentesting and Red Teaming

<table>
<thead>
<tr>
<th>Scope</th>
<th>Pentest</th>
<th>Red Team</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Limited to systems and applications</strong></td>
<td>A wider scope in order to cover all different infrastructures, even employees or physical assets</td>
<td></td>
</tr>
<tr>
<td><strong>Vulnerabilities detection tools, and exploitation tools or frameworks</strong></td>
<td>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&amp;C etc...</td>
<td></td>
</tr>
<tr>
<td><strong>Focus: Identification and exploitation of maximum amount of vulnerabilities</strong></td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

#### EU Conference 2020

“FULL-STACK CYBER-ATTACK”

Francisco Luis de Andrés
TEAM COLORS INVOLVED IN THE TIBER-EU EMULATED ATTACKS

Purple Team

- Supporting on test
- Hypothetical steps on replay

Emulated Scenarios

Red Team
- Attack
- Monitoring and Control

Blue Team
- Defense
- Monitoring and Control

White Team
- Optional

Supporting on test
Hypothetical steps on replay
STANDARIZING RED TEAM SCENARIOS
**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.
DIFFERENCES BETWEEN SIMULATION AND EMULATION (MIMIC)

SIMULATION

“A good simulation could become emulation”

BIG ROOM FOR INTERPRETATION

EMULATION

MIMIC TO MATCH AN EXISTING TARGET

“FULL-STACK CYBER-ATTACK”
Francisco Luis de Andrés
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.”

EFECTIVE 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.”

IT IS IMPORTANT TO COMPARE WITH THE SAME CRITERIA
FULL-STACK CYBER-ATTACK MODEL
FROM DML MODEL TO FULL-STACK CYBER-ATTACK MODEL

V 1.0

Who they are

What they want

How they plan to get it

Introducing a new abstraction model for Procedures

Creating a new layer

Who is attacked

Target Impact

DML-9 Identify
DML-8 Goals
DML-7 Strategy
DML-6 Tactics
DML-5 Techniques
DML-4 Procedures
DML-3 Tools
DML-2 Host & Network Artifacts
DML-1 Atomic Indicators
DML-0 None or Unknown

Changing the direction of the layers

Based on DML Detection Maturity Levels


High-Level

Low-Level

Removing all unnecessary layers from an attacker perspective
Searching through Shodan.io for a particular system e.g. IIS 6.5 and just running tools like Armitage (Metasploit) against any of the IP's or a massive attack.

Advanced actors coordinates their operations based on goals with solid strategies, teams by roles and TTP's. These actions are stealth, with own tools and well orchestrated actions. Can be repeated or executed simultaneously of other teams. E.g. Grey Energy.
**FULL-STACK CYBER-ATTACK MODEL**

**KEEPING AN EYE ON THREATS INSTEAD OF JUST VULNERABILITIES**

1. **CYBER ATTACKER / TEAM**
   - Threat actors
   - Intentions

2. **GOALS**
   - What they want and Why
   - Intentions

3. **STRATEGY**
   - How they plan to get it
   - Attack capabilities (Vulnerabilities/Exploits research, zero days black markets...)

4. **TACTICS**
   - Procedures

5. **TECHNIQUES**
   - Procedures
   - Countermeasures

6. **TOOLS**
   - Tools
   - Impact

7. **TARGET IMPACT**
   - Who is attacked
   - Consequences

**RISK EQUATION**

\[ \text{RISK} = \text{Threats} \times \text{Vulnerabilities} \times \text{Consequences} \]

\[ \text{THREAT} = \text{Intentions} \times \text{Capabilities} \]

**Eu Conference 2020**

“FULL-STACK CYBER-ATTACK”

Francisco Luis de Andrés
STATE OF THE ART
"FULL-STACK CYBER-ATTACK"

Francisco Luis de Andrés

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

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

- **Not representing complex attacks with concurrent teams**

- **Not considering jumps between different phases**

---

EU Conference 2020

Francisco Luis de Andrés
THERE ARE MANY KILL CHAIN ALTERNATIVE MODELS

Laliberte’s Kill Chain
Reconnaissance → Delivery → Exploitation → Infection → Command & Control → Lateral Movement & Privilege Escalation → Action on Objectives

Nachreiner’s Kill Chain
Reconnaissance → Delivery → Exploitation → Infection → Lateral Movement → Exfiltration → Action on Objectives

Bryant’s Kill Chain
Internal Reconnaissance → Internal Exploitation → Enterprise Privilege Escalation → Lateral Movement → Target Manipulation

Malone’s Internal Kill Chain
Target Reconnaissance → Target Exploitation → Weaponization → Installation → Execution

Malone’s Target Manipulation Kill Chain

Unified Cyber Kill Chain
Smoking Kills

... even if all we know about that, we continue using it irrationally ...
Target Profiling
Target Selection, investigation, and identification of key vulnerabilities allowing the attacker to advance.

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.

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 beaconing the C&C communications. To do so important question, special tactics and technics are applied by the attackers.

Target Execution
End State: Systems availability disruption.

