



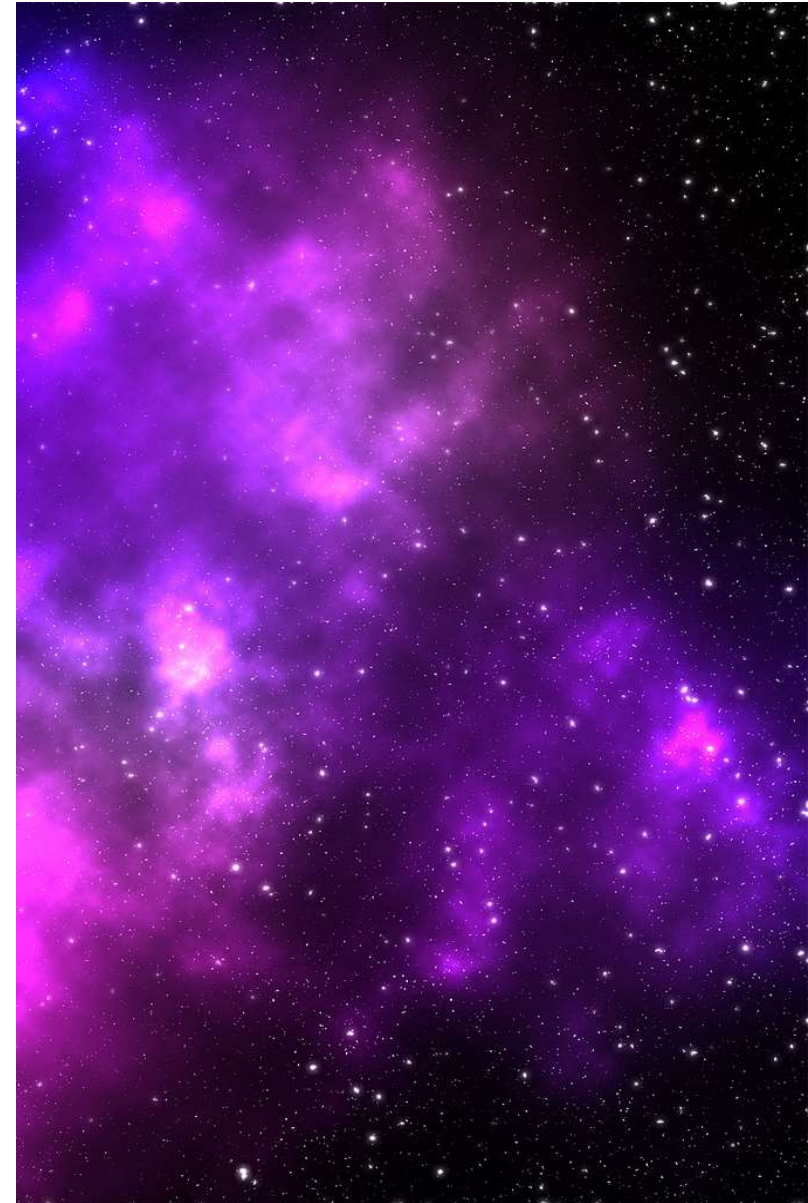
# Purple Teaming

Improving defense by simulating real world attacks

17.09.2020, Online, [felix.sieges@compass-security.com](mailto:felix.sieges@compass-security.com)

# Agenda

1. Introduction
  1. Differentiation
  2. Motivation
  3. Requirements
2. Frameworks
3. Exercise
  1. Attack Modeling
  2. Exercise Preperation
  3. Conducting the Exercise
4. Outcome
5. Conclusion
6. Questions



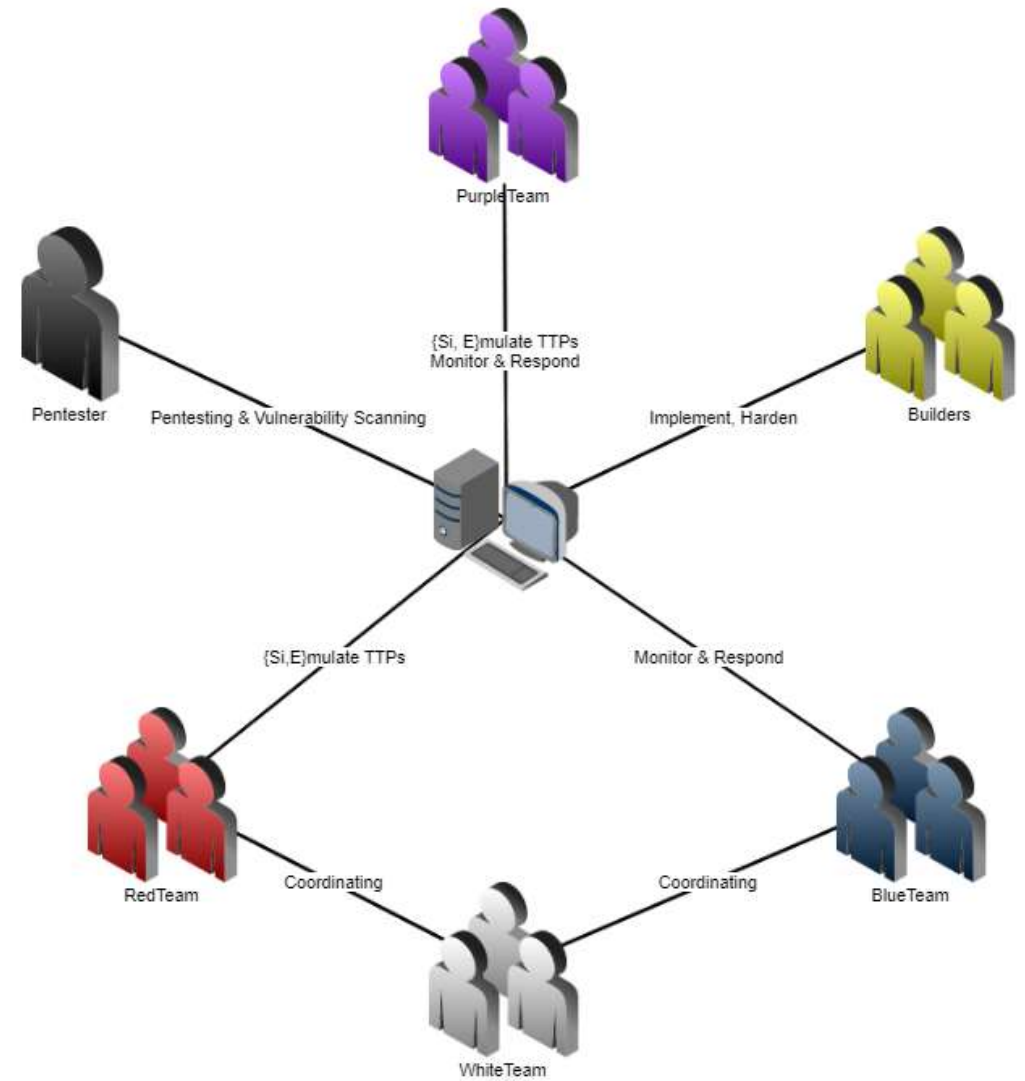


# Introduction To Purple Teaming

# Introduction

## Differentiation

- Teams
- Roles
- Targets



# Introduction

## Differentiation

- Red Team Attacks
- Blue Team Detects & Responds
- Debriefing, both work together



