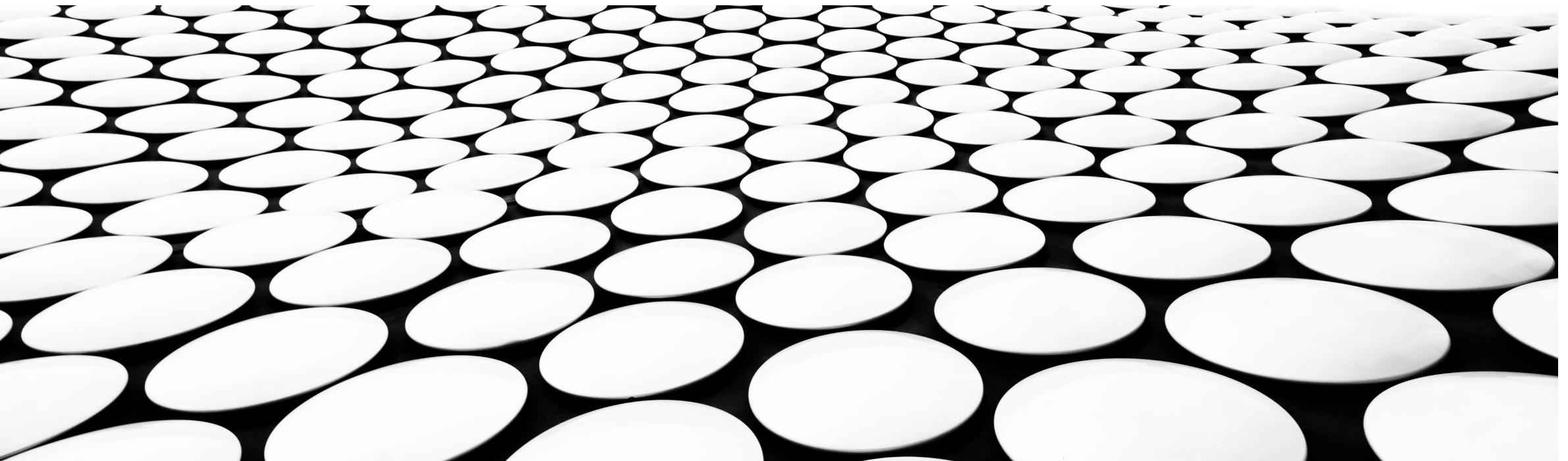


Malware Traffic Generation to Improve Security Incident Detections

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

- 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
 - Viproj VoIP Penetration Testing Kit



Threat Actors and Campaigns

6 new Microsoft's RCE vulnerabilities “Completely Penetrated” by Cyber criminals spend three months lurking in target networks

Cyber crime
COVID crisis



By **Ev**
Contrib

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

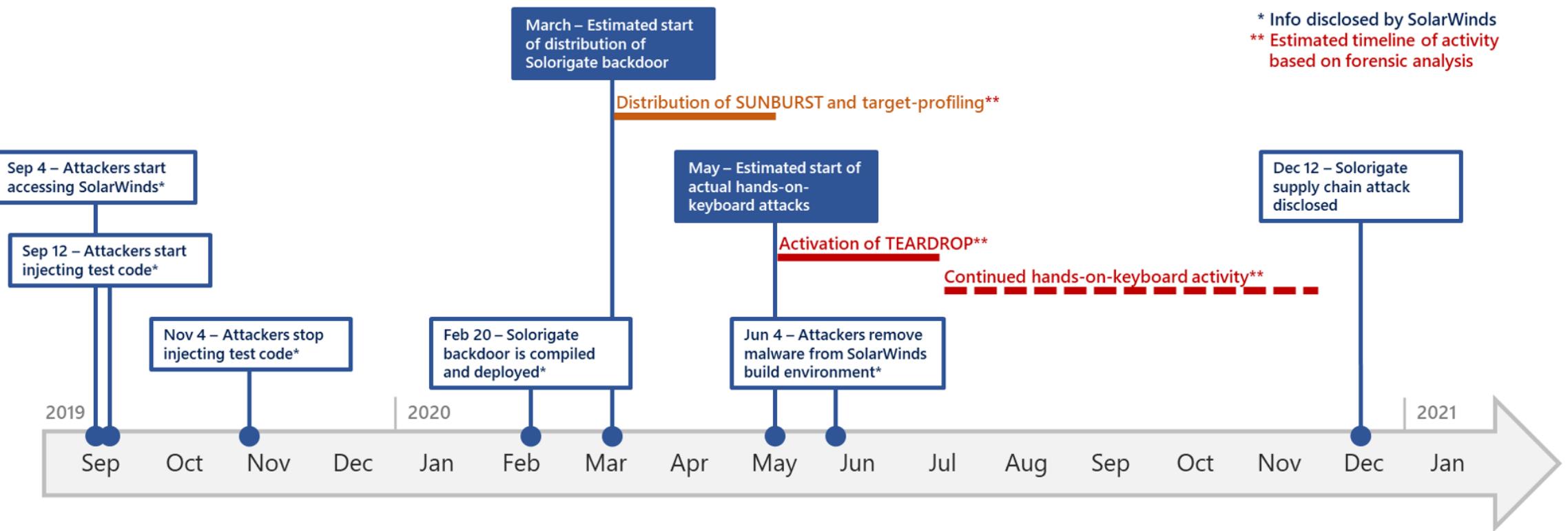
By **Alex Scroxton**, Security Editor

Published: 14 Jan 2020 13:00

DART said it has been co-sponsored advanced persistent threat actors and persisted in its network for eight months despite efforts to remove it.

