

# Converting threat actor campaigns to purple team exercises

Fatih Ozavci

# Before we begin the webinar

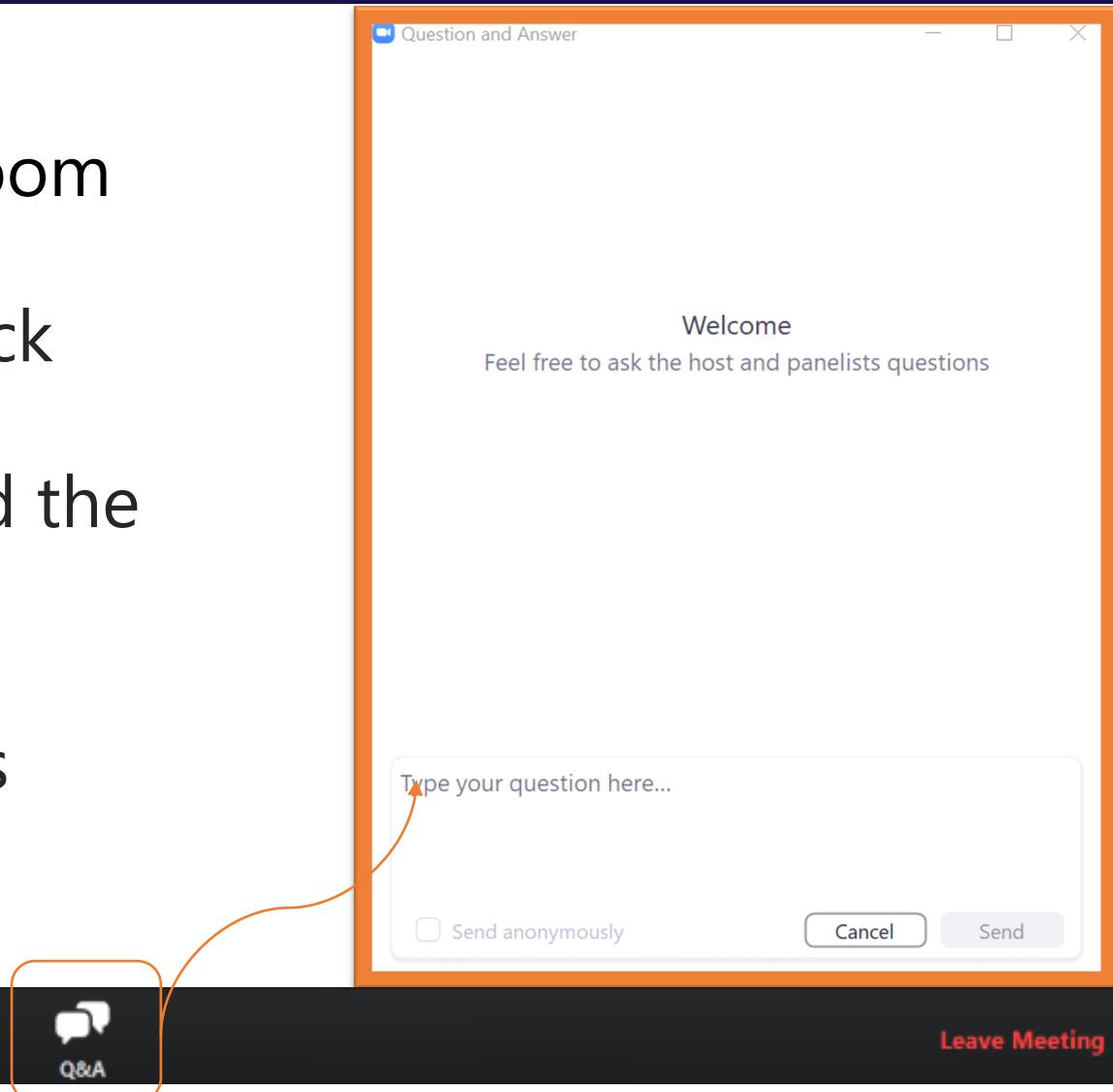
- Presenter will talk for about 40 minutes
- At the end of the presentation, we will take questions
- We will answer as many questions as time allows
- Use the **Q&A button** to submit your questions
- This session is being **recorded**
- Recording will be available on AISA website within 14 days

# To ask a question

## To ask a question:

- Click the **Q&A** button on the Zoom Toolbar
- Type your question and then click the **Send** button
- The moderator/speaker will read the question on your behalf

We will answer as many questions as possible.



Audio Settings ^



Chat



Q&A

Leave Meeting

AISA

# CONVERTING THREAT ACTOR CAMPAIGNS TO PURPLE TEAM EXERCISES

FATIH OZAVCI

# Fatih Ozavci

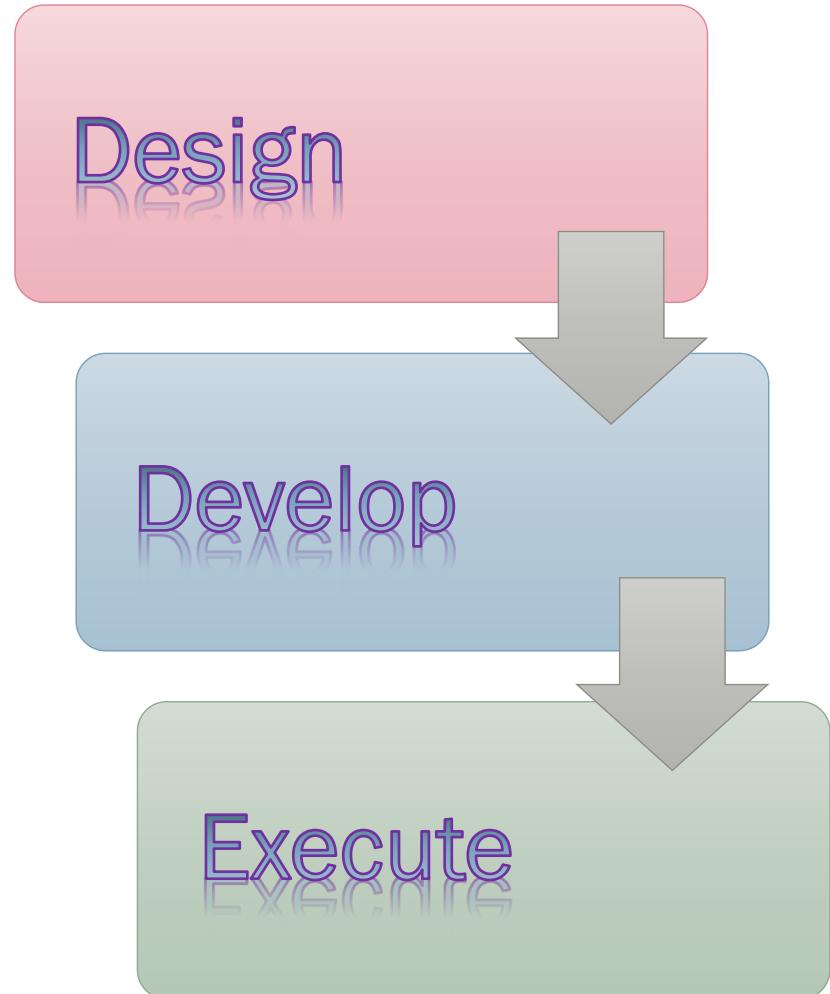
- Adversary Simulations and Research
- UNSW (ADFA) - Master of Cyber Security
- Security Researcher
  - *Vulnerabilities: Microsoft, Cisco, SAP*
- Speaker & Trainer
  - *Sessions: Black Hat USA, Def Con*
- Open Source Software Projects
  - *Petaq Purple Team C2 & Malware*
  - *Viproxy VoIP Penetration Testing Kit*



