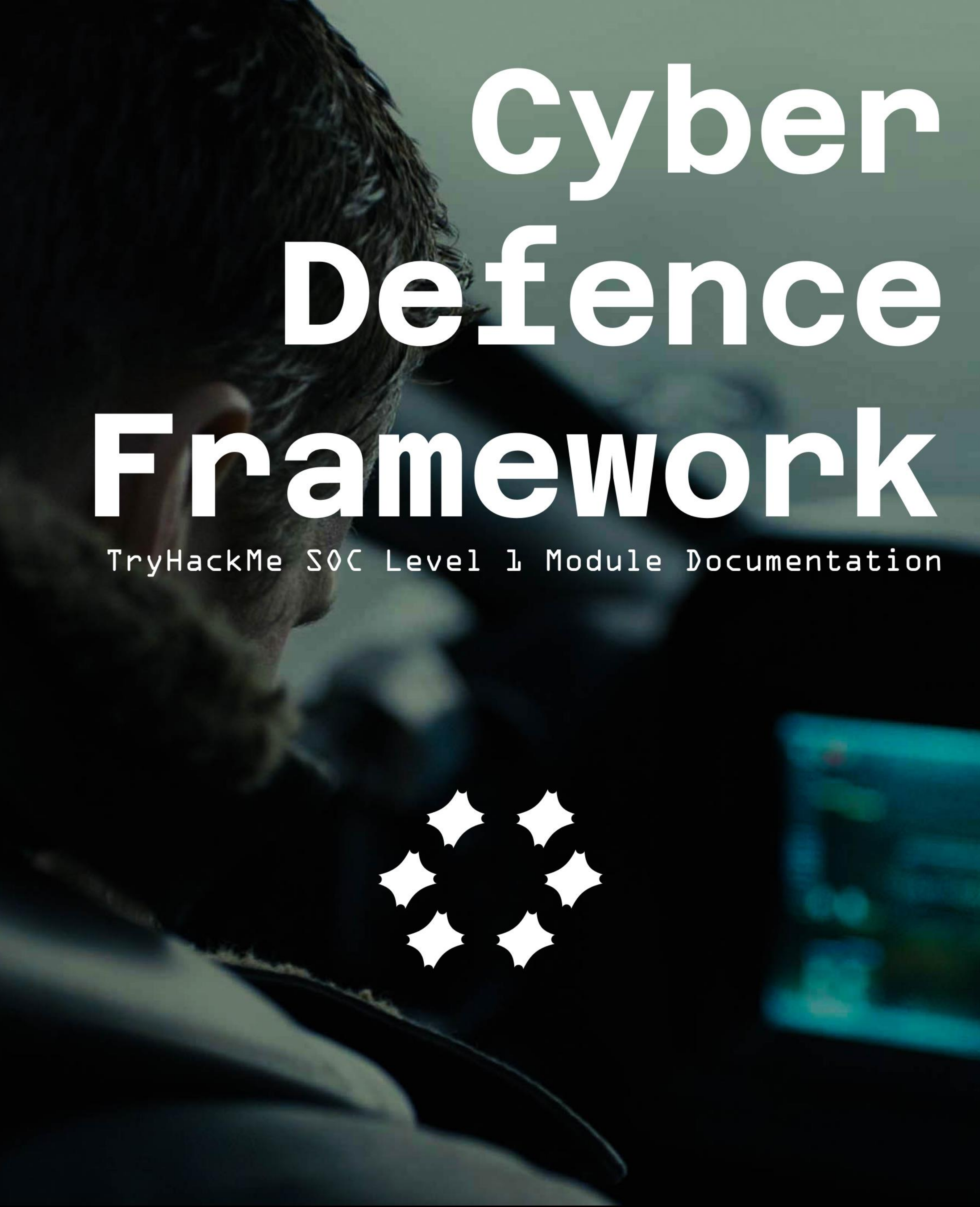


Cyber Defence Framework

TryHackMe SOC Level 1 Module Documentation

Prepared by Mikhail Amzar

14/06/2024

Contents

JUNIOR SECURITY ANALYST INTRO

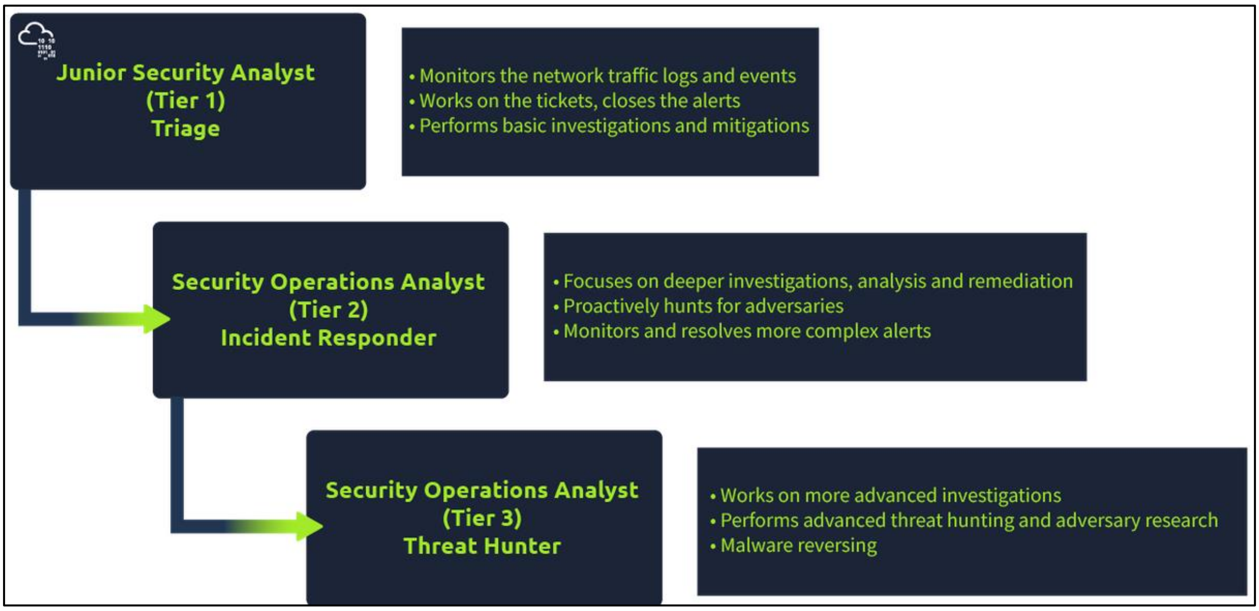
A career as a Junior Security Analyst

Responsibilities

- Monitor and investigate the alerts (most of the time, it's a 24x7 SOC operations environment)
- Configure and manage the security tools
- Develop and implement basic IDS (Intrusion Detection System) signatures
- Participate in SOC working groups, meetings
- Create tickets and escalate the security incidents to the Tier 2 and Team Lead if needed

Qualifications

- 0-2 years of experience with Security Operations
- Basic understanding of Networking (OSI model (Open Systems Interconnection Model) or TCP/IP model (Transmission Control Protocol/Internet Protocol Model)), Operating Systems (Windows, Linux), Web applications. To further learn about OSI and TCP/IP models, please refer to the Introductory Networking Room.
- Scripting/programming skills are a plus



Junior Security Analyst (Tier 1) Triage

- Monitors the network traffic logs and events
- Works on the tickets, closes the alerts
- Performs basic investigations and mitigations

Security Operations Analyst (Tier 2) Incident Responder

- Focuses on deeper investigations, analysis and remediation
- Proactively hunts for adversaries
- Monitors and resolves more complex alerts

Security Operations Analyst (Tier 3) Threat Hunter

- Works on more advanced investigations
- Performs advanced threat hunting and adversary research
- Malware reversing

Common terminology

Indicator of Compromise

IoC are forensic evidence/artefacts that may suggest potential intrusions on a host system or network.

TTP (Tactics, Techniques, and Procedures)

TTPs are the patterns of activities or methods associated with a specific threat actor.

PYRAMID OF PAIN

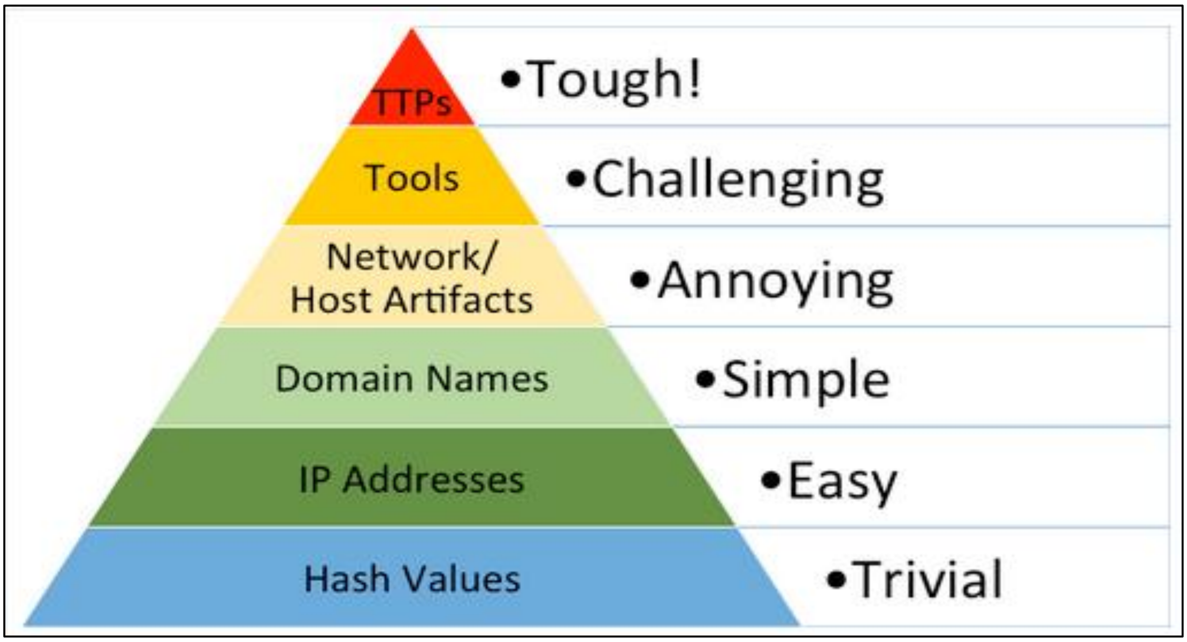
1.Introduction

https://www.picussecurity.com/resource/glossary/what-is-pyramid-of-pain
https://tryhackme.com/r/room/pyramidofpainax

What is Pyramid of Pain?

The Pyramid of Pain is a conceptual framework that illustrates the varying levels of difficulty and cost an adversary would encounter to evade detection and continue their attack, in the context of cybersecurity defenses.

It’s a framework, enabling security experts, predominantly blue teamers, to channel their resources on elements inducing the most pain to adversaries to alter.



a. Hash Values (Trivial)

Hash value is a numeric value of a fixed length that uniquely identifies data. A hash value is the result of a hashing algorithm.

Exm:
MD5 (128-bit hash value; No longer secure)
SHA-1 (160-bit hash value, 40-digit hexadecimal number; No longer secure)
SHA-2 | variant **SHA-256** (256-bits hash value, 64-digit hexadecimal number)

Security professionals usually use the hash values to gain insight into a specific malware sample, a malicious or a suspicious file, and to uniquely identify and reference the malicious artifact.
Even in security reports, sometimes malware or file’s hash value will be provided in the report.

e.g. Sites for reports:
The DFIR Report
FireEye Threat Research Blogs

Why is hash value trivial in the pyramid of pain?
Because sure, granted you have the malicious sample's signature in your arsenal to test against, or you're using an online tool that checks for it, you can detect it.
But even a single bit change in a malicious file will change the end hash value. So, an attacker can certainly leverage this.
That makes threat hunting using file hashes as the IoC, difficult.

b. IP Address (Easy)

IP address is a logical address that is used to identify devices on a network.