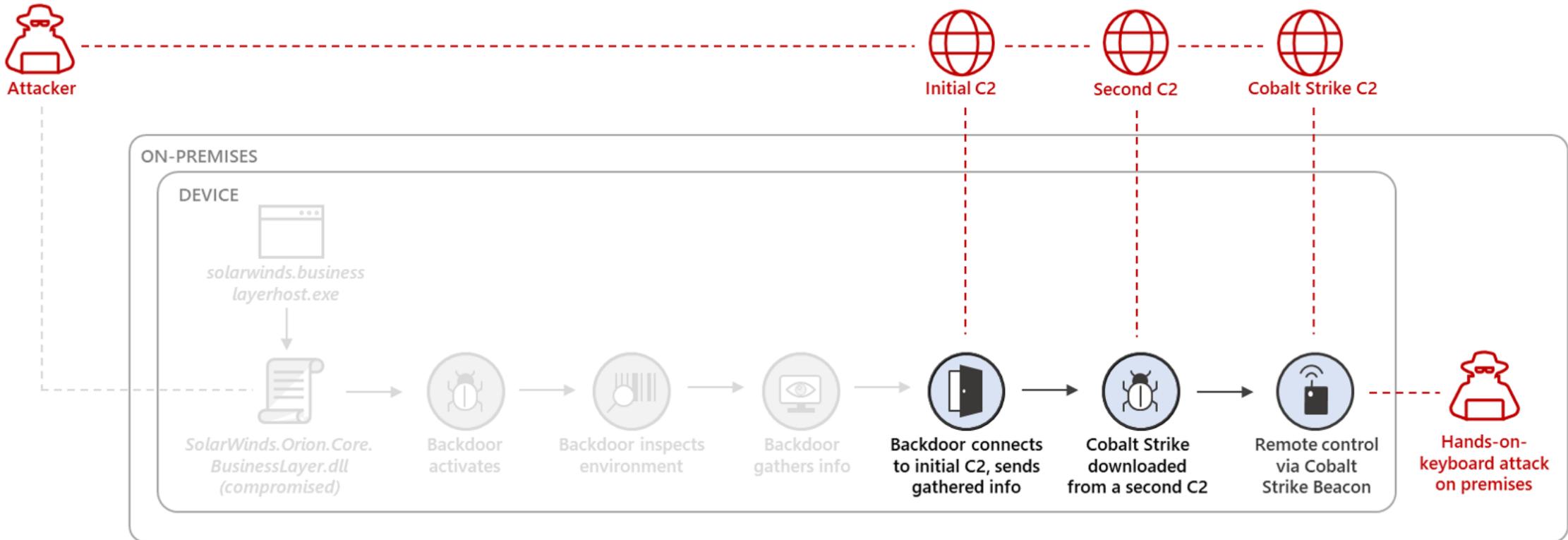
Cybereason – founded by veterans of Israel’s 8200 cyber unit – is declining to name.

Solarigate Attack Timeline



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

Solarigate Attack C2 Communications

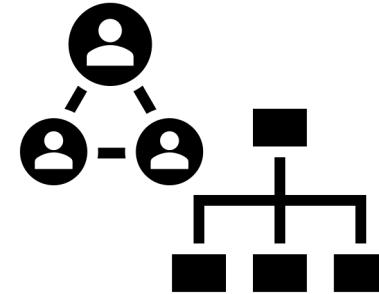


<https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solarigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>

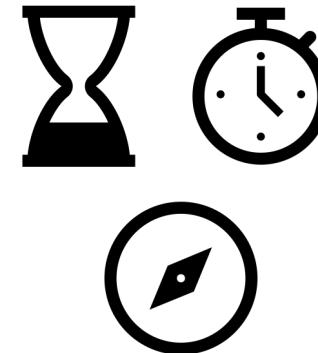
Why Do They Stay?