<https://linkedin.com/in/fozavci>

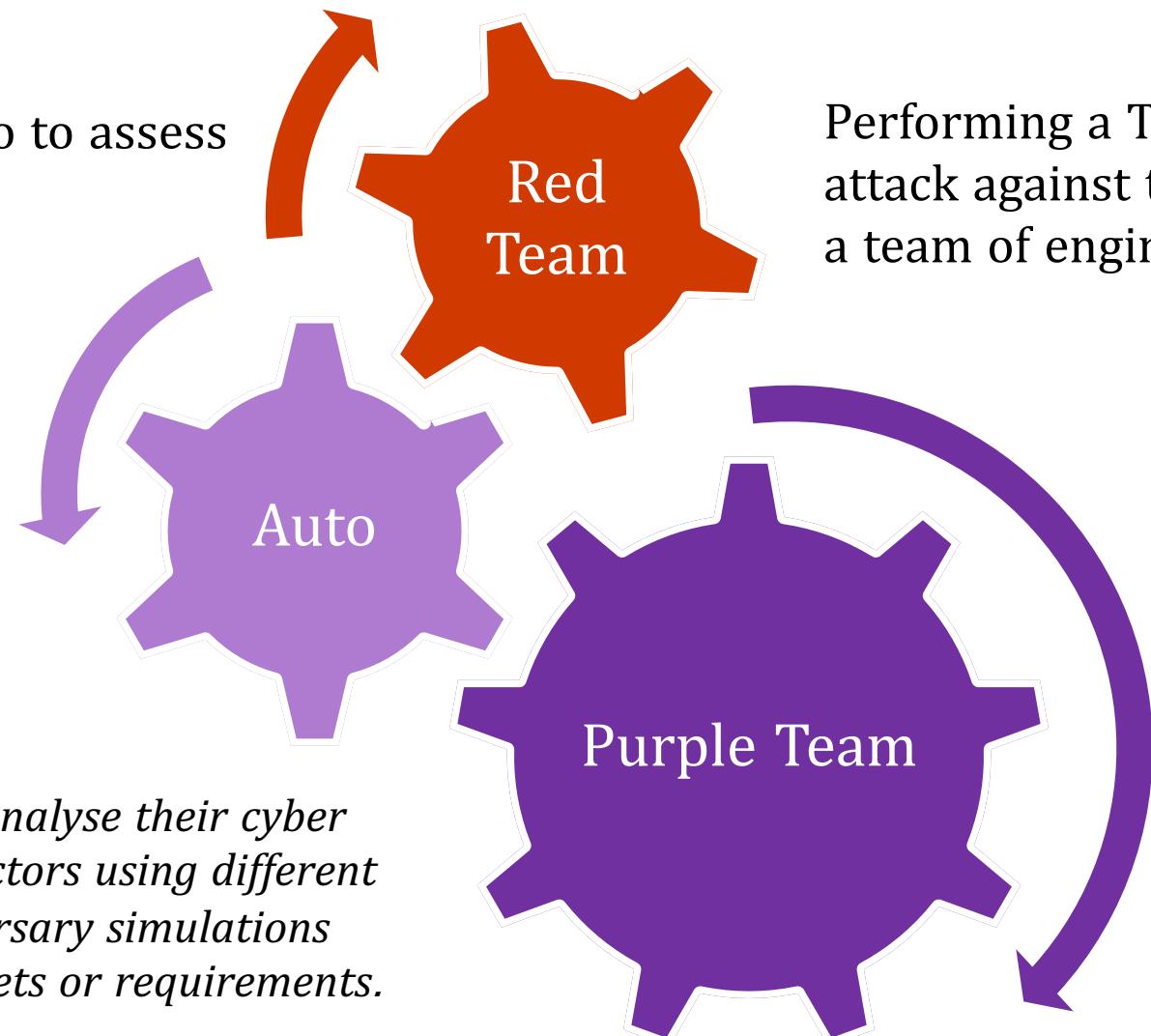
# Agenda

- Adversary Simulations & Scenarios
- TA505 Tradecraft and Projections
- Implementation
  - *C2 & Malware Development*
  - *Customised New and Old Techniques*
- Execution
  - *Flags, Support Systems and Tips*
- Demonstrations



# Adversary Simulation Types

Automating a scenario to assess the defence controls implemented (MITRE ATT&CK)



*Organisations desire to analyse their cyber defence against threat actors using different implementations of adversary simulations depending on their budgets or requirements.*

Performing a Threat Intelligence-Led cyber attack against the targeted environment with a team of engineers (CBEST, CORIE, ICAST)

Performing a cyber attack with blue team collaboration to improve people and defence together (MITRE ATT&CK)

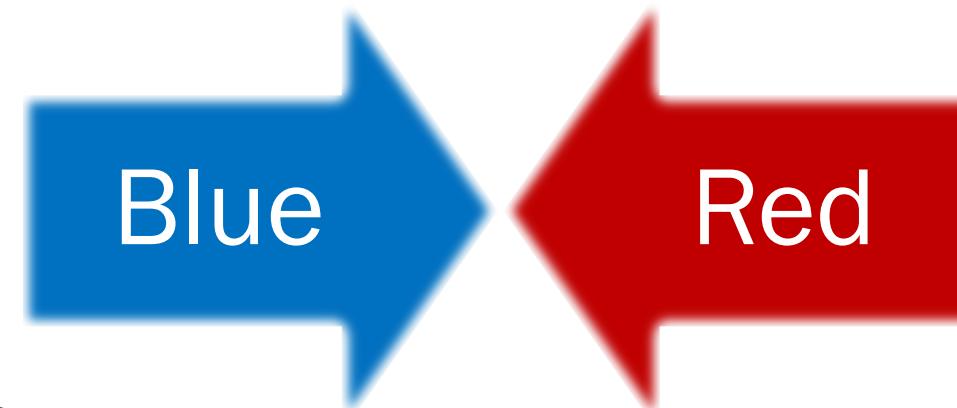
# What Are We Simulating?

- Because, the regulation said so? (CBEST, CORIE, ICAST, MITRE)
- Security Breach Experienced
- External/Internal Red Team Exercise
- General Assessment of the Security Controls and Perimeter
- Threat Actor actively/potentially targeting the organisation
  - *Ransomware & Extortion*
  - *Blockchain Mining*
  - *Long Term Access*



# Team Structure

Threat Intelligence  
Cyber Response  
Cyber Detection  
Security Awareness  
Security Operations