IP Address as Indicators of Compromise?

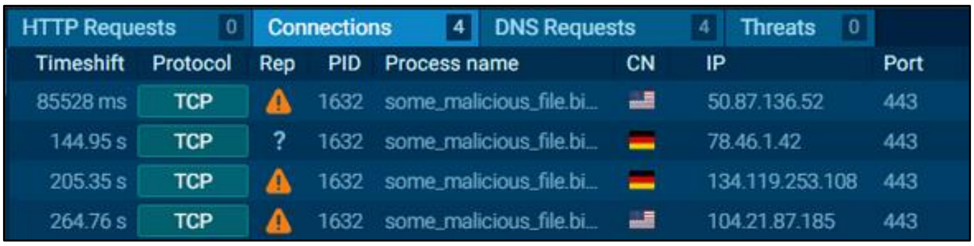
From a defense standpoint, knowledge of the IP addresses an adversary uses can be valuable. A common defense tactic is to block, drop, or deny inbound requests from IP addresses on your parameter or external firewall.

But! This tactic is often not bulletproof as it's trivial for an experienced adversary to recover simply by using a new public IP address.

Bonus
One of the ways an adversary can make it challenging to successfully carry out IP blocking is by using **Fast Flux**.

According to Akamai, **Fast Flux** is a DNS technique used by botnets to hide phishing, web proxying, malware delivery, and malware communication activities behind compromised hosts acting as proxies. The purpose of using the Fast Flux network is to make the communication between malware and its command-and-control server (C&C) challenging to be discovered by security professionals.

You can analyze malware and its communication in a virtual environment using tools like: Any Run



Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port
85528 ms	TCP	⚠	1632	some_malicious_file.bi...	🇺🇸	50.87.136.52	443
144.95 s	TCP	?	1632	some_malicious_file.bi...	🇩🇪	78.46.1.42	443
205.35 s	TCP	⚠	1632	some_malicious_file.bi...	🇩🇪	134.119.253.108	443
264.76 s	TCP	⚠	1632	some_malicious_file.bi...	🇺🇸	104.21.87.185	443

..

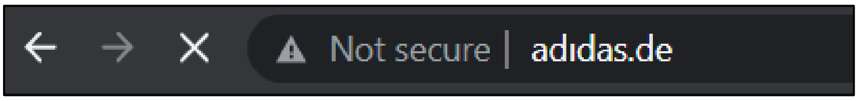
c. Domain Names (Simple)

Domain Names as IoC?

Domain Names can be a little more of a pain for the attacker to change as they would most likely need to purchase the domain, register it and modify DNS records.

Unfortunately for defenders, many DNS providers have loose standards and provide APIs to make it even easier for the attacker to change the domain.

Attackers can trick victims by manipulating the display of domain/URLs using a few methods.
Punycode (converting characters into another)

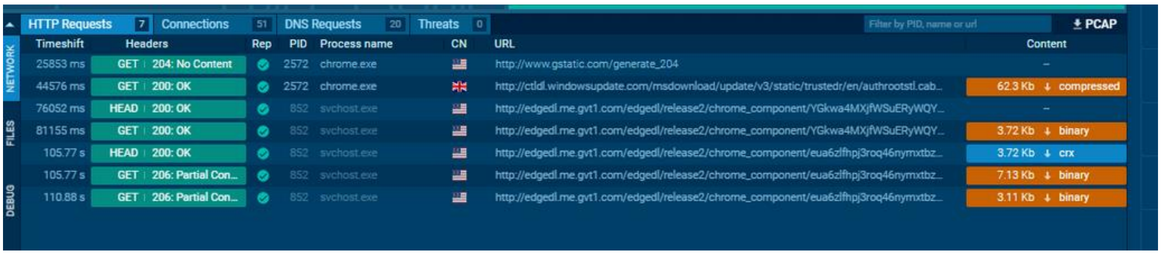


adıdas.de

Hiding malicious URLs using URL shortener services.

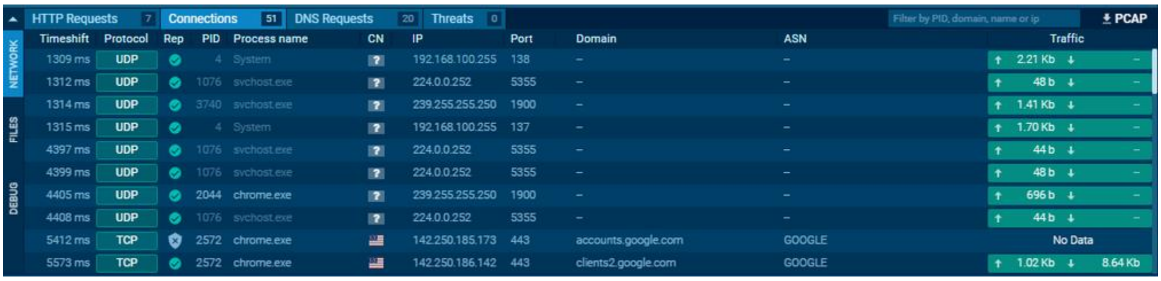
- bit.ly
- goo.gl
- ow.ly
- s.id
- smarturl.it
- tiny.pl
- tinyurl.com
- x.co

Bonus
Viewing connections in Any Run
Below: Seeing what resources are being retrieved from a webserver.



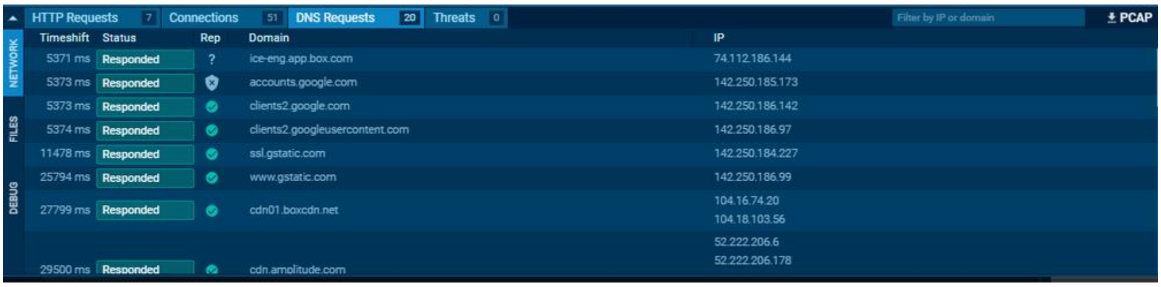
Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
25853 ms	GET 204: No Content	✓	2572	chrome.exe		http://www.gstatic.com/generate_204	–
44576 ms	GET 200: OK	✓	2572	chrome.exe		http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab...	62.3 Kb ↓ compressed
76052 ms	HEAD 200: OK	✓	852	svchost.exe		http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/YGkwa4MXjfWSuERyWQY...	–
81155 ms	GET 200: OK	✓	852	svchost.exe		http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/YGkwa4MXjfWSuERyWQY...	3.72 Kb ↓ binary
105.77 s	HEAD 200: OK	✓	852	svchost.exe		http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/eua6zlfhpj3roq46nymxtbz...	3.72 Kb ↓ crx
105.77 s	GET 206: Partial Con...	✓	852	svchost.exe		http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/eua6zlfhpj3roq46nymxtbz...	7.13 Kb ↓ binary
110.88 s	GET 206: Partial Con...	✓	852	svchost.exe		http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/eua6zlfhpj3roq46nymxtbz...	3.11 Kb ↓ binary

Below: Seeing connections made by any process to another host. (Could be C2 traffic)



Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
1309 ms	UDP	✓	4	System	?	192.168.100.255	138	–	–	↑ 2.21 Kb ↓ –
1312 ms	UDP	✓	1076	svchost.exe	?	224.0.0.252	5355	–	–	↑ 48 b ↓ –
1314 ms	UDP	✓	3740	svchost.exe	?	239.255.255.250	1900	–	–	↑ 1.41 Kb ↓ –
1315 ms	UDP	✓	4	System	?	192.168.100.255	137	–	–	↑ 1.70 Kb ↓ –
4397 ms	UDP	✓	1076	svchost.exe	?	224.0.0.252	5355	–	–	↑ 44 b ↓ –
4399 ms	UDP	✓	1076	svchost.exe	?	224.0.0.252	5355	–	–	↑ 48 b ↓ –
4405 ms	UDP	✓	2044	chrome.exe	?	239.255.255.250	1900	–	–	↑ 696 b ↓ –
4408 ms	UDP	✓	1076	svchost.exe	?	224.0.0.252	5355	–	–	↑ 44 b ↓ –
5412 ms	TCP	⊗	2572	chrome.exe		142.250.185.173	443	accounts.google.com	GOOGLE	No Data
5573 ms	TCP	✓	2572	chrome.exe		142.250.186.142	443	clients2.google.com	GOOGLE	↑ 1.02 Kb ↓ 8.64 Kb

Below: Checking DNS requests.



Timeshift	Status	Rep	Domain	IP
5371 ms	Responded	?	ice-eng.app.box.com	74.112.186.144
5373 ms	Responded	⊗	accounts.google.com	142.250.185.173
5373 ms	Responded	✓	clients2.google.com	142.250.186.142
5374 ms	Responded	✓	clients2.googleusercontent.com	142.250.186.97
11478 ms	Responded	✓	ssl.gstatic.com	142.250.184.227
25794 ms	Responded	✓	www.gstatic.com	142.250.186.99
27799 ms	Responded	✓	cdn01.boxcdn.net	104.16.74.20 104.18.103.56
29500 ms	Responded	✓	cdn.amplitude.com	52.222.206.6 52.222.206.178

d. Host Artifact (Annoying)

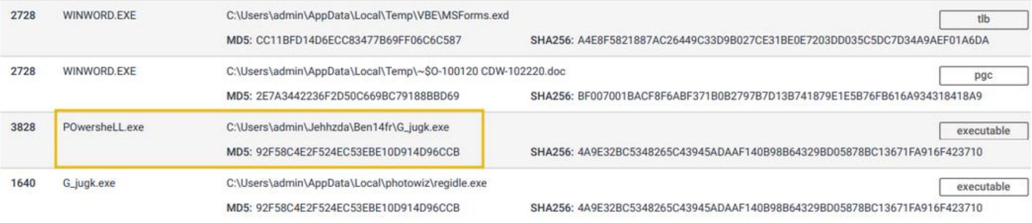
What are host artifacts?

Host artifacts are the **traces** or **observables** that attackers leave on the system, such as registry values, suspicious process execution, attack patterns or IOCs (Indicators of Compromise), files dropped by malicious applications, or anything exclusive to the current threat.

Host artifacts as IoC?

On this level, the attacker will feel a little more annoyed and frustrated if you can detect the attack.
The attacker would need to circle back at this detection level and change his attack tools and methodologies. This is very time-consuming for the attacker, and probably, he will need to spend more resources on his adversary tools.

