HITB SECCONF SIN-2021

Malware Protocol Simulations in Distributed Networks

Fatih Ozavci

Managing Security Consultant, The Missing Link

Track 1

“How can we safely simulate the malware and adversary network traffic to assess our data analytics, telemetry and defence solutions ?”

Blue Teamers, Data Analysts, Security Engineers

Agenda

Malware Communications

Cyber Analytics for Detecting Malware Communications

Ways to Generate Malware Communications

Tehsat – Malware Traffic Generator

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

themissinglink®

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

Threat Actors and Campaigns

6 new wa

Cyber criminals will
COVID crisis to impr

By Evan Schuman
Contributing Colum

Microsoft's Respo
SIX Advanced Th
Network of "Large

By **CBR Staff Writer** (

Microsoft's Detection and Respo
discovered six threat actors in
multinational company", after being
apparent intrusion by an unnamed a

DART said it has been contracted to d
sponsored advanced persistent threa
company and persisted in its networ
to remove it.

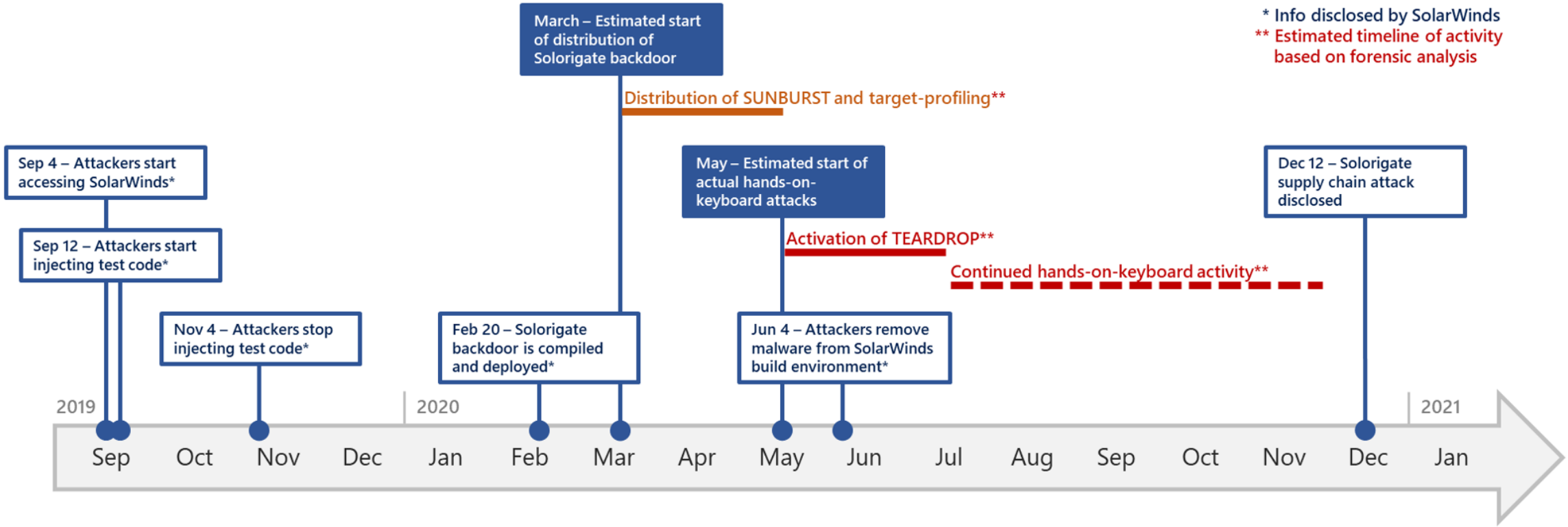
10 Major Global Telcos "Completely Penetrated" by Chinese APT

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.

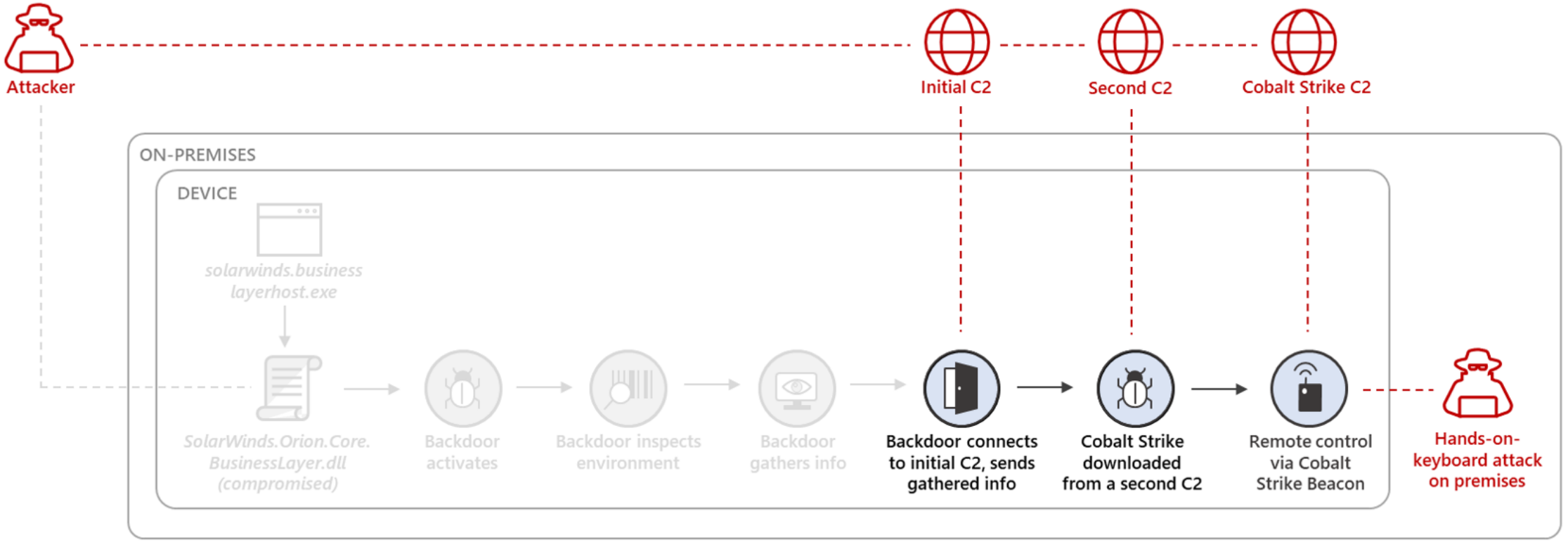
The attackers were in networks for at least two years. They had extracted over 100GB of data from the primary telco assessed, and were using their access to so-called Call Detail Records (CDRs) to track the movements and interactions of high-profile individuals that Cybereason – founded by veterans of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