Red Team  
Offensive Security  
Penetration Testing  
External Provider

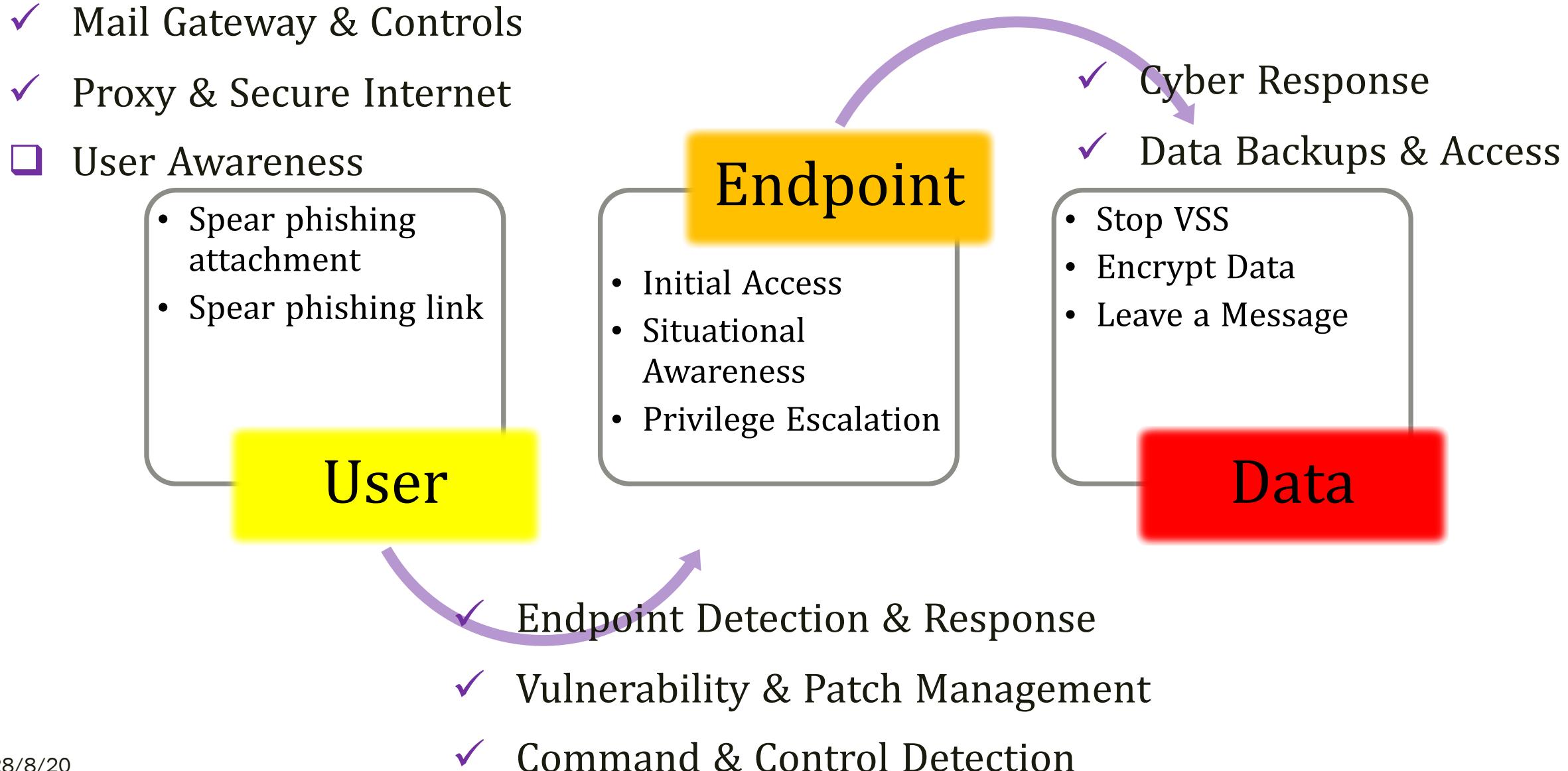
Consider Some Guest Players

# Coverage: Mitre Att&ck

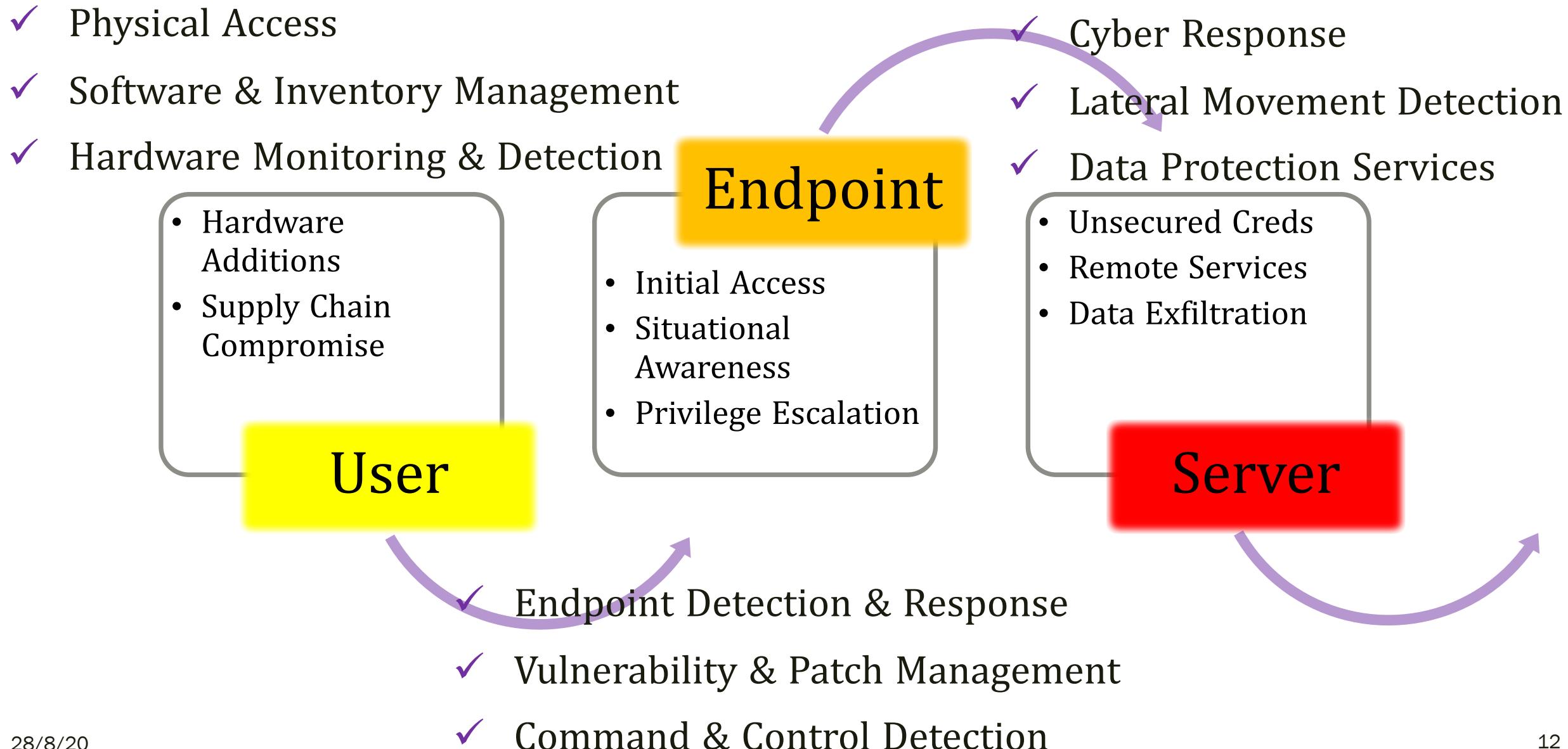
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	10 techniques	18 techniques	12 techniques	34 techniques	14 techniques	24 techniques	9 techniques	16 techniques	16 techniques	9 techniques	13 techniques
Drive-by Compromise	Command and Scripting Interpreter (7)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Browser Bookmark Discovery	Internal Spearphishing	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction	Data Encrypted for Impact
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	BITS Jobs	Exploitation for Credential Access	Cloud Service Dashboard	Cloud Service Discovery	Lateral Tool Transfer	Clipboard Data	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Manipulation (3)
Hardware Additions	Native API	Boot or Logon Autostart Execution (11)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Discovery	Domain Trust Discovery	Remote Service Session Hijacking (2)	Data from Cloud Storage Object	Data Obfuscation (3)	Exfiltration Over C2 Channel	Defacement (2)
Phishing (3)	Scheduled Task/Job (5)	Boot or Logon Initialization Scripts (5)	Direct Volume Access	Execution Guardrails (1)	File and Directory Discovery	File and Directory Discovery	Remote Services (6)	Data from Information Repositories (2)	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Replication Through Removable Media	Shared Modules	Browser Extensions	Create or Modify System Process (4)	Exploitation for Defense Evasion	File and Directory Permissions Modification (2)	File and Directory Permissions Modification (2)	Replication Through Removable Media	Data from Local System	Encrypted Channel (2)	Firmware Corruption	Endpoint Denial of Service (4)
Supply Chain Compromise (3)	System Services (2)	Compromise Client Software Binary	Event Triggered Execution (15)	Group Policy Modification	Group Policy Modification	Group Policy Modification	Software Deployment Tools	Data from Network Shared Drive	Ingress Tool Transfer	Inhibit System Recovery	Network Denial of Service (2)
Trusted Relationship	User Execution (2)	Create Account (3)	Exploitation for Privilege Escalation	Hide Artifacts (6)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Taint Shared Content	Data from Removable Media	Multi-Stage Channels	Resource Hijacking	Resource Hijacking
Valid Accounts (4)	Windows Management Instrumentation	Create or Modify System Process (4)	Group Policy Modification	Impair Defenses (6)	Impair Defenses (6)	Impair Defenses (6)	Use Alternate Authentication Material (4)	Data Staged (2)	Non-Application Layer Protocol	Scheduled Transfer	Service Stop
		Event Triggered Execution (15)	Hijack Execution Flow (11)	Indicator Removal on Host (6)	OS Credential Dumping (8)	OS Credential Dumping (8)	Use Alternate Authentication Material (4)	Email Collection (3)	Non-Standard Port	Protocol Tunneling	System Shutdown/Reboot
		External Remote Services	Hijack Execution Flow (11)	Process Injection (11)	Steal Application Access Token	Steal Application Access Token	Use Alternate Authentication Material (4)	Input Capture (4)	Proxy (4)	Transfer Data to Cloud Account	
		Hijack Execution Flow (11)	Process Injection (11)	Scheduled Task/Job (5)	Steal or Forge Kerberos Tickets (3)	Steal or Forge Kerberos Tickets (3)	Use Alternate Authentication Material (4)	Man in the Browser	Remote Access Software		
		Implant Container Image	Scheduled Task/Job (5)	Indirect Command Execution	Steal Web Session Cookie	Steal Web Session Cookie	Use Alternate Authentication Material (4)	Man in the Browser	Proxy (4)		
		Office Application	Valid Accounts (4)	Masquerading (6)	Two-Factor	Two-Factor	Use Alternate Authentication Material (4)	Man in the Browser	Remote Access Software		