# Introduction

## Differentiation - Simulation

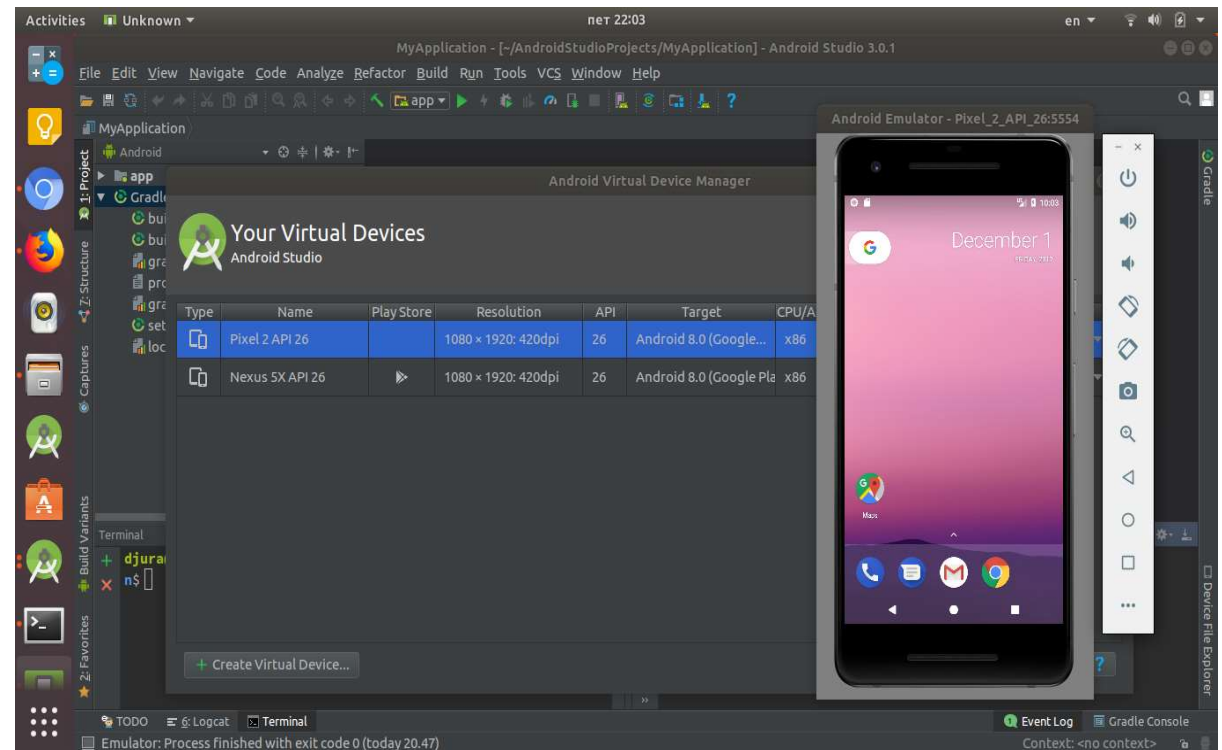
A simulation imitates actual behavior and properties.



# Introduction

## Differentiation - Emulation

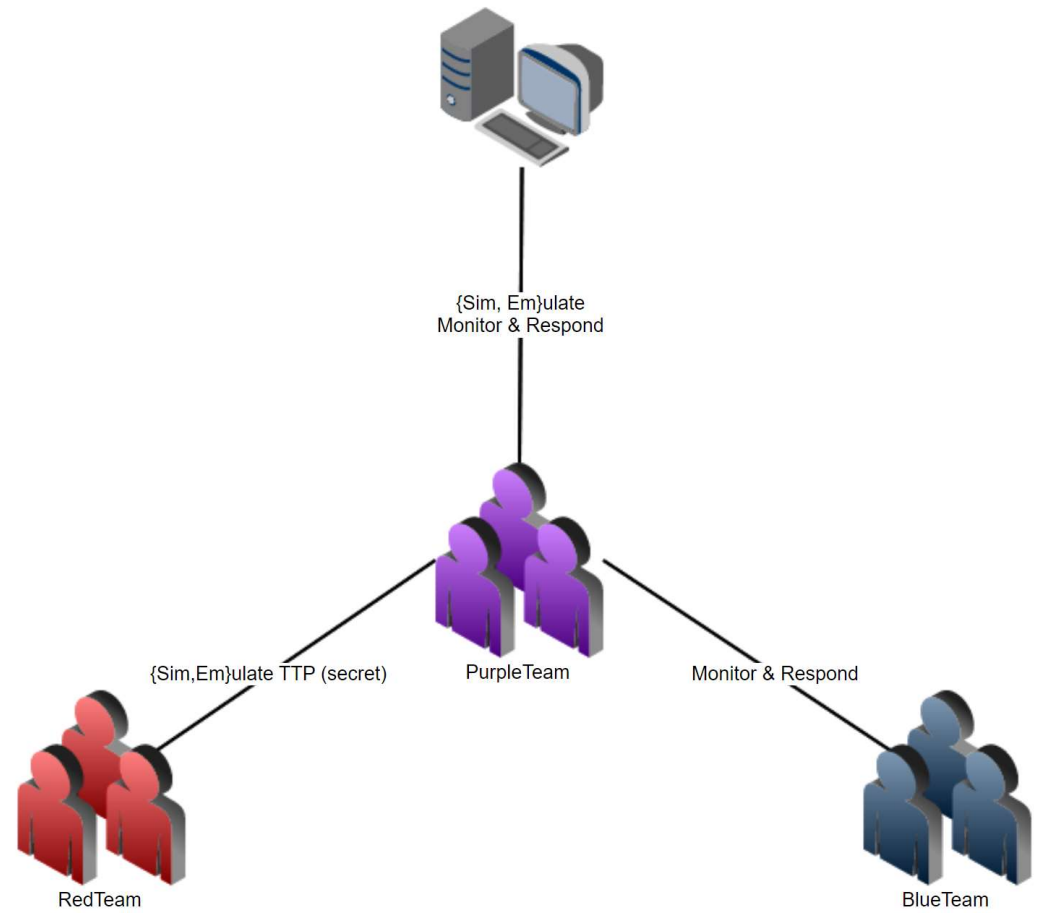
An emulation creates a duplicate which conforms to reality.



# Introduction

## Differentiation

- Cross Functional Team
- One Common Target
- Direct Feedback Loop
- Transparency

