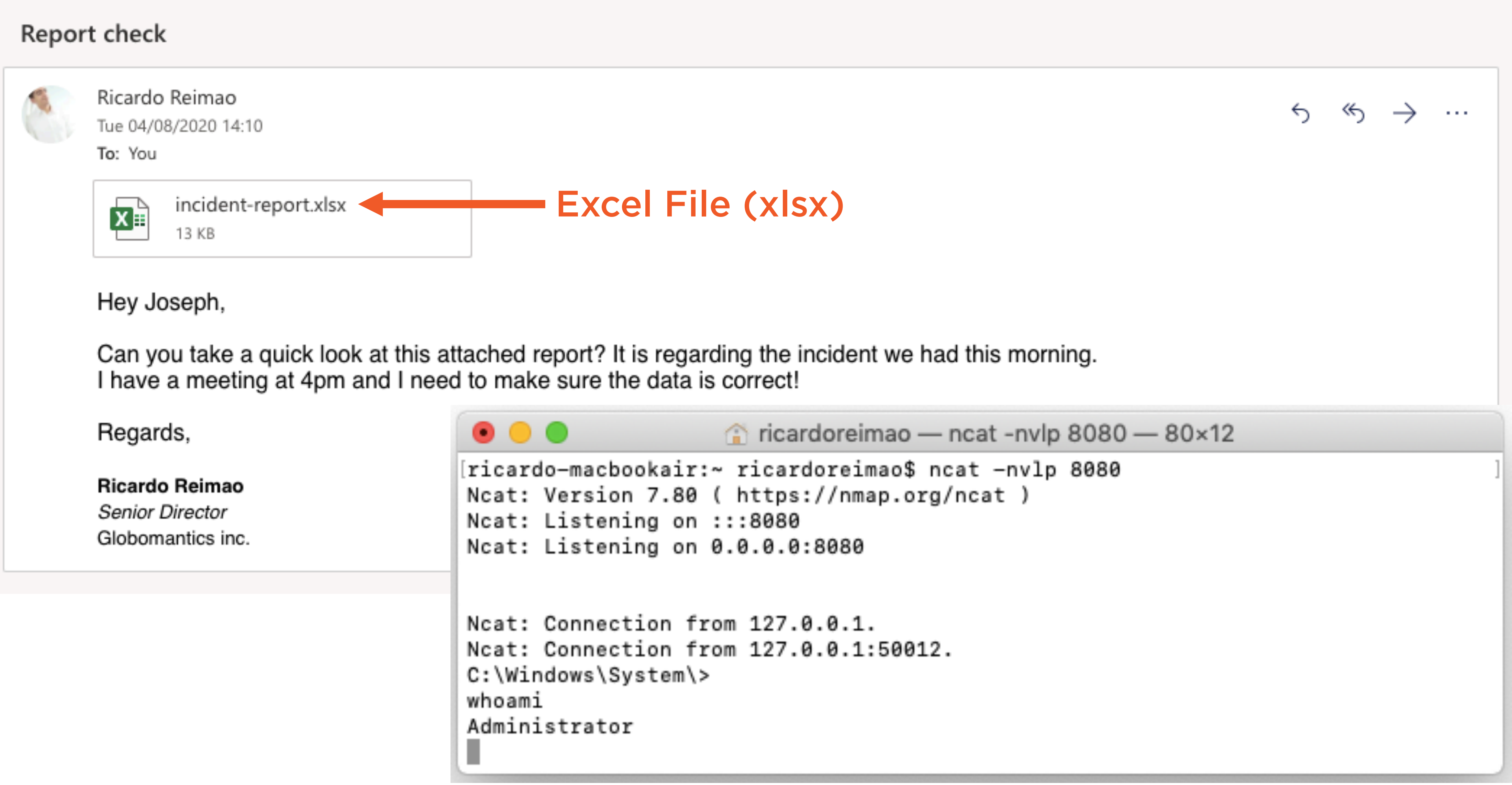
Execution with macro_pack

Ricardo Reimao

CYBER SECURITY CONSULTANT

Masquerading Malicious Files



Report check

Ricardo Reimao
Tue 04/08/2020 14:10
To: You

incident-report.xlsx
13 KB

Excel File (xlsx)

Hey Joseph,

Can you take a quick look at this attached report? It is regarding the incident we had this morning.
I have a meeting at 4pm and I need to make sure the data is correct!