<https://attack.mitre.org/>

# Scenarios (Ransomware)

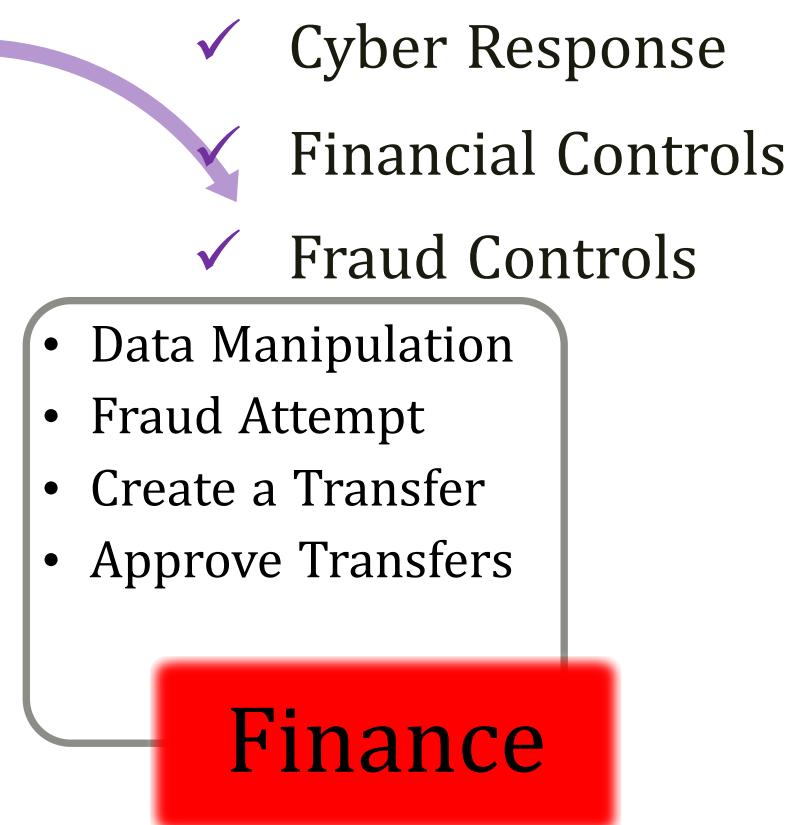
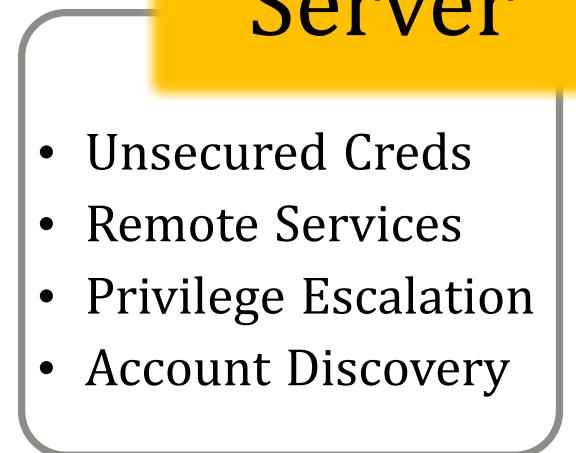
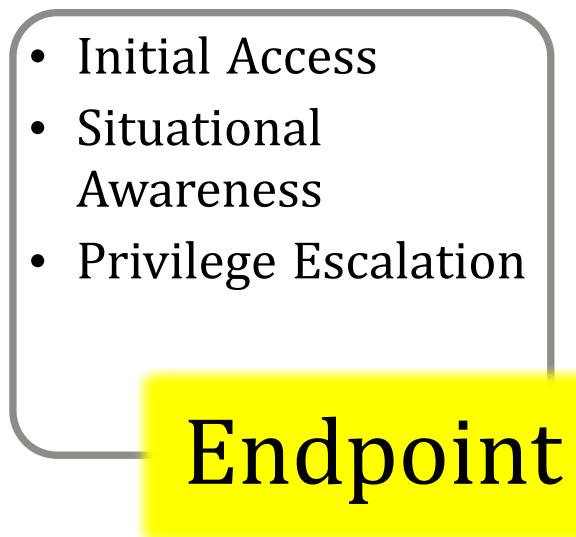


# Scenarios (Supply Chain)



# Scenarios (Assume Breach)

- ✓ Endpoint Detection & Response
- ✓ Vulnerability & Patch Management
- ✓ Command & Control Detection



- ✓ Cyber Response
- ✓ Lateral Movement Detection

- ✓ Cyber Response
- ✓ Financial Controls
- ✓ Fraud Controls

# The Threat Actor (TA505+)

- TA505 is a threat group actively targeting financial institutions, including Australia, since 2014 using custom tools (e.g. FlawedAmmyy , ServHelper, SDBot) and offensive security tools (e.g. Cobalt Strike, TinyMet).
- They constantly changed/updated their RAT used as tradecraft. So, it's logical to assume that TA505 would start using .NET Tradecraft after Cobalt Strike received *execute-assembly* feature to run .NET assemblies with process injections.
- This adversary simulation is based on TA505 TTPs, but also additional .NET Tradecraft and custom C2 suites (e.g. Petaq C2). Therefore it's called TA505+ .

# TA505+ Tradecraft Map

Mitre Att&ck ID	Malware	Description	Replacement
S0384	Dridex	HTTP C2, encrypted C2 traffic, VNC feature, P2P Relay	Petaq Implant
S0381	FlawedAmmyy	HTTP C2, WMI enumeration for AV, system information	Petaq Implant
S0383	FlawedGrace	Fully featured malware	Petaq Implant
S0460	Get2	Downloader for FlawedGrace, FlawedAmmyy, Snatch and SDBot	Petaq Dropper
S0039	Net	Internal Windows command, enum and mapping	No replacement
S0461	SDBot	TA505's new installer and loader	Petaq Dropper
S0382	ServHelper	TA505's new malware replacing the old ones in 2018	Petaq Implant
S0266	TrickBot	Spyware used against financial institutions, replaced Dyre. Used for mainly situational awareness and information collection.	.NET Applications

Mitre Att&ck ID	Malware	Description	Replacement
S0154	Cobalt Strike	Fully featured and commercial C2.	Petaq Service
	Metasploit Framework	Fully featured and commercial exploitation framework	No replacement

