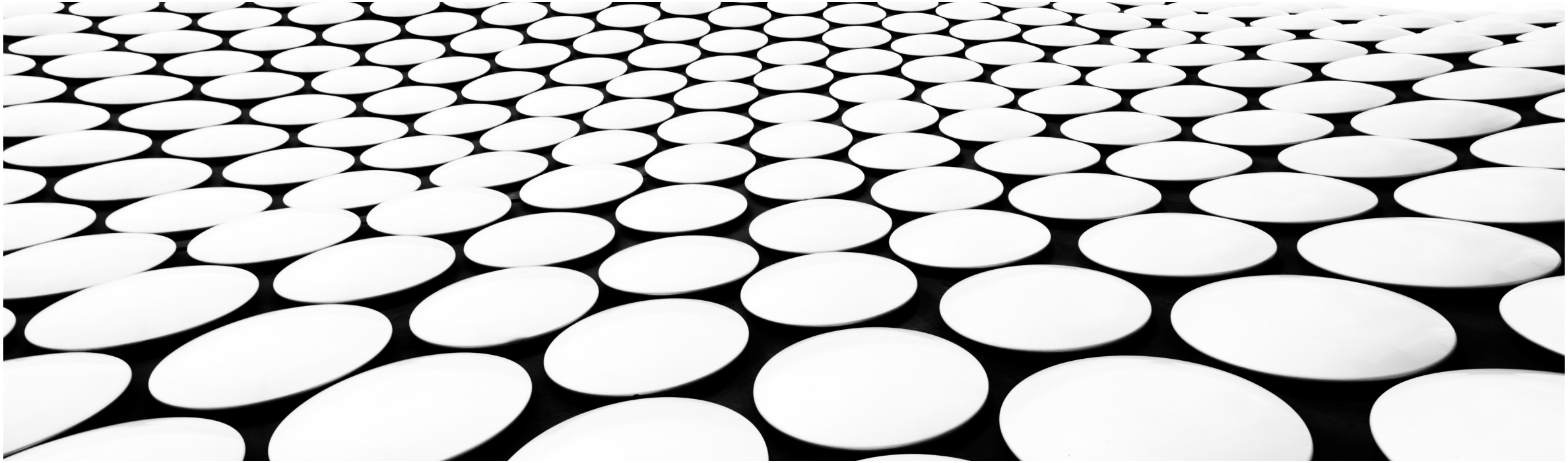
Malware Traffic Generation to Improve Security Incident Detections

Fatih Ozavci – Managing Security Consultant



Agenda

- Threat Actors
- Adversary Simulations
- Demonstrating The Long Game with TA505+ Simulation Pack
- Malware Communications
- Cyber Analytics for Detecting Malware Communications
- Ways to Generate Malware Communications
- Tehsat – Malware Traffic Generator

Fatih Ozavci

AusCERT 2021

- 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®

Threat Actors and Campaigns

AusCERT 2021

6 new

Cyber crimi
COVID crisis

By Ev
Contrib

Microsoft's R
SIX Advanc

10 Major Global Telcos "Completely Penetrated" by

Cyber criminals spend three months lurking in target networks

Cyber criminals are spending longer hiding in target networks before launching their attacks, as more organised groups turn to business disruption to achieve their objectives

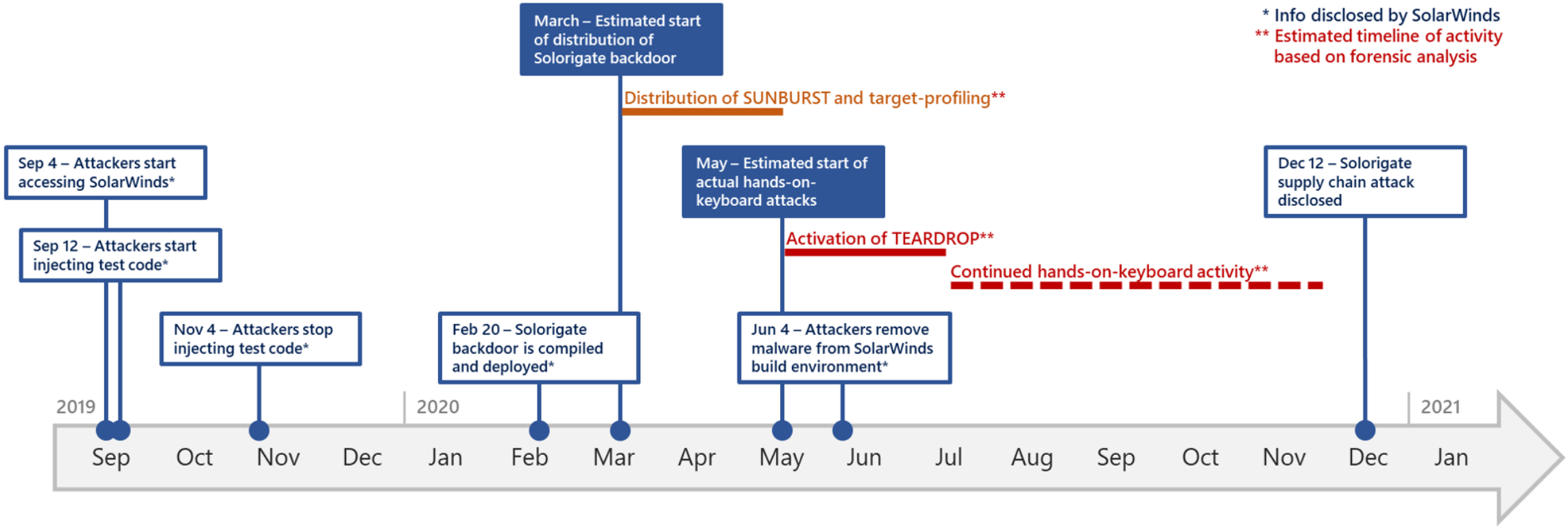
By **Alex Scroxton,** Security Editor

Published: **14 Jan 2020 13:00**

DART said it has been co
sponsored advanced per
company and persisted in its network for eight months despite efforts to remove it.