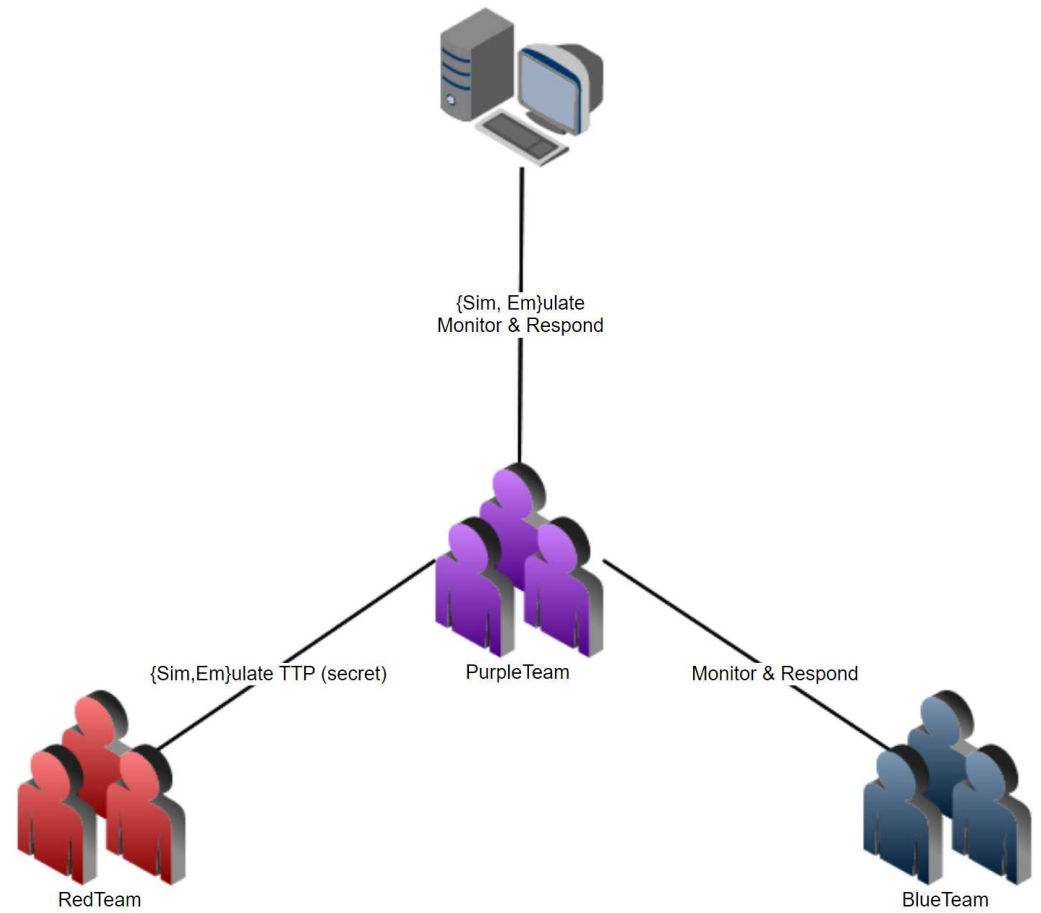




# Introduction

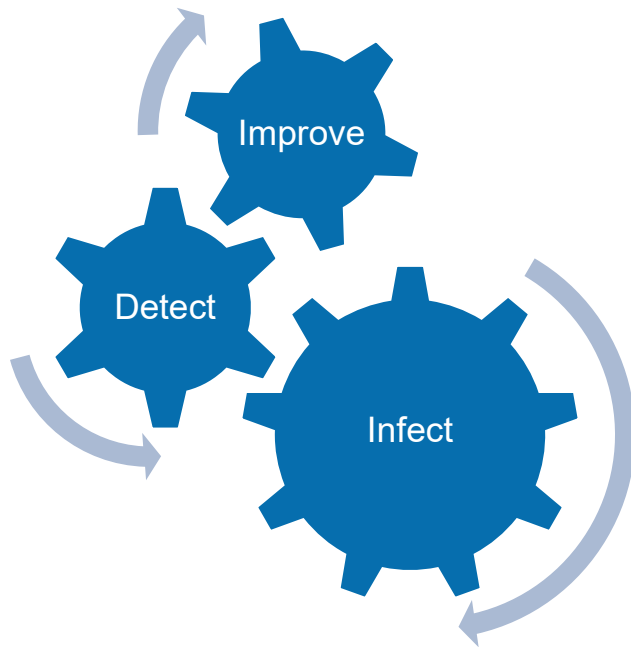
## Differentiation

- Atomic unit tests
- Automated approach
- Manual approach



# Introduction

## Motivation



Discover

Save Open Share Inspect

process\_path: splunkd KQL [Calendar Icon] Jul 10, 2020 @ 10:00:00.000 → now [Refresh Icon] Re

Add filter

Search field names

Filter by type 0

fields

Process

fields

.domain

.name

timestamp

session

extension

originalFileName

30 hits

Jul 10, 2020 @ 10:00:00.000 - Jul 27, 2020 @ 11:06:46.634 — Auto

Count

@timestamp per 12 hours

Time

\_source

```
> Jul 10, 2020 @ 16:14:34.253 process_path: c:\users\public\splunkd.exe z_elastic_ecs.ecs.version: 1.5.0 z_elastic_ecs.user.name: SYSTEM
z_elastic_ecs.user.type: User z_elastic_ecs.user.identifier: S-1-5-18 z_elastic_ecs.user.domain: NT AUTHORITY
z_elastic_ecs.event.kind: event z_elastic_ecs.event.action: Process accessed (rule: ProcessAccess)
z_elastic_ecs.event.code: 10 z_elastic_ecs.event.provider: Microsoft-Windows-Sysmon
z_elastic_ecs.event.created: 2020-07-10T23:14:35.724Z process_guid: D0E0E8E7-E5D6-5F08-6603-00000000A00
```

# Introduction

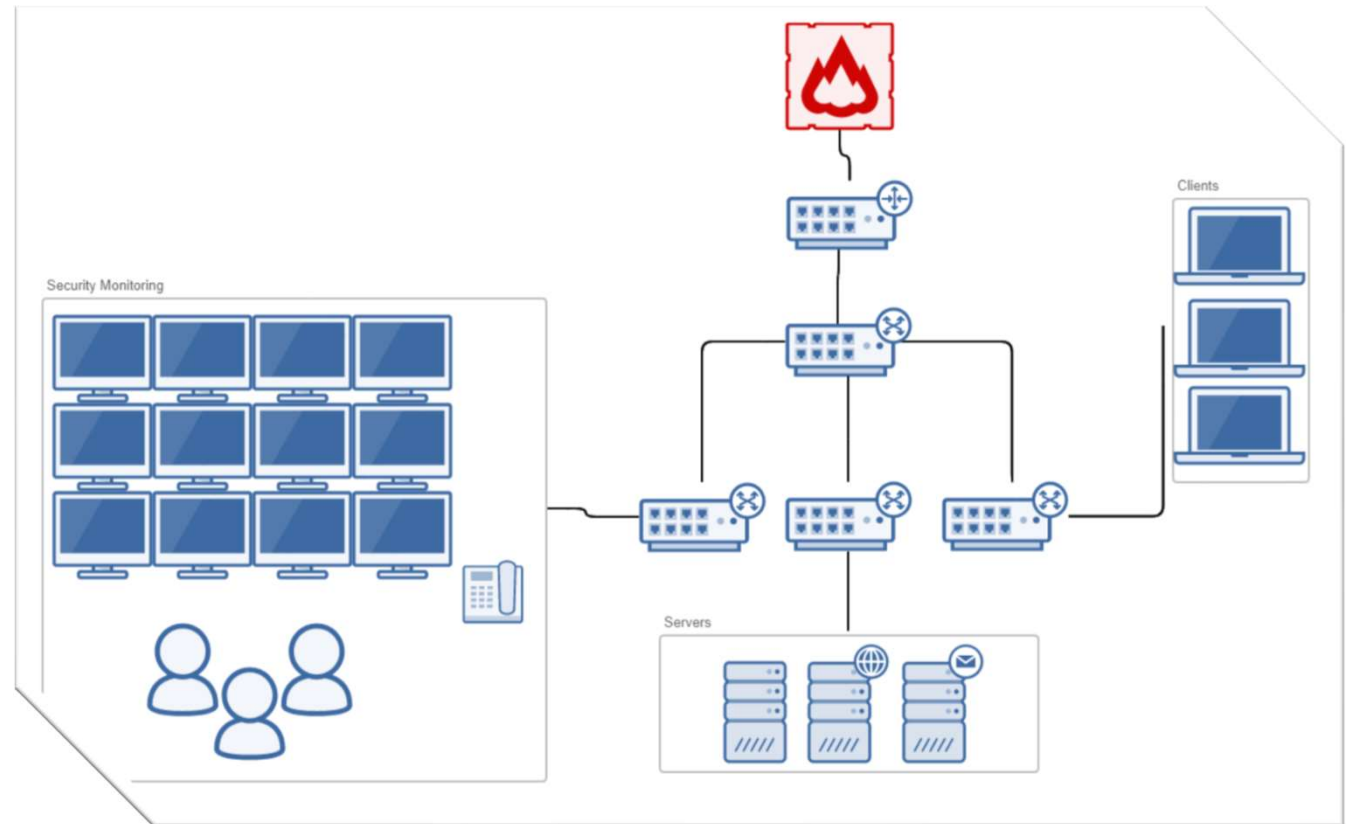
## Requirements

### Existing Monitoring:

- Central Logging
- SIEM
- EDR

### Existing Teams:

- internal/external SOC
- Threat Hunter
- Security Admins
- „someone who looks into it“