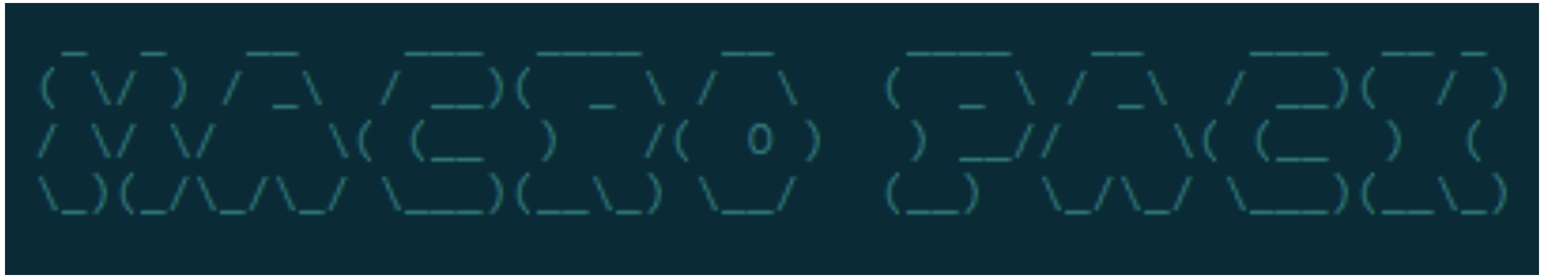
Regards,

Ricardo Reimao
Senior Director
Globomantics inc.

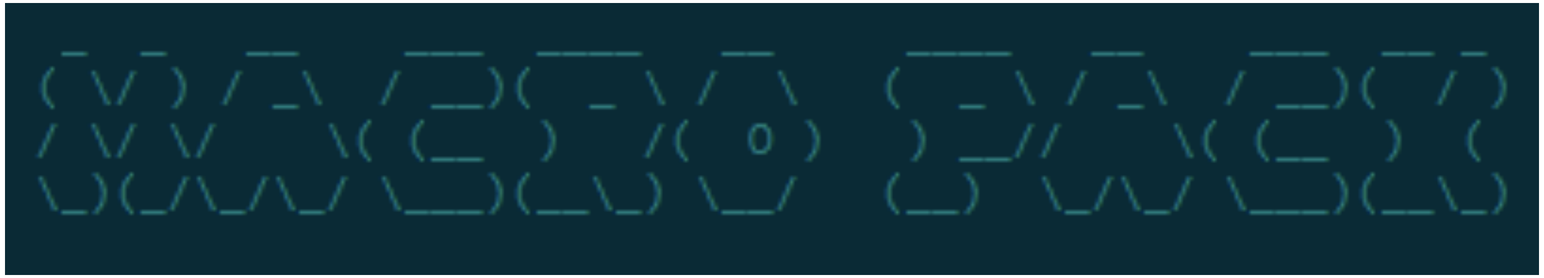
ricardoreimao — ncat -nvlp 8080 — 80×12

```
ricardo-macbookair:~ ricardoreimao$ ncat -nvlp 8080
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::8080
Ncat: Listening on 0.0.0.0:8080


Ncat: Connection from 127.0.0.1.
Ncat: Connection from 127.0.0.1:50012.
C:\Windows\System\>
whoami
Administrator
```