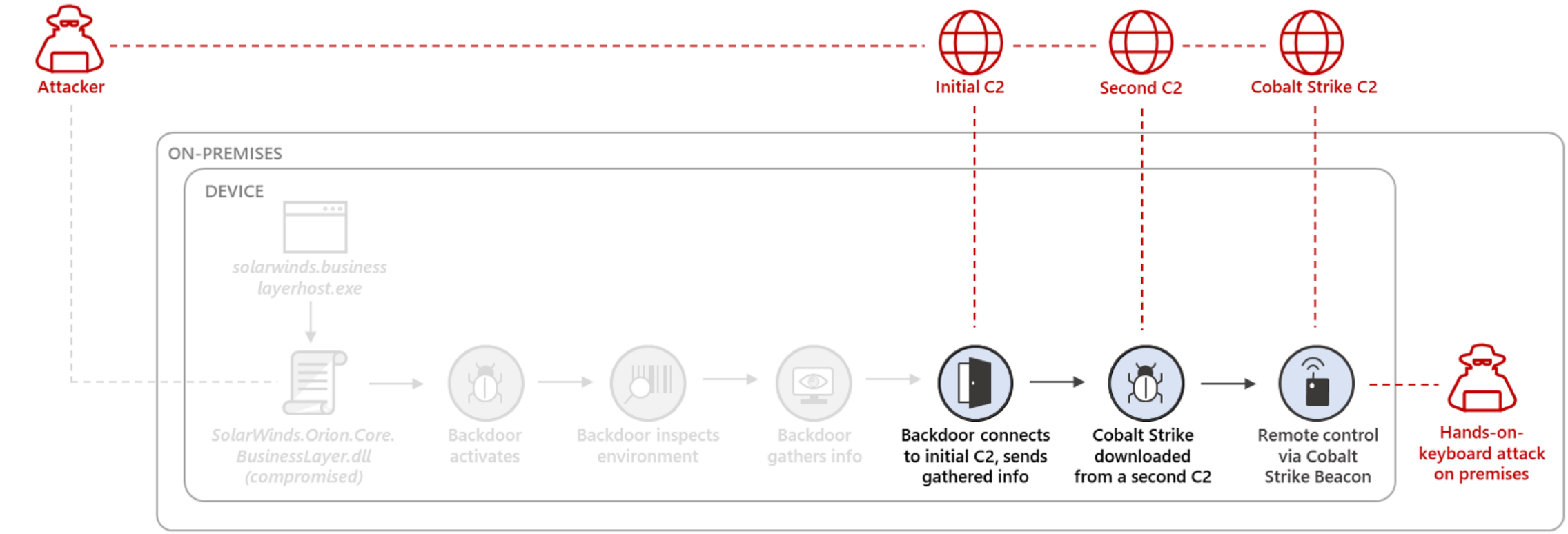
Cybereason – founded by veterans of Israel's 8200 cyber unit – is declining to name.

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/

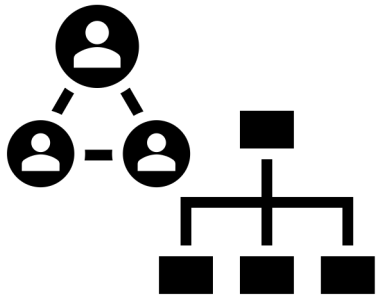
Solarigate Attack C2 Communications



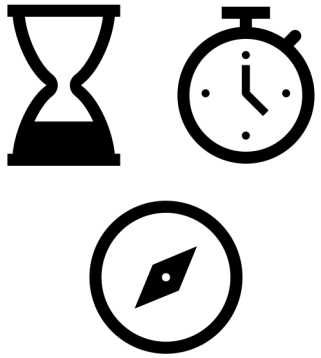
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

Why Do They Stay?