Exm screenshots:
Report: https://assets.tryhackme.com/additional/pyramidofpain/task5-report.pdf
Below: Files dropped/modified by malicious actor



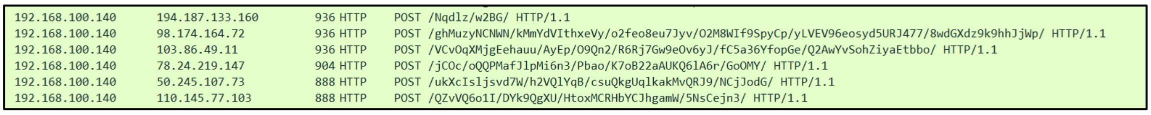
2728	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\VBE\MSForms.exd **MD5:** CC11BFD14D6ECC83477B69FF06C6C587	**SHA256:** A4E8F5821887AC26449C33D9B027CE31BE0E7203DD035C5DC7D34A9AEF01A6DA	tlb
2728	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\~$O-100120 CDW-102220.doc **MD5:** 2E7A3442236F2D50C669BC79188BBD69	**SHA256:** BF007001BACF8F6ABF371B0B2797B7D13B741879E1E5B76FB616A934318418A9	pgc
3828	POwersheLL.exe	C:\Users\admin\Jehhzda\Ben14fr\G_jugk.exe **MD5:** 92F58C4E2F524EC53EBE10D914D96CCB	**SHA256:** 4A9E32BC5348265C43945ADAAF140B98B64329BD05878BC13671FA916F423710	executable
1640	G_jugk.exe	C:\Users\admin\AppData\Local\photowiz\regidle.exe **MD5:** 92F58C4E2F524EC53EBE10D914D96CCB	**SHA256:** 4A9E32BC5348265C43945ADAAF140B98B64329BD05878BC13671FA916F423710	executable

e. Network Artifacts (Annoying)

Network artifacts like:

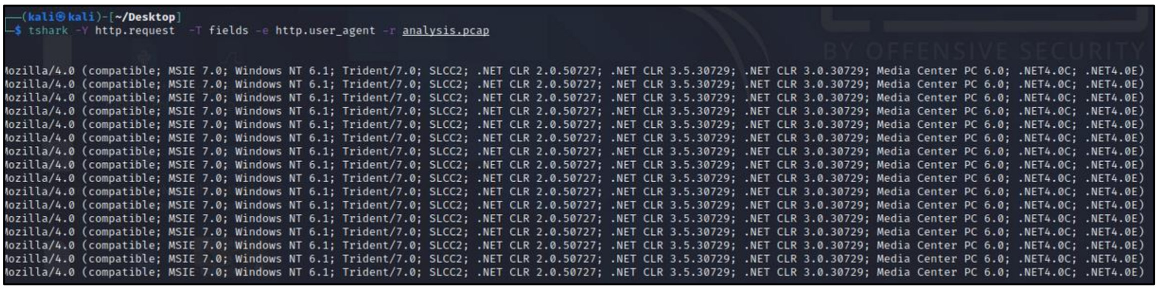
- user-agent string
  - The User-Agent is defined by RFC2616 as the request-header field that contains the information about the user agent originating the request.
- C2 information
- URI patterns
- HTTP POST requests
- Use network protocol analyzer like **TShark** or explore IDS logging (like from **Snort** source).

HTTP POST request Exm:



```
192.168.100.140    194.187.133.160    936 HTTP    POST /Nqdlz/w2BG/ HTTP/1.1
192.168.100.140    98.174.164.72      936 HTTP    POST /ghMuzyNCNWN/kMmYdVIthxeVy/o2feo8eu7Jyv/O2M8WIf9SpyCp/yLVEV96eosyd5URJ477/8wdGXdz9k9hhJjWp/ HTTP/1.1
192.168.100.140    103.86.49.11       936 HTTP    POST /VCvOqXMjgEehauu/AyEp/O9Qn2/R6Rj7Gw9eOv6yJ/fC5a36YfopGe/Q2AwYvSohZiyaEtbbo/ HTTP/1.1
192.168.100.140    78.24.219.147      904 HTTP    POST /jCOc/oQQPMafJlpMi6n3/Pbao/K7oB22aAUKQ6lA6r/GoOMY/ HTTP/1.1
192.168.100.140    50.245.107.73      888 HTTP    POST /ukXcIsljsvd7W/h2VQlYqB/csuQkgUqlkakMvQRJ9/NCjJodG/ HTTP/1.1
192.168.100.140    110.145.77.103     888 HTTP    POST /QZvVQ6o1I/DYk9QgXU/HtoxMCRHbYCJhgamW/5NsCejn3/ HTTP/1.1
```

TShark analysis Exm:



```
┌──(kali㉿kali)-[~/Desktop]
└─$ tshark -Y http.request  -T fields -e http.user_agent -r analysis.pcap

lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
```

f. Tools (Challenging)

At this stage, we have levelled up our detection capabilities against the artifacts. **The attacker would most likely give up trying to break into your network or go back and try to create a new tool that serves the same purpose.**
It will be a game over for the attackers as they would need to invest some money into building a new tool (if they can do so), find the tool that has the same potential, or even get some training to learn how to be proficient in a certain tool.

What would an attacker do?

Attackers would use the utilities to create:

- Malicious macro documents (maldocs) for spearphishing attempts.
- A backdoor that can be used to establish C2 (Command and Control Infrastructure).
- Any custom .EXE, and .DLL files, payloads, or password crackers.

Antivirus signatures, detection rules, and YARA rules can be great weapons for you to use against attackers at this stage.
MalwareBazaar and Malshare for samples, malicious feeds, YARA results – useful for threat hunting and incident response.
SOC Prime Threat Detection Marketplace for detection rules shared by other security professionals.

g. TTP (Tactics, Techniques, Procedures) – (Tough)

Useful resource with regard to studying TTPs is the MITRE ATT&CK Matrix.
If you manage to detect a specific attack and know the techniques, it should be easy to remediate swiftly.

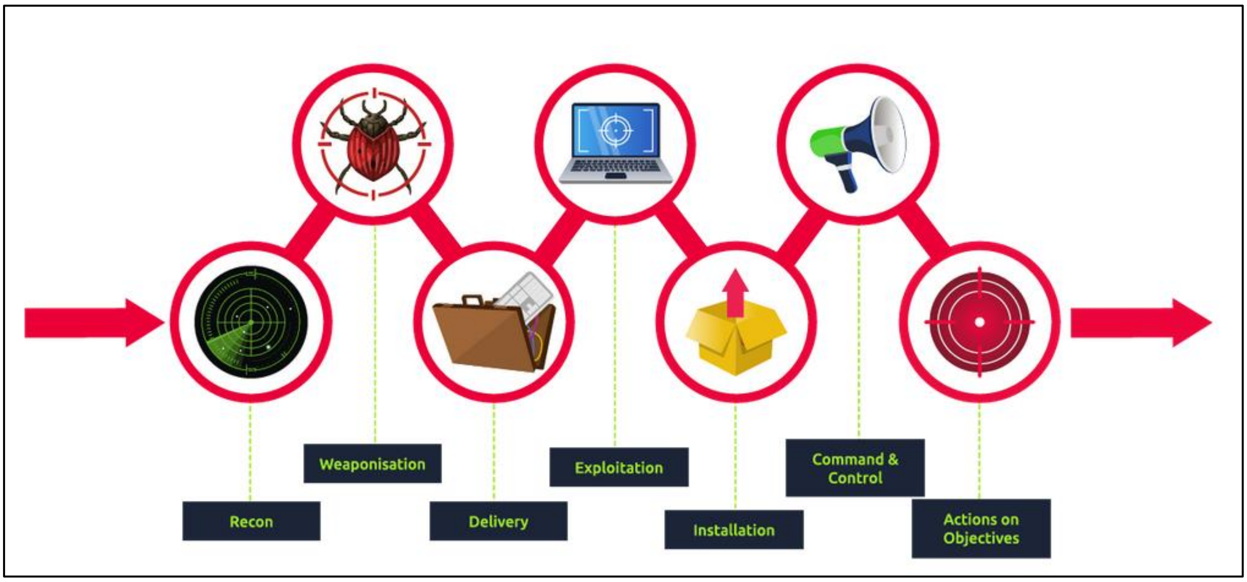
For, example if you could detect a Pass-the-Hash attack using Windows Event Log Monitoring and remediate it, you would be able to find the compromised host very quickly and stop the lateral movement inside your network. At this point, the attacker would have two options:
Go back, do more research and training, reconfigure their custom tools.
Give up and find another target.
Option 2 sounds less time and resource consuming.

CYBER KILL CHAIN

Introduction to CKC

What's is it and what's it for?

The CKC framework defines the steps used by adversaries or malicious actors in cyberspace. To succeed, an adversary needs to go through all phases of the Kill Chain.
*The Cyber Kill Chain framework is designed for **identification** and **prevention** of the network intrusions. Learn what the adversaries need to do to achieve their goals so that you can stop them.*



Use the knowledge of Cyber Kill Chain to:

- Assess your network and system security.
- Identify missing security controls.
- Close security gaps in your infra.

As defender, we must identify and **break the kill chain.**

The CKC Phases

1.Reconnaissance

Reconnaissance is the process of discovering and collecting information on the system and the victim. The reconnaissance phase is the planning phase for the adversaries and they may use methods like:

- OSINT (Open Source Intelligence) – Publicly available data
- OSINT tools such as theHarvester , Hunter.io , OSINT Framework

2.Weaponization

The phase where an attacker may plan and create their malicious payload, set up their C2 techniques, etc.
Perhaps the attacker creates their own malware and payload here (like some APTs), perhaps they choose to buy malware off the dark web etc.
In the Weaponization phase, the attacker would:

a) Create an infected Microsoft Office document containing a malicious macro or VBA (Visual Basic for Applications) scripts.
b) An attacker can create a malicious payload or a very sophisticated worm, implant it on the USB drives, and then distribute them in public. An example of the virus.
c) An attacker would choose Command and Control (C2) techniques for executing the commands on the victim's machine or deliver more payloads. You can read more about the C2 techniques on MITRE ATT&CK.
d) An attacker would select a **backdoor** implant (the way to access the computer system, which includes bypassing the security mechanisms).

What's malware?
Malware is a program or software that is designed to damage, disrupt, or gain unauthorized access to a computer.

What's an exploit?
An exploit is a program or a code that takes advantage of the vulnerability or flaw in the application or system.

What's a payload?
A payload is a malicious code that the attacker runs on the system.

Interesting links:
If you want to learn about macro and VBA, please refer to the article "Intro to Macros and VBA For Script Kiddies" by TrustedSec.
DarkWeb

3.Delivery

The phase where the attacker decides the method for transmitting their payload.

What are the examples of delivery methods that the attacker can use?
Phishing email, Malicious USB distribution (USB drop attack), Watering hole attack, Drive by attack.

4.Exploitation

To gain access to the system, an attacker needs to exploit the vulnerability. This phase is basically about the attackers' method of exploitation.

How does the attacker carry out their exploit in this phase?
Perhaps the victim triggered it by opening malicious attachments or links.

- Zero-day exploit
  - *Zero-day exploit or a zero-day vulnerability is an unknown exploit in the wild that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong. A zero-day exploit leaves NO opportunity for detection at the beginning.*
- Exploiting unpatched known vulnerabilities in software, hardware, or even human.
- An attacker triggers the exploit for server-based vulnerabilities.

For web-based or server-based vulnerabilities, a good place to learn is PortSwigger WSA and https://tryhackme.com/room/owasptop10 .

5.Installation

In this phase, Attacker might install something on the system they compromised, that would allow them to have **persistence** in the system.

Check out the Windows Persistence Room on TryHackMe to learn how an attacker can achieve persistence on Windows.

The persistence can be achieved through:

- Installing a **web shell** on the webserver. A web shell is a malicious script written in web development programming languages such as ASP, PHP, or JSP used by an attacker to maintain access to the compromised system. Because of the web shell simplicity and file formatting (.php, .asp, .aspx, .jsp, etc.) can be difficult to detect and might be classified as benign. You may check out this great article released by Microsoft on various web shell attacks.
- Installing a backdoor on the victim's machine. For example, the attacker can use Meterpreter to install a backdoor on the victim's machine. Meterpreter is a Metasploit Framework payload that gives an interactive shell from which an attacker can interact with the victim's machine remotely and execute malicious code.
- Creating or modifying Windows services. This technique is known as T1543.003 on MITRE ATT&CK (MITRE ATT&CK® is a knowledge base of adversary tactics and techniques based on real-world scenarios). An attacker can create or modify the Windows services to execute malicious scripts or payloads regularly as a part of the persistence. An attacker can use the tools like **sc.exe** (sc.exe lets you Create, Start, Stop, Query, or Delete any Windows Service) and Reg to modify service configurations. The attacker can also **masquerade** the malicious payload by using a service name that is known to be related to the Operating System or legitimate software.
- Adding the entry to the "run keys" for the malicious payload in the Registry or the Startup Folder. By doing that, the payload will execute each time the user logs in on the computer. According to MITRE ATT&CK, there is a startup folder location for individual user accounts and a system-wide startup folder that will be checked no matter what user account logs in. You can read more about the Registry Run Keys / Startup Folder persistence on one of the MITRE ATT&CK techniques.