HOWEVER ... WHERE ARE THE TTP’s?
Francisco Luis de Andrés

EU Conference 2020

“FULL-STACK CYBER-ATTACK”

TACTICS & TECHNIQUES REPOSITORY CLASIFIED BY MITRE ATT@CK

<table>
<thead>
<tr>
<th>TACTICS</th>
<th>TECHNIQUES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Access</td>
<td>Execution</td>
</tr>
<tr>
<td>Drive-by</td>
<td>Compromise</td>
</tr>
<tr>
<td>Applet</td>
<td></td>
</tr>
<tr>
<td>Hardware Additions</td>
<td>Component Object Model and Distributed COM</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Spearphishing Link</td>
<td>Spearphishing Link</td>
</tr>
<tr>
<td>Execution through API</td>
<td>Execution through Module Load</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>SyMV Hijacking</td>
<td>Component Firmware</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Password Hijacking</td>
<td>Component Firmware</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Password Hijacking</td>
<td>Component Firmware</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Password Hijacking</td>
<td>Component Firmware</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Password Hijacking</td>
<td>Component Firmware</td>
</tr>
</tbody>
</table>

HOWEVER ... WHERE IS THE STRATEGY?
CAT METHODOLOGY BASED ON FULL-STACK CYBER-ATTACK
INTELLIGENCE-LED CYBER ATTACK METHODOLOGY (CAT)

FULL-STACK CYBER-ATTACK

1. CYBER CRIMINALS / TEAMS

2. OBJECTIVES

3. STRATEGY

4. TACTICS

5. TECHNIQUES

6. TOOLS

7. TARGET’s IMPACT

ABSTRACTION

High-Level

Low-Level

TARGET’s IMPACT

PESTLE Analysis

CAT Taxonomy

MITRE ATT@CK & OTHER TTP’S …

CAMN & CATO

SCRIPS, ZERO DAYS...

EU Conference 2020

“FULL-STACK CYBER-ATTACK”

Francisco Luis de Andrés
INTELLIGENCE-LED CYBER ATTACK METHODOLOGY (CAT)

OBJECTIVE
PESTLE

STRATEGY
Cat Taxonomy

TTP’s
Mitre Att@ck

Methodology
C@T

Intelligence-Led Cyber Attack
### 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 communications

#### 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

---

**Environment: “Macro - CTI”**

Cyber Threat Intelligence Landscape Analysis

**PESTEL: Political, Economical, Social, Technical, Environmental (Geographical), Legal**
EXAMPLE HOW CAT PHASE SEVEN IS INTEGRATED WITH MITRE TTP's

STRATEGY

CAT phase 7: TARGET EXECUTION

TACTICS

TA0009 – Collection

TACTICS

TA0010 – Exfiltration

TECHNIQUES

T1123 - Audio Capture

T1119 - Automated Collection

T1115 - Clipboard Data

T1020 - Automated Exfiltration

T1002 - Data Compressed

T1022 - Data Encrypted

TECHNIQUES
INDRIK SPIDER CYBER ATTACK, CAT 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 than $200,000,00 USD.

Fuente: [https://www.crowdstrike.com](https://www.crowdstrike.com)
“FULL-STACK CYBER-ATTACK”
Francisco Luis de Andrés
### ACTOR: INDRIK SPIDER  ATTACK: BITPAYMER, DRIDEX & EMPIRE

<table>
<thead>
<tr>
<th>TARGET PROFILING</th>
<th>COMPROMISE</th>
<th>INFILTRATION</th>
<th>PERSISTENCE</th>
<th>INTERNAL RECONNAISSANCE</th>
<th>LATERAL MOVEMENTS</th>
<th>TARGET EXECUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Team 1</strong></td>
<td>TA001:Target Selection, TA0016 - People Information Gathering, TA0017 - Organizational Information Gathering.</td>
<td>TA0001:Initial Access, T1192 - Spearphishing Link, Redirection to a compromised website Wordpress Joomla</td>
<td>Link &gt; web &gt; system update &gt; Trojan Dridex &amp; Empire framework</td>
<td>Beacon activation, registry keys created by random value at ...\Run. Listeners activation. Empire agents distrib.</td>
<td>TA0007 – Discovery. Empire: Identity network hosts, and many other data using empire scripting...</td>
<td>TA0001- Compromise: PS empire agent execution; TA0002- Execution: Malware; TA0006- Credential Access: Mimikatz,...</td>
</tr>
</tbody>
</table>

- **TA0001** Initial Access, T1192 - Spearphishing Link, Redirection to a compromised website Wordpress Joomla
- **TA0002** Execution, Install. trojan Dridex & PS Empire Into the DC
- **TA0007** Discovery. Empire: Identity network hosts, and many other data using empire scripting...

| **Team 2**       | n Hosts attacked up to get admin control over the Active Directory | TA0001- Compromise: TA0002- Execution: Malware; TA0006- Credential Access: Mimikatz... |

| **Team 3**       | TA0001 - Initial Access, Compromise remote execution PS Empire agent Into the domain controller | TA0002 - Execution, Install. trojan Dridex & PS Empire Into the DC | Privilege escalation domain admin, Download BitPayment and spread it using the AD GPO by the batch file gpupdate.bat | BitPaymer ransomware execution, in all critical assets previously detected by wp_encrypt |

---

**EU Conference 2020**

“FULL-STACK CYBER-ATTACK”

Francisco Luis de Andrés

11:16  38 / 40
FUTURE DEVELOPMENT:
CAMN PROJECT
Cyber Attack Modeling Notation
THANK YOU !!!

Francisco Luis de Andrés Pérez

e-mail: flandres@ciso.es