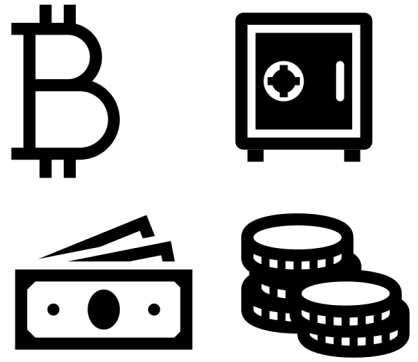
Organisation



Key People



Opportunity

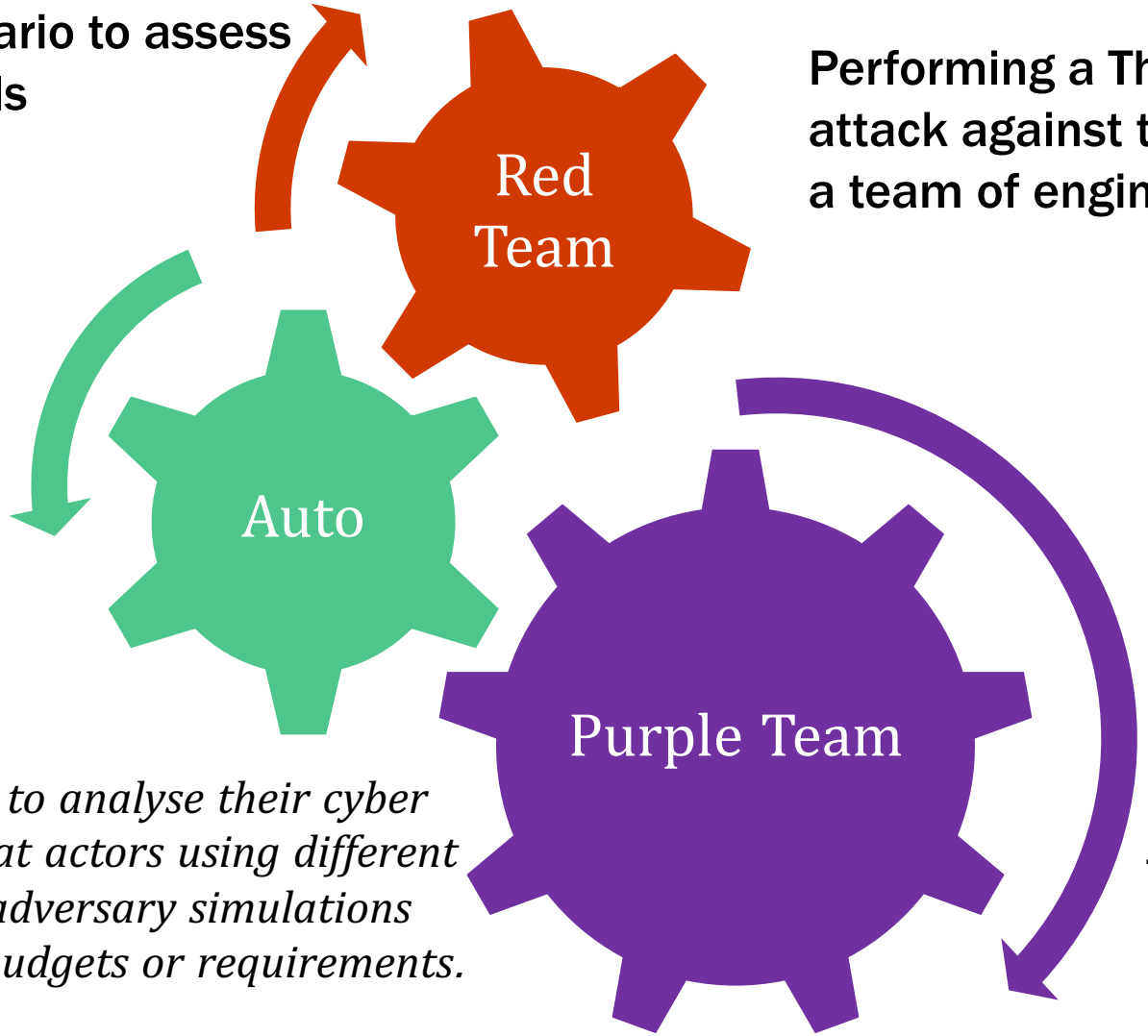


Crown Jewels

AusCERT 2021

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)

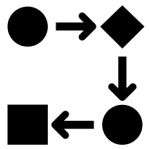
Organisations desire to analyse their cyber defence against threat actors using different implementations of adversary simulations depending on their budgets or requirements.

Operating A Full Scale Red Team Scenario

AusCERT 2021

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

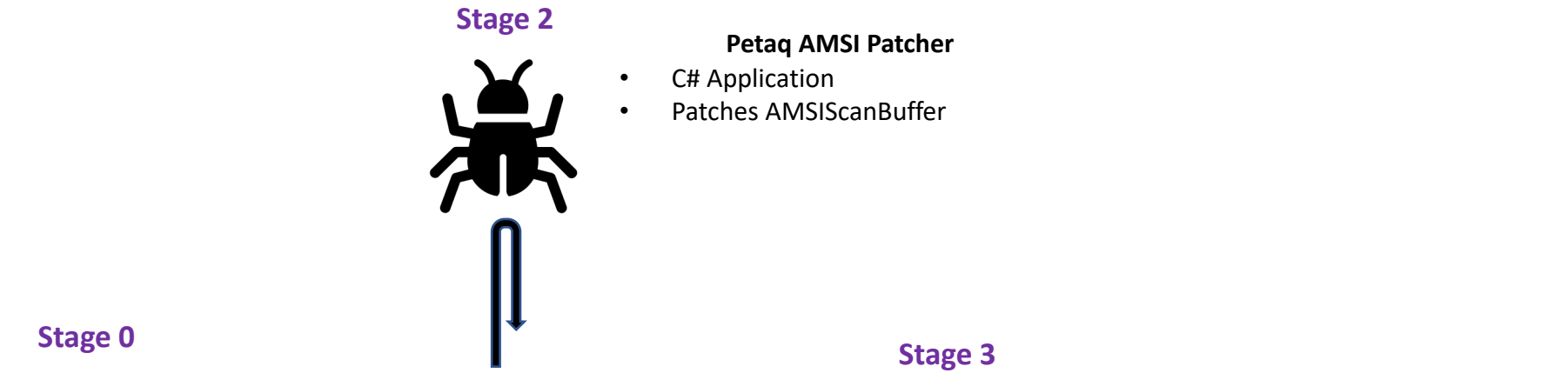
- Techniques
- Tactics
- Procedures

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+ .