In this phase, the attacker can also use the **Timestomping** technique to avoid detection by the forensic investigator and also to make the malware appear as a part of a legitimate program. The Timestomping technique lets an attacker modify the file's timestamps, including the modify, access, create and change times.

6.Command & Control (C2)

After gaining persistence, the attacker opens up their C2 channel to remotely control and manipulate the victim. This term is also known as **C&C or C2 Beaconing** as a type of malicious communication between a C&C server and malware on the infected host.

- Common C2 channels today like HTTP p80, HTTPS p443 (Blends in with legitimate web traffic to evade firewall).

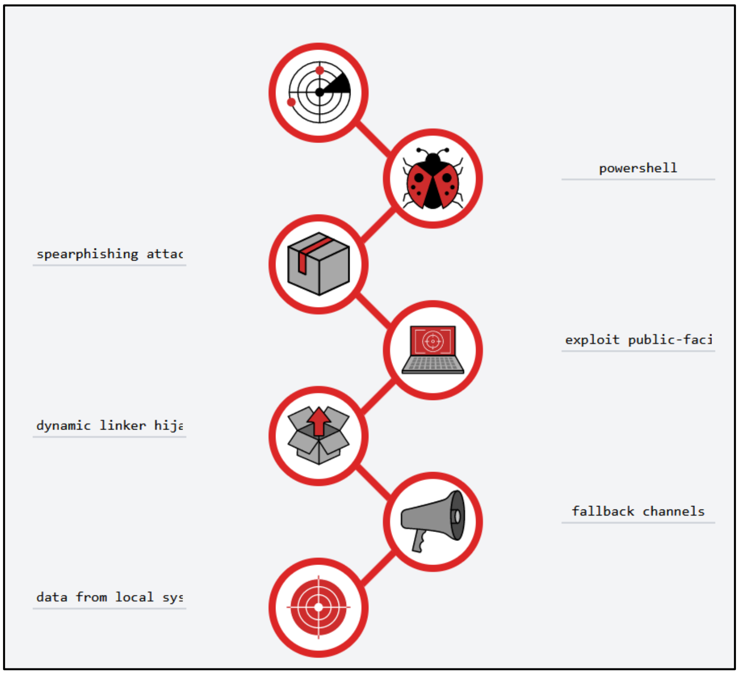
- DNS, Infected machine making DNS request to the DNS server that belongs to the attacker (DNS Tunneling).

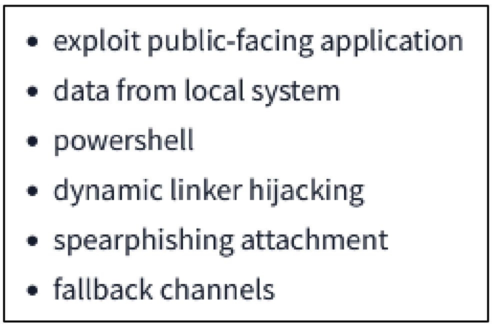
7.Exfiltration (Actions on Objectives)

Now the attacker acts on his ultimate objective. What is the goal of their attack?

Can be anything like

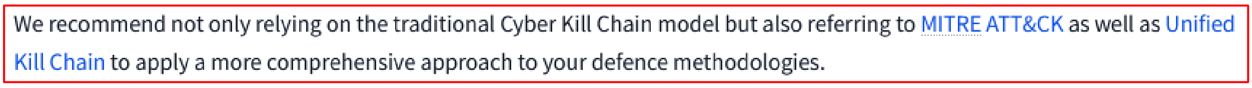
- Collect the credentials from users.
- Perform privilege escalation (gaining elevated access like domain administrator access from a workstation by exploiting the misconfiguration).
- Internal reconnaissance (for example, an attacker gets to interact with internal software to find its vulnerabilities).
- Lateral movement through the company's environment.
- Collect and exfiltrate sensitive data.
- Deleting the backups and shadow copies. Shadow Copy is a Microsoft technology that can create backup copies, snapshots of computer files, or volumes.
- Overwrite or corrupt data.





- exploit public-facing application
- data from local system
- powershell
- dynamic linker hijacking
- spearphishing attachment
- fallback channels

Last time the Cyber Kill Chain was updated was 2011. The absence of update may cause security gaps in the framework, as such, you should also rely on other tools as well because the landscape today has evolved.



We recommend not only relying on the traditional Cyber Kill Chain model but also referring to MITRE ATT&CK as well as Unified Kill Chain to apply a more comprehensive approach to your defence methodologies.

UNIFIED KILL CHAIN

Introduction to UKC

- https://www.unifiedkillchain.com/
- https://tryhackme.com/r/room/unifiedkillchain

What is a kill chain?

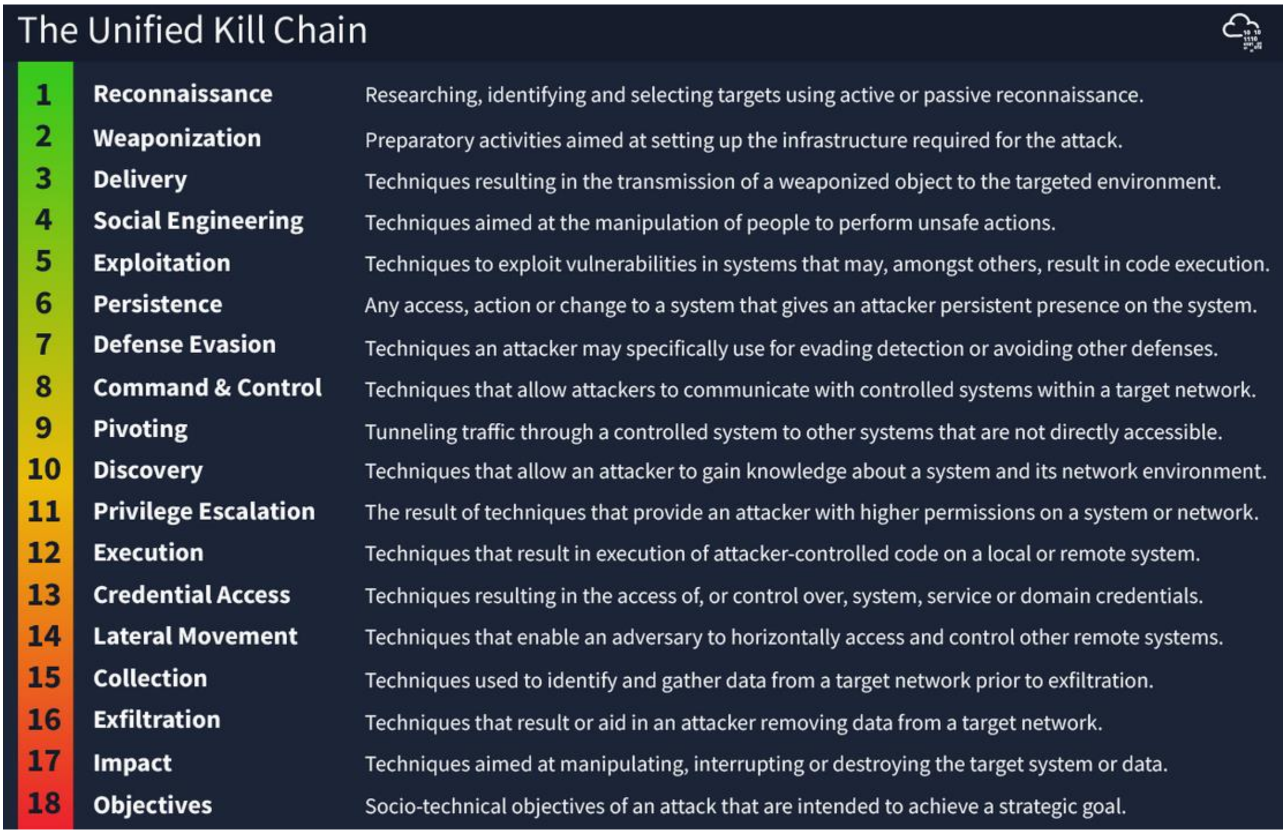
Like in Cyber Kill Chain, kill chain refers to the steps and methodology an attacker uses to approach and intrude their victim. **From a defenders' perspective:** Objective is to understand the Kill Chain. As a defender you want to know what the attacker will do, in order to know how to stop them (implementing security measures).

What is Threat Modelling?

Identifying risk, vulnerabilities, and assets to take steps in improving the security of a system. The purpose of doing threat modelling is to reduce risk with a system and to mitigate threats.

Other frameworks concerned with threat modeling - STRIDE, DREAD, CVSS.

18 Phases in the Unified Kill Chain



The Unified Kill Chain

1	Reconnaissance	Researching, identifying and selecting targets using active or passive reconnaissance.
2	Weaponization	Preparatory activities aimed at setting up the infrastructure required for the attack.
3	Delivery	Techniques resulting in the transmission of a weaponized object to the targeted environment.
4	Social Engineering	Techniques aimed at the manipulation of people to perform unsafe actions.
5	Exploitation	Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.
6	Persistence	Any access, action or change to a system that gives an attacker persistent presence on the system.
7	Defense Evasion	Techniques an attacker may specifically use for evading detection or avoiding other defenses.
8	Command & Control	Techniques that allow attackers to communicate with controlled systems within a target network.
9	Pivoting	Tunneling traffic through a controlled system to other systems that are not directly accessible.
10	Discovery	Techniques that allow an attacker to gain knowledge about a system and its network environment.
11	Privilege Escalation	The result of techniques that provide an attacker with higher permissions on a system or network.
12	Execution	Techniques that result in execution of attacker-controlled code on a local or remote system.
13	Credential Access	Techniques resulting in the access of, or control over, system, service or domain credentials.
14	Lateral Movement	Techniques that enable an adversary to horizontally access and control other remote systems.
15	Collection	Techniques used to identify and gather data from a target network prior to exfiltration.
16	Exfiltration	Techniques that result or aid in an attacker removing data from a target network.
17	Impact	Techniques aimed at manipulating, interrupting or destroying the target system or data.
18	Objectives	Socio-technical objectives of an attack that are intended to achieve a strategic goal.