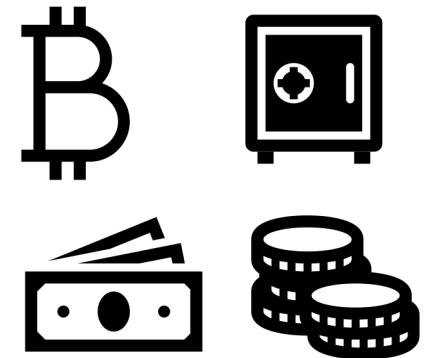
Organisation



Key People



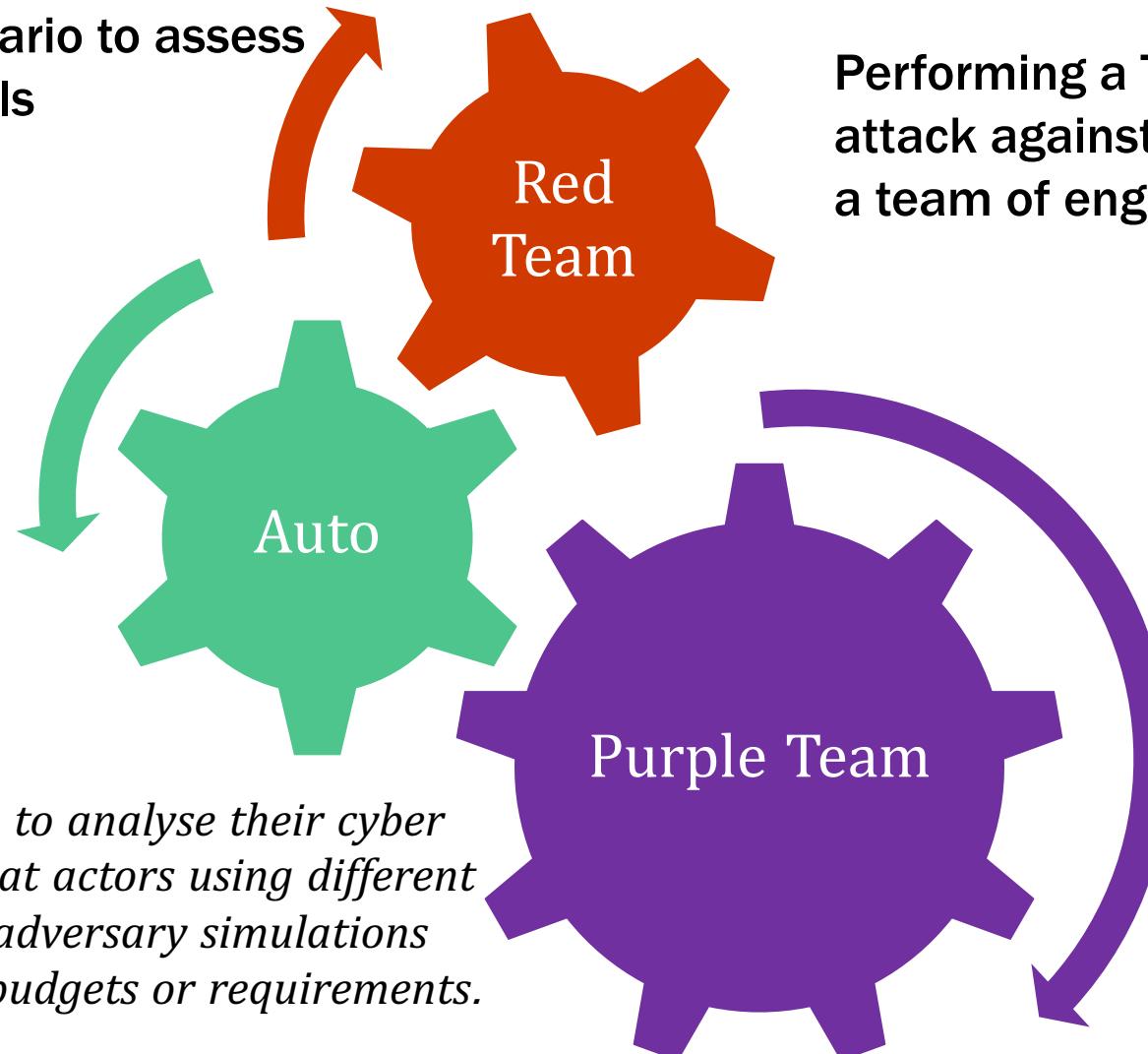
Opportunity



Crown Jewels

Adversary Simulation Types

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

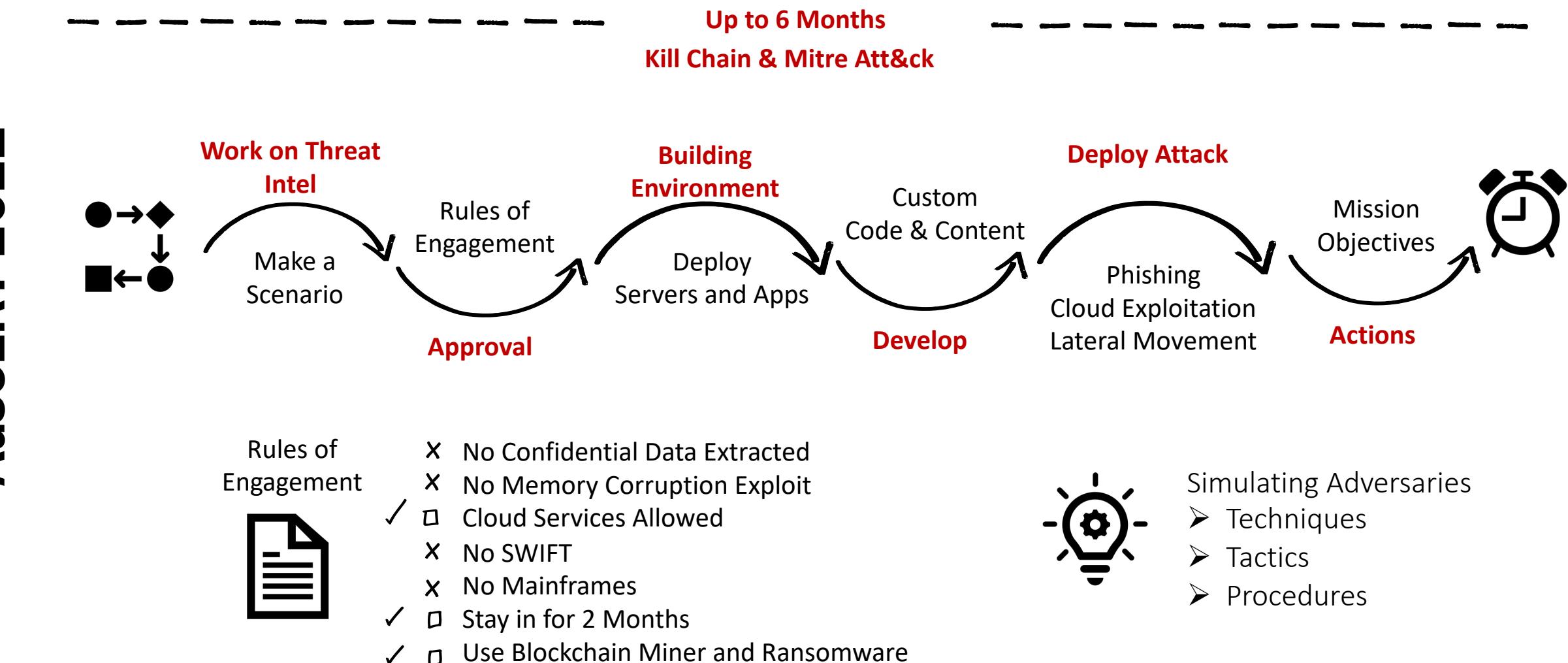


Performing a Threat Intelligence-Led cyber attack against the targeted environment with a team of engineers (CBEST, CORIE, ICAST)