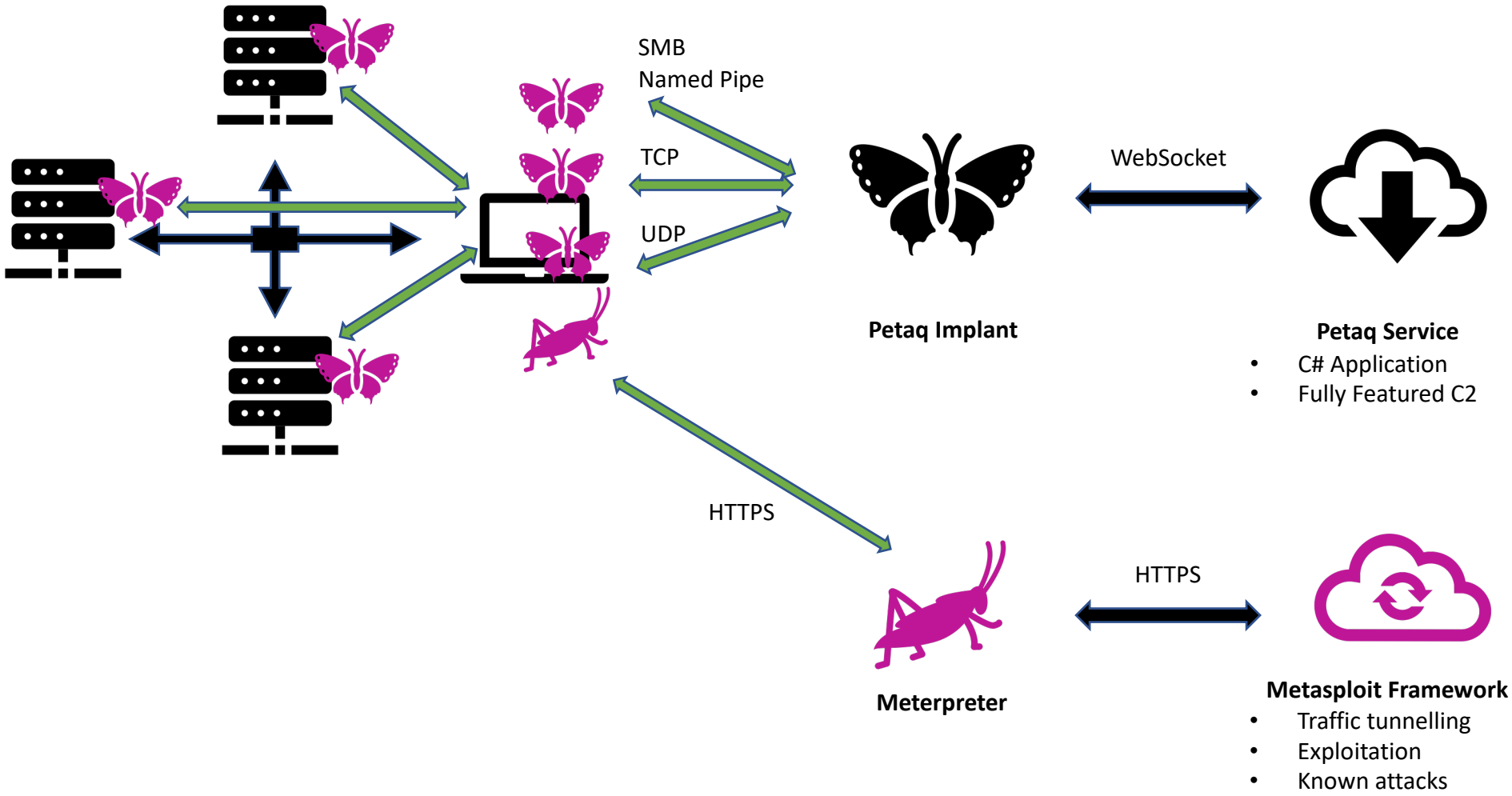
https://github.com/fozavci/ta505plus

Initial Compromise & Defence Evasion

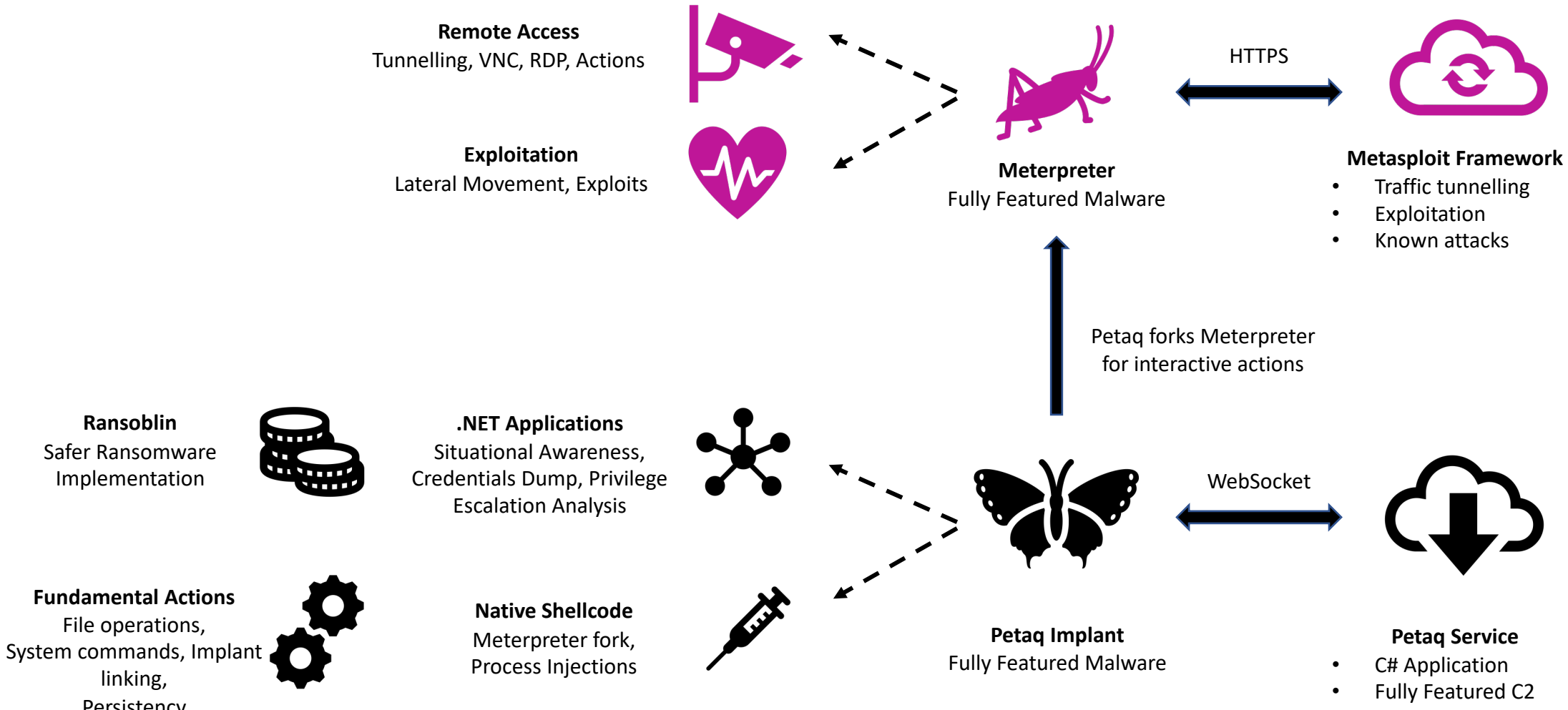


No Initial Windows Defender Detection + Patched/Bypassed Windows Defender + Fileless Malware