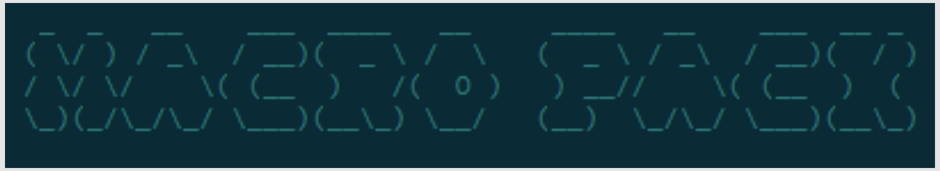
```
  _  _   __    ___  ____   __     ____   __    ___  __ _ 
 ( \/ ) / _\  / __)(  _ \ /  \   (  _ \ / _\  / __)(  / )
 / \/ \/    \( (__  )   /(  O )   ) __//    \( (__  )  ( 
 \_)(_/\_/\_/ \___)(__\_) \__/   (__)  \_/\_/ \___)(__\_)
```



```
 _  _   __    ___  ____   __     ____   __    ___  __ _ 
( \/ ) / _\  / __)(  _ \ /  \   (  _ \ / _\  / __)(  / )
/ \/ \/    \( (__  )   /(  O )   ) __//    \( (__  )  ( 
\_)(_/\_/\_/ \___)(__\_) \__/   (__)  \_/\_/ \___)(__\_)
```

Author: Emeric Nasi
@EmericNasi

macro_pack is a tool used to automatize obfuscation and generation of Office documents, VB scripts, shortcuts, and other formats for pentest, demo, and social engineering assessments.