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)

Operating A Full Scale Red Team Scenario

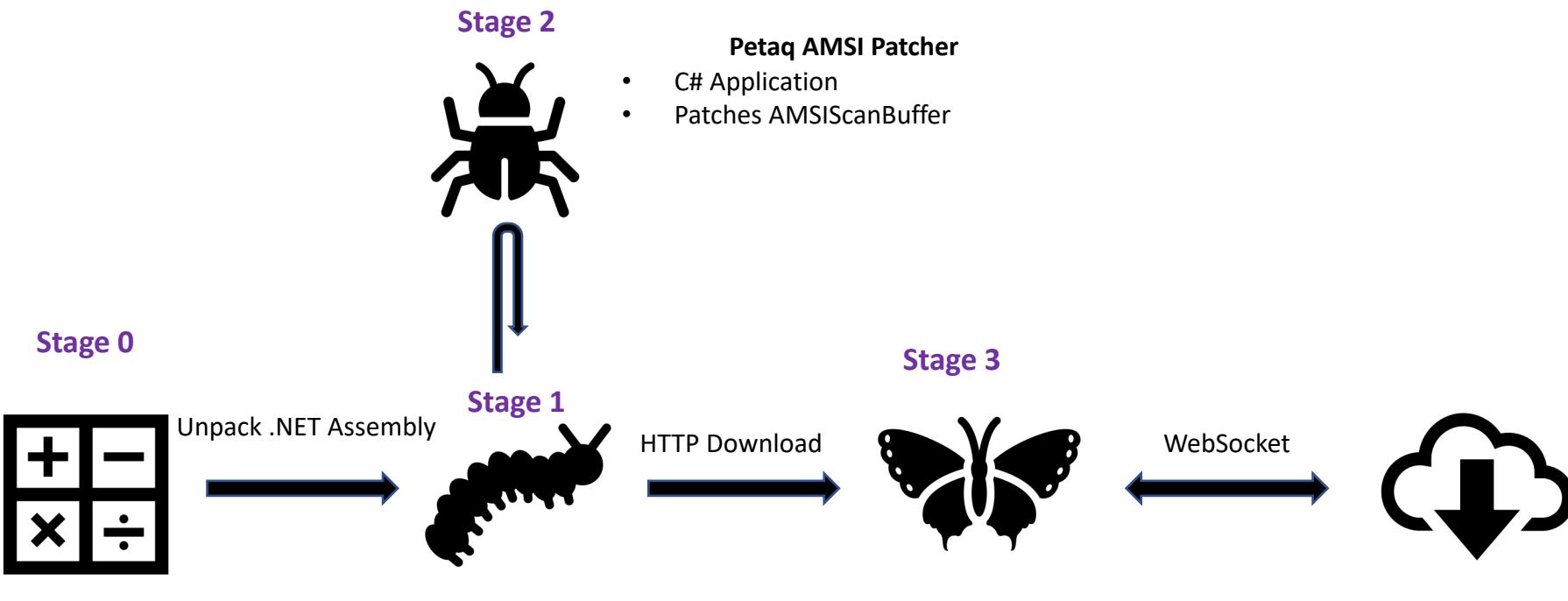


TA505+ Adversary Simulation Pack

- TA505 is a threat group actively targeting financial institutions, including Australia, since 2014 using custom tools (e.g. FlawedAmmeyy , 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

