TA505+ Adversary Simulation

Fatih Ozavci

https://linkedin.com/in/fozavci

https://github.com/fozavci

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+ .
- Threat Intelligence Reports about TA505
  - https://attack.mitre.org/groups/G0092/
  - https://www.cybereason.com/blog/threat-actor-ta505-targets-financial-enterprises-using-lolbins-and-a-new-backdoor-malware
  - https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader
  - https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf

Kill Chain Implementation for TA505+

1

Reconnaissance

- Collecting Threat Intelligence
- Tradecraft mapping for TA505

2

Weaponization

- Preparing Excel File
- Developing Petaq Loader
- Developing Petaq AMSI Patcher
- Developing Ransoblin

3

Delivery

- Assume Breach (User executes)
- Delivering the Excel file via Web
- Petaq Implant lands as stages
- Petaq Service used for delivery

4

Exploitation

- Excel file gets executed by User
- Petaq Loader runs AMSI patch
- Petaq Loader runs Petaq Implant

5

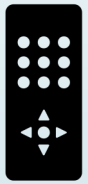
Installation

- Petaq Implant adds itself to Registry

6

Command & Control

- Petaq Service drives Petaq Implant
- Runs .NET Applications in memory
- Forks Metasploit Framework sessions



7

Actions on Objectives

- .NET and PowerShell Applications
- Ransoblin runs for ransoming files
- Metasploit Framework used for exploits, VNC, RDP

Locheed Martin – Kill Chain: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

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 replacing Get2	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	
T1059.001	Command and Scripting Interpreter: PowerShell	PowerUp for privilege escalation enumeration
T1059.005	Command and Scripting Interpreter: Visual Basic	
T1059.007	Command and Scripting Interpreter: JavaScript/JScript	
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	
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

Applications Developed & Customised

Petaq Dropper

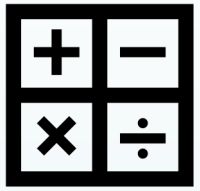
- C# Application
- Loads .NET Assemblies (Implant & AMSI patcher)
- https://github.com/fozavci/ta505plus

Petaq Implant

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

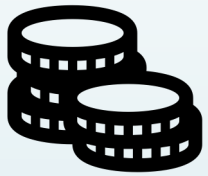
Petaq Service

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



Malicious Excel File

- Excel 4.0 Macro
- Generated using ExcelntDonut
- https://github.com/fozavci/ta505plus



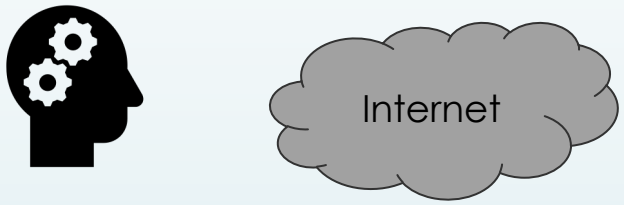
Ransoblin

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

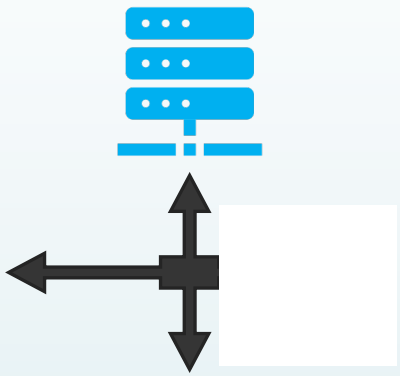
Petaq AMSI Patcher

- C# .NET 2.0 Application
- Patches AMSIScanBuffer
- https://github.com/fozavci/petaq_amsi