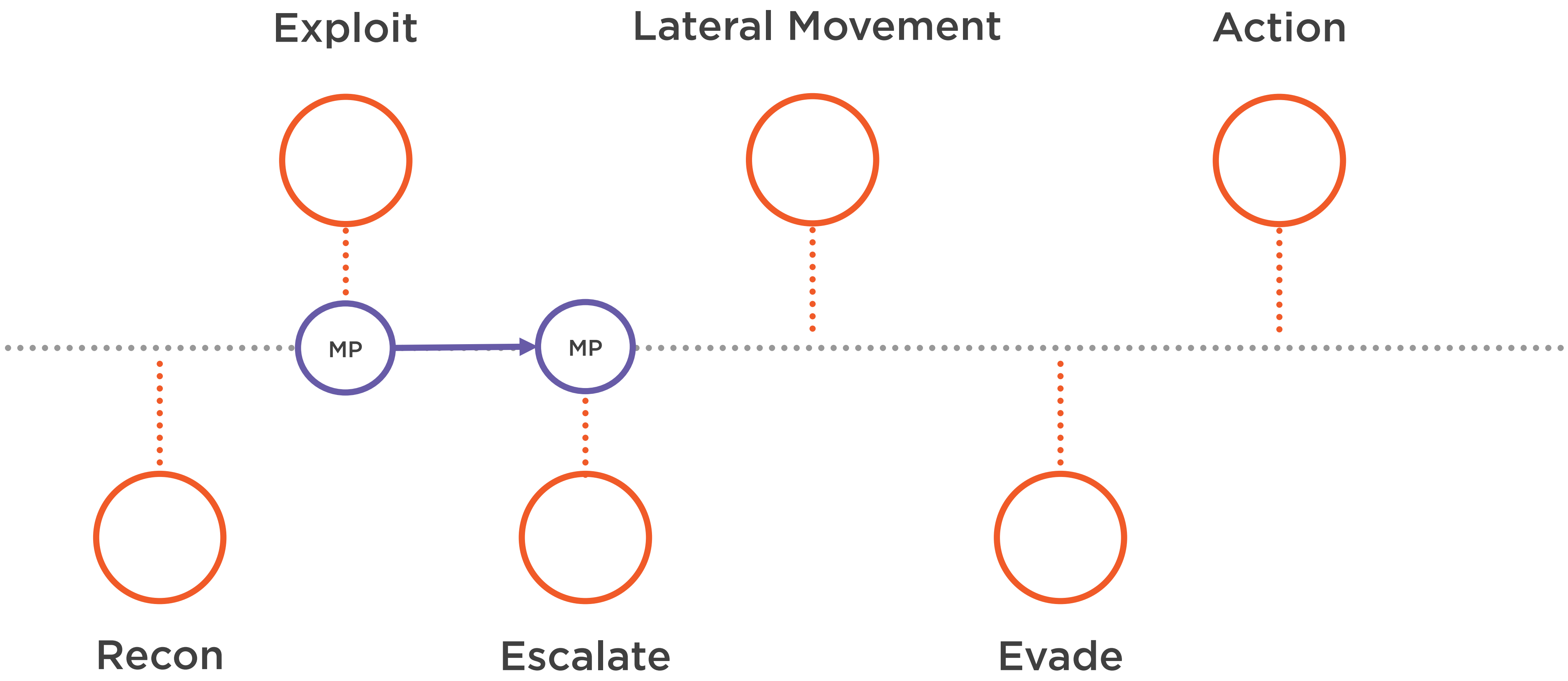


Open source tool (Apache V2.0)
https://github.com/sevagas/macro_pack

Automate the incorporation of malicious code into Microsoft Office files (masquerading)