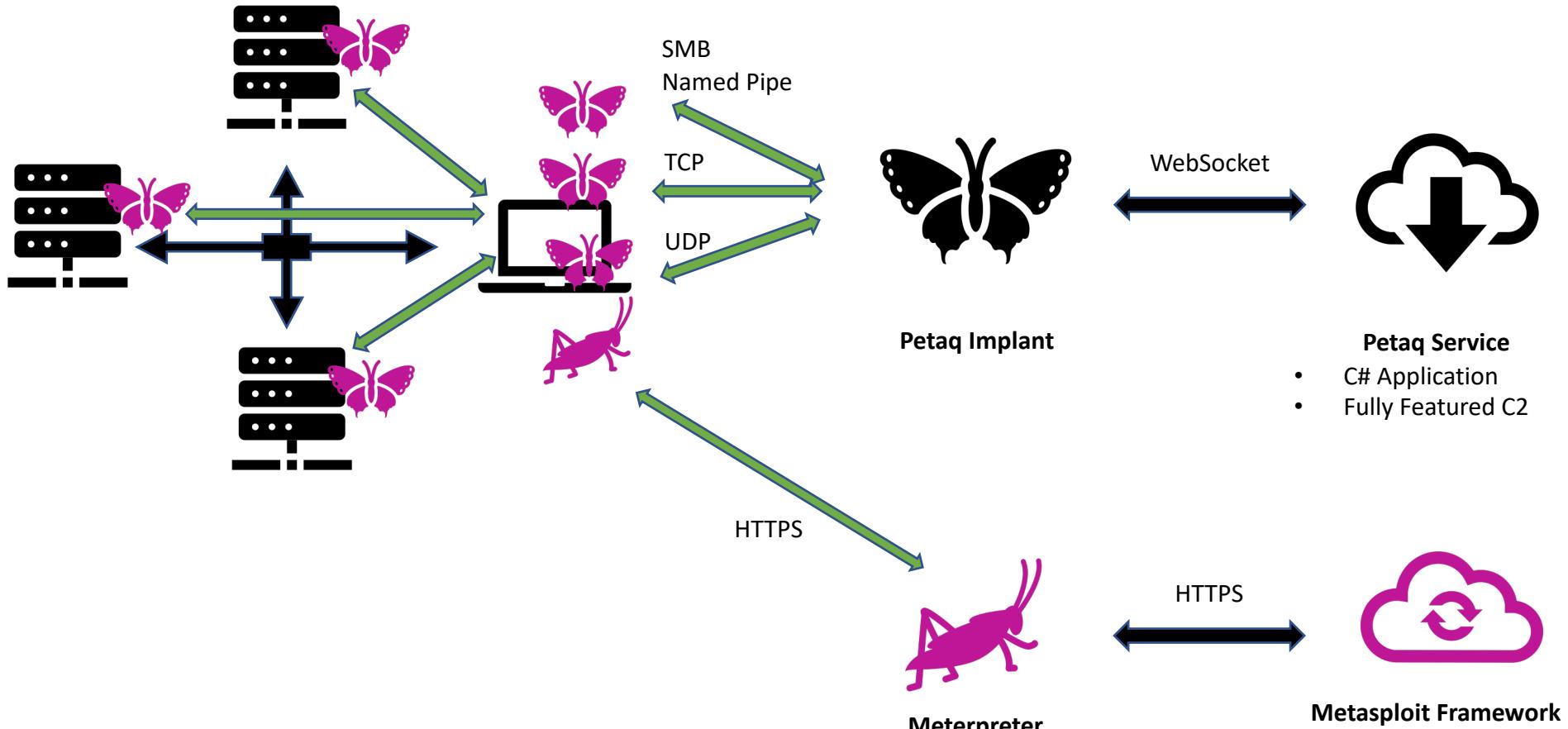


No Initial Windows Defender
Detection

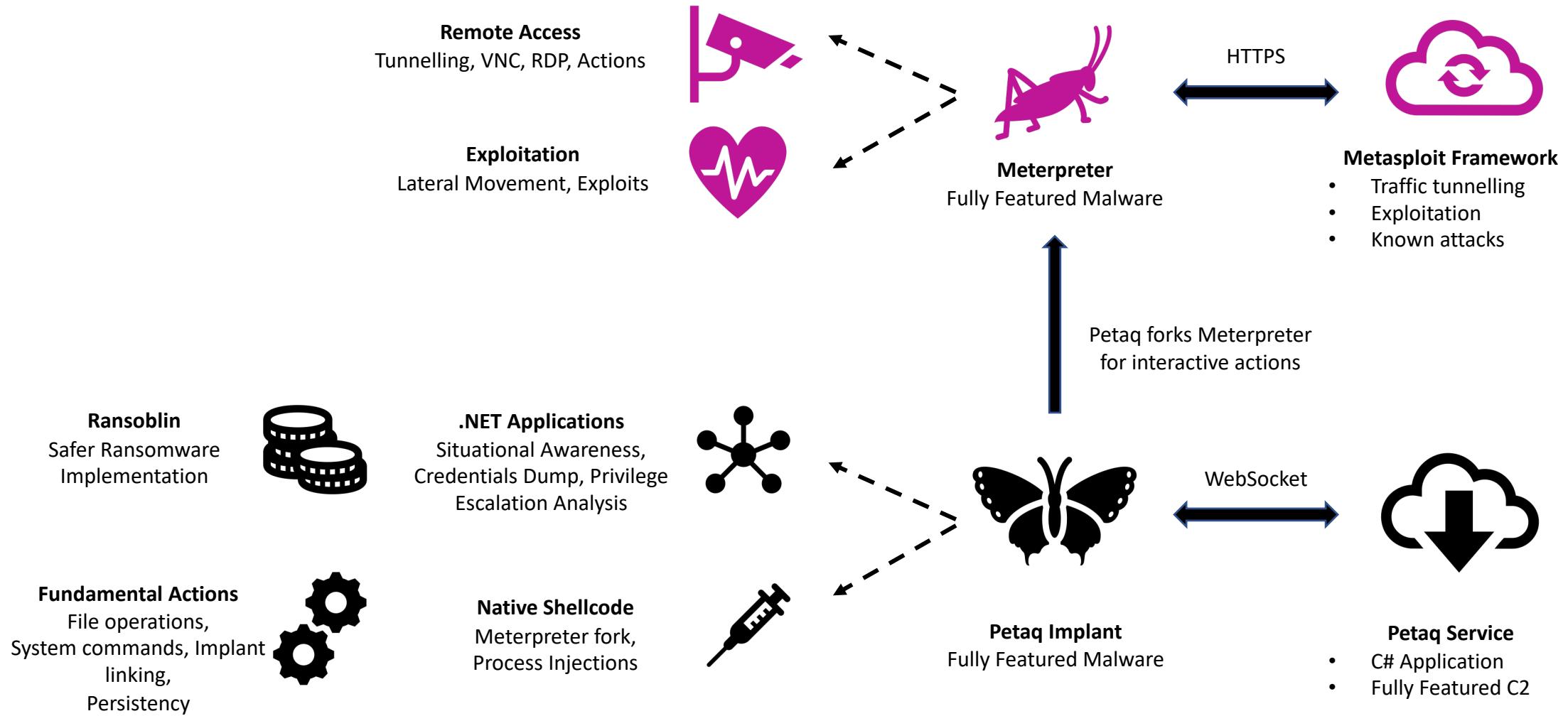
+
Patched/Bypassed
Windows Defender

+
Fileless Malware

Internal Implant Communications



Actions on Objectives



Mitre Att&ck for Tradecraft Mapping

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

<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