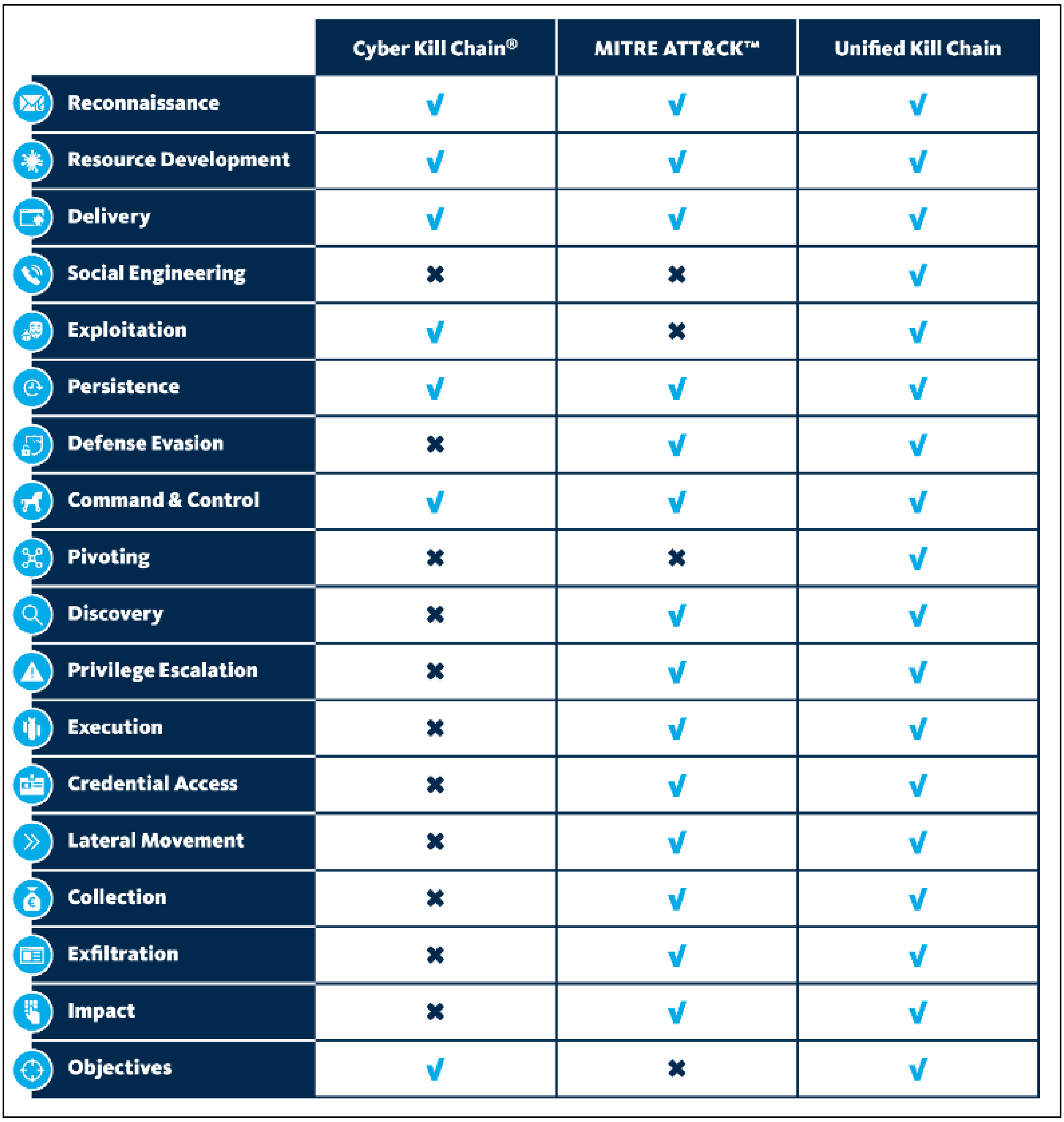
..

Benefits of the UKC

Benefits	How do other frameworks compare?

Modern (released in 2017, updated in 2022).	Some frameworks, such as MITRE's were released in 2013, when the cybersecurity landscape was very different.
The UKC is extremely detailed (18 phases).	Other frameworks often have a small handful of phases.
The UKC covers an entire attack - from reconnaissance, exploitation, post-exploitation and includes identifying an attacker's motivation.	Other frameworks cover a limited number of phases.
The UKC highlights a much more realistic attack scenario. Various stages will often re-occur. For example, after exploiting a machine, an attacker will begin reconnaissance to pivot another system.	Other frameworks do not account for the fact that an attacker will go back and forth between the various phases during an attack.

Scope of the Unified Kill Chain



	Cyber Kill Chain®	MITRE ATT&CK™	Unified Kill Chain
Reconnaissance	✓	✓	✓
Resource Development	✓	✓	✓
Delivery	✓	✓	✓
Social Engineering	✖	✖	✓
Exploitation	✓	✖	✓
Persistence	✓	✓	✓
Defense Evasion	✖	✓	✓
Command & Control	✓	✓	✓
Pivoting	✖	✖	✓
Discovery	✖	✓	✓
Privilege Escalation	✖	✓	✓
Execution	✖	✓	✓
Credential Access	✖	✓	✓
Lateral Movement	✖	✓	✓
Collection	✖	✓	✓
Exfiltration	✖	✓	✓
Impact	✖	✓	✓
Objectives	✓	✖	✓

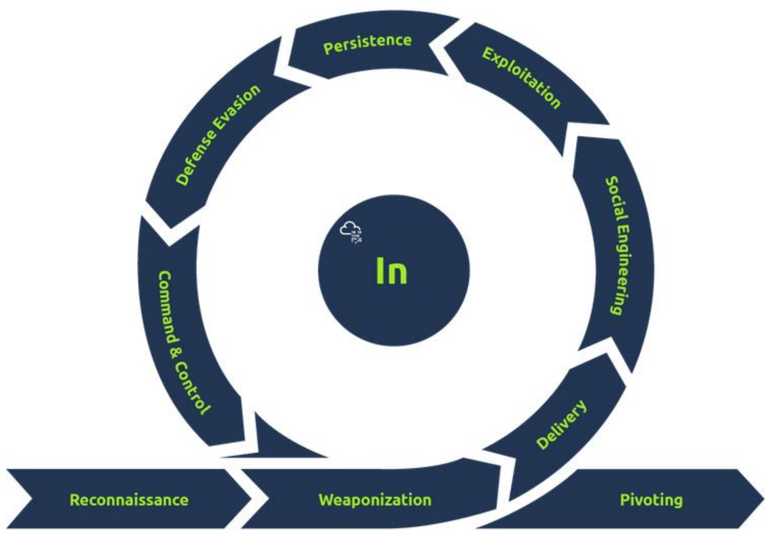
Series of phases

Phase In >	Phase Through >	Phase Out
Initial foothold	Network Propagation	Action on Objectives

1.Phase In (Initial Foothold)

The focus of this phase is for an attacker to gain access to a system or networked environment. This series of phases also accommodates for an attacker creating a form of persistence (such as files or a process that allows the attacker to connect to the machine at any time)

Reconnaissance
Weaponization
Delivery
Social Engineering
Exploitation
Persistence
Defense Evasion
Command & Control
Pivoting



Reconnaissance (MITRE Tactic TA0043)

This phase of the UKC describes techniques that an adversary employs to gather information relating to their target. This can be achieved through means of passive and active reconnaissance. The information gathered during this phase is used all throughout the later stages of the UKC (such as the initial foothold).

- Discovering what systems and services are running on the target, this is beneficial information in the weaponization and exploitation phases of this section.
- Finding contact lists or lists of employees that can be impersonated or used in either a social engineering or phishing attack.
- Looking for potential credentials that may be of use in later stages, such as pivoting or initial access.
- Understanding the network topology and other networked systems can be used to pivot too.

Weaponization (MITRE Tactic TA0001)

This phase of the UKC describes the adversary setting up the necessary infrastructure to perform the attack. For example, this could be setting up a command-and-control server, or a system capable of catching reverse shells and delivering payloads to the system.

Social Engineering (MITRE Tactic TA0001)

This phase of the UKC describes techniques that an adversary can employ to manipulate employees to perform actions that will aid in the adversaries attack. For example, a social engineering attack could include:

- Getting a user to open a malicious attachment.
- Impersonating a web page and having the user enter their credentials.

- Calling or visiting the target and impersonating a user (for example, requesting a password reset) or being able to gain access to areas of a site that the attacker would not previously be capable of (for example, impersonating a utility engineer).

Exploitation (MITRE Tactic TA0002)
This phase of the UKC describes how an attacker takes advantage of weaknesses or vulnerabilities present in a system. The UKC defines "Exploitation" as abuse of vulnerabilities to perform code execution. For example:

- Uploading and executing a reverse shell to a web application.
- Interfering with an automated script on the system to execute code.
- Abusing a web application vulnerability to execute code on the system it is running on.

Persistence (MITRE Tactic TA0003)
This phase of the UKC is rather short and simple. Specifically, this phase of the UKC describes the techniques an adversary uses to maintain access to a system they have gained an initial foothold on. For example:

- Creating a service on the target system that will allow the attacker to regain access.
- Adding the target system to a Command & Control server where commands can be executed remotely at any time.
- Leaving other forms of backdoors that execute when a certain action occurs on the system (i.e. a reverse shell will execute when a system administrator logs in).

Defence Evasion (MITRE Tactic TA0005)
The "Defence Evasion" section of the UKC is one of the more valuable phases of the UKC. This phase specifically is used to understand the techniques an adversary uses to evade defensive measures put in place in the system or network. For example, this could be:

- Web application firewalls.
- Network firewalls.
- Anti-virus systems on the target machine.
- Intrusion detection systems.

Command & Control (MITRE Tactic TA0011)
The "Command & Control" phase of the UKC combines the efforts an adversary made during the "Weaponization" stage of the UKC to establish communications between the adversary and target system.
An adversary can establish command and control of a target system to achieve its action on objectives. For example, the adversary can:

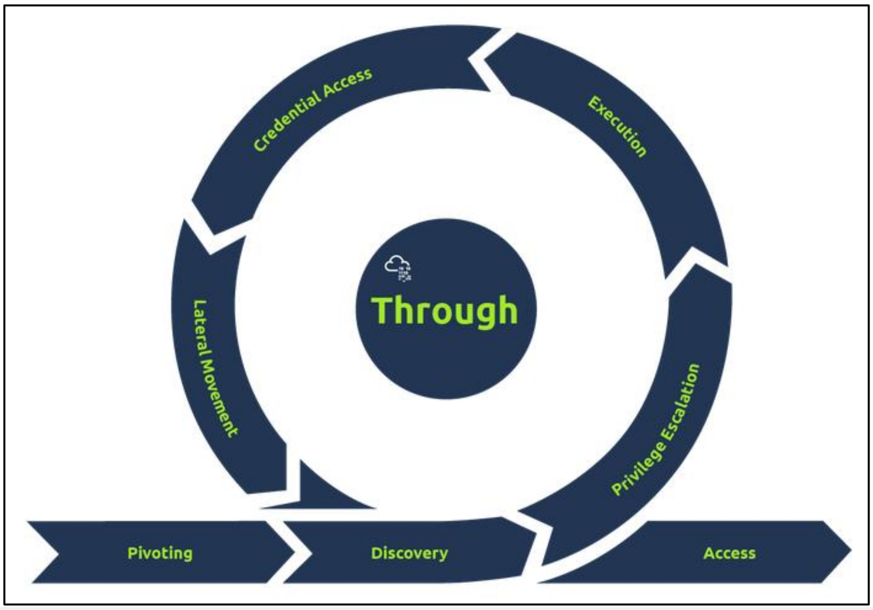
- Execute commands.
- Steal data, credentials and other information.
- Use the controlled server to pivot to other systems on the network.

Pivoting (MITRE Tactic TA0008)
"Pivoting" is the technique an adversary uses to reach other systems within a network that are not otherwise accessible (for example, they are not exposed to the internet). There are often many systems in a network that are not directly reachable and often contain valuable data or have weaker security.

For example, an adversary can gain access to a web server that is publicly accessible to attack other systems that are within the same network (but are not accessible via the internet).

2.Phase Through (Network Propagation)

This phase follows a successful foothold being established on the target network.
An attacker would seek to gain additional access and privileges to systems and data to fulfil their goals. The attacker would set up a base on one of the systems to act as their pivot point and use it to gather information about the internal network.

Pivoting	
Discovery	
Privilege Escalation	
Execution	
Credential Access	
Lateral Movement	

Pivoting (MITRE Tactic TA0008)
Once the attacker has access to the system, they would use it as their staging site and a tunnel between their command operations and the victim's network. The system would also be used as the distribution point for all malware and backdoors at later stages.