Solarigate Attack Timeline



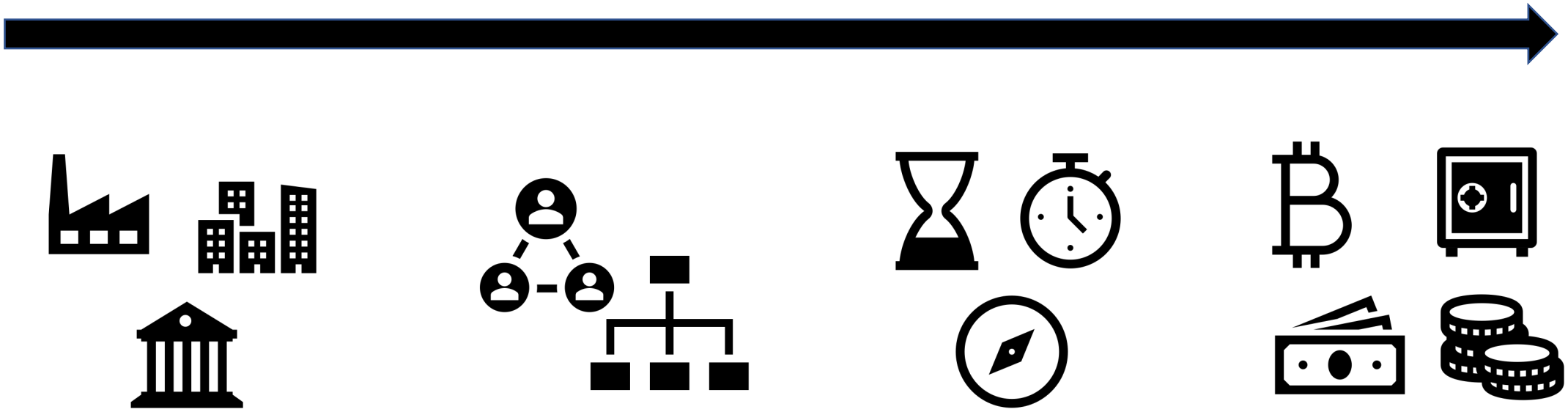
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

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/

Compromise Journey



Organisation

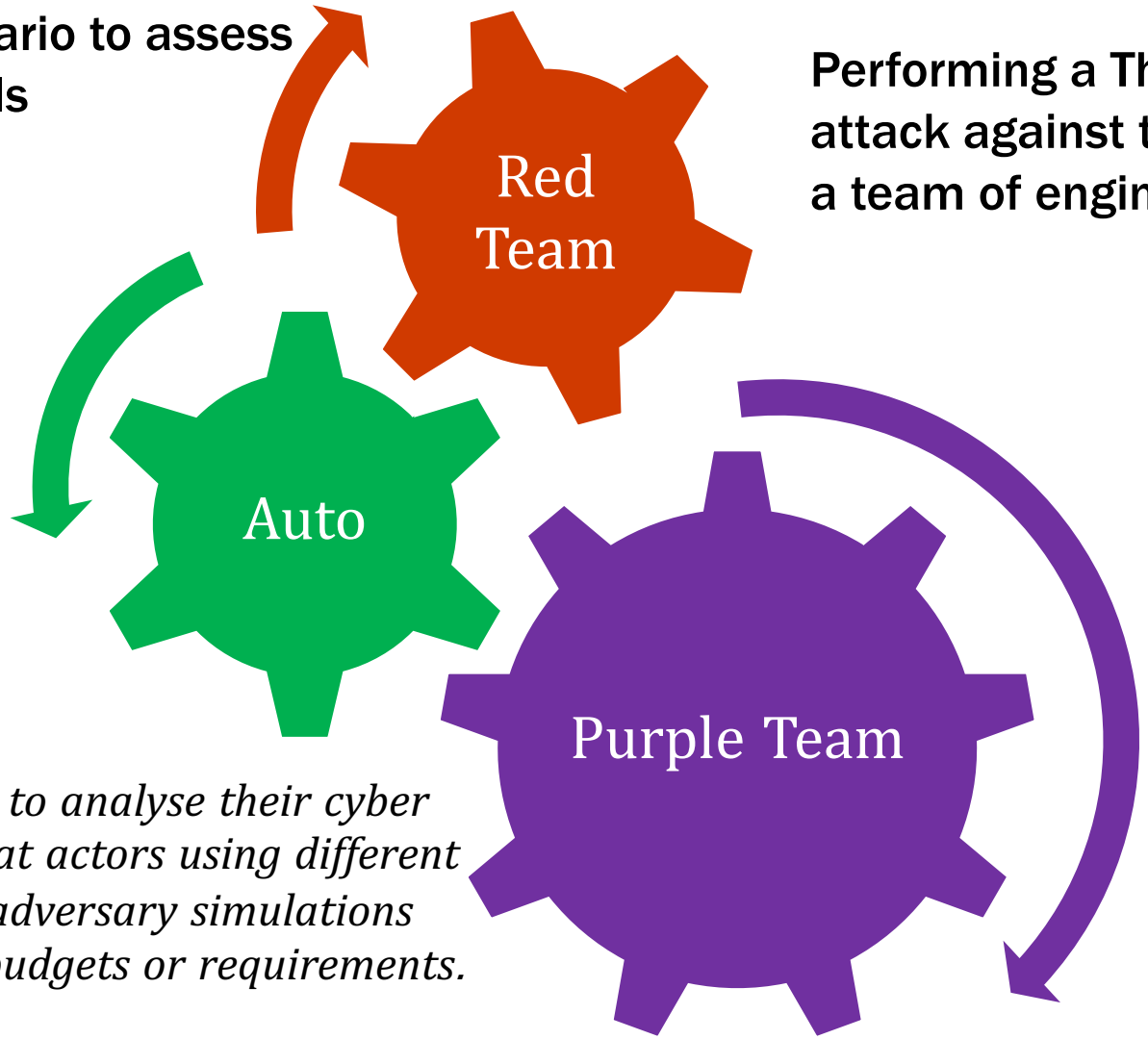
Key People

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)