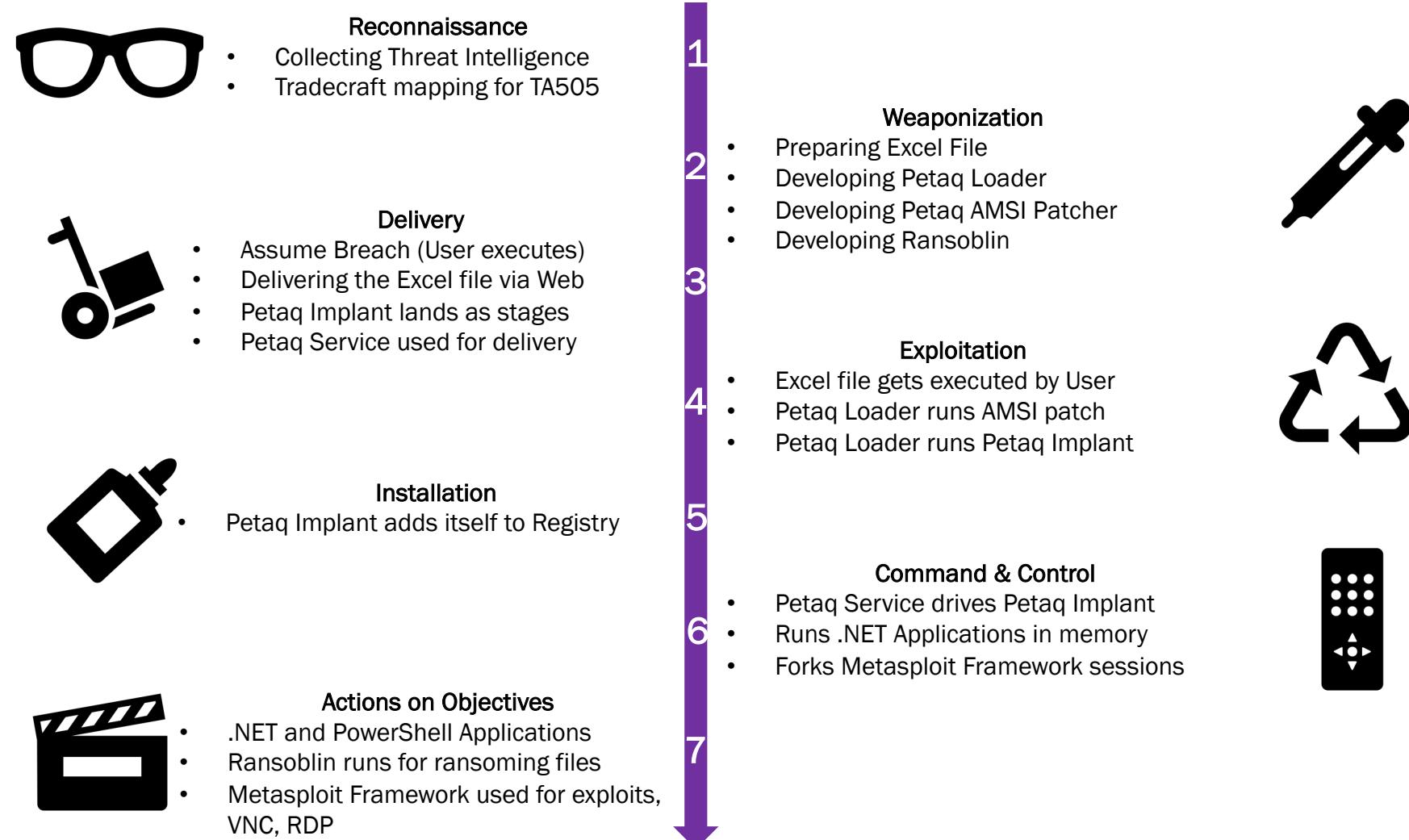
# TA505+ Technique Map

Mitre Att&ck ID	Name	Implementation
T1087.003	Account Discovery: Email Account	Not Implemented
T1071.001	Application Layer Protocol: Web Protocols	Petaq Implant communicated with C2 using HTTP Web Sockets, Meterpreter used HTTPS
T1059.001	Command and Scripting Interpreter: PowerShell	PowerUp for privilege escalation enumeration
T1059.005	Command and Scripting Interpreter: Visual Basic	Not Implemented
T1059.007	Command and Scripting Interpreter: JavaScript/JScript	Not Implemented
T1059.003	Command and Scripting Interpreter: Windows Command Shell	Several situational commands run on CMD
T1555.003	Credentials from Password Stores: Credentials from Web Browsers	Not Implemented
T1486	Data Encrypted for Impact	Ransoblin used for ransomware simulation
T1568.001	Dynamic Resolution: Fast Flux DNS	Not Implemented
T1105	Ingress Tool Transfer	Petaq Dropper -> Implant -> Meterpreter
T1105.002	Inter-Process Communication: Dynamic Data Exchange	Replaced with Excel 4.0 Macro
T1078.002	Valid Accounts: Domain Accounts	Reusing the credentials extracted

# TA505+ Technique Map

Mitre Att&ck ID	Name	Implementation
T1027	Obfuscated Files or Information	Excel file and Powershell to be obfuscated
T1027.002	Software Packing	.NET Tradecraft run inline, not required
T1069	Permission Groups Discovery	Situational awareness commands
T1566.001	Phishing: Spearphishing Attachment	Excel file is presented, but not mailed
T1566.002	Phishing: Spearphishing Link	Excel file link is presented, but not mailed
T1055.001	Process Injection: Dynamic-link Library Injection	DLL Injection via Petaq Implant
T1218.007	Signed Binary Proxy Execution: Msiexec	Msiexec command run via Petaq Implant
T1218.011	Signed Binary Proxy Execution: Rundll32	RunDLL32 called via Petaq Implant
T1553.002	Subvert Trust Controls: Code Signing	Not implemented
T1552.001	Unsecured Credentials: Credentials In Files	Implemented with a sample file on desktop
T1204.002	User Execution: Malicious File	Excel file is the malicious file for execution
T1204.001	User Execution: Malicious Link	Excel file is the malicious file for execution

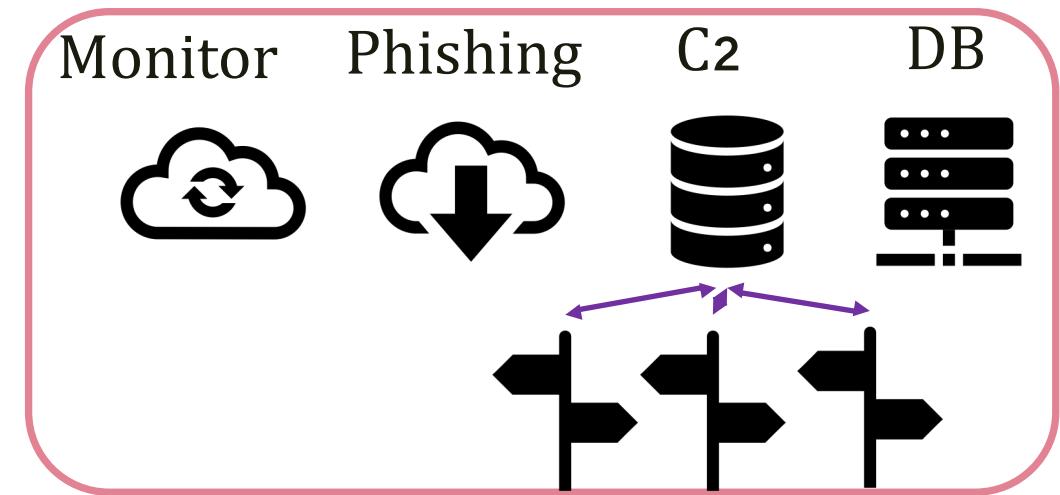
# Kill Chain Implementation for TA505+



# Platform

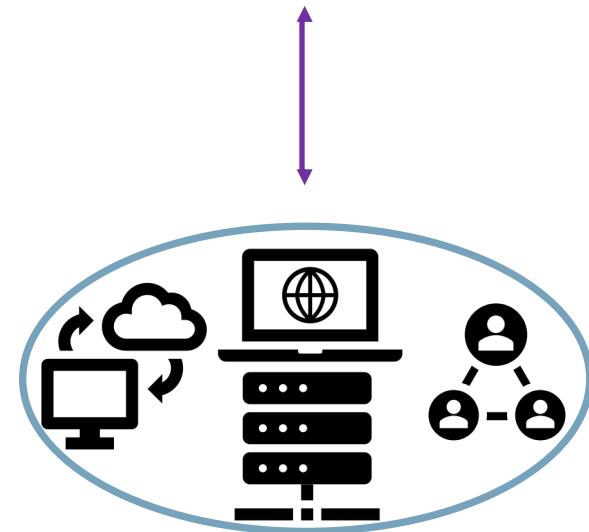
## ➤ Cloud Deployment

- *Provider Selection*
- *Services: Storage, DB, VM, OS*
- *Domains: Fronted, Aged, Classified*



## ➤ Operational Security

- *Real-Time Monitoring*
- *Encrypting Data in Transit and at Rest*
- *Implement Compliance Requirements*



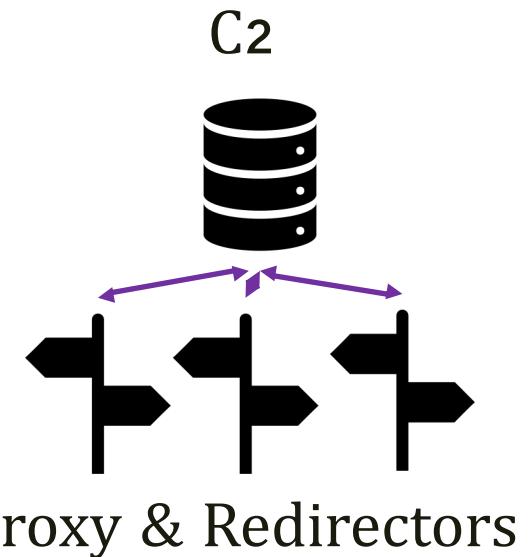
# Software: Command & Control

## ➤ Command & Control Service Selection

- *What does the threat actor use?*
- *What operating systems are targeted?*
- *Multi Instance: Long Term, Short Term, Interactive*
- *C2 Protocols, Cloud Native, Multi User, Logging...*