# Frameworks

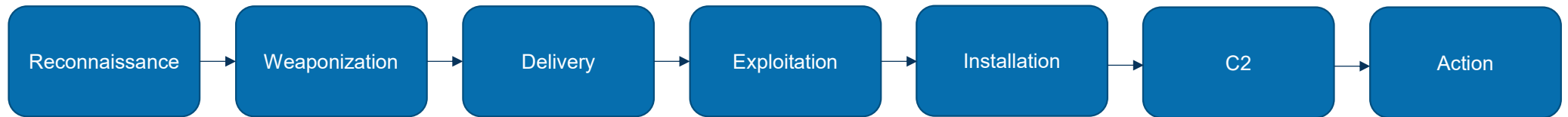
## Organizing Purple Teams

# Frameworks

## Kill Chains

- Lockheed Martin's Kill Chain

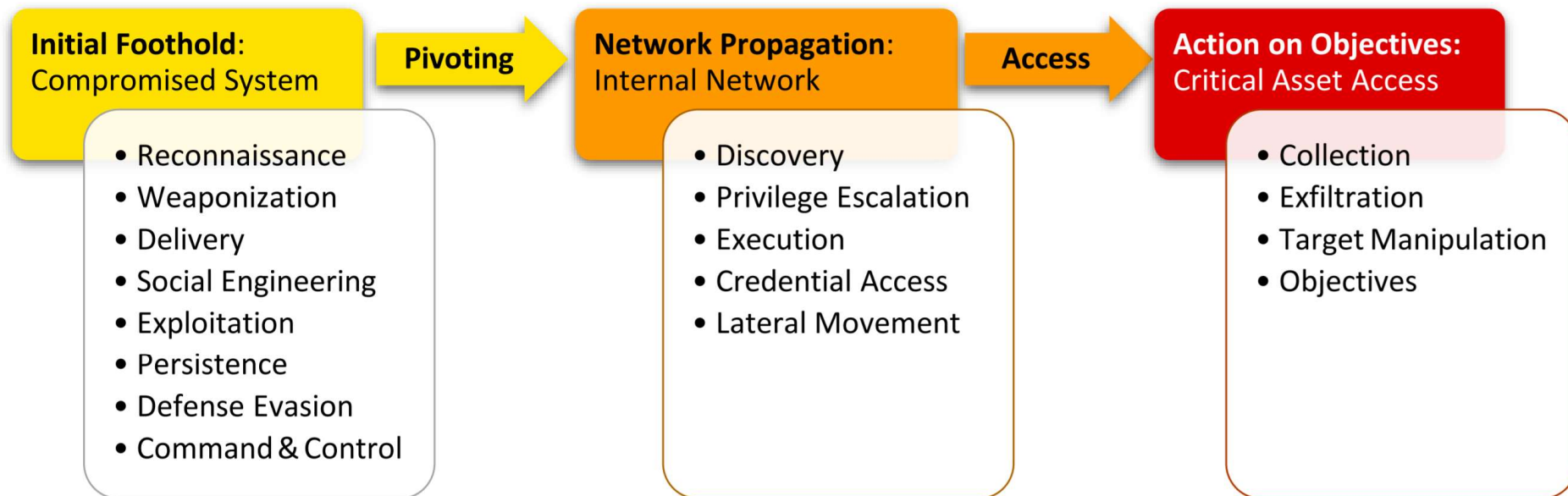
<https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>



# Frameworks

## Kill Chains

- Unified Kill-Chain



[https://www.csacademy.nl/images/scripties/2018/Paul\\_Pols\\_-\\_The\\_Unified\\_Kill\\_Chain\\_1.pdf](https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf)

# Frameworks

ATT&CK Matrix, a common language!

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

## Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK<sup>®</sup> Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, AWS, GCP, Azure, Azure AD, Office 365, SaaS.

[View on the ATT&CK<sup>®</sup> Navigator](#)

[About the Enterprise domain](#)

[Version Permalink](#)

layouts ▾

show sub-techniques

hide sub-techniques

help

<b>Initial Access</b> 9 techniques	<b>Execution</b> 10 techniques	<b>Persistence</b> 18 techniques	<b>Privilege Escalation</b> 12 techniques	<b>Defense Evasion</b> 34 techniques	<b>Credential Access</b> 14 techniques	<b>Discovery</b> 24 techniques	<b>Lateral Movement</b> 9 techniques	<b>Collection</b> 16 techniques	<b>Command and Control</b> 16 techniques	<b>Exfiltration</b> 9 techniques	<b>Impact</b> 13 techniques
---------------------------------------	-----------------------------------	-------------------------------------	--	---	---	-----------------------------------	---	------------------------------------	---	-------------------------------------	--------------------------------

# Frameworks


## Command and Control

### Automated Frameworks:

- [Atomic RedTeam](#)
- MITRE Caldera

### Manual Frameworks:

- Cobalt Strike
- Covenant
- Metasploit
- Empire



Click a Tab to Start Exploring

Information	Code + UI	Channels	Agents	Capabilities	Support
C2	Version Reviewed	Implementation			
Apfell	1.3	Docker			
Caldera	2	pip3			
Cobalt Strike	2	binary			
Covenant	0.3	Docker			
Dali	POC	pip3			
Empire	2.5	install.sh			

<https://www.thec2matrix.com/matrix>



# Demo

## MITRE Caldera – a short intro



# Exercise

## The initial stages

# Exercise

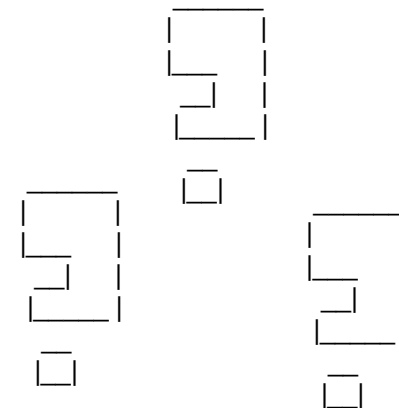
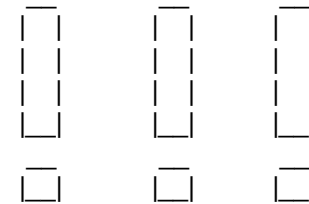
## What to {s,i,e}mulate?

You know:

- Threat Actors targeting your business
- Threat Actors targeting your sector
- Repeat a Red Team
- Prepare a Red Team

You dont know:

- Create your own adversary
- Ransomware targets everyone
- Do unit testing for use cases



# Exercise

## Modeling

Emulating an adversary requires good knowledge of the TTPs

How to get that knowledge?

- Threat Intelligence
- Malware Analysis
- ATT&CK Matrix



# Exercise

## Modeling

ATT&CK sub-techniques have now been released! [Take a tour](#), [read the blog post](#) or [release notes](#), or see the [previous version](#) of the site.

### SOFTWARE

- Overview
- 3PARA RAT
- 4H RAT
- ABK
- adbupd
- Adups
- ADVSTORESHELL
- Agent Smith
- Agent Tesla
- Agent htz

[Home](#) > [Software](#)

## Software

Software is a generic term for custom or commercial code, operating system utilities, open-source software, or other tools used to conduct behavior modeled in ATT&CK. Some instances of software have multiple names associated with the same instance due to various organizations tracking the same set of software by different names. The team makes a best effort to track overlaps between names based on publicly reported associations, which are designated as "Associated Software" on each page (formerly labeled "Aliases"), because we believe these overlaps are useful for analyst awareness.

Software entries include publicly reported technique use or capability to use a technique and may be mapped to Groups who have been reported to use that Software. The information provided does not represent all possible technique use by a piece of Software, but rather a subset that is available solely through open source reporting.

- Tool - Commercial, open-source, built-in, or publicly available software that could be used by a defender, pen tester, red teamer, or an adversary. This category includes both software that generally is not found on an enterprise system as well as software generally available as part of an operating system that is already present in an environment. Examples include PsExec, Metasploit, Mimikatz, as well as Windows utilities such as Net, netstat, Tasklist, etc.
- Malware - Commercial, custom closed source, or open source software intended to be used for malicious purposes by adversaries. Examples include PlugX, CHOPSTICK, etc.