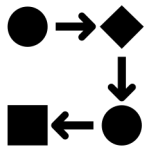
Performing a cyber attack with blue team collaboration to improve people and defence together (MITRE ATT&CK)

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

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

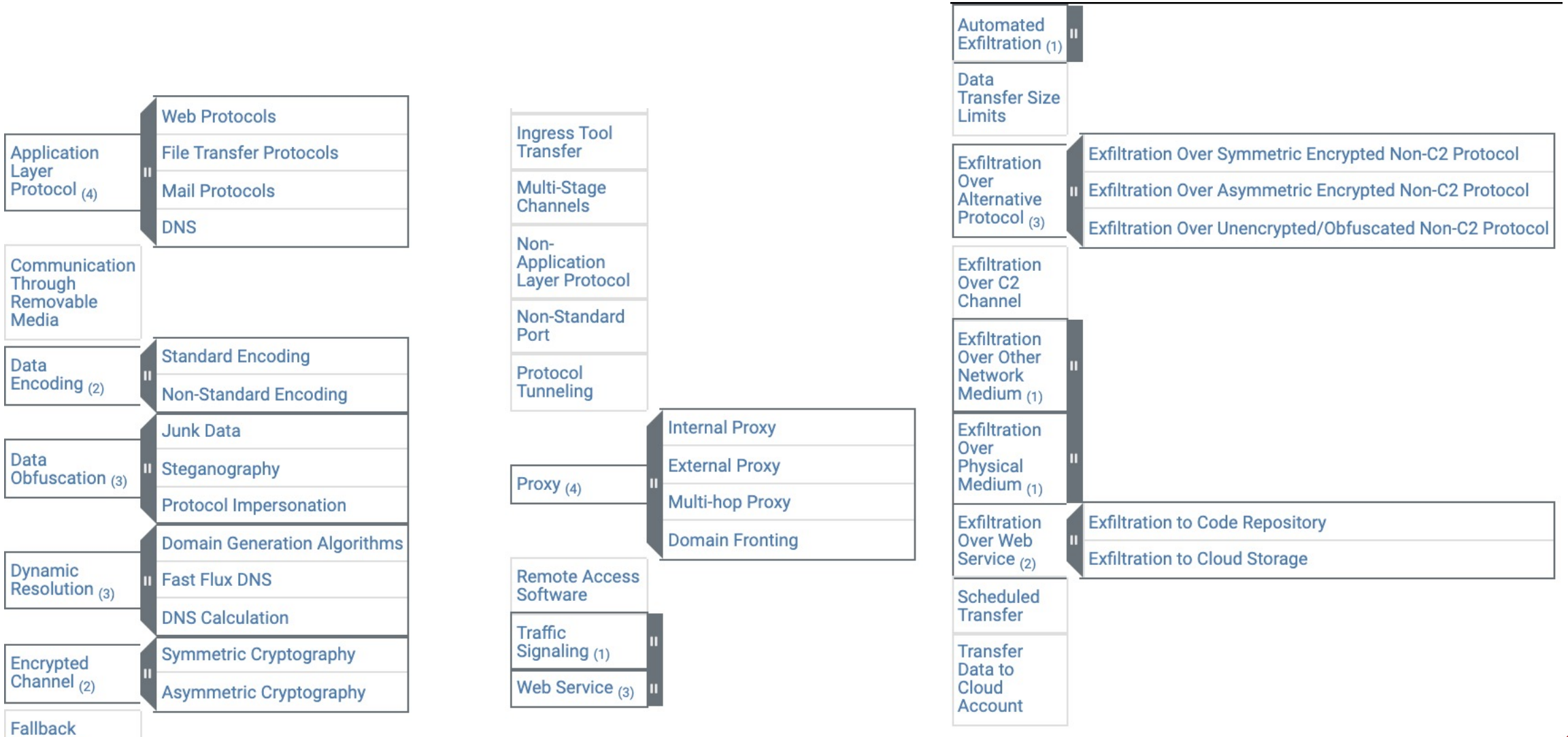
- Known-Good vs Known-Bad (What if you're already compromised?)
- Does Known-Bad Cover All Threat Actor Techniques

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

C2, Beaconing and Exfiltration



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

Simulating Malware Traffic

Collaborative Exercise

Upside

- Easy Deployment & Tests
- Following Threat Intelligence
- Easy Data Analytics Cases
- Less/No Hostile Activities

Downside

- Lack of Realistic Traffic/Exploits
- Limited Lateral Movement
- Offensive Mind

Automated Traffic Generation

Upside

- Realistic Approach
- Exploitation
- Realistic Lateral Movement
- Professionally Masked C2

Downside

- Time & Budget
- Operator & Software
- Compliance Violations

Simulating Malware Traffic

Collaborative Exercise

Upside

- Easy Deployment & Tests
- Following Threat Intelligence
- Easy Data Analytics Cases
- Less/No Hostile Activities

Downside

- Lack of Realistic Traffic/Exploits
- Limited Lateral Movement
- Offensive Mind

1. Find Relevant TI Report
2. Prepare a Simulation Pack
3. Automate the Tasks
4. Observe the Defence

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"

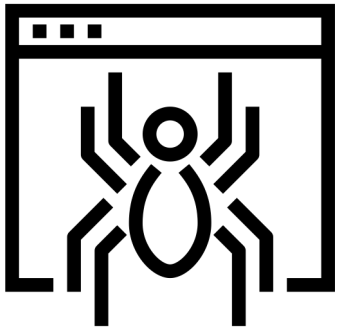
Protocols : HTTP(S), WebSocket, SMB Named Pipe, TCP, UDP