Discovery (MITRE Tactic TA0007)
The adversary would uncover information about the system and the network it is connected to. Within this stage, the knowledge base would be built from the active user accounts, the permissions granted, applications and software in use, web browser activity, files, directories and network shares, and system configurations.

Privilege Escalation (MITRE Tactic TA0004)
Following their knowledge-gathering, the adversary would try to gain more prominent permissions within the pivot system. They would leverage the information on the accounts present with vulnerabilities and misconfigurations found to elevate their access to one of the following superior levels:

- *SYSTEM/ ROOT.*
- *Local Administrator.*
- *A user account with Admin-like access.*
- *A user account with specific access or functions.*

Execution (MITRE Tactic TA0002)
Recall when the adversary set up their attack infrastructure. Once the attacker has access to the system, they would use it as their staging site and a tunnel between their command

operations and the victim's network. The system would also be used as the distribution point for all malware and backdoors at later stages. and weaponised payloads?

This is where they deploy their malicious code using the pivot system as their host. Remote trojans, C2 scripts, malicious links and scheduled tasks are deployed and created to facilitate a recurring presence on the system and uphold their persistence.

Credential Access (MITRE Tactic TA0006)

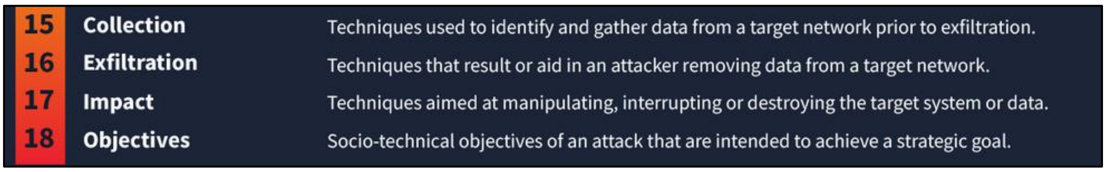
Working hand in hand with the Privilege Escalation stage, the adversary would attempt to steal account names and passwords through various methods, including keylogging and credential dumping. This makes it harder to detect during their attack as they would be using legitimate credentials.

Lateral Movement (MITRE Tactic TA0008)

With the credentials and elevated privileges, the adversary would seek to move through the network and jump onto other targeted systems to achieve their primary objective. The stealthier the technique used, the better.

3.Phase Out (Action on Objectives)

This phase wraps up the journey of an adversary's attack on an environment, where they have critical asset access and can fulfil their attack goals. These goals are usually geared toward compromising the confidentiality, integrity and availability (CIA) triad.



15	Collection	Techniques used to identify and gather data from a target network prior to exfiltration.
16	Exfiltration	Techniques that result or aid in an attacker removing data from a target network.
17	Impact	Techniques aimed at manipulating, interrupting or destroying the target system or data.
18	Objectives	Socio-technical objectives of an attack that are intended to achieve a strategic goal.

Collection

Exfiltration

Impact

Objectives

Collection MITRE Tactic (TA0009)

After all the hunting for access and assets, the adversary will be seeking to gather all the valuable data of interest. This, in turn, compromises the confidentiality of the data and would lead to the next attack stage – Exfiltration. The main target sources include drives, browsers, audio, video and email.

Exfiltration (MITRE Tactic TA0010**)**

To elevate their compromise, the adversary would seek to steal data, which would be packaged using encryption measures and compression to avoid any detection. The C2 channel and tunnel deployed in the earlier phases will come in handy during this process.

Impact (MITRE Tactic TA0040**)**

If the adversary seeks to compromise the integrity and availability of the data assets, they would manipulate, interrupt or destroy these assets. The goal would be to disrupt business and operational processes and may involve removing account access, disk wipes, and data encryption such as ransomware, defacement and denial of service (DoS) attacks.

Objectives

With all the power and access to the systems and network, the adversary would seek to achieve their strategic goal for the attack.
For example, if the attack was financially motivated, they may seek to encrypt files and systems with ransomware and ask for payment to release the data. In other instances, the attacker may seek to damage the reputation of the business, and they would release private and confidential information to the public.

DIAMOND MODEL

Intro of Diamond Model

https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

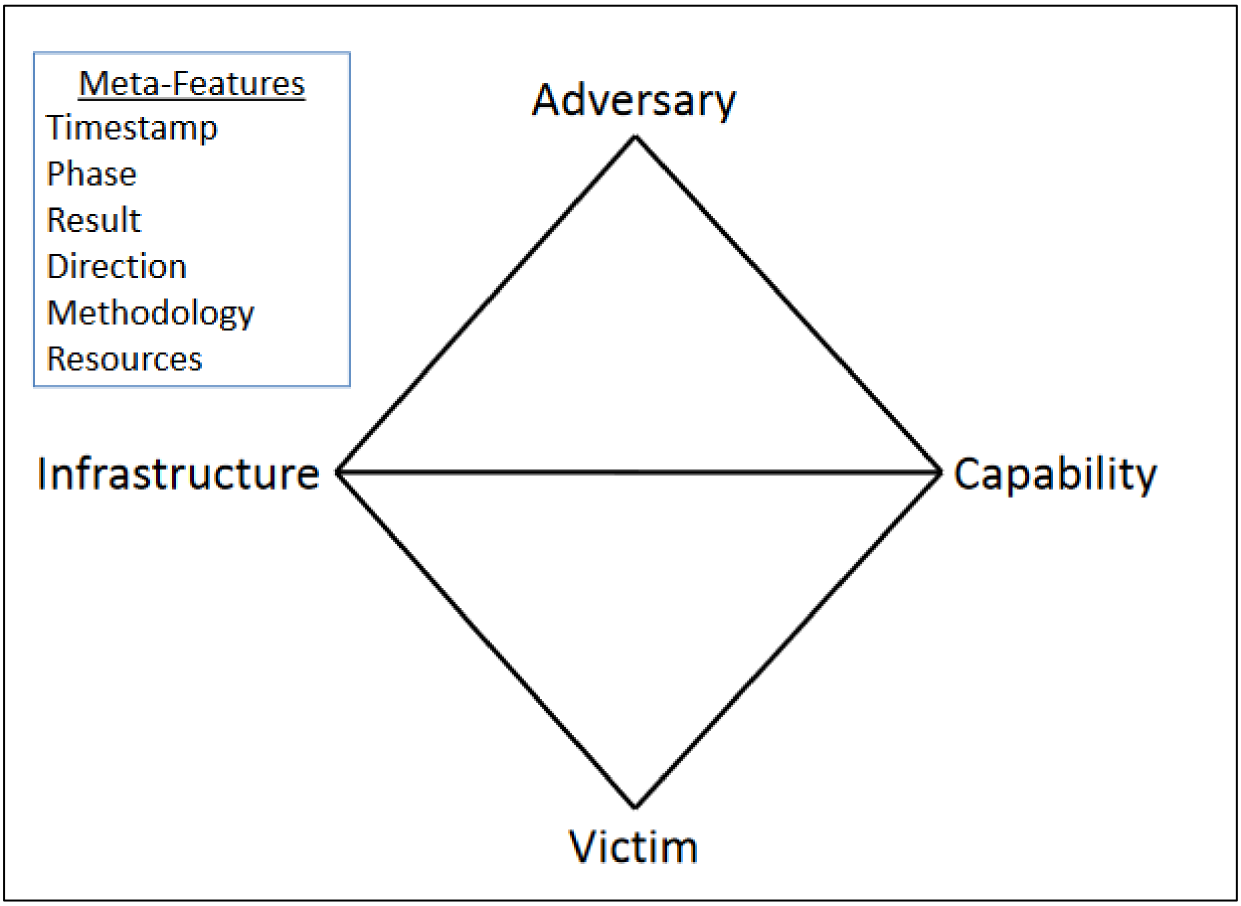
What is the Diamond Model

The Diamond Model of Intrusion Analysis is **a model to describe cyber attacks**. It contains 4 parts - adversary, infrastructure, capability, and target/victim.

The *Diamond Model* carries the essential concepts of intrusion analysis and adversary operations while allowing the flexibility to expand and encompass new ideas and concepts. The model provides various opportunities to integrate intelligence in real-time for network defense, automating correlation across events, classifying events with confidence into adversary campaigns, and forecasting adversary operations while planning and gaming mitigation strategies.

Why should you learn about the Diamond Model?

The Diamond Model can help you identify the elements of an intrusion
The Diamond Model can also help explain to other people who are non-technical about what happened during an event or any valuable information on the malicious threat actor.



Core Features (4)

1. Adversary

An adversary is also known as an attacker, enemy, cyber threat actor, or hacker. The adversary is the person who stands behind the cyberattack.

Cyberattacks can be an instruction or a breach.
According to the creators of the Diamond Model, an adversary is an actor or organization responsible for utilizing a capability against the victim to achieve their intent. Adversary knowledge can generally be mysterious, and this core feature is likely to be empty for most events – at least at the time of discovery.

It is essential to know the distinction between adversary operator and adversary customer because it will help you understand intent, attribution, adaptability, and persistence by helping to frame the relationship between an adversary and victim pair.

- ***Adversary Operator*** is the "hacker", someone conducting the intrusion.
- ***Adversary Customer*** is the entity that stand to benefits from the activity in the intrusion. It **can** be the same person with Adversary Operator, or it can be different.

2. Victim

Target of the adversary. A victim can be an organization, person, target email address, IP address, domain, etc.

A victim can be an opportunity for the attackers to get a foothold on the organization they are trying to attack. There is always a victim in every cyberattack. For example, the spear-phishing email (a well-crafted email targeting a specific person of interest) was sent to the company, and someone (victim) clicked on the link. In this case, the victim is the selected target of interest for an adversary.

It's essential to understand the difference between the victim persona and the victim assets because they serve different analytic functions.

- **Victim Personae** – People (or Org, industries, job roles, etc) being targeted and whose assets are being attacked.
- **Victim Assets** – The attack surface includes the set of systems, network, email, hosts, IP addresses, social media accounts, etc, to which the adversary direct their capabilities.

3. Capability

Capability is the skill, tools, and techniques used by the adversary in the event. The capability highlights the adversary's tactics, techniques, and procedures (TTPs).

The capability can include all techniques used to attack the victims, from the less sophisticated methods, such as manual password guessing, to the most sophisticated techniques, like developing malware or a malicious tool.

- **Capability Capacity** is all the vulnerabilities and exposures that the individual capability can use.

- An **Adversary Arsenal** is a set of capabilities that belong to an adversary. The combined capacities of an adversary's capabilities make it the adversary's arsenal.

4. Infrastructure

Infrastructure is also known as software or hardware. Infrastructure is the physical or logical interconnections that the adversary uses to deliver a capability or maintain control of capabilities. The infrastructure can also be IP addresses, domain names, email addresses, or even a malicious USB device found in the street that is being plugged into a workstation.
For example, a command-and-control centre (C2) and the results from the victim (data exfiltration).

- **Type 1** Infrastructure is the infrastructure controlled or owned by the *adversary*.

- **Type 2** Infrastructure is the infrastructure controlled by an *intermediary*. Sometimes the intermediary might or might not be aware of it. This is the infrastructure that a victim will see as the adversary. Type 2 Infrastructure has the purpose of obfuscating the source and attribution of the activity. Type 2 Infrastructure includes malware staging servers, malicious domain names, compromised email accounts, etc.

- **Service Providers** are organizations that provide services considered critical for the adversary availability of Type 1 and Type 2 Infrastructures, for example, Internet Service Providers, domain registrars, and webmail providers.

Additional Components

Event Meta Features

6 possible meta-features can be added to the Diamond Model. Meta-features are not required, but they can add some valuable information or intelligence to the Diamond Model.