Internal Implant Communications

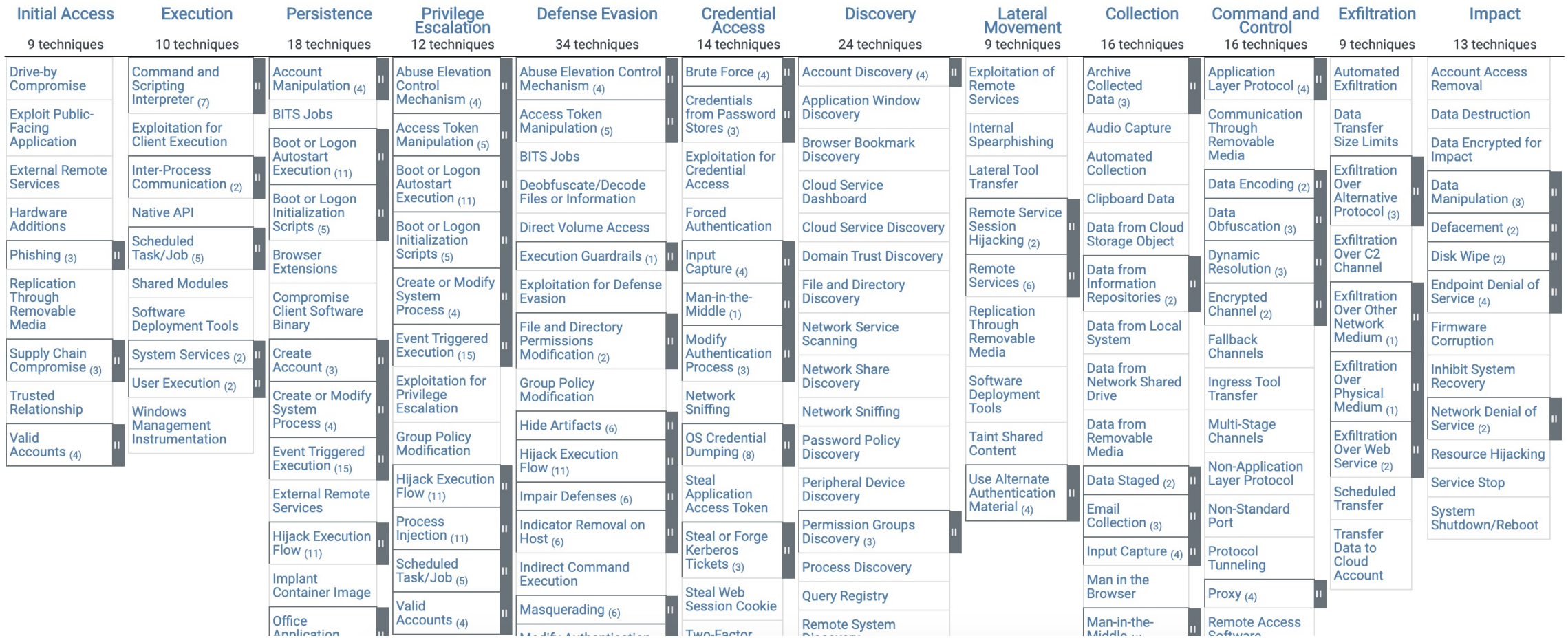


Actions on Objectives



Mitre Att&ck for Tradecraft Mapping

AusCERT 2021



https://attack.mitre.org

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

Petaq C2 and Malware

- Petaq Purple Team Command & Control Server (MIT License)
  - *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*

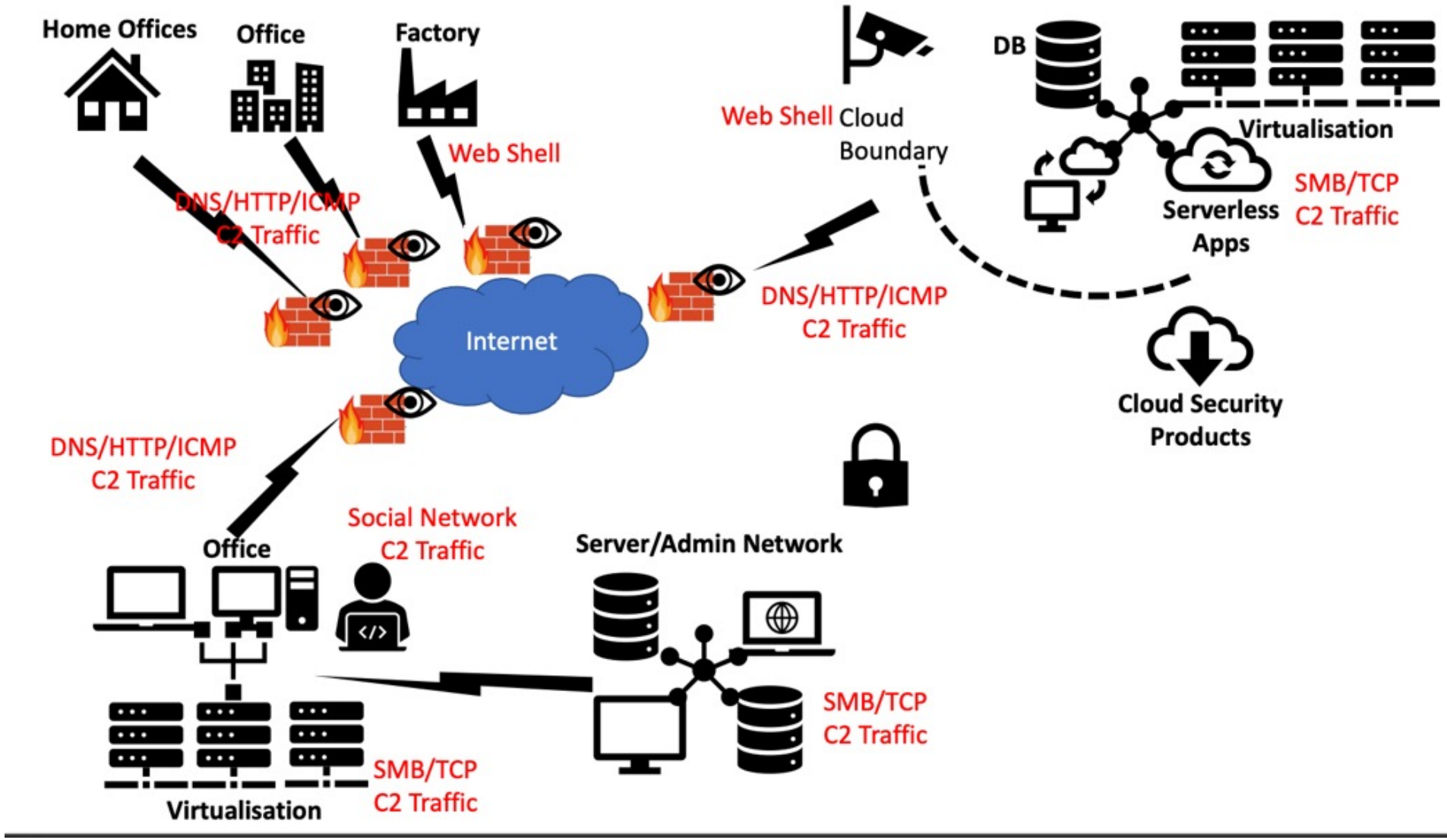
- Petaq is suitable to interactive and scenario based exercises