Execution : CMD, .NET Assembly, Source, Shellcode Injection, PowerShell

Features : WMI Lateral Movement, Nested Implant Linking, Encryption

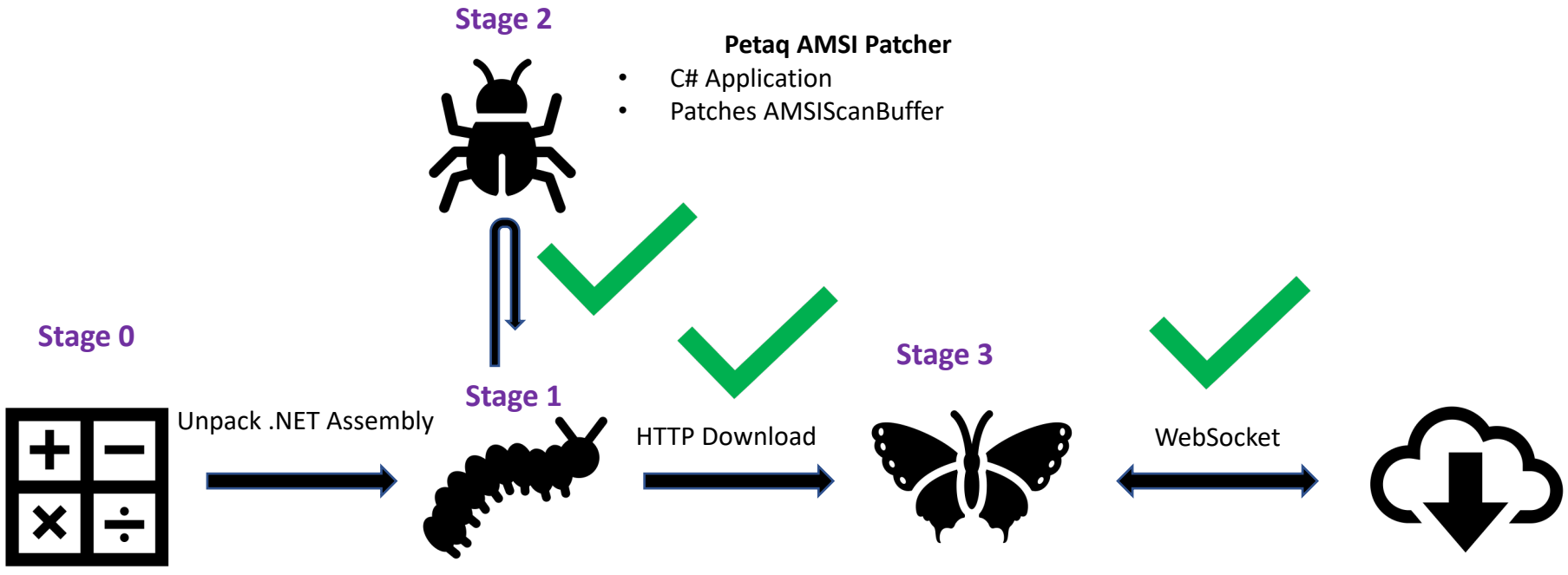
Scenario Based Automation and TTP Support