- ***Timestamp*** - is the date and time of the event. Each event can be recorded with a date and time that it occurred, such as 2021-09-12 02:10:12.136. The timestamp can include when the event started and stopped. Timestamps are essential to help determine the patterns and group the malicious activity. For example, if the intrusion or breach happened at 3 am in the United States, it might be possible that the attack was carried out from a specific country with a different time zone and standard business hours.

- ***Phase*** - these are the phases of an intrusion, attack, or breach. According to the Diamond Model creators and the Axiom 4, "Every malicious activity contains two or more phases which must be successfully executed in succession to achieve the desired result." Malicious activities do not occur as single events, but rather as a sequence of events. A great example can be the Cyber Kill Chain developed by Lockheed Martin. You can find out more about the Cyber Kill Chain by visiting the Cyber Kill Chain room on TryHackMe.
  The phases can be:
  - Reconnaissance
  - Weaponization
  - Delivery
  - Exploitation
  - Installation
  - Command & Control

- Actions on Objective

For example, an attacker needs to do some research to discover the target or a victim. Then they would try to exploit the target, establish a command-and-control centre and, lastly, exfiltrate the sensitive information.

- ***Result*** - While the results and post-conditions of an adversary's operations will not always be known or have a high confidence value when they are known, they are helpful to capture. It is crucial to capture the results and post-conditions of an adversary's operations, but sometimes they might not always be known. The event results can be labelled as "success," "failure," or "unknown." The event results can also be related to the CIA (confidentiality, integrity, and availability) triad, such as Confidentiality Compromised, Integrity Compromised, and Availability Compromised. Another approach can also be documenting all of the post-conditions resulting from the event, for example, information gathered in the reconnaissance stage or successful passwords/sensitive data exfiltration.

- ***Direction*** - This meta-feature helps describe host-based and network-based events and represents the direction of the intrusion attack. The Diamond Model of Intrusion Analysis defines seven potential values for this meta-feature: Victim-to-Infrastructure, Infrastructure-to-Victim, Infrastructure-to-Infrastructure, Adversary-to-Infrastructure, Infrastructure-to-Adversary, Bidirectional or Unknown.

- ***Methodology*** - This meta-feature will allow an analyst to describe the general classification of intrusion, for example, phishing, DDoS, breach, port scan, etc.

- ***Resources*** - According to the Diamond Model, every intrusion event needs one or more external resources to be satisfied to succeed. Examples of the resources can include the following: software (e.g., operating systems, virtualization software, or Metasploit framework), knowledge (e.g., how to use Metasploit to execute the attack and run the exploit), information (e.g., a username/password to masquerade), hardware (e.g., servers, workstations, routers), funds (e.g., money to purchase domains), facilities (e.g., electricity or shelter), access (e.g., a network path from the source host to the victim and vice versa, network access from an Internet Service Provider (ISP)).

Social-Political Component

The social-political component describes the needs and intent of the adversary, for example, financial gain, gaining acceptance in the hacker community, hacktivism, or espionage.

The scenario can be that the victim provides a "product", for example, computing resources & bandwidth as a zombie in a botnet for crypto mining (producing new cryptocurrencies by solving cryptographic equations through the use of computers) purposes, while the adversary consumes their product or gets financial gain.

Technology Component

Technology - the technology meta-feature or component highlights the relationship between the core features: capability and infrastructure. The *capability* and *infrastructure* describe how the adversary operates and communicates. A scenario can be a watering-hole attack which is a methodology where the adversary compromises legitimate websites that they believe their targeted victims will visit.

MITRE

- ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) Framework
- CAR (Cyber Analytics Repository) Knowledge Base
- ENGAGE (sorry, not a fancy acronym)
- D3FEND (Detection, Denial, and Disruption Framework Empowering Network Defense)
- AEP (ATT&CK Emulation Plans)

ATT&CK Framework

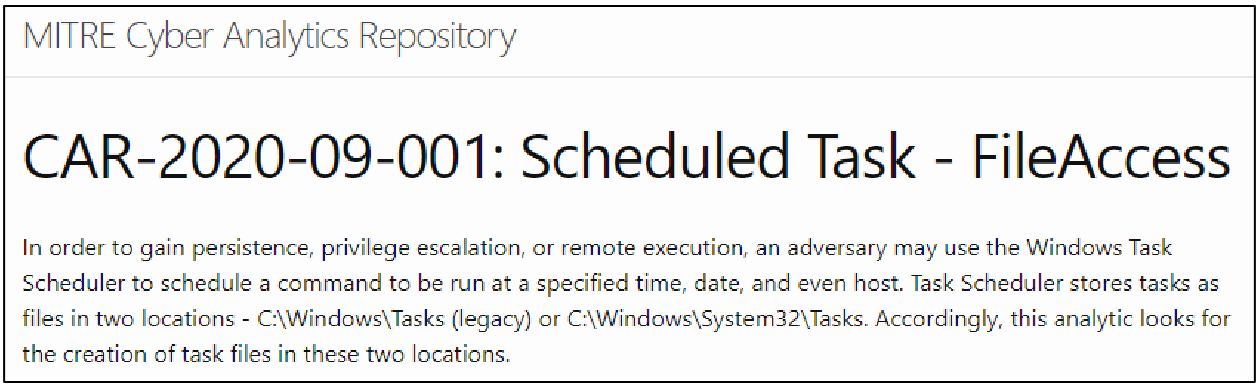
MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.
https://attack.mitre.org/

The same data can be viewed via the **MITRE ATT&CK® Navigator**: "*The ATT&CK® Navigator is designed to provide basic navigation and annotation of ATT&CK® matrices, something that people are already doing today in tools like Excel. We've designed it to be simple and generic - you can use the Navigator to visualize your defensive coverage, your red/blue team planning, the frequency of detected techniques, or anything else you want to do*."

CAR Knowledge Base (Cyber Analytics Repository)

(CAR) is a knowledge base of analytics developed by *MITRE* based on the *MITRE* ATT&CK® adversary model. CAR defines a data model that is leveraged in its pseudocode representations but also includes implementations directly targeted at specific tools (e.g., *Splunk*, EQL) in its analytics.

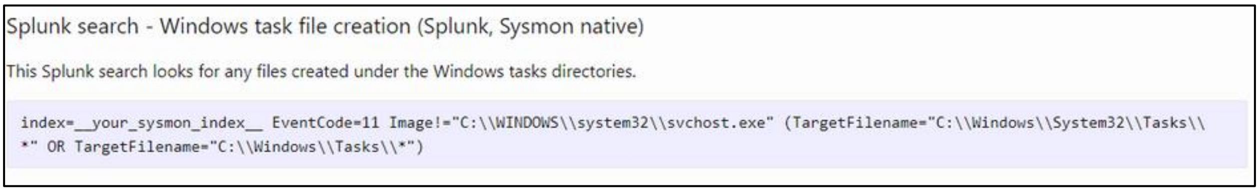
To summarize, CAR is a great place for finding **analytics** that takes us further than the Mitigation and Detection summaries in the ATT&CK® framework. This tool is **not** a replacement for ATT&CK® but an added resource.



MITRE Cyber Analytics Repository

CAR-2020-09-001: Scheduled Task - FileAccess

In order to gain persistence, privilege escalation, or remote execution, an adversary may use the Windows Task Scheduler to schedule a command to be run at a specified time, date, and even host. Task Scheduler stores tasks as files in two locations - C:\Windows\Tasks (legacy) or C:\Windows\System32\Tasks. Accordingly, this analytic looks for the creation of task files in these two locations.

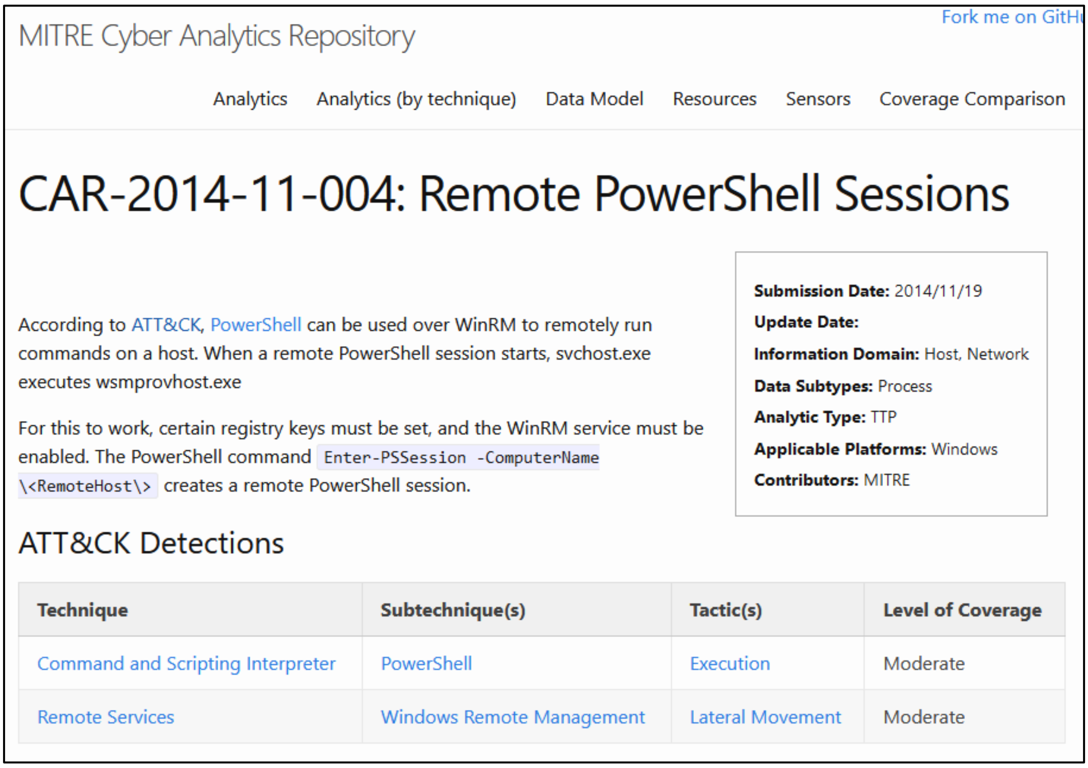


Splunk search - Windows task file creation (Splunk, Sysmon native)

This Splunk search looks for any files created under the Windows tasks directories.

```
index=__your_sysmon_index__ EventCode=11 Image!="C:\\WINDOWS\\system32\\svchost.exe" (TargetFilename="C:\\Windows\\System32\\Tasks\\
*" OR TargetFilename="C:\\Windows\\Tasks\\*")
```

Exm:



CAR-2014-11-004: Remote PowerShell Sessions

According to ATT&CK, PowerShell can be used over WinRM to remotely run commands on a host. When a remote PowerShell session starts, svchost.exe executes wsmprovhost.exe

For this to work, certain registry keys must be set, and the WinRM service must be enabled. The PowerShell command `Enter-PSSession -ComputerName \<RemoteHost\>` creates a remote PowerShell session.