## ➤ Safer C2 Choices

- *Scythe (Commercial, Safer and Flexible for Automation)*
- *Cobalt Strike (Commercial, Favorite of Threat Actors and Red Teams)*
- *Covenant (C#, Open Source, Mostly Stable)*
- *SilentTrinity (.NET and Python, Open Source, Stable)*

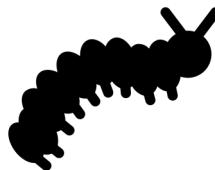


# Software: Petaq C2

- Petaq Purple Team Command & Control Server (MIT License)
  - *P'takh (petaQ) is a Klingon insult, meaning something like "weirdo"*
  - *Protocols : HTTPS, WebSocket, SMB Named Pipe, TCP, UDP*
  - *Execution : CMD, .NET Assembly, Source, Shellcode Injection, PowerShell*
  - *Features : WMI Lateral Movement, Nested Implant Linking, Encryption*
  - *Scenario Based Automation and TTP Support*
- Petaq is suitable to interactive and scenario based exercises

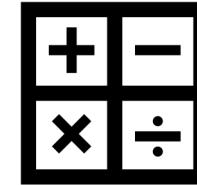
<https://github.com/fozavci/petaqc2>

# Applications Developed & Customised



## Petaq Dropper

- C# Application
- Loads .NET Assemblies (Implant & AMSI patcher)
- <https://github.com/fozavci/ta505plus>



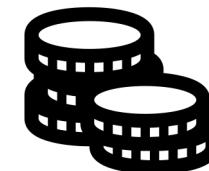
## Malicious Excel File

- Excel 4.0 Macro
- Generated using ExcelIntDonut
- <https://github.com/fozavci/ta505plus>



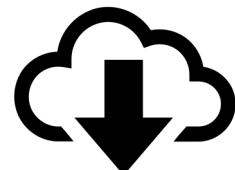
## Petaq Implant

- C# .NET 4.5 Application
- Fully featured malware, all essential features
- Runs commands, powershell, .Net, shellcode
- Links other remote implants as nested implants
- <https://github.com/fozavci/petaqc2>



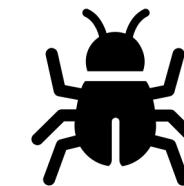
## Ransoblin

- C# .NET 4.5 & Core 3.1 Application
- Safer Ransomware implementation
- <https://github.com/fozavci/ransoblin>



## Petaq Service

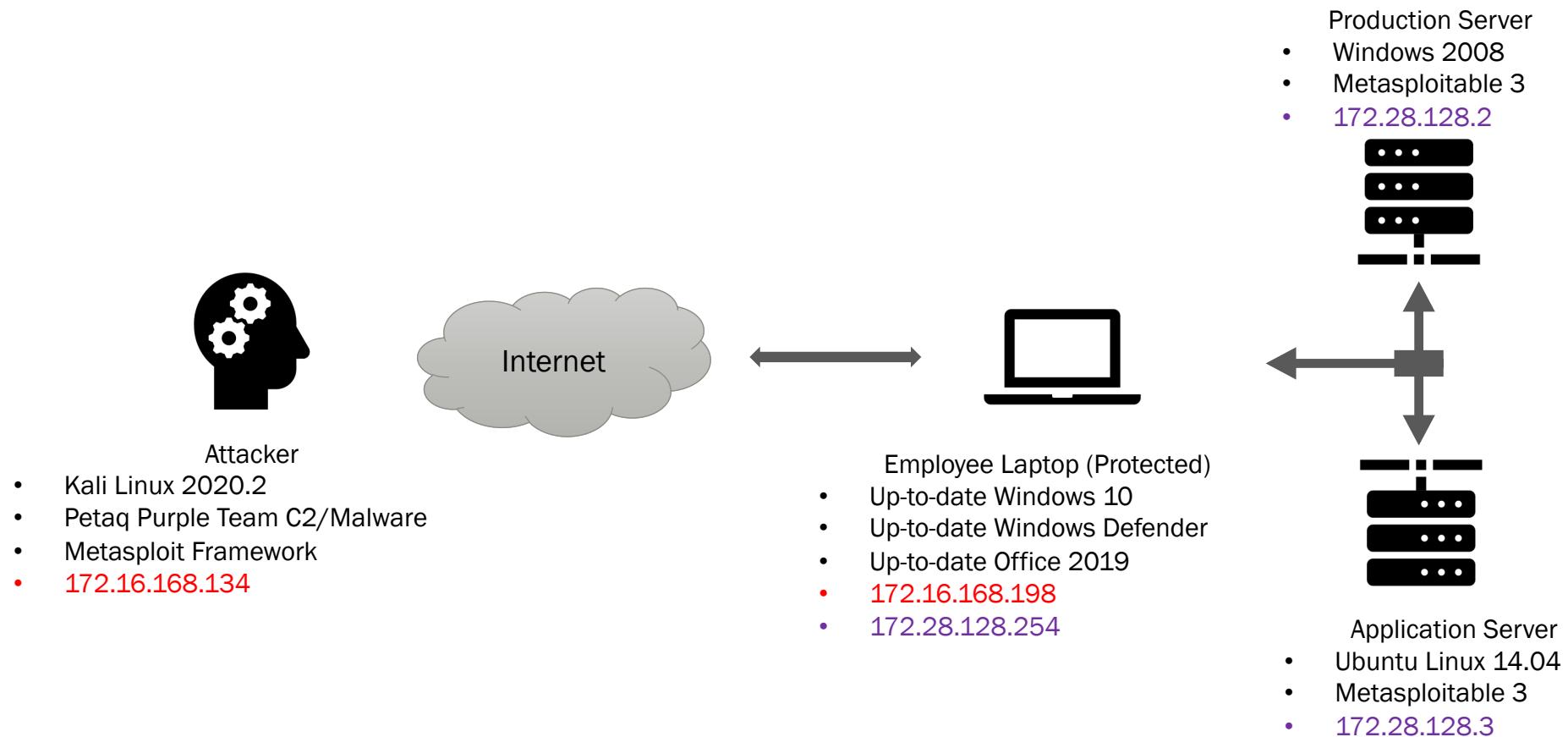
- C# .NET Core 3.1 Application
- C2 running through HTTP Websockets
- <https://github.com/fozavci/petaqc2>