* Petaq is suitable to interactive and scenario based exercises

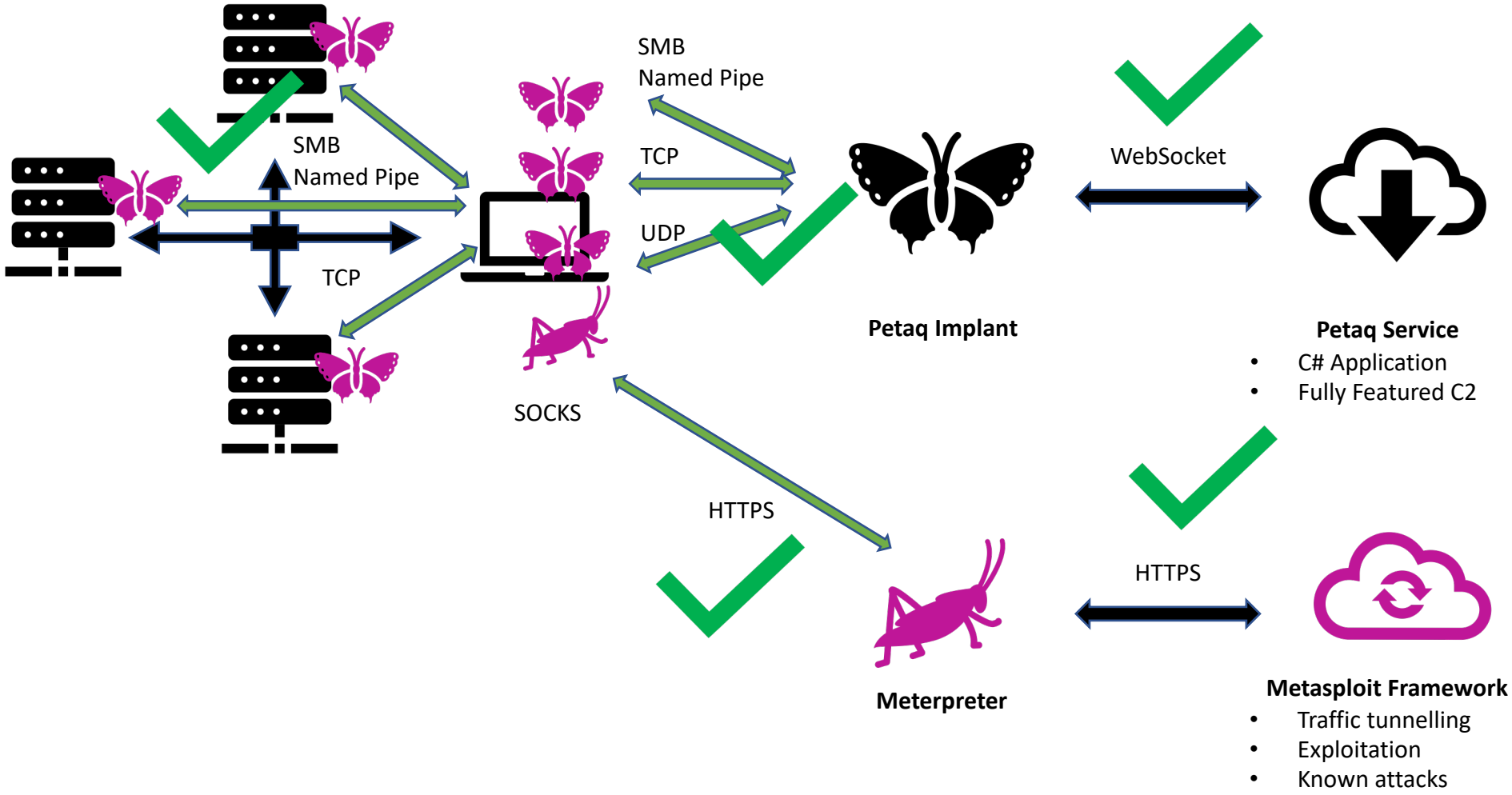


https://github.com/fozavci/petaqc2

Deployment Traffic



Tunnelling and Linking Traffic

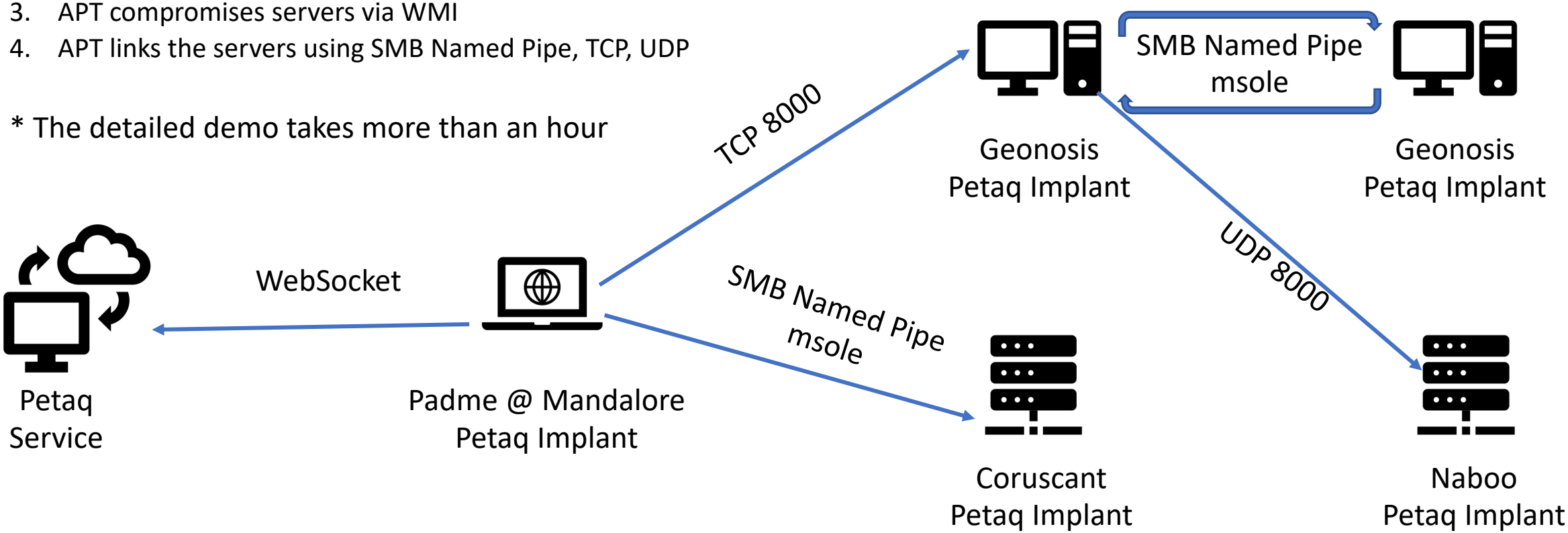


Traffic Generation with Petaq C2

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

Challenges

Adversary Simulations Take a Long Time

Only Limited Number of C2 Communications Simulated

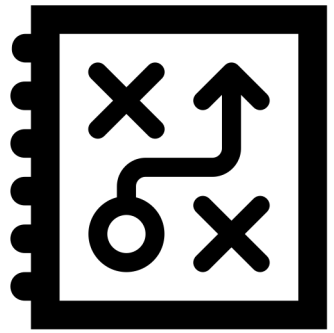
- Threat Actor Specific
- Evasion is Priority
- Lack of Blue Team Communications