Submission Date: 2014/11/19
Update Date:
Information Domain: Host, Network
Data Subtypes: Process
Analytic Type: TTP
Applicable Platforms: Windows
Contributors: MITRE

ATT&CK Detections

Technique	Subtechnique(s)	Tactic(s)	Level of Coverage
Command and Scripting Interpreter	PowerShell	Execution	Moderate
Remote Services	Windows Remote Management	Lateral Movement	Moderate

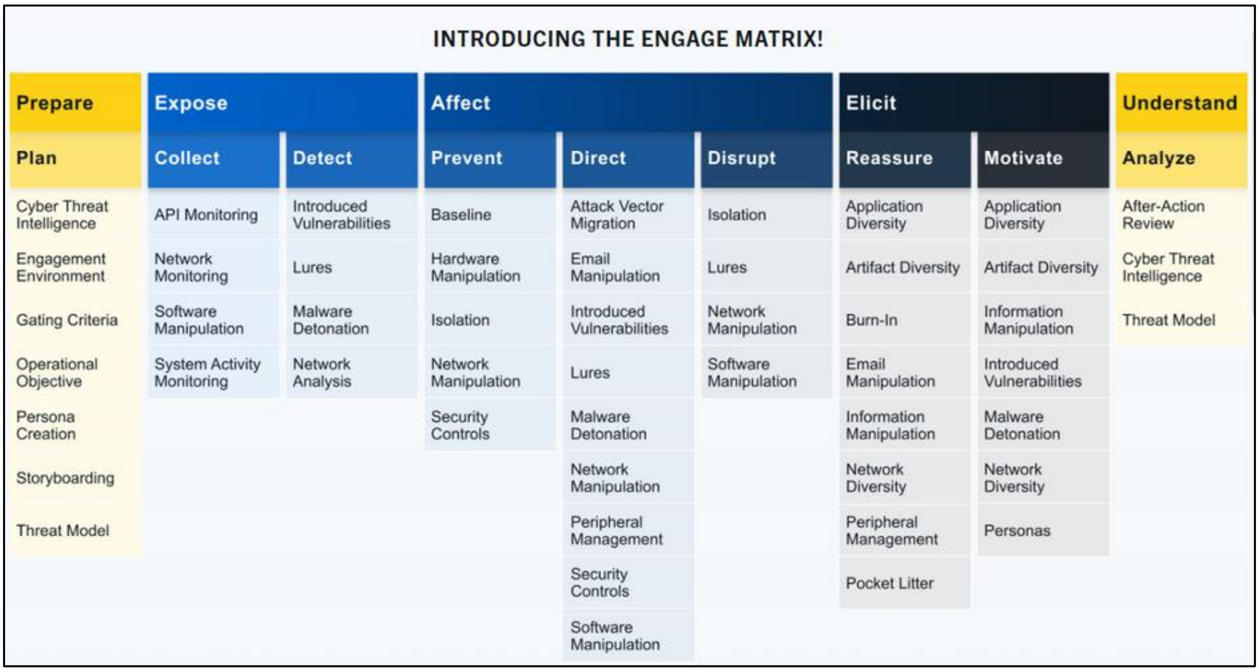
MITRE Engage

***MITRE* Engage** is a framework for planning and discussing adversary engagement operations that empowers you to engage your adversaries and achieve your cybersecurity goals.

MITRE Engage is considered an **Adversary Engagement Approach**. This is accomplished by the implementation of **Cyber Denial** and **Cyber Deception**.
Adversary Engagement Approach – Implementing **Cyber Denial** & **Cyber Deception**.
https://engage.mitre.org/matrix/

The Engage website provides a starter kit to get you 'started' with the Adversary Engagement Approach. The starter kit is a collection of whitepapers and PDFs explaining various checklists, methodologies, and processes to get you started.

Cyber Denial	We prevent the adversary's ability to conduct their operations
Cyber Deception	We intentionally plant artifacts to mislead the adversary



INTRODUCING THE ENGAGE MATRIX!

Prepare	Expose		Affect			Elicit		Understand
Plan	Collect	Detect	Prevent	Direct	Disrupt	Reassure	Motivate	Analyze
Cyber Threat Intelligence	API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity	After-Action Review
Engagement Environment	Network Monitoring	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity	Cyber Threat Intelligence
Gating Criteria	Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation	Threat Model
Operational Objective	System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities	
Persona Creation			Security Controls	Malware Detonation		Information Manipulation	Malware Detonation	
Storyboarding				Network Manipulation		Network Diversity	Network Diversity	
Threat Model				Peripheral Management		Peripheral Management	Personas	
				Security Controls		Pocket Litter		
				Software Manipulation				

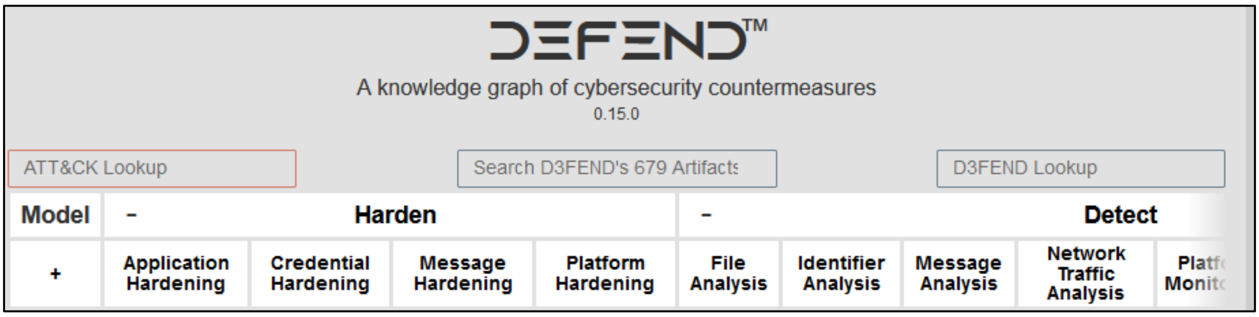
Describing the categories in MITRE ENGAGE:

- **Prepare** the set of operational actions that will lead to your desired outcome (input)
- **Expose** adversaries when they trigger your deployed deception activities
- **Affect** adversaries by performing actions that will have a negative impact on their operations
- **Elicit** information by observing the adversary and learn more about their modus operandi (TTPs)
- **Understand** the outcomes of the operational actions (output)

MITRE D3FEND

(Detection-Denial-Disruption Framework Empowering Network Defense)

MITRE D3FEND is A knowledge graph of cybersecurity countermeasures.
Collection of knowledge based on defense strategy/actions and can be cross referenced with ATT&CK. https://d3fend.mitre.org/
Exm:



A knowledge graph of cybersecurity countermeasures

0.15.0

Model	- Harden				- Detect				
+	Application Hardening	Credential Hardening	Message Hardening	Platform Hardening	File Analysis	Identifier Analysis	Message Analysis	Network Traffic Analysis	Platf Monit

You're provided with information on what is the technique (**definition**), how the technique works (**how it works**), things to think about when implementing the technique (**considerations**), and how to utilize the technique (**example**).

Note, as with other MITRE resources, you can filter based on the ATT&CK matrix.
Since this resource is in beta and will change significantly in future releases, we won't spend that much time on D3FEND.

ATT&CK Emulation Plans

If these tools provided to us previously by MITRE are not enough, under MITRE ENGENUITY, we have **CTID**, the **Adversary Emulation Library**, and **ATT&CK® Emulation Plans**.

MITRE formed an organization named The Center of Threat-Informed Defense (**CTID**). This organization consists of various companies and vendors from around the globe. Their objective is to conduct research on cyber threats and their TTPs and share this research to improve cyber defenses for all.

Some of the companies and vendors who are participants of **CTID**:

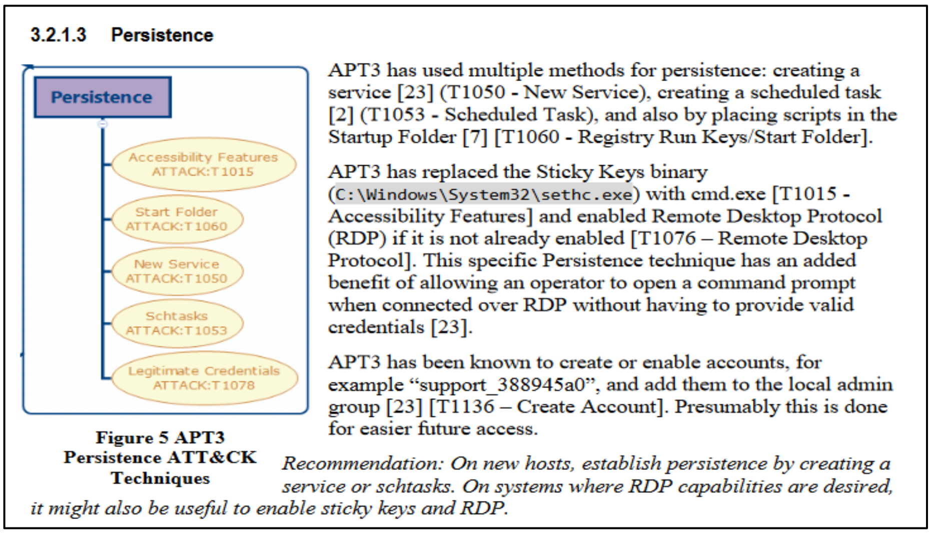
- AttackIQ (founder)
- Verizon
- Microsoft (founder)
- Red Canary (founder)
- Splunk

Adversary Emulation Library & ATT&CK® Emulations Plans

The Adversary Emulation Library is a public library making adversary emulation plans a free resource for blue/red teamers. The library and the emulations are a contribution from CTID. There are several ATT&CK® Emulation Plans currently available: APT3, APT29, and FIN6. The emulation plans are a step-by-step guide on how to mimic a specific threat group. If any of the C-Suite were to ask, "how would we fare if APT29 hits us?" This can easily be answered by referring to the results of the execution of the emulation plan.

Github: https://github.com/center-for-threat-informed-defense/adversary_emulation_library/tree/master

Exm showing details of APT3 Persistance operation and techniques:


Persistence
Accessibility Features ATTACK:T1015
Start Folder ATTACK:T1060
New Service ATTACK:T1050
Schtasks ATTACK:T1053
Legitimate Credentials ATTACK:T1078

3.2.1.3 Persistence

APT3 has used multiple methods for persistence: creating a service [23] (T1050 - New Service), creating a scheduled task [2] (T1053 - Scheduled Task), and also by placing scripts in the Startup Folder [7] [T1060 - Registry Run Keys/Start Folder].

APT3 has replaced the Sticky Keys binary (`C:\Windows\System32\sethc.exe`) with cmd.exe [T1015 - Accessibility Features] and enabled Remote Desktop Protocol (RDP) if it is not already enabled [T1076 – Remote Desktop Protocol]. This specific Persistence technique has an added benefit of allowing an operator to open a command prompt when connected over RDP without having to provide valid credentials [23].

APT3 has been known to create or enable accounts, for example "support_388945a0", and add them to the local admin group [23] [T1136 – Create Account]. Presumably this is done for easier future access.

Figure 5 APT3 Persistence ATT&CK Techniques

Recommendation: On new hosts, establish persistence by creating a service or schtasks. On systems where RDP capabilities are desired, it might also be useful to enable sticky keys and RDP.

ATT&CK and Threat Intelligence

Threat Intelligence (TI) or **Cyber Threat Intelligence (CTI)** is the information, or TTPs, attributed to the adversary.

By using threat intelligence, as defenders, we can make better decisions regarding the defensive strategy. Large corporations might have an in-house team whose primary objective is to gather threat intelligence for other teams within the organization, aside from using threat intel already readily available. Some of this threat intel can be open source or through a subscription with a vendor, such as CrowdStrike. In contrast, many defenders wear multiple hats (roles) within some organizations, and they need to take time from their other tasks to focus on threat intelligence. To cater to the latter, we'll work on a scenario of using ATT&CK® for threat intelligence. The goal of threat intelligence is to make the information actionable.

Conclusion of MITRE

Many vendors of security products and security teams across the globe consider these contributions from MITRE invaluable in the day-to-day efforts to thwart evil. The more information we have as defenders, the better we are equipped to fight back. Some of you might be looking to transition to become a SOC analyst, detection engineer, cyber threat analyst, etc. these tools/resources are a must to know.

As mentioned before, though, this is not only for defenders. As red teamers, these tools/resources are useful as well. Your objective is to mimic the adversary and attempt to bypass all the controls in place within the environment. With these resources, as the red teamer, you can effectively mimic a true adversary and communicate your findings in a common language that both sides can understand. In a nutshell, this is known as **purple teaming**.