Help us to exploit the easiest point of entry in a company: People

Kill Chain

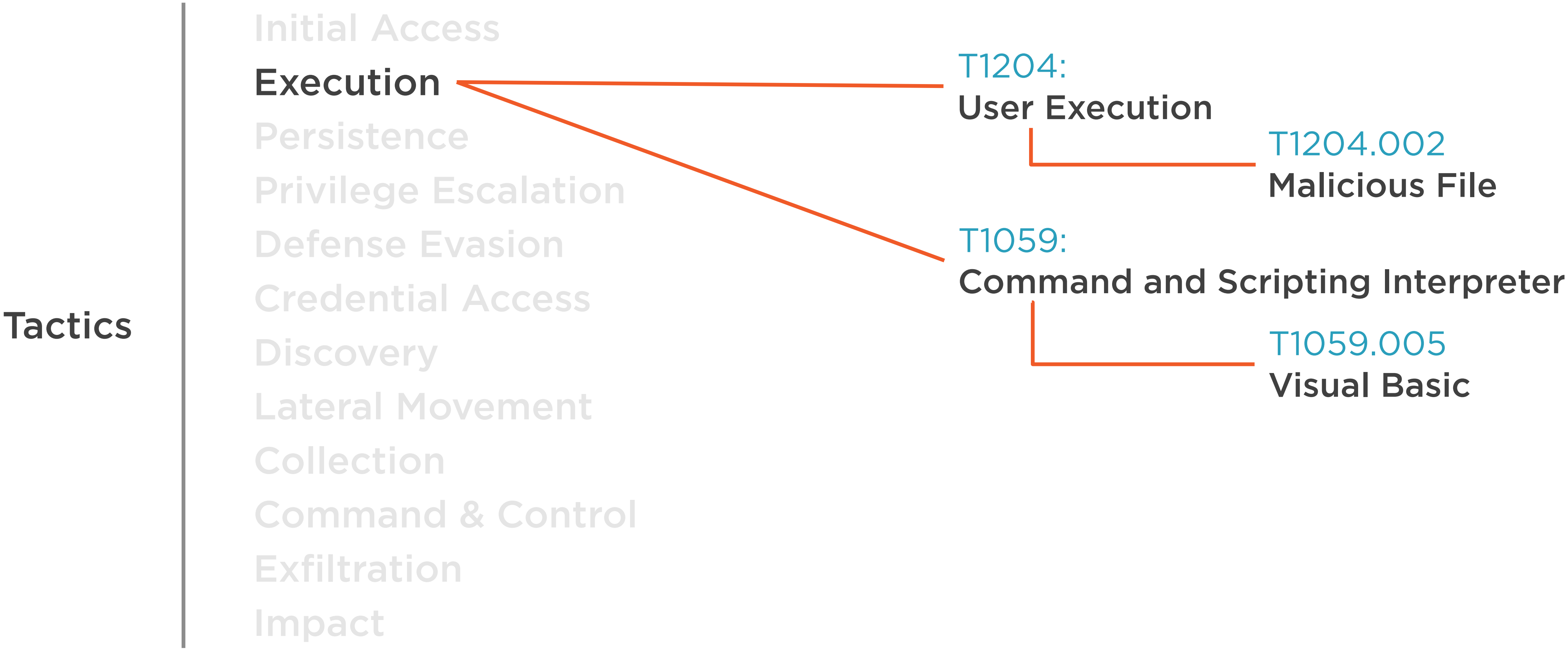

Exploit
Lateral Movement
Action
MP
MP
Recon
Escalate
Evade

MITRE ATT&CK

Tactics

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration
- Impact

MITRE ATT&CK



Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact

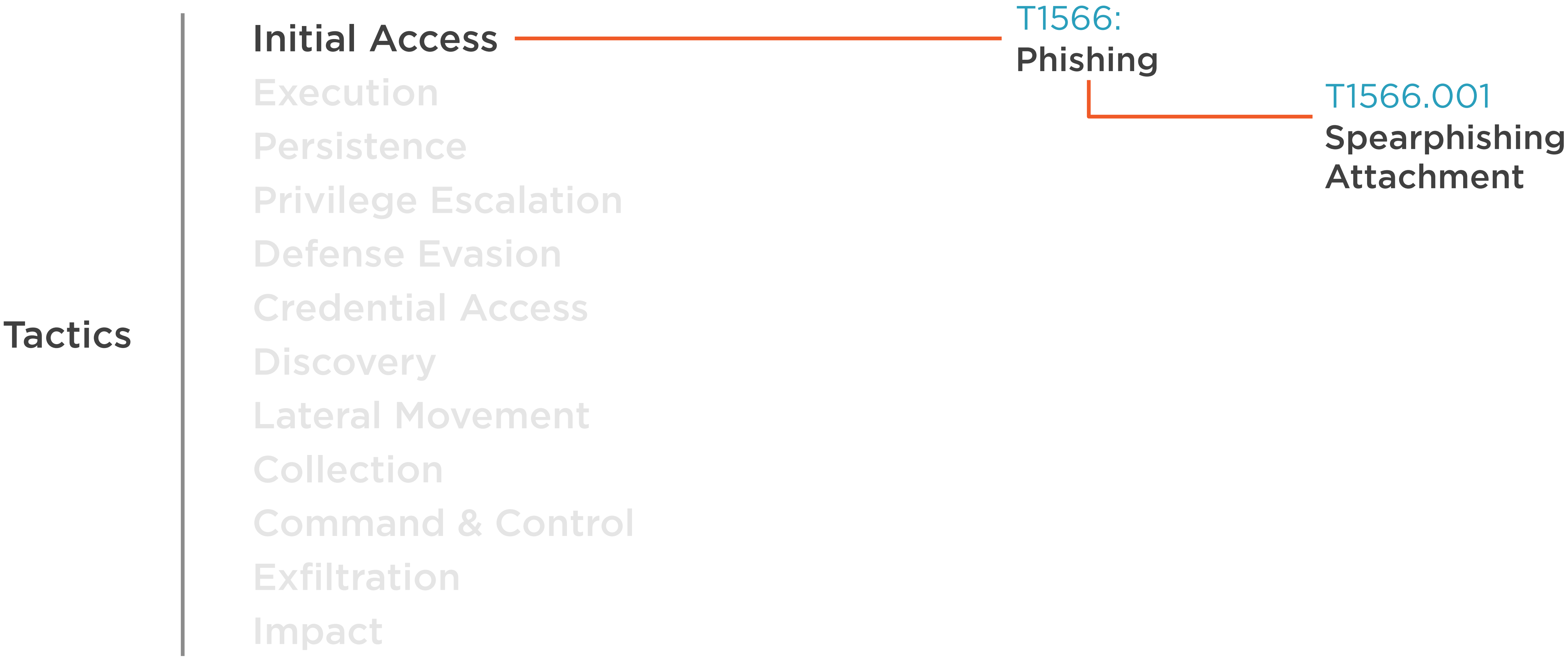
T1204:
User Execution

T1204.002
Malicious File

T1059:
Command and Scripting Interpreter

T1059.005
Visual Basic

MITRE ATT&CK



Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact

T1566:
Phishing

T1566.001
Spearphishing
Attachment

Staying Legal

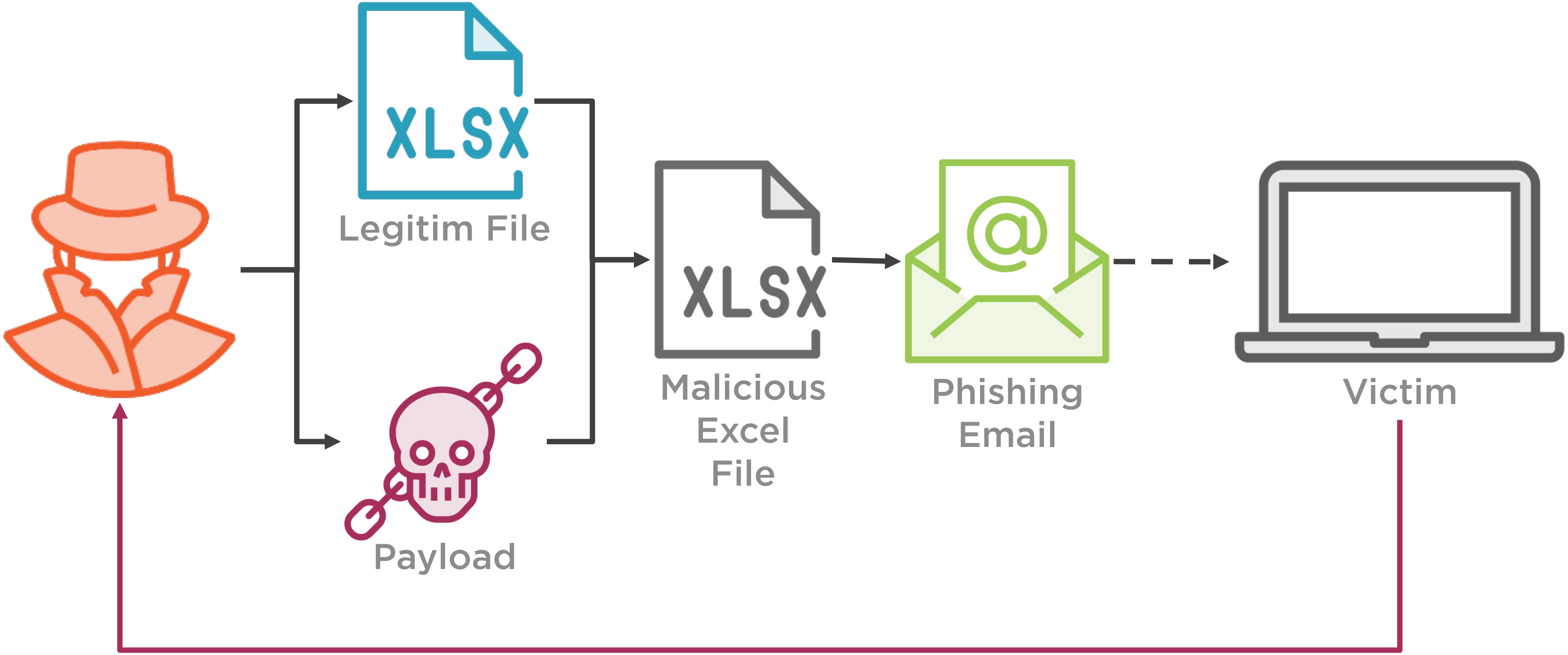
Sending malware without authorization is ILLEGAL in most countries

Letter of engagement, detailing dates and scope of what will be executed

Formal document, signed by the client, authorizing the types of attack you may perform

Always consult the client before any attack that may impact the network

Attack Explanation



Prerequisites

Attacker Machine

Windows 10
and/or
Kali Linux

Target Machine

Windows 10
or
Windows Server

Demo Place Holder

1. Installation Tips and Tricks

2. First use instructions and common usage syntax

3. Use of main features on live targets or in live environment

More Information

Official Documentation

Several other capabilities
https://github.com/sevagas/macro_pack

macro_pack Pro Mode

Several advanced features:
- Anti-virus bypassing
- Sandbox detection
- Weaponized templates

Initial Access

“Initial Access with WiFi-Pumpkin”

“Initial Access with Aircrack-ng”

Remediation

Security awareness trainings

Phishing simulation campaigns

Behavior-based detection systems

Thank you!

Ricardo Reimao
Cyber security consultant