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



Simulating Malware Traffic

1. Find Relevant TI Report
2. Prepare a Scenario
3. Build C2 Profiles
4. Observe the Defence
5. Go to 1

Automated Traffic Generation

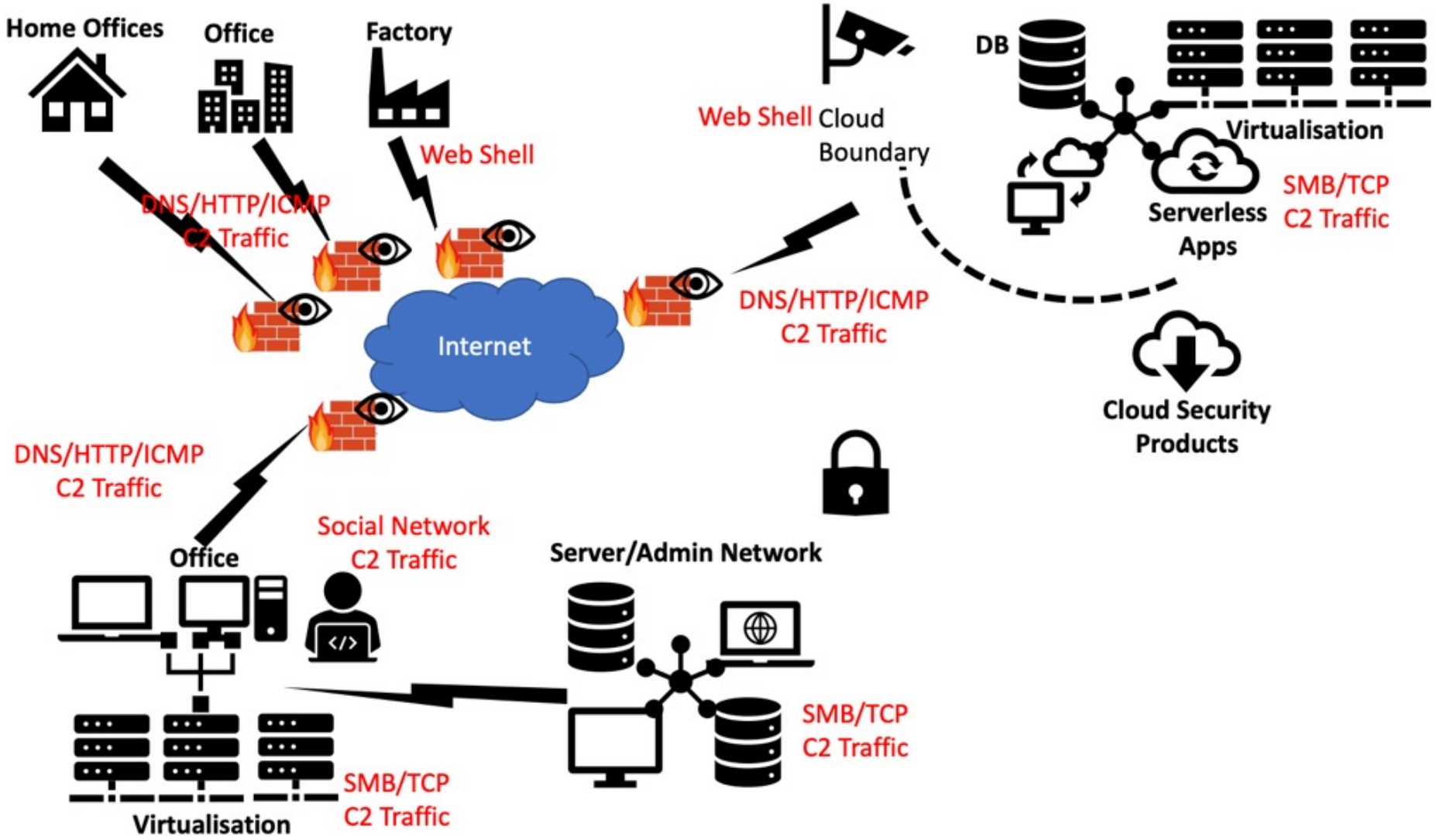
Upside

- Realistic Approach
- Exploitation
- Realistic Lateral Movement
- Professionally Masked C2

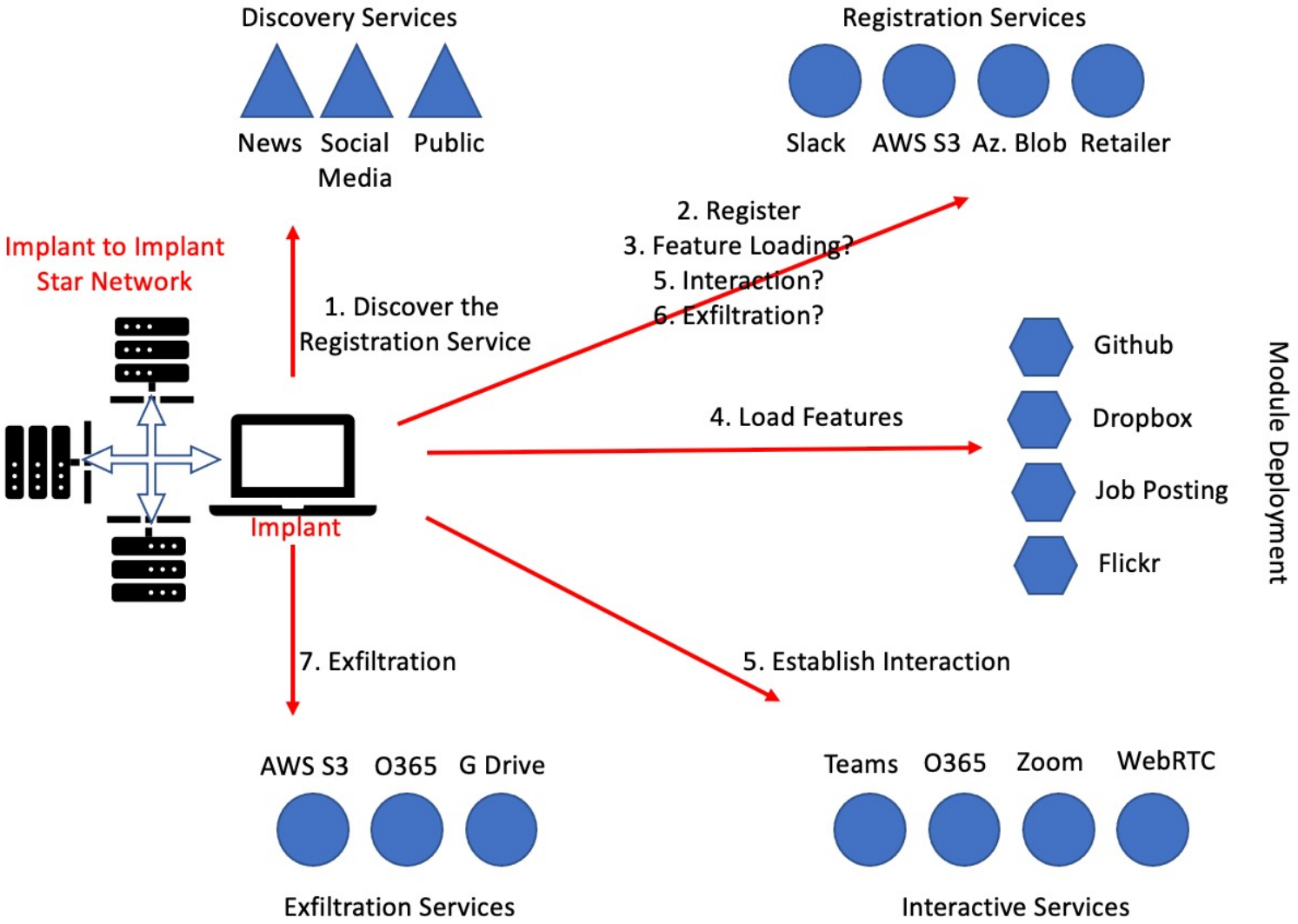
Downside

- Time & Budget
- Operator & Software
- Compliance Violations

Cloud & Covid Era



Distributed C2 Infrastructure



Tehsat Malware Traffic Generator

Tehsat (means **Deception** in Vulcan)