https://github.com/fozavci/petaqc2

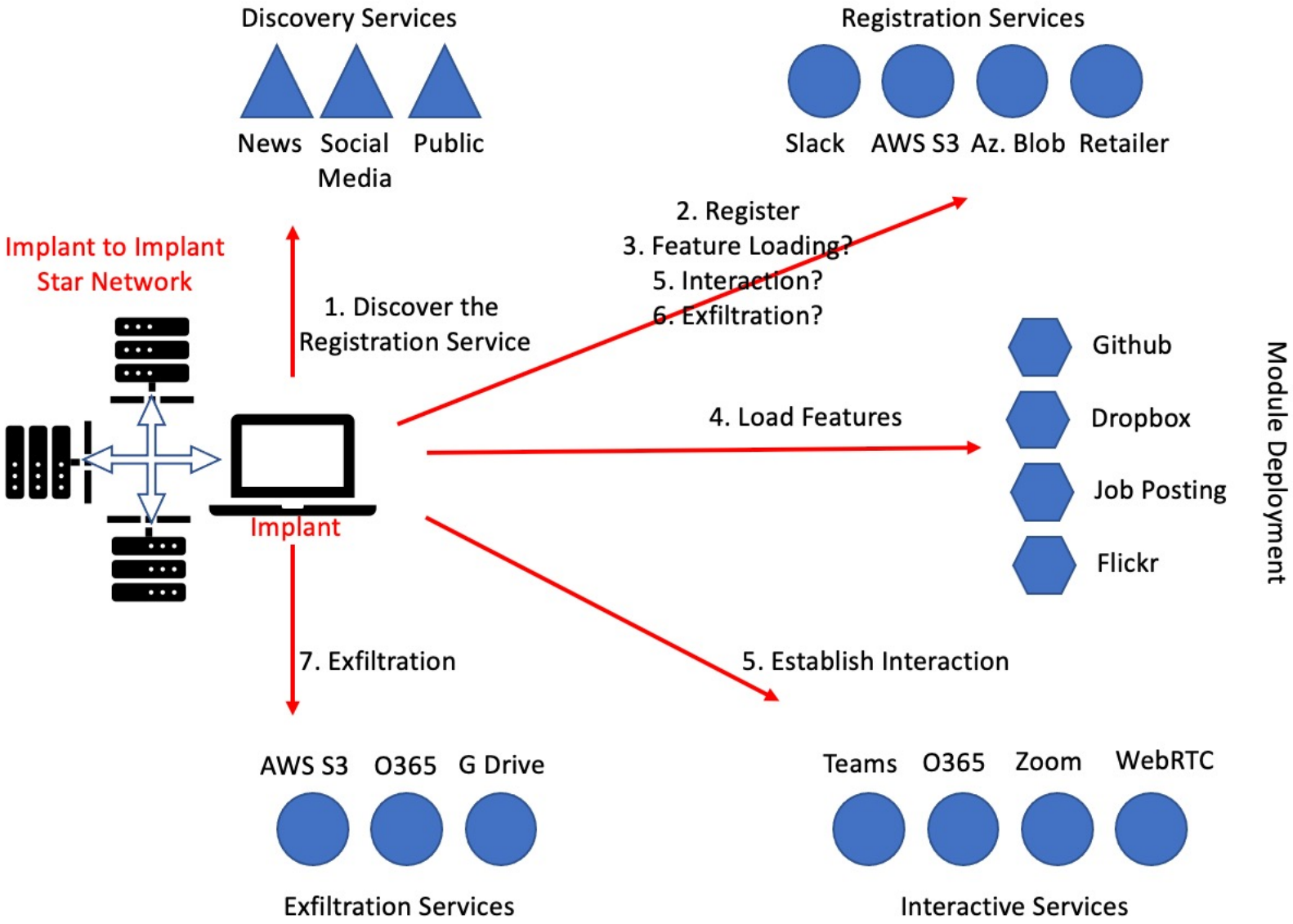
Challenges

- 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

Malware Communications in Cloud & Covid Era



Distributed C2 Approach for Malware



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

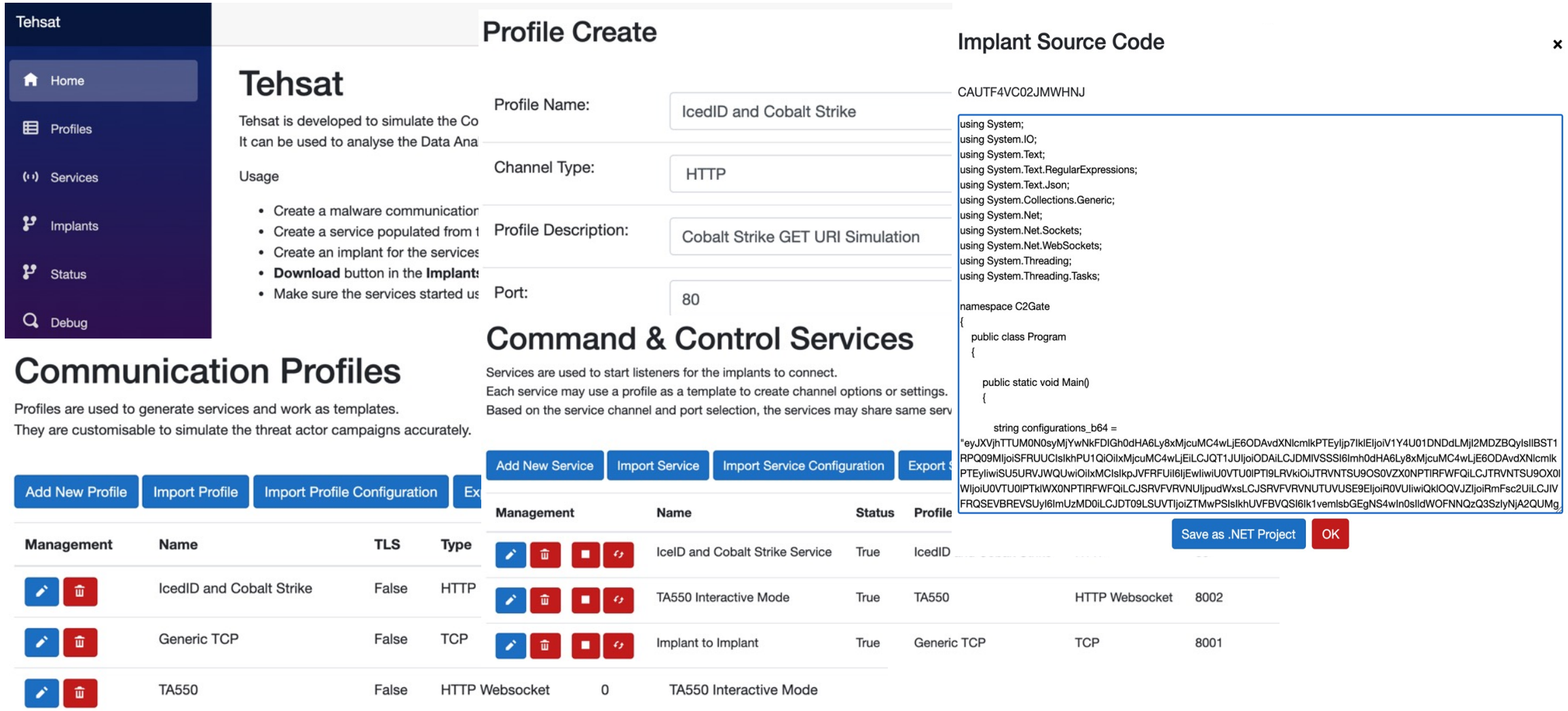
- Challenges
  - Limited Access to Threat Actor Tools and Techniques
  - Simulations for Distributed Networks Hard to Implement
  - No Easy Simulation Tool for Training, Alert Generation or Quick Tests