# Exercise

## Modeling

Home > Software > Emotet

### Emotet

Emotet is a modular malware variant which is primarily used as a downloader for other malware variants such as TrickBot and IcedID. Emotet first emerged in June 2014 and has been primarily used to target the banking sector. <sup>[1]</sup>

ID: S0367

Associated Software: Geodo

Type: MALWARE

Platforms: Windows

Contributors: Omkar Gudhate

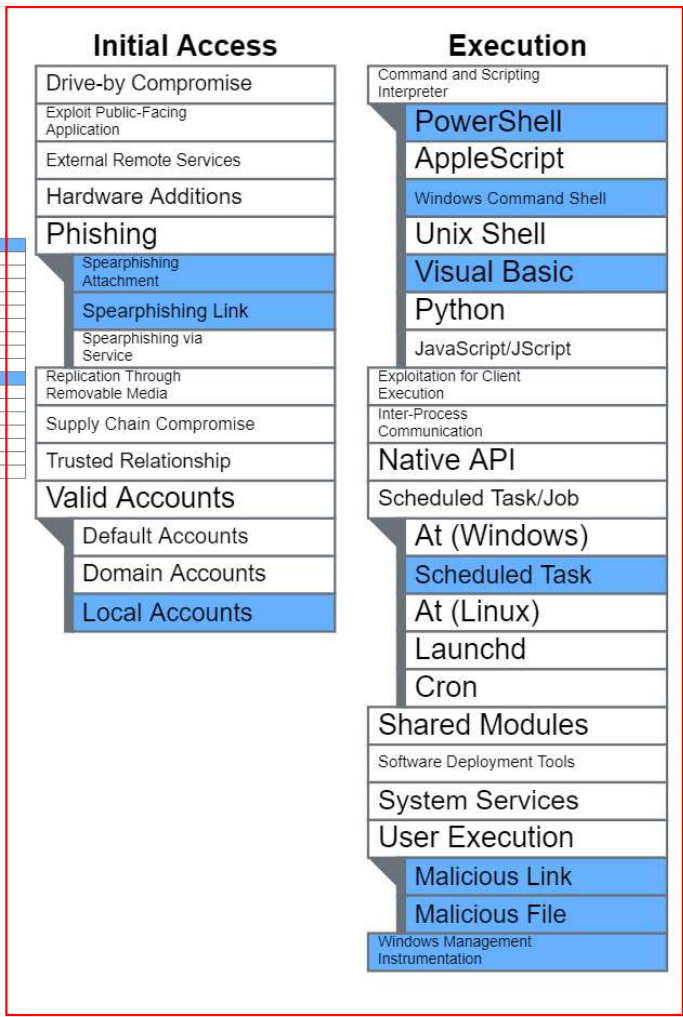
Version: 1.2

Created: 25 March 2019

Last Modified: 15 July 2020

# Exercise Modeling

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
Drive-by Compromise	PowerShell	Account Manipulation	Account Manipulation	Account Manipulation	Account Manipulation	Account Manipulation	Account Manipulation	Account Manipulation
Exploit Public-Facing Application	AppleScript	BITS Jobs	BITS Jobs	BITS Jobs	BITS Jobs	BITS Jobs	BITS Jobs	BITS Jobs
External Remote Services	Windows Command Shell	Time Providers	Time Providers	Time Providers	Time Providers	Time Providers	Time Providers	Time Providers
Hardware Additions	Visual Basic	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender
Phishing	Python	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender
Spearphishing Attachment	Python	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender
Spearphishing Link	Python	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender
Supply Chain Compromise	Python	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender
Trusted Relationship	Python	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender
Valid Accounts	Python	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender
Domain Accounts	Python	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender
Local Accounts	Python	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender
Drive-by Compromise	PowerShell	Account Manipulation	Account Manipulation	Account Manipulation	Account Manipulation	Account Manipulation	Account Manipulation	Account Manipulation
Exploit Public-Facing Application	AppleScript	BITS Jobs	BITS Jobs	BITS Jobs	BITS Jobs	BITS Jobs	BITS Jobs	BITS Jobs
External Remote Services	Windows Command Shell	Time Providers	Time Providers	Time Providers	Time Providers	Time Providers	Time Providers	Time Providers
Hardware Additions	Visual Basic	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender
Phishing	Python	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender
Spearphishing Attachment	Python	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender
Spearphishing Link	Python	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender
Supply Chain Compromise	Python	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender
Trusted Relationship	Python	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender
Valid Accounts	Python	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender
Domain Accounts	Python	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender
Local Accounts	Python	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender	Windows Defender



<https://mitre-attack.github.io/attack-navigator/enterprise/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fsoftware%2FS0367%2FS0367-enterprise-layer.json>

# Exercise

## Modeling

### Emotets Multi Stage Payload

#### Stage1

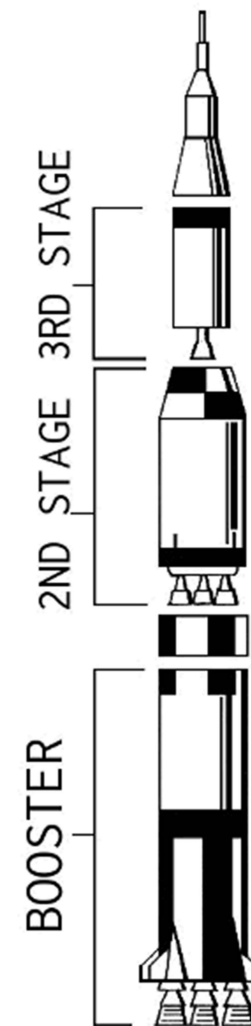
- Send an E-Mail with Spearphishing Link
- Download, open the document and activate macros

#### Stage2

- Execute Powershell through WMI
- Execute the the download cradle

#### Stage3

- Download and execute the Emotet binary
- Unpack the malicious payload to memory
- Copy several versions of the .exe to disk



[https://wpclipart.com/space/ships/more\\_space\\_craft/rocket\\_booster\\_and\\_stages.png](https://wpclipart.com/space/ships/more_space_craft/rocket_booster_and_stages.png)



# Excercise

## Modeling

### Emotet's persistence:

- Writes to registry (autostart)

### When it becomes local admin:

- Creates Services
- Drops Executable (as Service)

### Credential Access:

- Browser Passwords
- E-Mail Passwords

### Lateral Movement:

- Admin shares (C\$,Admin\$)