Graphical Interface to Prepare Malware Communications

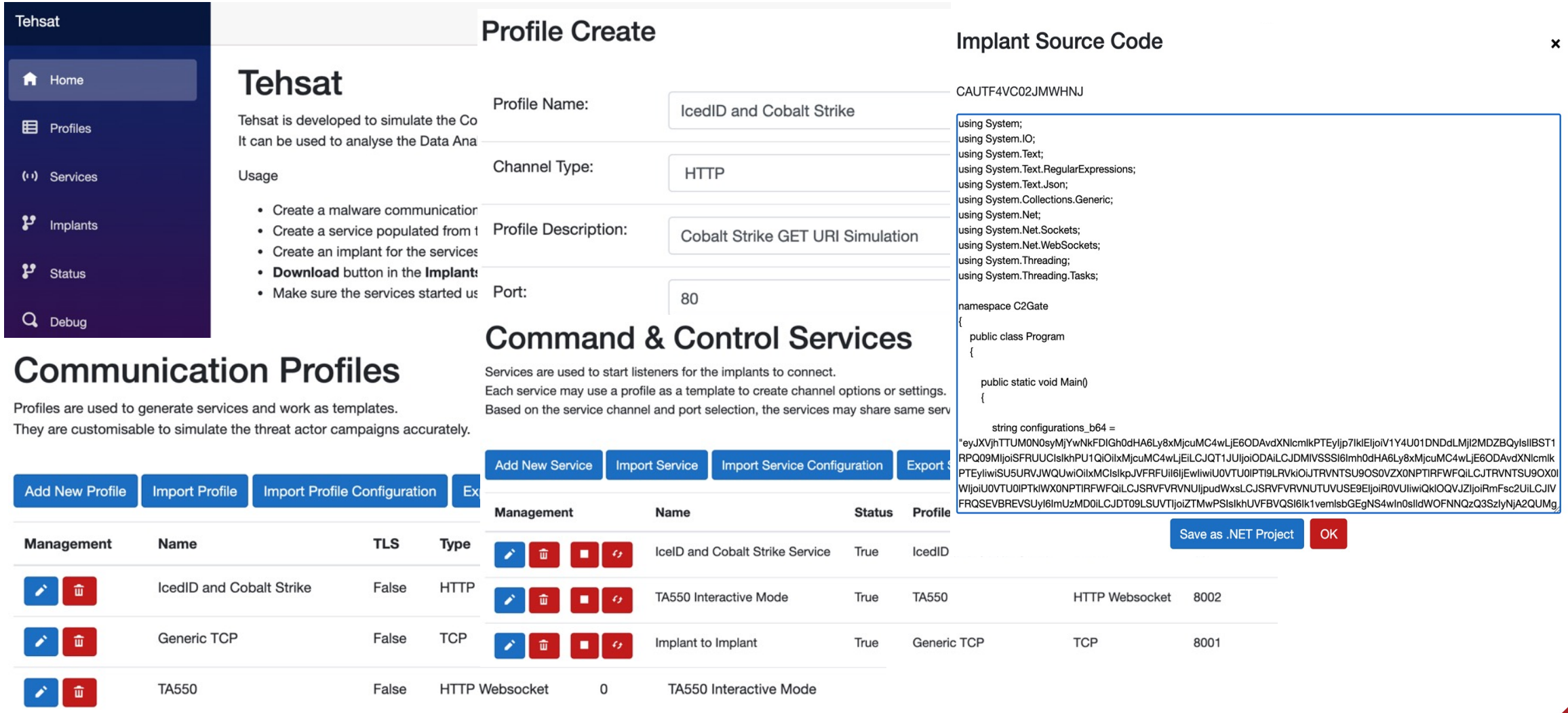
- Various Protocols (HTTP, TCP, UDP, Websocket)
- Easy and Detailed Customisation (HTTP headers, Request/Response, Agents)
- Service Creation Using Profiles
- Friendly Implant Generation per Scenario (Multi-Service)

Scenario Design Steps

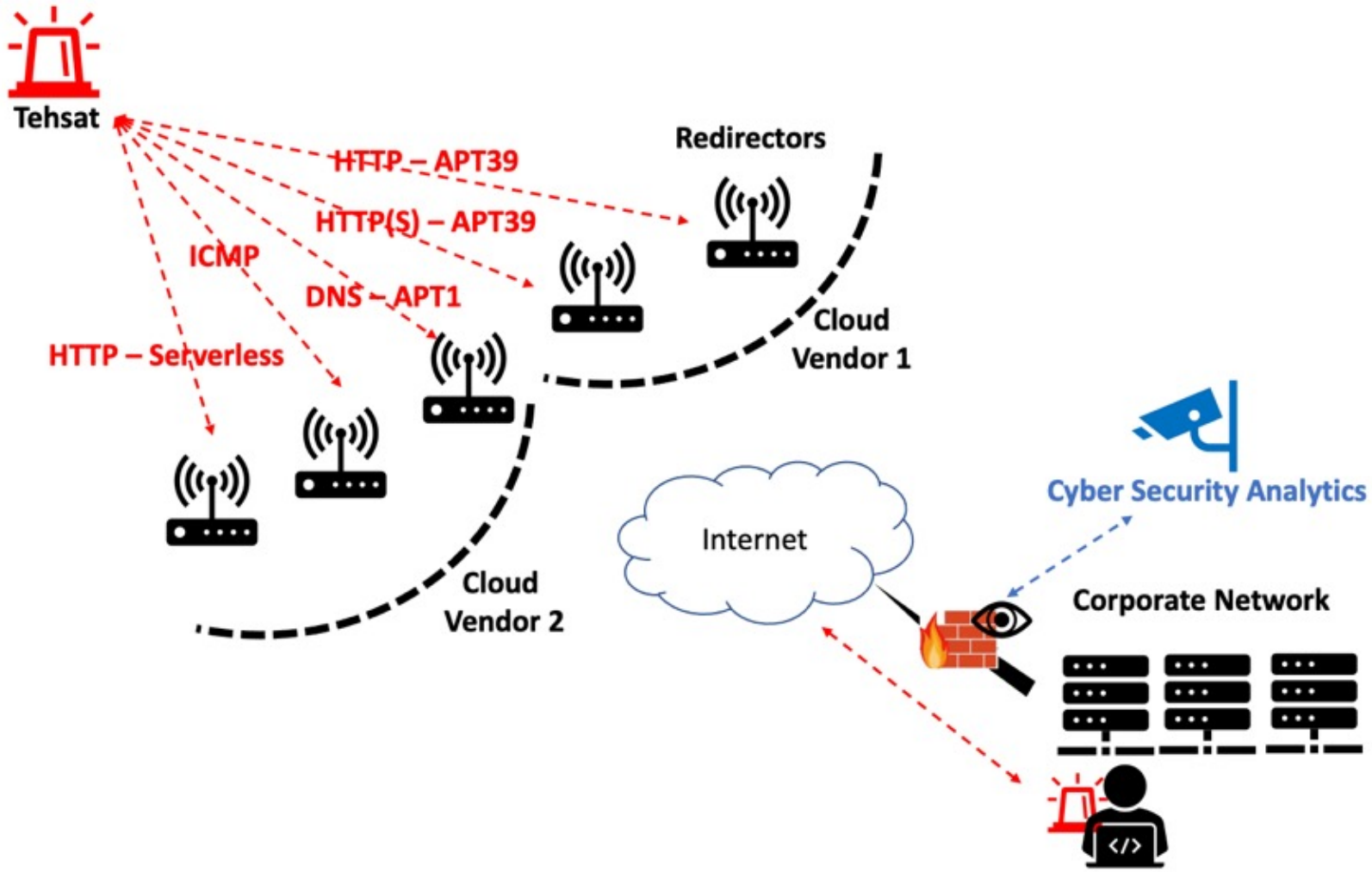
- Collect Communication Details from Threat Intelligence Reports
- Create Services for Kill Chain Phases (Registration, Long Term C2, Interactive C2)
- Create Implant for Selected Services
- Deploy Implant via PowerShell, Group Policy or a Single Command