Tehsat Malware Traffic Generator

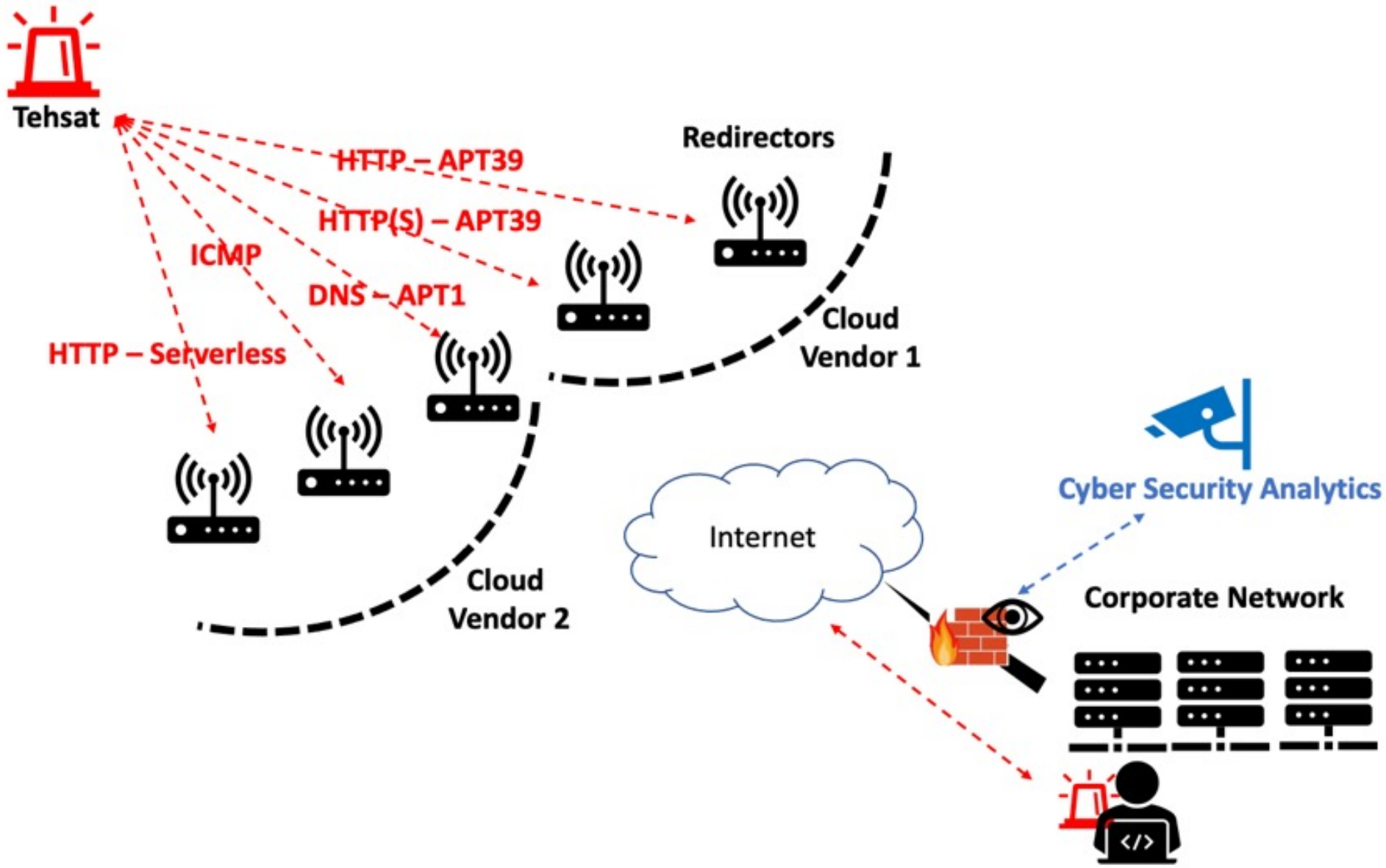
- Tehsat (means **Deception** in Vulcan)
- Graphical Interface to Prepare Malware Communications
  - Various Protocols (HTTP, TCP, UDP, Websocket)
  - Easy and Detailed Customisation (HTTP headers, Request/Response, Agents)
  - Service Creation Using Profiles
  - Friendly Implant Generation per Scenario (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
- Still Work in Progress