# Excercise Tracking

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	
Drive-by Compromise Exploit Public-Facing Application External Remote Services	Comment and Scripting Interpreter <b>PowerShell</b> <b>AppleScript</b> Windows Command Shell <b>Unix Shell</b> <b>Visual Basic</b> Python JavaScript/JScript	Account Manipulation <b>BITS Jobs</b> Boot or Login Autostart Execution Registry Root Keys / Startup Folder Authentication Package Time Providers Wingon Helper DLL Security Support Provider Kernel Modules and Extensions Re-opened Applications LSASS Driver Shortcut Modification Port Monitors File Modification Boot or login Initiative Targets Browser Extensions Component Based Software Entry Create Account Launch Agent Launch Daemon Event Triggered Execution Exploitation for Privilege Escalation Group Policy Modification Task Execution Flow Process Injection Dynamic-Link Library Injection Portable Executable Office Application Startup Thread Execution Hijacking Anonymous Procedure Call Thread Local Storage Private System Calls Proc Memory Eula Window Memory Injection Process Doppelganging Process Hollowing VDSO Hijacking Scheduled Task/Job At (Windows) <b>Scheduled Task</b> At (Linux) Launchd Cron Server Software Component Traffic Signaling Valid Accounts Default Accounts Domain Accounts <b>Local Accounts</b>	Abuse Elevation Control Mechanism Access Token Manipulation Boot or Login Autostart Execution Registry Root Keys / Startup Folder Authentication Package Time Providers Wingon Helper DLL Security Support Provider Kernel Modules and Extensions Re-opened Applications LSASS Driver Shortcut Modification Port Monitors File Modification Boot or login Initiative Targets Browser Extensions Component Based Software Entry Create Account Launch Agent Launch Daemon Event Triggered Execution Exploitation for Privilege Escalation Group Policy Modification Task Execution Flow Process Injection Dynamic-Link Library Injection Portable Executable Office Application Startup Thread Execution Hijacking Anonymous Procedure Call Thread Local Storage Private System Calls Proc Memory Eula Window Memory Injection Process Doppelganging Process Hollowing VDSO Hijacking Scheduled Task/Job At (Windows) <b>Scheduled Task</b> At (Linux) Launchd Cron Server Software Component Traffic Signaling Valid Accounts Default Accounts Domain Accounts <b>Local Accounts</b>	Abuse Elevation Control Mechanism Access Token Manipulation Boot or Login Autostart Execution Registry Root Keys / Startup Folder Authentication Package Time Providers Wingon Helper DLL Security Support Provider Kernel Modules and Extensions Re-opened Applications LSASS Driver Shortcut Modification Port Monitors File Modification Boot or login Initiative Targets Browser Extensions Component Based Software Entry Create Account Launch Agent Launch Daemon Event Triggered Execution Exploitation for Privilege Escalation Group Policy Modification Task Execution Flow Process Injection Dynamic-Link Library Injection Portable Executable Office Application Startup Thread Execution Hijacking Anonymous Procedure Call Thread Local Storage Private System Calls Proc Memory Eula Window Memory Injection Process Doppelganging Process Hollowing VDSO Hijacking Scheduled Task/Job At (Windows) <b>Scheduled Task</b> At (Linux) Launchd Cron Server Software Component Traffic Signaling Valid Accounts Default Accounts Domain Accounts <b>Local Accounts</b>	Abuse Elevation Control Mechanism Access Token Manipulation Boot or Login Autostart Execution Registry Root Keys / Startup Folder Authentication Package Time Providers Wingon Helper DLL Security Support Provider Kernel Modules and Extensions Re-opened Applications LSASS Driver Shortcut Modification Port Monitors File Modification Boot or login Initiative Targets Browser Extensions Component Based Software Entry Create Account Launch Agent Launch Daemon Event Triggered Execution Exploitation for Privilege Escalation Group Policy Modification Task Execution Flow Process Injection Dynamic-Link Library Injection Portable Executable Office Application Startup Thread Execution Hijacking Anonymous Procedure Call Thread Local Storage Private System Calls Proc Memory Eula Window Memory Injection Process Doppelganging Process Hollowing VDSO Hijacking Scheduled Task/Job At (Windows) <b>Scheduled Task</b> At (Linux) Launchd Cron Server Software Component Traffic Signaling Valid Accounts Default Accounts Domain Accounts <b>Local Accounts</b>	Brute Force <b>Password Guessing</b> Password Cracking Password Spraying Credential Stuffing Credentials from Keychain SecurityKey Memory Credential from Web Browsers Exploitation for Credential Access Input Capture Man-in-the-Middle Moody Authentication Process Network Sniffing OS Credential Dumping LSASS Memory Security Account Manager NTDS DCSync Proc Filesystem Recopied and re-executed Cached Domain Credentials LSA Secrets Shell Web Session Code Steal or Forge Kerberos Tickets Trustless Authentication Untrusted Credentials Access in Files Credentials in Registry Bash History Private Keys	Account Discovery <b>Local Account</b> <b>Domain Account</b> <b>Email Account</b> Browser Bookmarks Discovery Domain Trust File and Directory Discovery Network Service Discovery Network Share Discovery Network Policy Discovery Removable Media Discovery Software Deployment Tool Permission Groups Discovery Process Discovery Query Registry Remote System Discovery Software Discovery System Information Discovery System Network Connected Discovery System Owner/User Discovery System Service Discovery System Time Discovery Virtualization/Sandbox Evasion	Evolution of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking Remote Services Remote Desktop Protocol SMB/Windows Admin Shares SSH VNC Windows Remote Management Replication Through Removable Media Software Deployment Tool Email Forwarding Rule Task Shared Content Use Alternate Authentication Source	Active Collected Data Audio Capture Automated Collection Clipboard Data Data Staged Data from Information Operations Data from Local System Data from Network Shared Drive Data from Removable Media Email Collection <b>Local Email Collection</b> Remote Email Collection Screen Capture Input Capture Man in the Browser Man-in-the-Middle Screen Capture Video Capture

Initial Access	Execution
Drive-by Compromise	Command and Scripting Interpreter
Exploit Public-Facing Application	<b>PowerShell</b>
External Remote Services	AppleScript
Hardware Additions	<b>Windows Command Shell</b>
Phishing	Unix Shell
<b>Spearphishing Attachment</b>	<b>Visual Basic</b>
<b>Spearphishing Link</b>	Python
Spearphishing via Service	JavaScript/JScript
Replication Through Removable Media	Exploitation for Client Execution
Supply Chain Compromise	Inter-Process Communication
Trusted Relationship	Native API
Valid Accounts	Scheduled Task/Job
Default Accounts	At (Windows)
Domain Accounts	<b>Scheduled Task</b>
<b>Local Accounts</b>	At (Linux)
	Launchd
	Cron
	Shared Modules
	Software Deployment Tools
	System Services
	User Execution
	<b>Malicious Link</b>
	<b>Malicious File</b>
	Windows Management Instrumentation

<https://mitre-attack.github.io/attack-navigator/enterprise/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fsoftware%2FS0367%2FS0367-enterprise-layer.json>

# Excercise

## Preparations

### Infrastructure:

- internally or externally
- Domains
- IP-Adresses
- Hosting payloads
- Command and Control

### Testcases aligned to the ATT&CK TTPs

- Phishing E-Mail
- Malicious Documents
- Malware
- Testcases for persistence
- Attack Scripts & Payloads
- User which will get attacked

### Indicators of Compromise (IOCs)

#### Email subject lines

Payment Remittance Advice  
Numero Fattura 2019...

#### Malicious Word documents

eee144531839763b15051badbbda9daae38f60c02abaa7794a046f96a68cd10b  
fb25f35c54831b3641c50c760eb94ec57481d8c8b1da98dd05ba97080d54ee6a  
bee23d63404d97d2b03fbc38e4c554a55a7734d83dbd87f2bf1baf7ed2e39e3e  
5d9775369ab5486b5f2d0faac423e213cee20daf5aaaaa9c8b4c3b4e66ea8224

#### Hacked websites hosting the Emotet binary

danangluxury[.]com/wp-content/uploads/KTgQsbtu/  
gcesab[.]com/wp-includes/customize/zUfJervuM/  
autorepuestosdm[.]com/wp-content/CiIoXlptl/  
covergt[.]com/wordpress/geh7l30-xq85il-558/  
zhaoyouxiu[.]com/wp-includes/vxqo-84953w-5062/  
rockstareats[.]com/wp-content/themes/NUOAajdJ/  
inwil[.]com/wp-content/oyFhKHoe  
inesmanila[.]com/cgi-bin/otxpnmxm-3okvb2-29756/  
dateandoando[.]com/wp-includes/y0mcdp2zyq\_lx14j2wh2-0551284557/

#### Emotet binaries

8f05aa95aa7b2146ee490c2305a2450e58ce1d1e3103e6f9019767e5566f233e  
7080e1b236a19ed46ea28754916c43a7e8b68727c33cbf81b96077374f4dc205  
61e0ac40dc2680aad77a71f1e6d845a37ab12aa8cd6b638d2dbcebe9195b0f6  
f5af8586f0289163951adaaf7eb9726b82b05daa3bb0cc2c0ba5970f6119c77a  
6076e26a123aaff20c0529ab13b2c5f11259f481e43d62659b33517060bb63c5