Target Environment



Internet



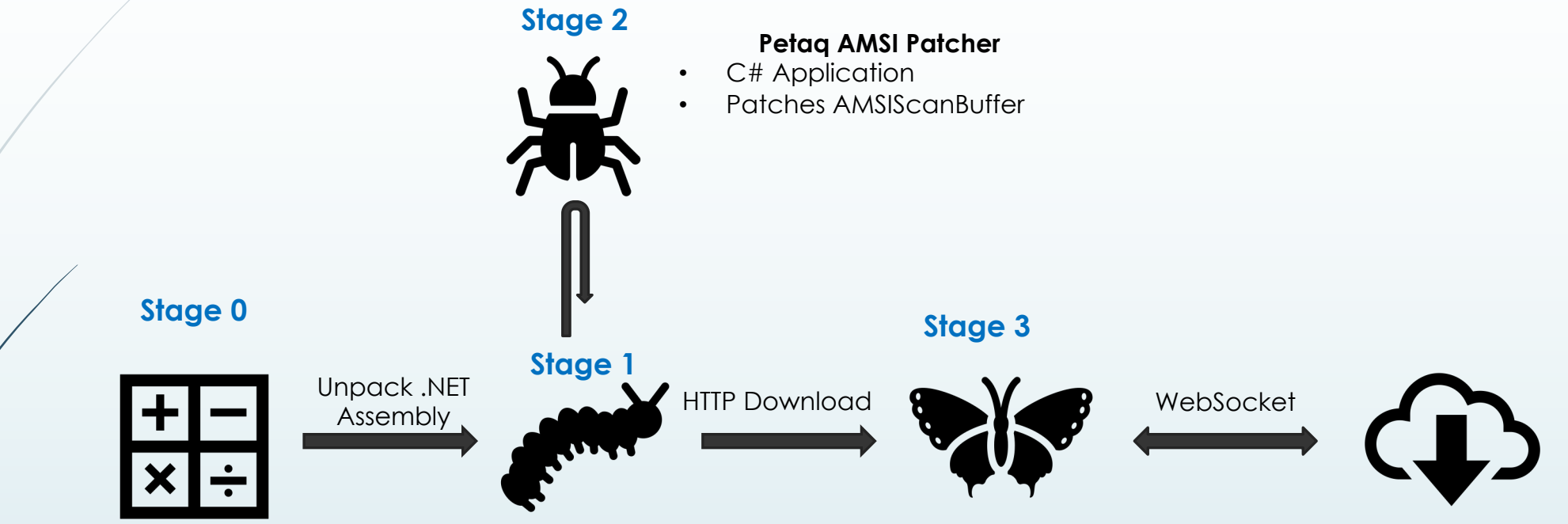
Production Server
- Windows 2008
- Metasploitable 3
- 172.28.128.2

Attacker
- Kali Linux 2020.2
- Petaq Purple Team C2/Malware
- Metasploit Framework
- 172.16.168.134

Employee Laptop (Protected)
- Up-to-date Windows 10
- Up-to-date Windows Defender
- Up-to-date Office 2019
- 172.16.168.198
- 172.28.128.254

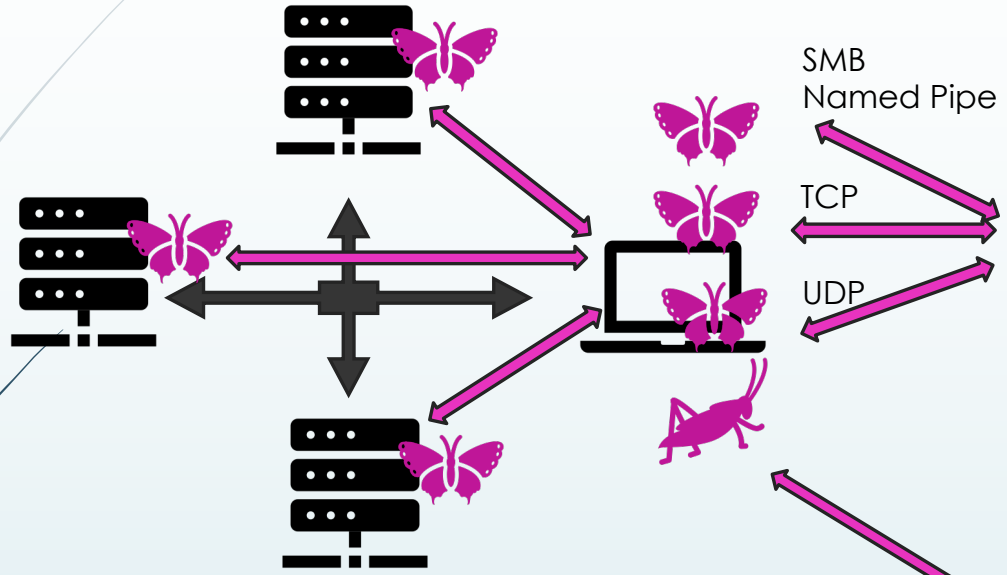
Application Server
- Ubuntu Linux 14.04
- Metasploitable 3
- 172.28.128.3