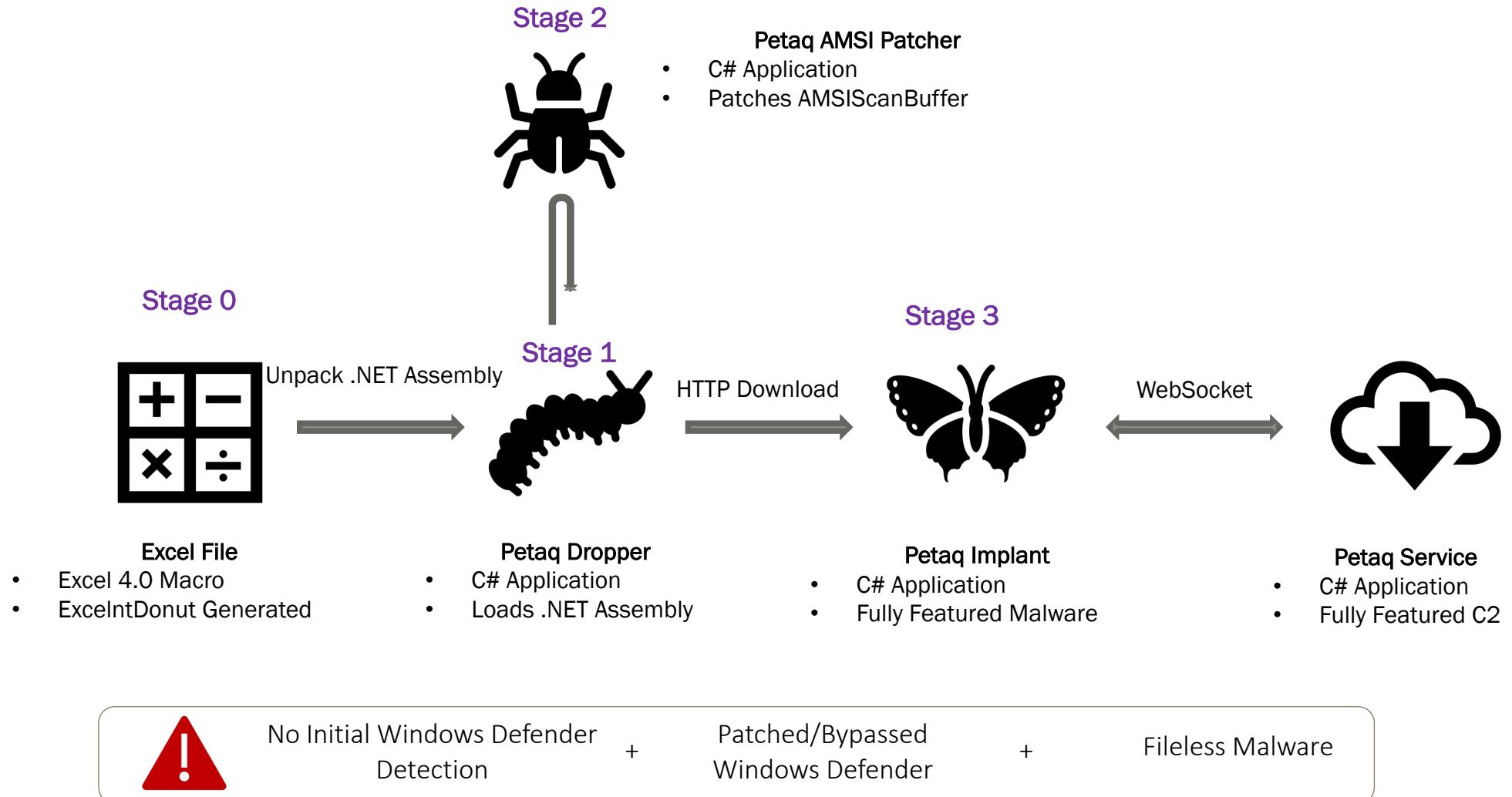
## Petaq AMSI Patcher

- C# .NET 2.0 Application
- Patches AMSIScanBuffer
- [https://github.com/fozavci/petaq\\_amsi](https://github.com/fozavci/petaq_amsi)

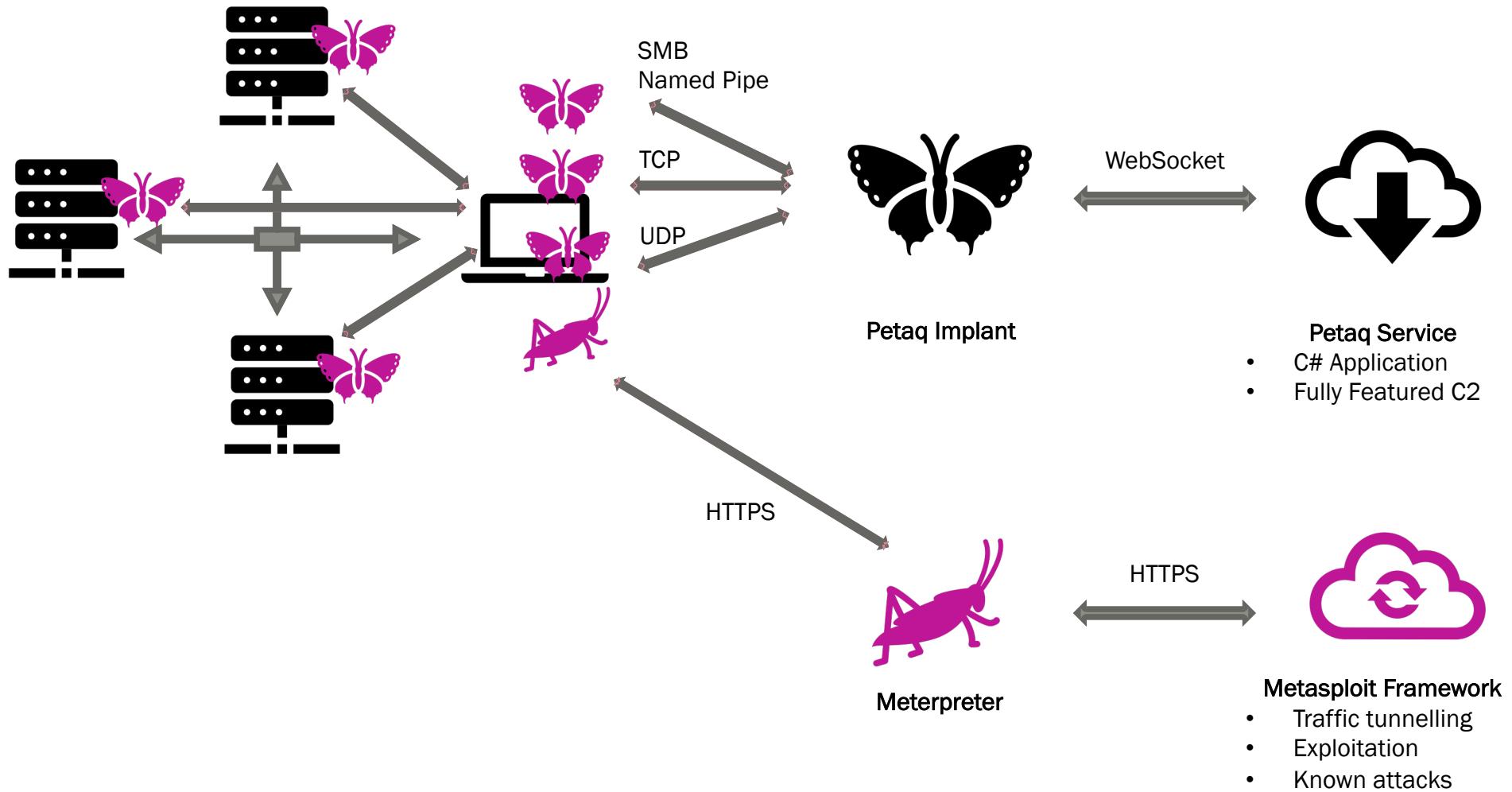
# Target Environment



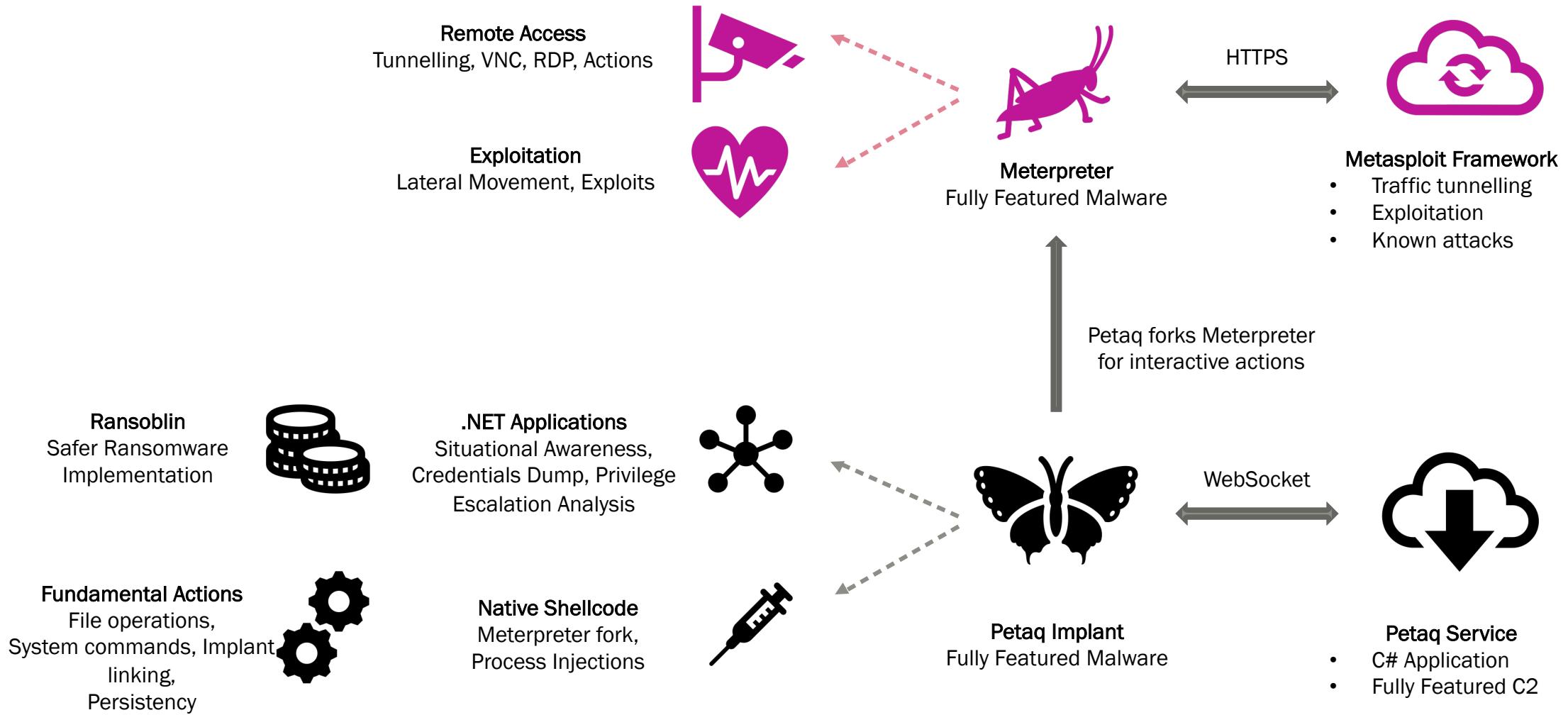
# Initial Compromise & Defence Evasion



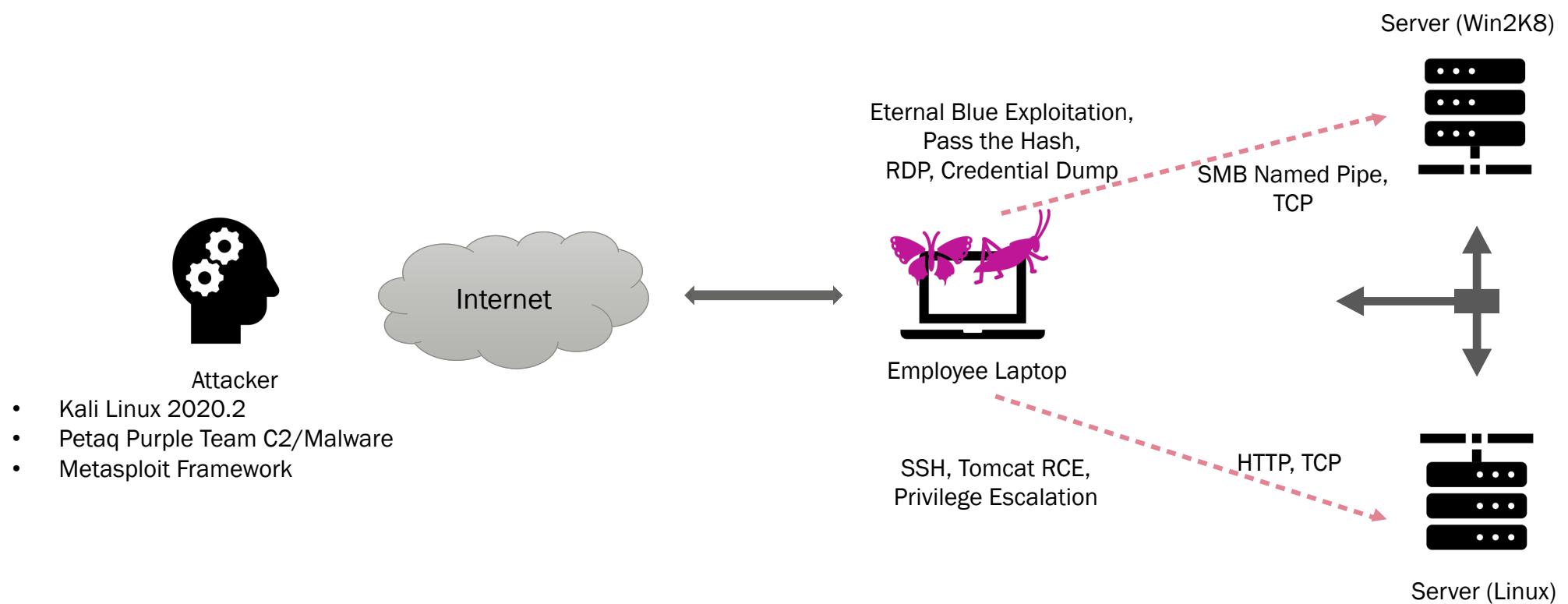
# Internal Implant Communications



# Actions on Objectives



# Lateral Movement



# Execution Tips

- Attacks take time to show up on SOC monitors and alerts.
  - *Run the attacks or scenario, and give a grace period*
  - *The exercise duration may be 2-3 days due to scope*
- Use a CTF or reporting software to give a metric to all parties.
- Assign a facilitator to the exercise.
  - *Maintain the pressure like the real life exercise*
  - *It's not a race, but a friendly competition*
- Blue team should receive all tradecraft, logs and IOCs



# Planting the Flags

- Flags are useful to assess the team capabilities such as reverse engineering, malware analysis and utilising the security controls.
  - *Phishing email (e.g. headers, content)*
  - *Initial malware stages (e.g. command, dropper, stage 1, stage 2)*
  - *C2 communications (e.g. profile, protocol)*
  - *Persistency options (e.g. registry, file IOCs, services)*
  - *Lateral movement (e.g. remote service, WMI query, creds)*
  - *Data exfiltration (e.g. fake DLP flags, C2 channels, WebDAV)*
- Use a Capture the Flag scoring website or application



# Development and Execution Videos

[https://www.youtube.com/playlist?list=PL-o-7RjmFOAUOBb\\_eZDL\\_9yM7YOMX-6c](https://www.youtube.com/playlist?list=PL-o-7RjmFOAUOBb_eZDL_9yM7YOMX-6c)

The image shows a screenshot of a YouTube playlist page. The title of the playlist is "TA505+ Adversary Simulation". It contains 27 videos, with the first seven listed below:

- 1 TA505+ Adversary Simulation: Reconnaissance - TA505 ThreatIntel and Introduction Fatih Ozavci 21:27
- 2 TA505+ Adversary Simulation: Weaponisation - 1 C2 and Malware Development Fatih Ozavci 11:15
- 3 TA505+ Adversary Simulation: Weaponisation - 2 Petaq AMSI Bypass Fatih Ozavci 18:07
- 4 TA505+ Adversary Simulation: Weaponisation - 3 Petaq Dropper Fatih Ozavci 10:46
- 5 TA505+ Adversary Simulation: Weaponisation - 4 Petaq Implant and Service Demonstration Fatih Ozavci 11:18
- 6 TA505+ Adversary Simulation: Weaponisation - 5 Petaq Implant Running Meterpreter Fatih Ozavci 9:29
- 7 TA505+ Adversary Simulation: Weaponisation - 6 Petaq UAC Bypass and Running Meterpreter Fatih Ozavci 12:23

The page also includes a "PLAY ALL" button, a "SUBSCRIBE" button, and a profile picture of the creator, Fatih Ozavci.

# Uplift the Game

## ➤ Add Variations to Command & Control

- *Cloud Native C2s (e.g. Serverless Apps, Direct DB Connections, JavaScript Everywhere)*
- *C2 Traffic Cloud to Cloud (e.g. Deploying the C2 in another tenant of target cloud)*
- *Domain Fronting (e.g. Leveraging Cloud Fronting services with Domain/SNI masking)*
- *Newest HTTP Protocols (e.g. Mobile push on HTTP/2 or HTTP/3, WebRTC, WebSocket)*

## ➤ Improve Evasion Techniques

- *Reloading a clean NTDLL and remapping API Calls*
- *Protecting the processes with Parent ID spoofing, Microsoft Process Tags and Hollowing*
- *Disabling the EDR monitoring in Kernel Space*

## ➤ Adjust the Pace of Exercise for the Scenario Requirement

# Conclusion

- Various exercise types exist, find/develop a tailor fit exercise
- Exercise development and customisation improves efficiency
- TA505 can still walkthrough newer systems with minor updates
- Benefits of Purple Team Exercises
  - *Overall defence level for certain threats*
  - *Security weaknesses or vulnerabilities*
  - *Uplifting the existing skills sets and resources*
  - *Measuring software and solution efficiency*
- Specialists first, software later...

# References

- *TA505+ Repository* (<https://github.com/fozavci/ta505plus>)
- *Petaq C2* (<https://github.com/fozavci/petaqc2>)
- *Petaq AMSI Patch* ([https://github.com/fozavci/petaq\\_amsi](https://github.com/fozavci/petaq_amsi))
- *Ransoblin* (<https://github.com/fozavci/ransoblin>)

THANKS