https://github.com/fozavci/tehsat

Tehsat Malware Traffic Generator



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)*

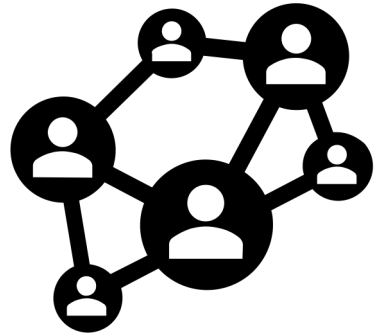
Use a Capture the Flag scoring website or application (e.g. Vectr – vectr.io)

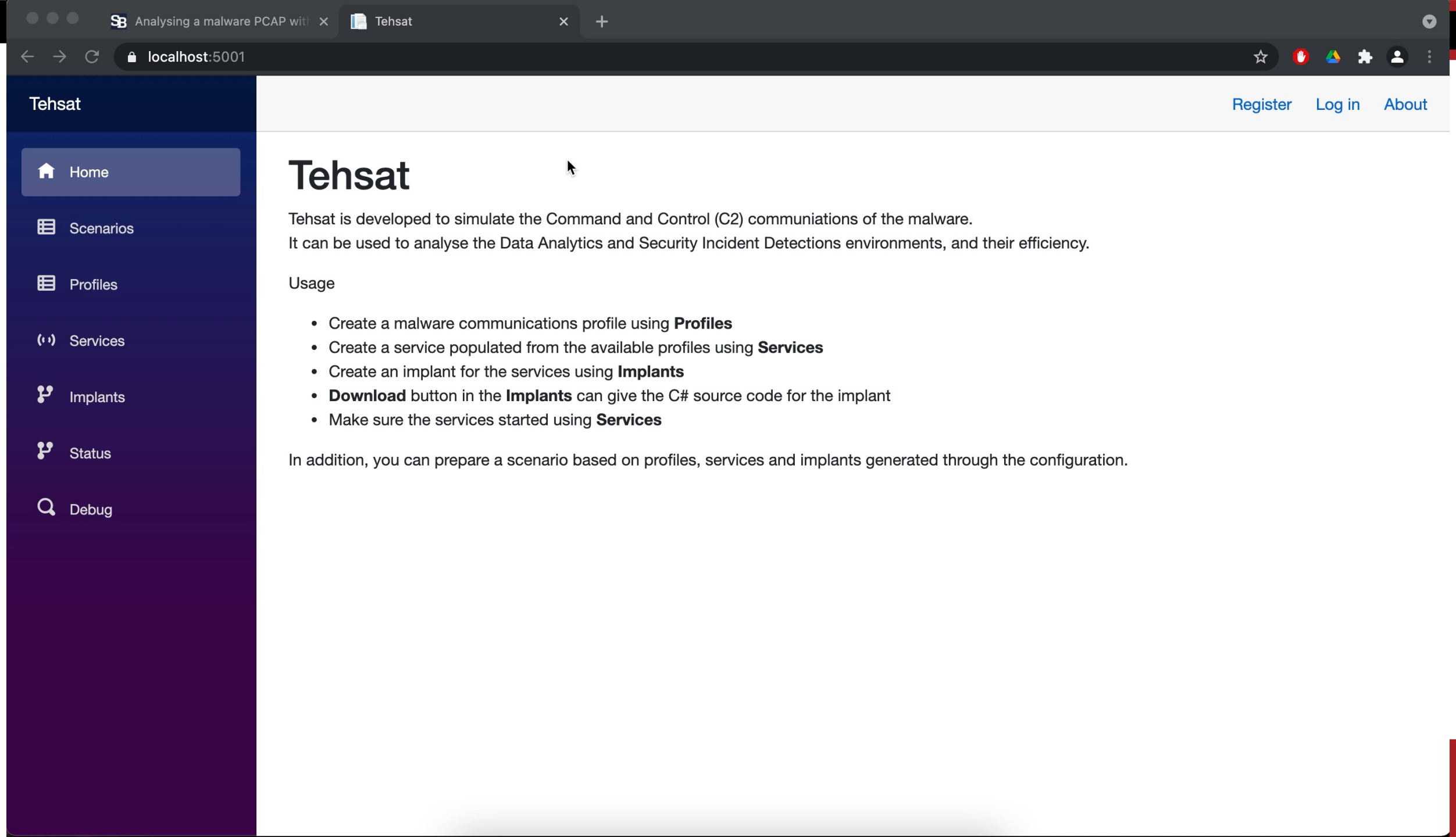
Uplift the Game

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.

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

HITB SECCONF SIN-2021

Thank You for Joining Us

Join our Discord channel to discuss more or ask questions

https://discord.gg/dXE8ZMvU9J