Initial Compromise & Defence Evasion



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

Internal Implant Communications



SMB
Named Pipe

TCP

UDP

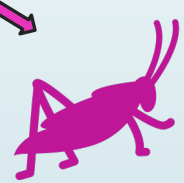
Petaq Implant

WebSocket

Petaq Service

- C# Application
- Fully Featured C2

HTTPS



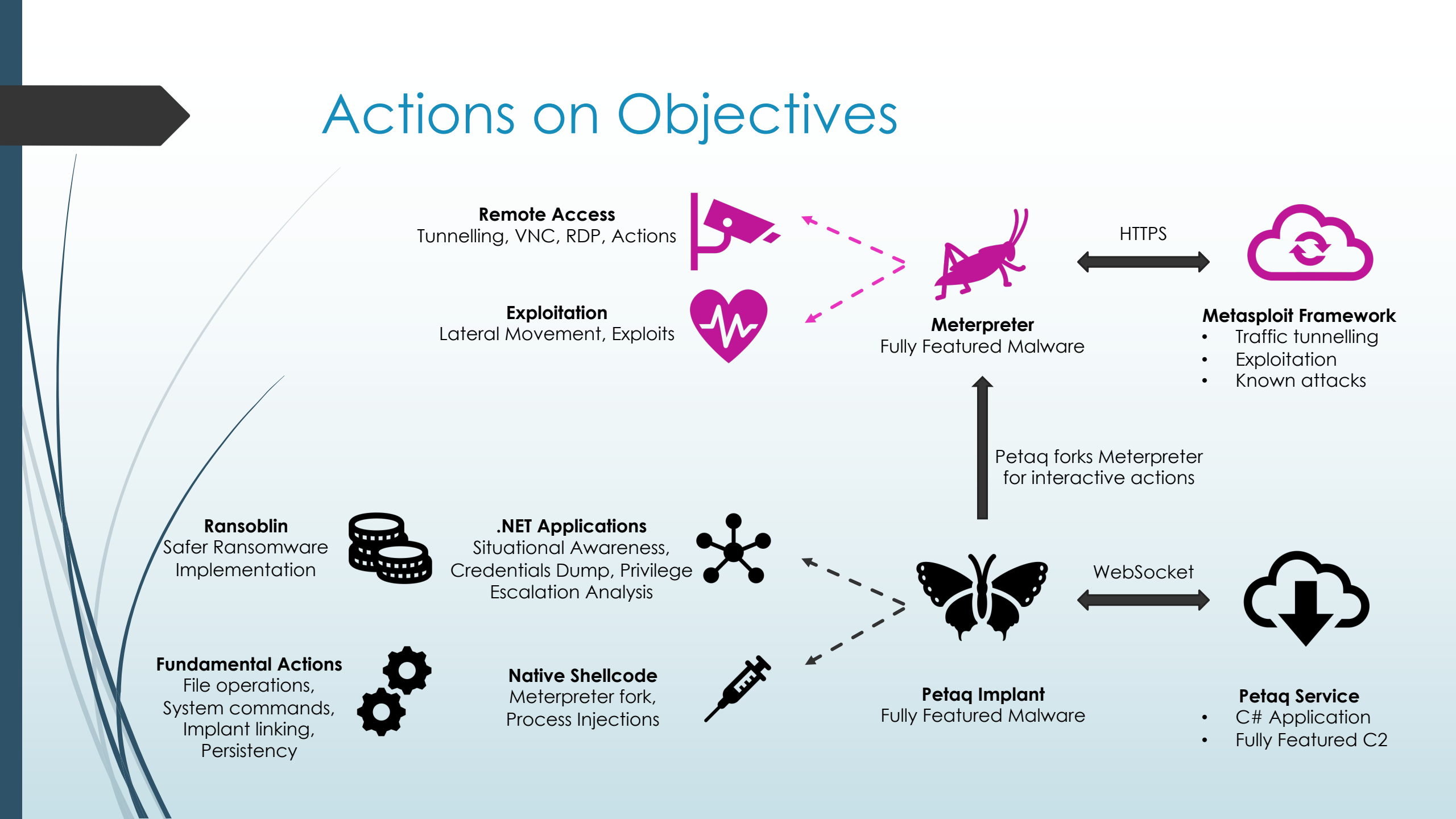
Meterpreter

HTTPS

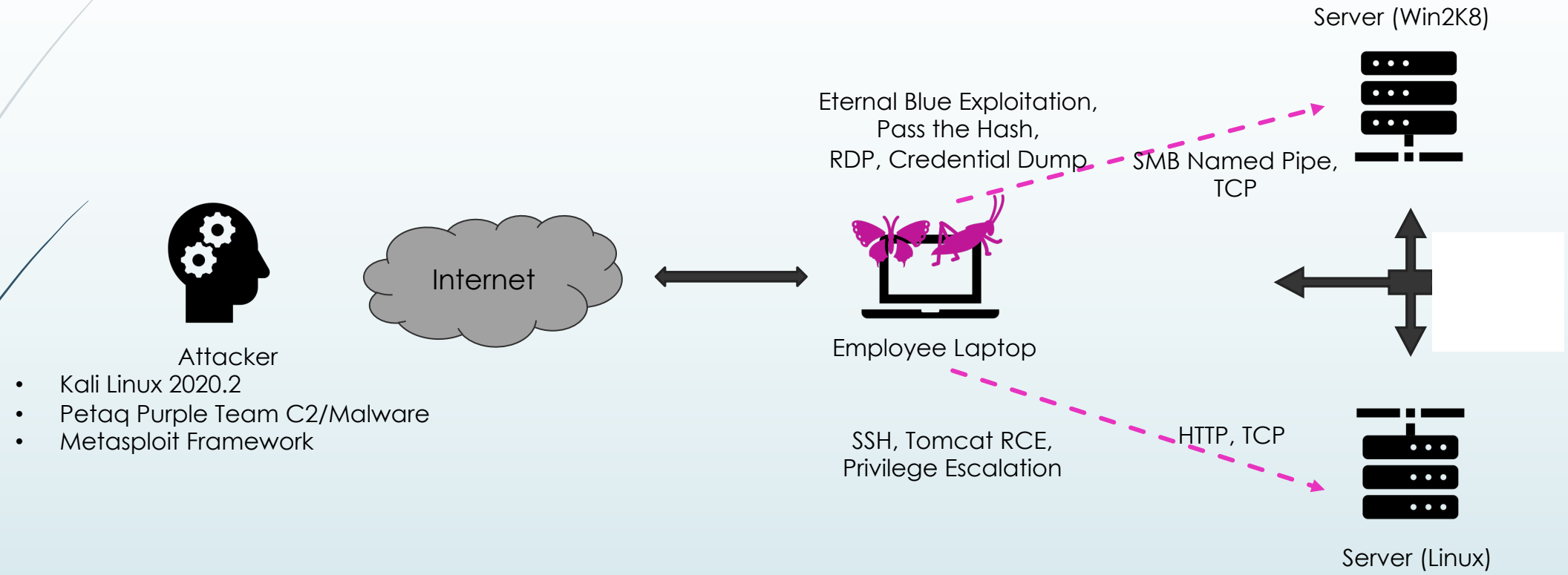
Metasploit Framework

- Traffic tunnelling
- Exploitation
- Known attacks

Actions on Objectives



Lateral Movement



- Kali Linux 2020.2
- Petaq Purple Team C2/Malware
- Metasploit Framework

Defence Evasion Techniques

- Anti-Malware Scan Interface (AMSI)
  - Used by Anti-Virus software such as Windows Defender
  - Bypass PoC: https://s3cur3th1ssh1t.github.io/Bypass_AMSI_by_manual_modification
  - Bypass PoC: https://github.com/rasta-mouse/AmsiScanBufferBypass/blob/master/ASBBypass/Program.cs
  - Old Bypass PoCs were prevented as Windows Defender updates and detects them
  - **Marshall.Copy replaced with WriteProcessMemory API for patching AMSI scan buffer**
- Event Tracing for Windows (ETW)
  - Used by Endpoint Detection and Response software such as Sysmon
  - **Bypass was not implemented due to time constraints, but can be added in a later date**
  - Bypass: https://modexp.wordpress.com/2020/04/08/red-teams-etw/
  - Detection: https://gist.github.com/Cyb3rWard0g/a4a115fd3ab518a0e593525a379adee3
- Kernel Security
  - Kernel Driver Utility for driver exploitation and manipulation, **not implemented nor used by TA505**
  - Bypass: https://github.com/hfiref0x/KDU