#### Post-infection traffic (C2s)

187[.]155[.]233[.]46  
83[.]29[.]180[.]97  
181[.]36[.]142[.]205

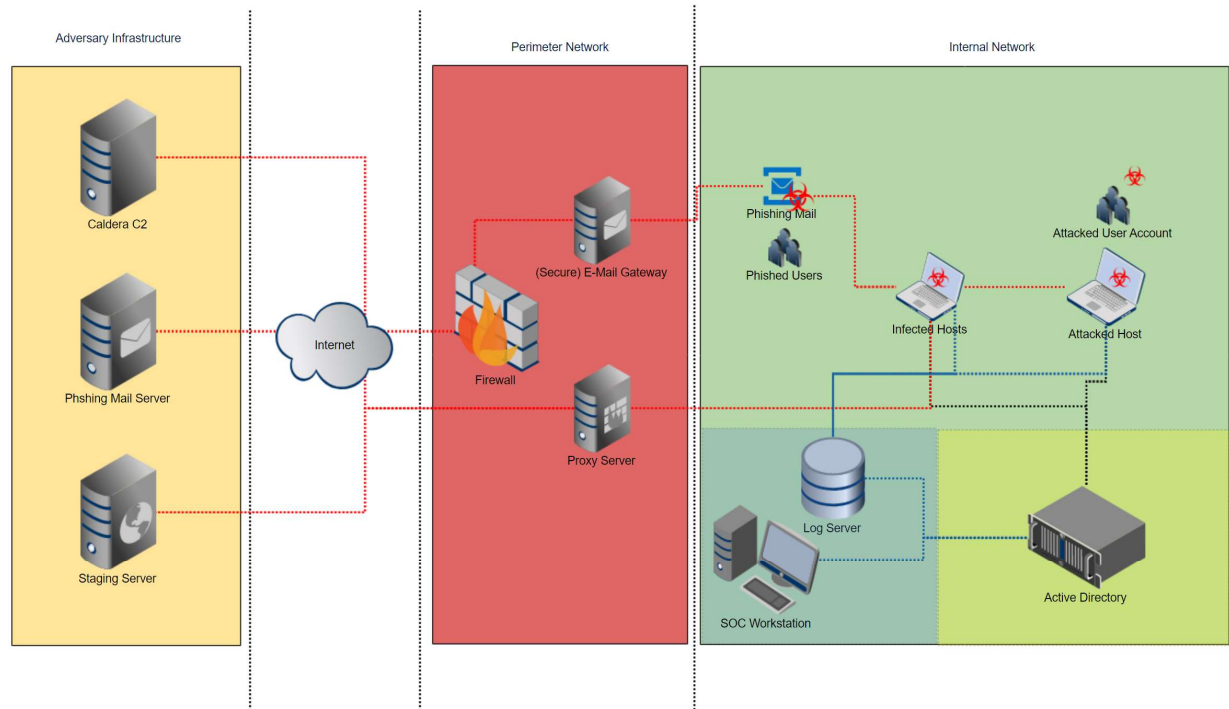
<https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/>

# Exercise

## Preparations

### Exercise Environment:

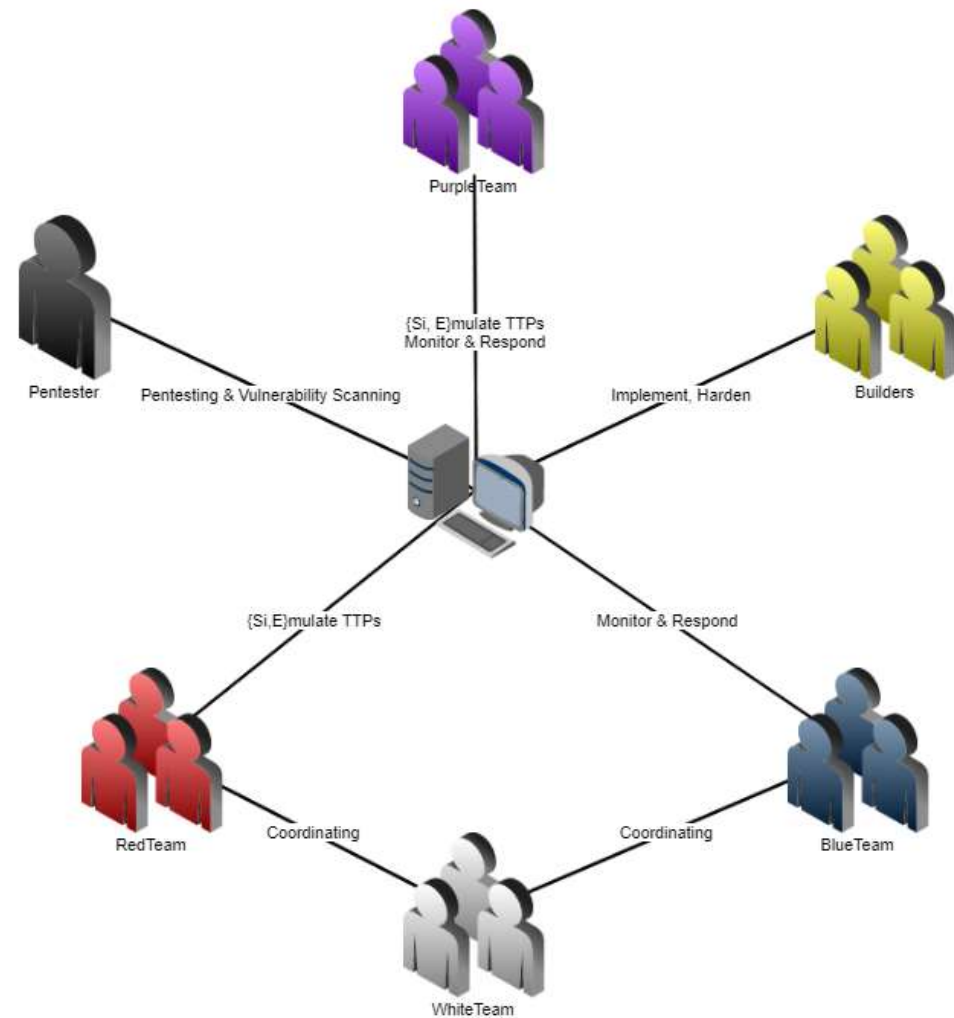
- Integrated Setup
- Add exclusions to preventive security software
- Make sure that everything is logged