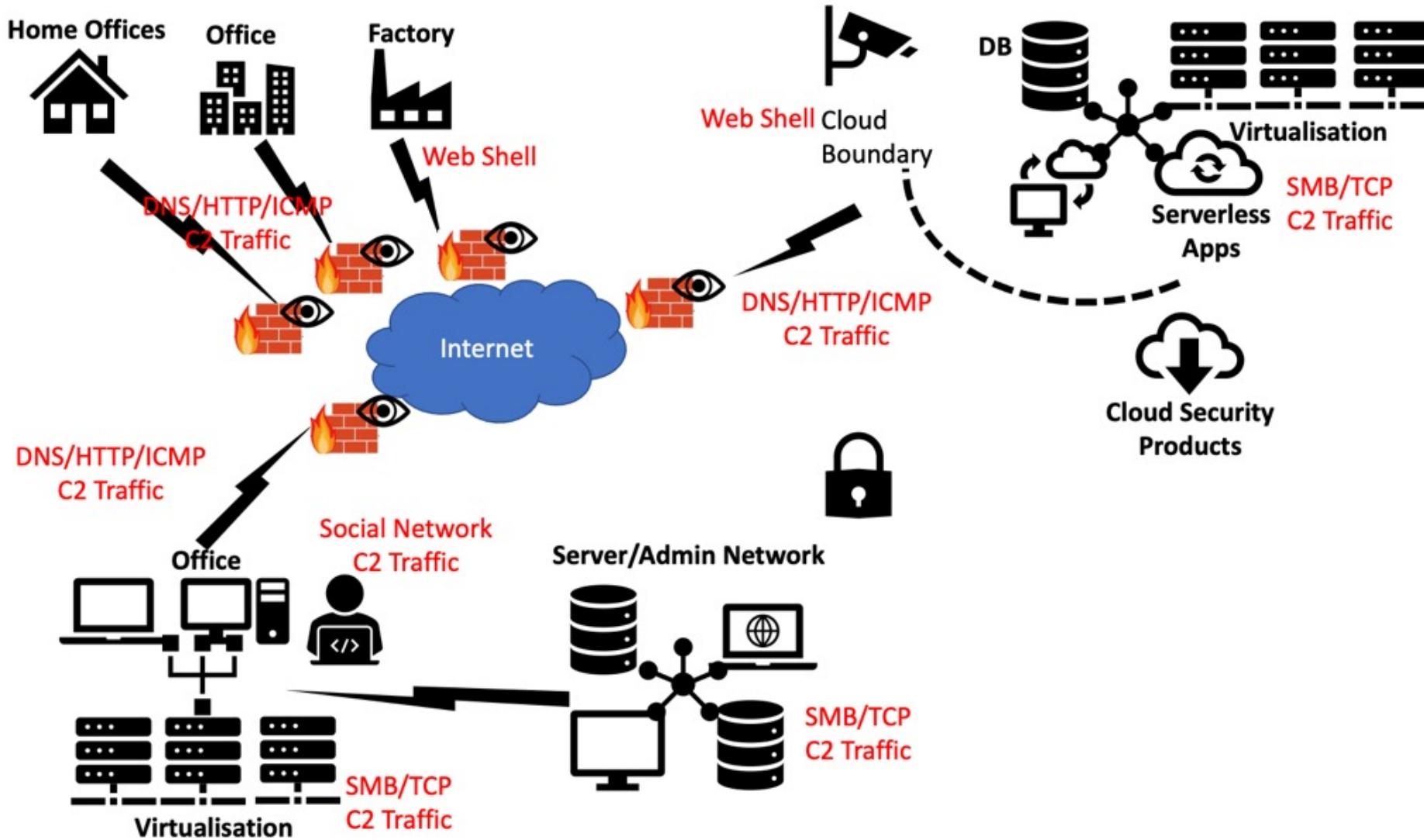
- Petaq Purple Team Command & Control Server (MIT License)
 - *P'takh (petaQ) is a Klingon insult, meaning something like "weirdo"*
 - *Protocols : HTTP(S), WebSocket, SMB Named Pipe, TCP, UDP*
 - *Execution : CMD, .NET Assembly, Source, Shellcode Injection, PowerShell*
 - *Features : WMI Lateral Movement,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

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

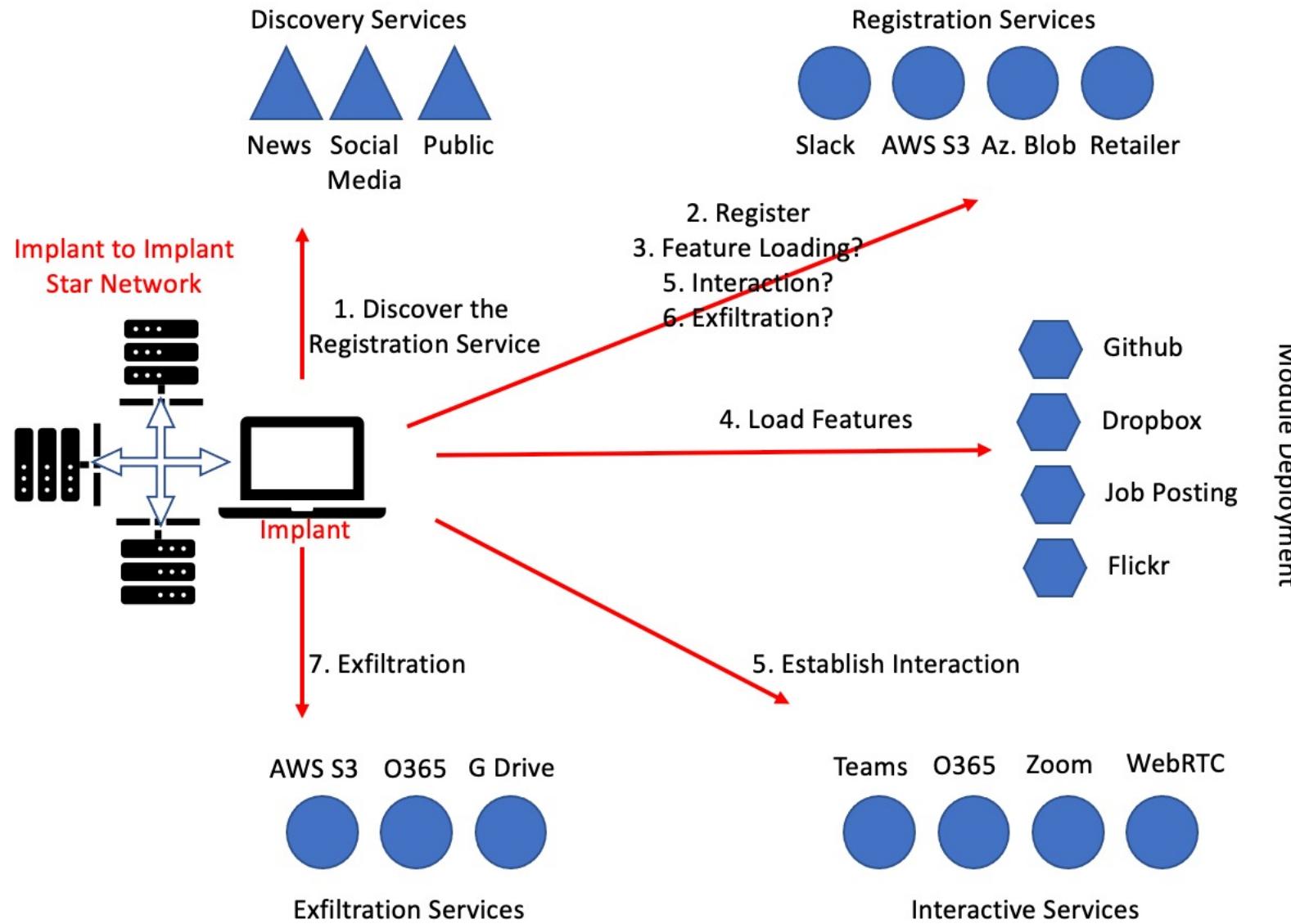
Challenges

- 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

Tehsat

- Home
- Profiles
- Services
- Implants
- Status
- Debug

Tehsat

Tehsat is developed to simulate the Cobalt Strike implant. It can be used to analyse the Data Analysis.

Usage

- Create a malware communication
- Create a service populated from the implants
- Create an implant for the services
- Download button in the Implant**
- Make sure the services started up correctly

Profile Create

Profile Name: IcedID and Cobalt Strike

Channel Type: HTTP

Profile Description: Cobalt Strike GET URI Simulation

Port: 80

Command & Control Services

Services are used to start listeners for the implants to connect. Each service may use a profile as a template to create channel options or settings. Based on the service channel and port selection, the services may share same service.

Add New Service	Import Service	Import Service Configuration	Export Service
IcedID and Cobalt Strike Service	True	IcedID	Save as .NET Project OK
TA550 Interactive Mode	True	TA550	HTTP Websocket 8002
Implant to Implant	True	Generic TCP	TCP 8001
TA550	0	TA550 Interactive Mode	

Implant Source Code

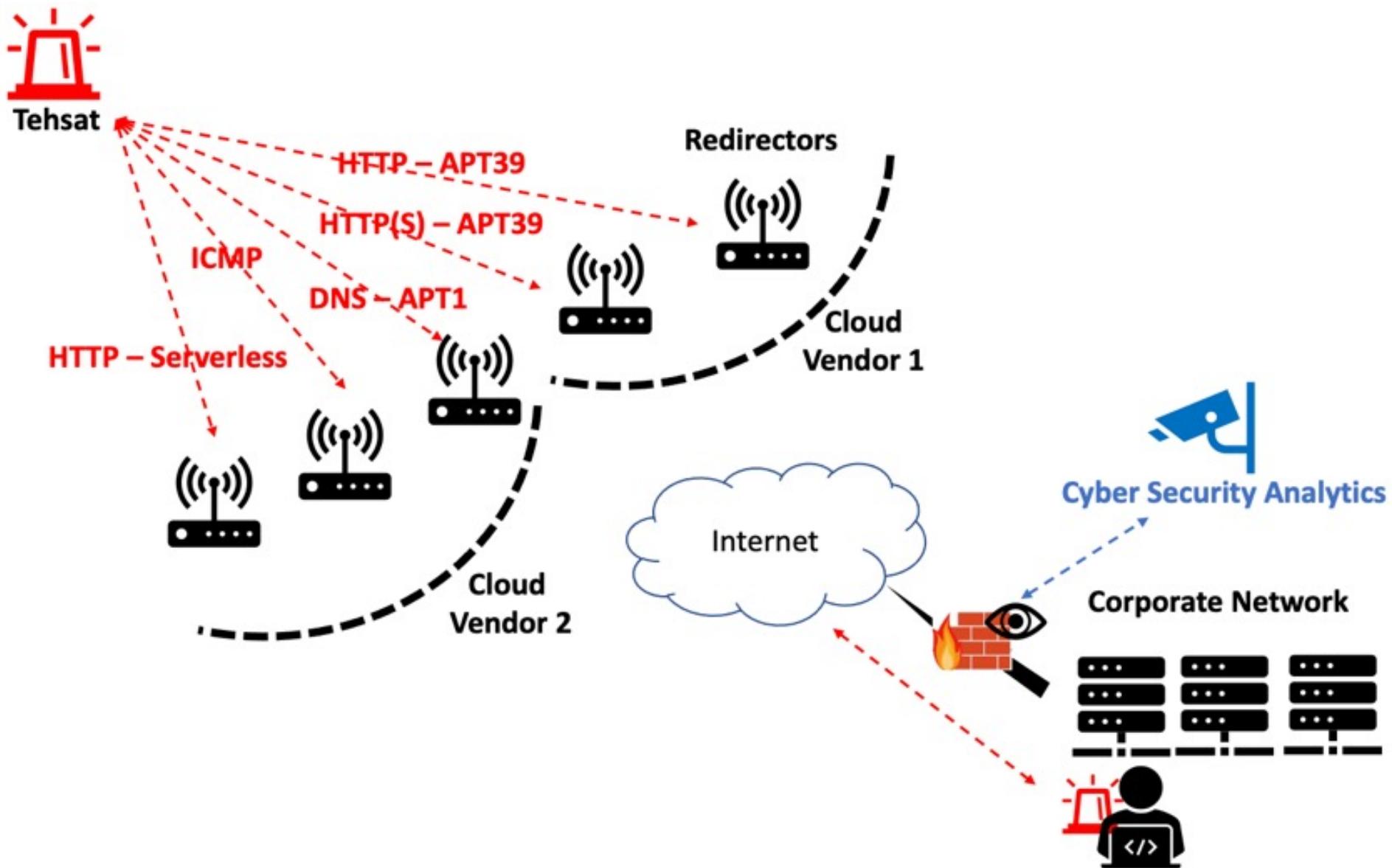
```
CAUTF4VC02JMWHNJ

using System;
using System.IO;
using System.Text;
using System.Text.RegularExpressions;
using System.Text.Json;
using System.Collections.Generic;
using System.Net;
using System.Net.Sockets;
using System.Net.WebSockets;
using System.Threading;
using System.Threading.Tasks;

namespace C2Gate
{
    public class Program
    {
        public static void Main()
        {

            string configurations_b64 =
"eyJXjhTTUMONosyMjYwNkFDIGh0dHA6Ly8xMjcuMC4wLjE6ODAvdXNlcmkPTEyIjp7IkIEljoiv1Y4U01DNDdLMjI2MDZBQylsIIBST1RPQ09MljoISFRUUClslkhPU1QiOlxMjcuMC4wLjEiLCJQT1JUljoODAiLCJDMyVSSl6lmh0dHA6Ly8xMjcuMC4wLjE6ODAvdXNlcmkPTEyliwiSU5URVJWQUwiOlxMclslkpJVFRFUil6IjEwlwiU0VTU0PTl9LRVkiOjTRVNTSU9OS0VZX0NPTIRFWFQlCJTRVNTSU9OX0IWljoUVTU0lPTkIWXONPTIRFWFQlCJSRVFVRVNUpudWxsLCJSRVFVRVNUTUVUSE9EljoirOVUliwiQklOCVJZljoirFnsc2UiLCJIVFRQSEVBREVSLy6ImUzMD0lCJDT09LSUVTijoZTMwPSlslkhuUVFBVQSI6Ik1vemlsbGEgNS4wln0sllwOFNNQzQ3SzlyNja2QUMg";
```

Tehsat Malware Traffic Generator





Home



Scenarios



Profiles



Services



Implants



Status



Debug

Tehsat

Tehsat is developed to simulate the Command and Control (C2) communications 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