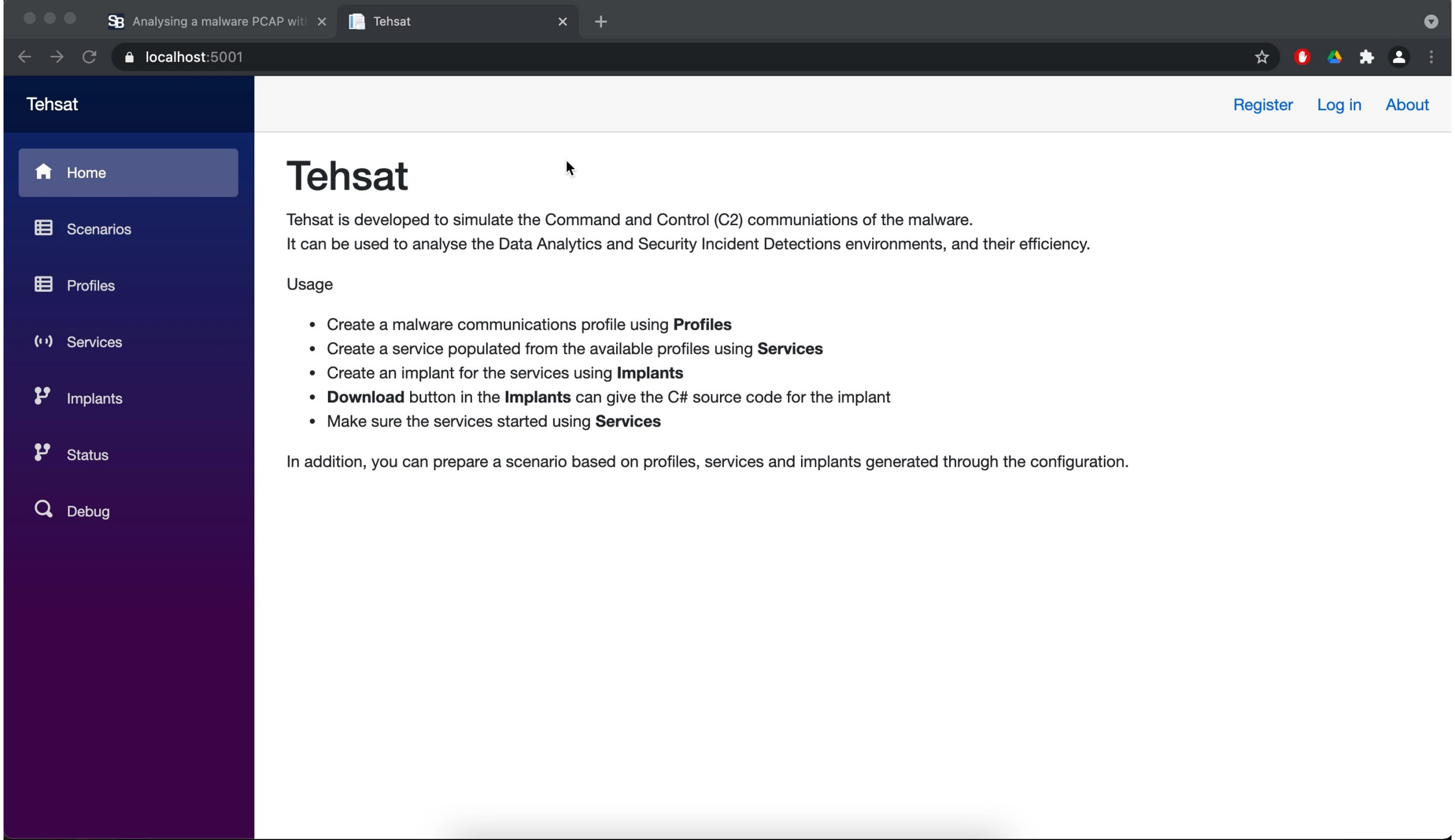
Tehsat Malware Traffic Generator

AusCERT 2021



Tehsat Malware Traffic Generator




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.

References

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

  https://github.com/fozavci/petaqc2

- TA505+ Adversary Simulation Pack
- Paper: Current State of Malware Command and Control Channels and Future Predictions

  https://github.com/fozavci/ta505plus

- Tehsat Malware Traffic Generator
- Paper: Simulating Malware Communications in Distributed Networks

Thanks