# Preparation

## People

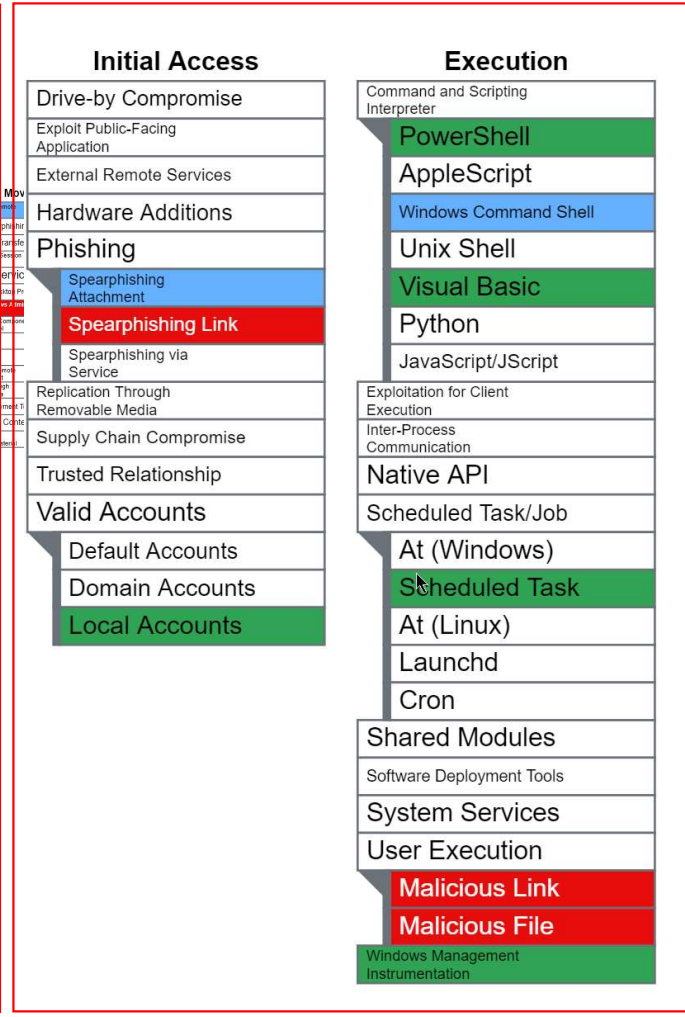
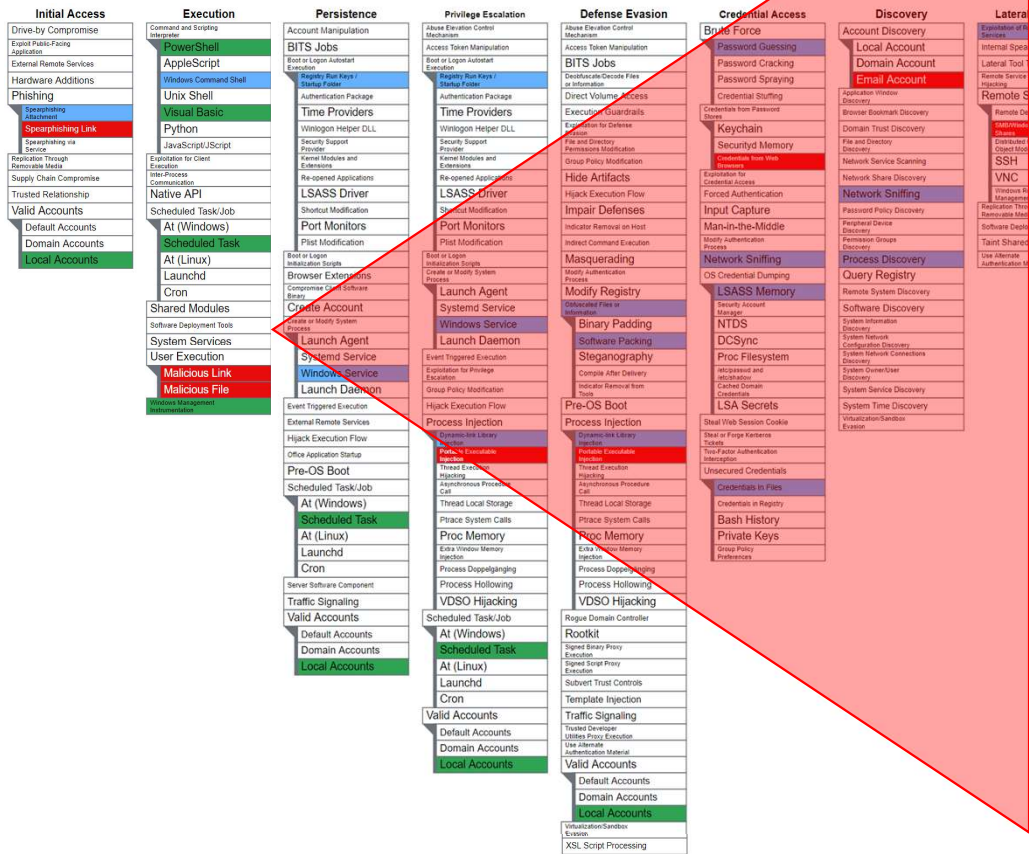
- IT-Security
- SIEM Team
- Threat Hunters
- Administrators
- CISO



# Demo

## Simulating Emotet

# Outcome Tracking



<https://mitre-attack.github.io/attack-navigator/enterprise/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fsoftware%2FS0367%2FS0367-enterprise-layer.json>

# Outcome

What was it good for?!

## Gaps

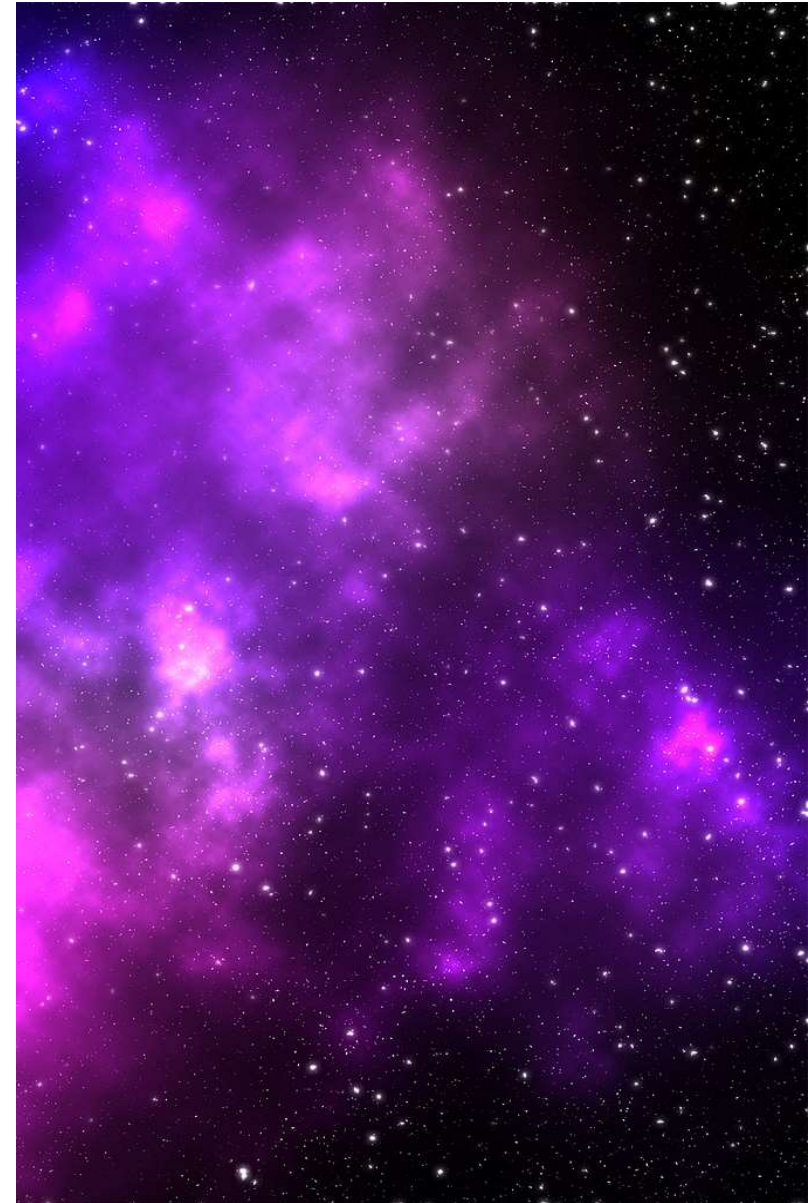
- Missing client logging
- Missing firewall logging
- Processes paralysis

## Validated


- Existing rules
- Logging on DC

## Future Opportunities

- Improve and Repeat







Purple Teaming:  
Combining Red and Blue team tactics in one  
exercise can help improve detection.  
In conclusion all teams have one common  
goal;  
Protect the network!



## Ressources and References

- <https://github.com/mitre/caldera>
- <https://github.com/DefensiveOrigins/APT06202001>
- <https://attack.mitre.org/>
- [https://www.csacademy.nl/images/scripties/2018/Paul\\_Pols - The Unified Kill Chain 1.pdf](https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf);  
Paul Pols
- <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>; Eric M. Hutchins , Michael J. Cloppert , Rohan M. Amin,  
Ph.D.
- <https://thehelk.com/intro.html>; @Cyb3rWard0g
- <https://www.thec2matrix.com/matrix>; jorgeorchilles @brysonbort @Adam\_Mashinchi
- <https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign>